

物联网（IoT）基础

网络技术+协议+用例

IoT Fundamentals

Networking Technologies, Protocols,
and Use Cases for the Internet of Things



[美] 大卫·汉斯（David Hanes） 冈萨洛·萨尔盖罗（Gonzalo Salgueiro）
帕特里克·格罗塞特（Patrick Grossetete） 著
罗伯·巴顿（Rob Barton） 杰罗姆·亨利（Jerome Henry）

李华成 译 田果 审

随时、随地、随心阅读



物联网 (IoT) 基础

网络技术+协议+用例

IoT Fundamentals

Networking Technologies, Protocols,
and Use Cases for the Internet of Things



[美] 大卫·汉斯 (David Hanes) 冈萨洛·萨尔盖罗 (Gonzalo Salgueiro)
帕特里克·格罗塞特 (Patrick Grossetete) 著
罗伯·巴顿 (Rob Barton) 杰罗姆·亨利 (Jerome Henry)

李华成 译 田果 审



中国工信出版集团



人民邮电出版社
POSTS & TELECOM PRESS

当当云阅读

物联网（IoT）基础

网络技术+协议+用例

IoT Fundamentals

Networking Technologies, Protocols, and Use Cases for the
Internet of Things

[美] 大卫·汉斯 (David Hanes) 冈萨洛·萨尔盖罗 (Gonzalo Salgueiro)

帕特里克·格罗塞特 (Patrick Grossetete)

罗伯·巴顿 (Rob Barton) 杰罗姆·亨利 (Jerome Henry) ©著

李华成 © 译 田 果 © 审

人 民 邮 电 出 版 社

北 京

图书在版编目 (CIP) 数据

物联网 (IoT) 基础: 网络技术+协议+用例 / (美) 大卫·汉斯 (David Hanes) 等著; 李华成译. — 北京: 人民邮电出版社, 2021. 3

ISBN 978-7-115-55779-7

I. ①物… II. ①大… ②李… III. ①物联网 IV. ①TP393.4②TP18

中国版本图书馆CIP数据核字 (2020) 第266847号

著 [美] 大卫·汉斯 (David Hanes)
[美] 冈萨洛·萨尔盖罗 (Gonzalo Salgueiro)
[美] 帕特里克·格罗塞特 (Patrick Grossetete)
[美] 罗伯·巴顿 (Rob Barton)
[美] 杰罗姆·亨利 (Jerome Henry)

译 李华成

责任编辑 傅道坤

责任印制 王 郁 彭志环

人民邮电出版社出版发行 北京市丰台区成寿寺路11号

邮编 100164 电子邮件 315@ptpress.com.cn

网址 <https://www.ptpress.com.cn>

山东百润本色印刷有限公司印刷

开本: 800×1000 1/16

印张: 25.25

字数: 542千字 2021年3月第1版

印数: 1 - 1800册 2021年3月山东第1次印刷

著作权合同登记号 图字: 01-2017-5034 号

定价: 139.80元

读者服务热线: (010) 81055410 印装质量热线: (010) 81055316

反盗版热线: (010) 81055315

广告经营许可证: 京东市监广登字20170147号

目录

[版权声明](#)

[内容提要](#)

[序](#)

[关于作者](#)

[章节贡献人](#)

[关于技术审稿人](#)

[献辞](#)

[致谢](#)

[前言](#)

[资源与支持](#)

[第1章 物联网是什么](#)

[1.1 物联网的起源](#)

[1.2 物联网与数字化](#)

[1.3 物联网的影响](#)

[1.4 IT与OT的融合](#)

[1.5 物联网的挑战](#)

[1.6 小结](#)

[第2章 物联网网络架构与设计](#)

[2.1 新型网络架构背后的驱动力](#)

[2.2 比较物联网的架构](#)

[2.3 简化的物联网架构](#)

[2.4 核心物联网功能协议栈](#)

[2.5 物联网数据管理与计算堆栈](#)

[2.6 小结](#)

[第3章 智能对象：物联网之“物”](#)

[3.1 传感器、执行器和智能对象](#)

[3.2 传感器网络](#)

[3.3 小结](#)

[第4章 连接智能对象](#)

[4.1 通信标准](#)

[4.2 物联网接入技术](#)

[4.3 小结](#)

[第5章 IP作为物联网网络层](#)

[5.1 IP的商业案例](#)

[5.2 优化的需要](#)

[5.3 针对物联网来优化IP](#)

[5.4 概要文件和合规性](#)

[5.5 小结](#)

[第6章 物联网应用协议](#)

[6.1 传输层](#)

[6.2 物联网应用传输方法](#)

[6.3 小结](#)

[第7章 物联网的数据和分析](#)

[7.1 物联网数据分析简介](#)

[7.2 机器学习](#)

[7.3 大数据分析工具和技术](#)

[7.4 边缘流分析](#)

[7.5 网络分析](#)

[7.6 小结](#)

[第8章 物联网安全](#)

[8.1 OT安全简史](#)

[8.2 OT安全面临的常见挑战](#)

[8.3 IT和OT安全实践及系统的差异](#)

[8.4 正式的风险分析结构（OCTAVE和FAIR）](#)

[8.5 安全在运营环境中的阶段性应用](#)

[8.6 小结](#)

[第9章 制造业](#)

[9.1 互联制造业简介](#)

[9.2 互联工厂的体系结构](#)

[9.3 工业自动化控制协议](#)

[9.4 互联工厂的安全](#)

[9.5 互联工厂的边缘计算](#)

[9.6 小结](#)

[第10章 石油和天然气业](#)

[10.1 石油和天然气行业简介](#)

[10.2 作为数字化驱动的行业关键挑战](#)

[10.3 提高运营效率](#)

[10.4 油气物联网架构](#)

[10.5 小结](#)

[第11章 公用事业](#)

[11.1 电力行业简介](#)

[11.2 GridBlocks参考模型](#)

[11.3 主变电站电网和变电站自动化](#)

[11.4 系统控制GridBlock——变电站广域网](#)

[11.5 场域网（FAN）GridBlock](#)

[11.6 保障智能电网的安全](#)

[11.7 智能电网的未来](#)

[11.8 小结](#)

[第12章 智慧互联城市](#)

[12.1 面向智慧城市的物联网战略](#)

[12.2 智慧城市物联网架构](#)

[12.3 智慧城市安全架构](#)

[12.4 智慧城市用例示例](#)

[12.5 小结](#)

[第13章 交通运输业](#)

[13.1 交通和运输业系统](#)

[13.2 交通运输业的挑战](#)

[13.3 运输业物联网用例](#)

[13.4 运输行业的物联网架构](#)

[13.5 小结](#)

[第14章 采矿业](#)

[14.1 当今采矿业及其挑战](#)

[14.2 物联网在现代采矿业中的挑战](#)

[14.3 采矿业物联网战略](#)

[14.4 采矿业物联网体系结构](#)

[14.5 小结](#)

[第15章 公共安全](#)

[15.1 公共安全概述](#)

[15.2 公共安全物联网蓝图](#)

[15.3 应急响应物联网架构](#)

[15.4 物联网公共安全信息处理](#)

[15.5 校车安全](#)

[15.6 小结](#)

版权声明

Authorized translation from the English language edition, entitled IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things 1e by Hanes, Salgueiro, Grossetete, Barton, Henry, published by Pearson Education, Inc, publishing as Cisco Press, Copyright © 2017.

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from Pearson Education, Inc.

CHINESE SIMPLIFIED language edition published by PEARSON EDUCATION ASIA LTD., and POSTS & TELECOMMUNICATIONS PRESS Copyright © 2021.

本书封面贴有Pearson Education（培生教育出版集团）激光防伪标签。无标签者不得销售。

内容提要

本书从较高的层面对物联网（IoT）的核心概念以及部署方案进行了介绍。

本书分为15章，内容涵盖了物联网的概念，物联网的网络架构与设计，物联网中的智能对象以及智能对象的相互连接，IP作为物联网的网络协议，物联网中的应用协议，物联网的数据和分析，物联网的安全保障，物联网在制造业、石油和天然气行业、公用事业、智慧城市、交通运输以及采矿业中的用例，物联网的公共安全等内容。

本书讲解由浅入深，理论与案例结合，特别适合对物联网关键概念以及发展应用前景感兴趣的读者阅读。

序

这是一份来自过去的问候。我在2017年2月的科技时代为你们写下了这篇序言。那时（对我来说就是现在），大多数汽车仍然有人驾驶。我们也仍然需要借助红绿灯来指挥交通，而且大部分红绿灯都是定时的，与街道的拥堵情况无关。在我写这篇序言的时候，大多数家用电表都是机械的，而公用事业人员必须挨家挨户地去获取电表上的读数。绝大多数烤面包机也还不能发布推文。

我是在2013年加入Cisco的，之后在2015年成为公司物联网技术团队的领导。这几年来，我们这个团队见证了一次又一次广泛、深刻而又迅猛的技术变革，因此一本书的序言往往只有很短的保质期。

但我们可以为即将到来的变化和机遇做好准备。我们未来要使用的工具，会和我们现在构建这个互联网时所使用的工具存在巨大的区别。我们需要对物联网的基本原理拥有坚如磐石的理解：我们今天在哪里，我们面临的挑战在何处，我们的机会在何方。本书是由Cisco最顶尖的工程师和技术人才创作的，我们可以一起朝着这个方向建设我们的未来。

物联网之“物”在哪里？

我希望本书能成为读者的工具书，即使读者要到2020年才会读到它，彼时物联网（如果我们仍然这么称呼它的话）设备的数量可能已经达到了500亿，而2016年这个数字还只有区区64亿。由于能够处理和共享传感器的信息以及其他数据，并且针对这些数据作出响应，所以制造业工厂将比以往任何时候都更加智能和高效。像汽车这样的复杂机器会被全面计量，一直计量到组件级别。计量它们的大量数据流会被实时发送给庞大的分析系统，让这些数据服务于生命安全、生态和金融服务，甚至制造它们的制造厂。拖拉机、茶杯、卷尺等都会变得如此智能，最终让各个产品公司都转变为服务公司。

这会是这个世界有史以来最大的技术变革。

目前，收集、整理、分析和传输这些数据的网络协议还在快速发展。我们有一个强大而稳定的互联网，但它的目的是连接人和通用的计算机，而不是连接数十亿个不断发送机器数据流的高度专业化设备。

我们的全球网络被设计成模拟的点对点连接，而且在大多数情况下，它都不会对自己连接的设备和收发数据加以区分。目前，包括Cisco在内的几家公司正设法在数十亿台联网设备与数据和分析仓库之间增加一层中介，这些数据和仓库将成为企业和其他应用程序的数据仓库（我们目前称这一层为“边缘”）。

由于设备产生的大量数据和遥测数据需要通过无线方式发送，所以我们也尽自己所能来提高数据传输的可靠性和速度，同时降低延迟和发送每个比特所消耗的能量。在这场竞争中，出现了几种新兴的无线标准。几年后，还会出现一些新标准，因为不同类型的设备和应用程序需要不同的无线系统。目前，移动运营商是行业巨头，能源和运输公司等数据服务的最大消费者也加入了这一行列。在未来几年，我们会见证大量的竞争和创新，因为新老公司都在争相成为所有这些信息的传输者。

我们还在努力确保物联网设备本身能够提升网络的安全性。现在（在读者读到这段文字时已经成为过去），网络本身对应该发送什么类型的数据、不应该发送什么类型的数据了解非常有限。设备可以被劫持来攻击其他设备或网络本身。当读者读到这里的时候，相信这个安全问题以及物联网所面临的其他挑战（比如可扩展性和互操作性问题）会更接近于解决。本书也会在接近这个目标的过程中发挥它的作用。本书可以帮助读者以连贯和全面的方式掌握物联网的基础。物联网正准备改变我们的世界，本书为理解和驾驭不断变化的物联网领域提供了必要的基础知识。

接受曲线

显然，按照我2017年的观点来看，我们还有很多工作要做，才能最终让物联网成为一种所有企业都可以轻松连接的结构。不过，我相信这个目标终将实现，而且会很快实现。这既是因为我们正在Cisco开发相关的工具，也是因为我一直都在与那些参与物联网发展的商业领袖和企业家们进行交流。

建立物联网解决方案，保证它们的安全性，使它们变得便宜和易于维护，处理它们产生的数据并从中获利，这些都是巨大的机遇。我的团队所做的工作，就是让这些工作对你们来说更加简单，而你我所接受的教育则是这一切的起点。

——Rowan Trollope

Cisco物联网及应用部门高级副总裁兼总经理

关于作者

David Hanes, CCIE #3491, 是一位专注于物联网的技术领导者, 当前供职于云支持技术援助中心 (TAC) 的Cisco技术服务部门。他在新技术的孵化方面颇有经验, 当前作为领导负责为Cisco的IoT云解决方案提供技术支持。他在协作和认知计算等领域也具有技术专长。

在IoT和协作领域, David拥有多项已发布的专利, 还有几项专利正在申请之中。他以RFC贡献者和作者的身份, 积极活跃于SIP论坛和IETF。David撰写并贡献了多种行业出版物和白皮书, 还是Fax, Modem, and Text for IP Telephony一书 (由Cisco Press出版) 的合著者。他曾在世界范围内的行业和技术会议上发言, 并被Cisco Live授予“名人堂演讲者”的荣誉。

自1997年加入Cisco以来, David曾先后担任过广域网、广域网交换和多业务语音团队的TAC工程师、多服务语音团队的领导、处理各种VoIP技术的升级工程师, 以及为现场试验提供支持的工程师。在加入Cisco之前, David是Sprint的一位系统工程师, 他在Sprint公司第一次获得了帧中继和X.25协议相关的计算机网络经验。他拥有北卡罗莱纳州立大学的电气工程学位。

Gonzalo Salgueiro, CCIE #4541, 技术服务部门的首席工程师, 当前从事新兴技术以及新兴技术所提供的服务方面的研究。Gonzalo在Cisco工作了20多年, 他是多个技术领域 (包括协作、ML/AI、云计算和物联网等) 的专家和创新者。

Gonzalo是众多行业组织的资深成员, 也是一位杰出的演讲人员, 会定期在世界各地举办的各种技术行业会议和Cisco活动中发表演讲。他目前担任众多行业的领导角色, 其中包SIP论坛的董事会成员、INSIPID和SIPBRANDY IETF工作组的联合主席, IETF物联网理事会的成员, 以及SIP论坛中WebRTC任务组、IPv6任务组、FoIP任务组的联合主席。他还是各种行业组织和标准化组织的积极贡献人员。

Gonzalo是Fax, Modem, and Text for IP Telephony一书 (由Cisco Press出版) 的合著者。他还与人共同写作了24篇IETF RFC、4篇IEEE论文、4篇ITU论文, 以及大量关于各种不同技术主题的行业和学术论文。他还是65项以上专利 (已发布和正在申请中) 的共同发明人, 并为各种互操作和开源工作做出了贡献。Gonzalo在迈阿密大学获得了物理学硕士学位。

Patrick Grossetete是一名杰出的工程师兼技术营销人员, 在Cisco物联网连接团队 (Internet of Things Connected Group) 从事现场通信架构和设计相关的工作。他原来供职于Arch Rock公司 (该公司后来被Cisco收购), 在该公司担任产品管理和客户解决方案主管, 重点研究IPv6无线传感器网络技术在智能电网、能源和环境优化中的应用。

此前, Patrick是Cisco公司一个产品管理团队的领导, 负责Cisco IOS软件技术, 其中包括IPv6和IPv6移动性。Patrick定期在包括IPv6论坛在内的会议和行业活动中发言 (他在1999年作为Cisco公司的代表加入了IPv6论坛)。Patrick还是欧盟委员会资助项目 (包括GEANT和ENVIROFI) 的审稿人。

Patrick是Global IPv6 Strategies和Deploying IPv6 Networks两书 (由Cisco Press出版) 的合著者, 还与他人共同写作了多篇白皮书, 比如Unified Field Area Network Architecture for Distribution Automation (2014) 和IPv6 Architecture for Field Area Networks (2012)。在2003年6月, 他在圣地亚哥峰会上获得了IPv6论坛互联网先锋奖, 现在是IPv6论坛的研究员。在Cisco和Arch Rock工作之前, Patrick在数字设备公司担任

咨询工程师，提供网络设计和部署方面的咨询。他在法国巴黎控制数据研究所获得了计算机科学学位。

Rob Barton, CCIE #6660 (R&S和安全), CCDE #2013:6, 是Cisco数字化转型与创新组织的首席系统工程师。Rob是一名注册专业工程师(P. Eng), 在IT行业工作了20多年, 其中的后17年在Cisco工作。Rob毕业于英属哥伦比亚大学, 获得了工程物理学学位, 他当时专攻计算机和无线电通信方向。Rob感兴趣的领域包括无线通信、IPv6、IoT和工业控制系统。Rob还是End-to-End QoS, 2nd Edition (由Cisco Press出版)的合著者。他现在与妻子和两个孩子居住在加拿大温哥华。

Jerome Henry, CCIE #24750, 是Cisco公司企业基础设施和解决方案部门的首席工程师。Jerome有15年以上的Cisco技术课程授课经验, 先后在15个以上的国家采用4种语言进行授课, 其受众涵盖了本科生、网络从业人员以及Cisco内部系统工程师。Jerome凭借其在无线和网络方面的专长, 于2012年加入Cisco公司。在此之前, 他供职于欧洲航空航天局的一个团队, 负责异构网络和无线集成方面的咨询和讲解。这个团队后来被Cisco收购, 在Cisco公司负责提供无线解决方案。随后, 他与Cisco Learning部门的同事工作过一段时间, 负责网络课程的开发, 以及编写新兴技术的培训材料。

Jerome是一位无线网络认证专家(CWNE #45), 开发了多门Cisco课程, 写作了多本无线书籍, 还录制了多个视频课程。Jerome也是IEEE的成员, 于2013年升级为高级会员, 他还参与了WiFi联盟工作组, 重点关注IoT和低功耗。Jerome凭借其10000多小时的课时, 荣获IT培训最佳教师银奖。他住在北卡罗来纳州的三角研究园。

章节贡献人

以下章节的内容由具有相关行业知识的特定人员提供，在此向他们表示感谢。

物联网的数据和分析（第7章）：

Brian Sak, CCIE #14441, Cisco大数据分析部门技术解决方案架构师。

Cisco Kapil Bakshi, 美国公共部门大数据与云计算杰出系统工程师。

物联网安全（第8章）：

Robert Albach, Cisco工业安全投资组合部高级产品经理。

Rik Irons-McLean, Cisco能源解决方案架构主管。

制造业（第9章）：

Brandon Lackey, 科技企业家, DronePilots网络公司联合创始人。

Ted Grevers, Cisco物联网垂直解决方案工程经理。

石油和天然气业（第10章）：

Willy Fotso Guifo, 物联网服务高级经理, Cisco油气垂直行业全球业务主管。

Dimitrios Tasidis, 解决方案架构师, Cisco油气垂直行业物联网服务技术主管。

智慧互联城市（第12章）：

Munish Khetrpal, Cisco智慧互联城市部门业务发展总监。

Prachi Goel, Cisco智慧互联城市解决方案管理组项目分析师。

采矿业（第14章）：

Lyle Tanner, Cisco客户解决方案架构师。

公共安全（第15章）：

Kevin Holcomb, Cisco物联网垂直解决方案技术营销工程师。

Kevin McFadden, Cisco垂直解决方案架构师。

关于技术审稿人

Robb Henshaw是Cisco Jasper的物联网云全球通信主管。2016年3月，Cisco收购了全球物联网平台领导企业Jasper，而Robb正是该公司的全球通信高级经理。在加盟Jasper之前，他花了15年的时间来为移动和无线企业建立和运行全球通信项目，这些企业包括Airespace（被Cisco收购）、Proxim Wireless和SugarSync（被J2 Global收购）。

Samuel Pasquier是Cisco企业网络部门（ENG, Enterprise Networking Group）物联网连接产品组合的产品管理团队负责人。他在加利福尼亚州的圣何塞工作，负责与销售团队和工程团队紧密合作，开发整个物联网连接产品组合的产品战略和路线图以及Cisco雾计算软件解决方案（IOx），并且将它们付诸执行。

自2004年以来，Samuel一直供职于Cisco。他在Catalyst 6500的工程团队中担任了6年的软件技术主管。他设计、实现并维护了这个平台上的大量核心基础设施特性。这些经验让Samuel对软件开发和体系结构拥有了非常深刻的理解。他是Catalyst 6500/6800产品线的经理，在Catalyst 6800上市后带领产品经理团队对Catalyst 6500的产品进行了全面的更新。

在担任目前的职务之前，Samuel领导产品经理团队，给Catalyst固定端口系列接入层交换机（Catalyst 2960-X、3750、3650和3850）定义了发展的路线图。

Samuel拥有法国信息与技术学院（EPITA）的计算机科学硕士学位，并经常在网络行业会议中发表演讲。

献辞

感谢我的爱妻Holly。你不仅是我最好的朋友，也是我动力的源泉和我最忠实的拥趸。我生命中的一切成就，无不归功于你无条件给予我的爱和支持。我的孩子Haley、Hannah和Kyle，你们的快乐与祝福让我的生活时刻充满着靓丽的色彩。

我也想把本书献给我伟大的父母。我要把本书献给我父亲，是他激发了我对学习的热忱，并不断激励我去攀登新的高峰，同时我也要我把本书献给我母亲，是她给了我攀登这些峰峦的勇气与信念。

——David Hanes

谨以本书献给我的家人。首先，我要感谢我深爱的妻子和最好的朋友Becky，是她给了我灵感，使我每天都能够梦想成真。我过去、现在、永远都会对你充满感激。致我们4个了不起的孩子：Alejandro、Sofia、Gabri和Mateo，是你们让我的生活中充满了无穷的欢乐、伟大的奇迹和不竭的动力。我爱你们！

其次，我也要把本书献给我的父母Alberto和Elena，你们是我的灵感来源，是你们让我拥有了今天的一切。对于你们所做的牺牲和付出，我无法用言语来表达我不变的感激之情。

最后，我要把本书献给我的祖母Nelida，她去年刚刚离开了我们。而我直到最近才意识到自己基因中的善良和风度源自何方。

——Gonzalo Salgueiro

献给Mya和每一位行将生活在物联网时代的人们。

——Patrick Grossetete

首先，我想把本书献给我美丽的妻子Loretta。你是我最大的拥趸和啦啦队长，在过去的20年里你教会了我很多。如果没有你不断地鼓励（以及我在创作另一本图书时给予的包容和忍让），这些作品将永无问世之日。由于你的支持，我才能够把自己学到的知识传授给下一代互联网工程师。

我还想把本书献给我的父母Richard和Peggy。如果不是你们在我4岁时送给了我第一套乐高玩具，我就不会对科学和工程领域萌发出如此强烈的兴趣。儿时和爸爸探讨物理和微积分的记忆清晰如昨日，我们一起收看“力学世界”（The Mechanical Universe）的场景也历历在目。

我爱你们！

——Rob Barton

本书献给我的孩子Ines和Hermes。你们的好奇心是我每日进行研究的动力之源。

—Jerome Henry

致谢

我们要感谢在本书写作过程中为我们提供过帮助的人们。

Michael Boland: 你的建议和你在采矿业的专业知识都是本书创作过程中的宝贵财富。我们真诚地感谢你为本书写作所付出的时间, 以及你提供的宝贵思路与建议。

Maik Seewald: Maik, 你是一位真正的互联网工程师! 你的协助和建议让本书最终能够解释清楚公用事业领域中标准与协议的方向, 让本书中的技术得以紧跟时代发展的步伐。

Rick Geiger: Rick, 你是世界上最顶尖的公用事业专家之一。谢谢你对公用事业这一章提供的帮助和建议。

Ken Batke: 感谢你对公用事业章节的贡献和指导。非常感谢你的反馈。

Mahyar Khosravi: Mahyar, 感谢你在石油和天然气领域为我们提供的专业知识, 以及所有对石油和天然气章节提供的反馈和建议。

Dave Cronberger: 非常感谢Dave对本书提供的出色指导与反馈。Dave, 你从不介意直言不讳地提出建议, 让我们的工作重回正轨。你对制造业章节的评论和反馈对我们极为宝贵。

Kyle Connor和Barb Rigel: Kyle和Barb, 谢谢你们对运输业章节进行的详细审查与反馈。在这个日新月异的行业, 你们提供的指导和见解为整个团队带来了巨大的帮助。

Eleanor Bru: Ellie是本书的开发编辑, 和你一起工作非常愉快。感谢你的付出与包容, 感谢你让图书审校的过程进行得如此顺利。

Mary Beth Ray: 我们还要向Mary Beth表示衷心的感谢, 感谢你让我们坚持到底, 一路支持我们完成了这个具有挑战性的项目, 并且在创作本书中为我们提供了一切必备的素材和支持。

Mandie Frank: 作为我们的项目编辑, Mandie帮助我们解决了所有的问题, 并完成了本书的最后润饰。谢谢你, Mandie, 谢谢你扶持我们走到了最后。

Kitty Wilson: 作为我们的文字编辑, 感谢你付出了这么长的时间将本书最终定稿。非常感谢你对细节的细致关注。

也要感谢我们的管理团队, 感谢你们给予的坚定支持与理解, 为了不延误交稿时间, 我们都付出了太多的工作。

David要特别感谢Marty Martinez、Rob Taylor、Jitendra Lal和Shane Kirby的指导和支持。

Gonzalo要感谢TS的领导团队, 特别是Marc Holloman, Marty Martinez和Tom Berghoff。如果没有他们坚定不移的鼓励、信念和支持, 本书也无法出版。

Patrick要感谢物联网连接团队的产品管理和工程团队, 正是你们的支持和不懈努力才让这些物联网产品得以问世。

Jerome要特别感谢Matt MacPherson分享了他企业、5G和物联网融合方面的智慧与远见。

Rob要感谢他的领导团队，包括Rick Huijbregts博士和Bernadette Wightman，你们在本书写作期间给予了他强有力的支持。你们对创新的关注是数字转型革命的核心，同时也让他从中获得了大量的启发。

前言

一个重大的技术变革正围绕着物联网（IoT）在我们的世界悄然发生。物联网就是要连接那些还没有联网的一切。当今世界的大多数对象都没有连接到计算机网络，但这种情况正在迅速改变。我们周围很多以前没有连接的对象如今已经具备了与其他对象和人通信的能力，这反过来又催生了我们日常生活中的新服务，提升了我们日常生活的效率。这是物联网的基本前提，也解释了为什么一些人认为物联网将像工业革命一样具有变革性。

作为本书的作者团队，我们拥有数十年的计算机网络经验，并且在过去很多年都专注于物联网和相关技术。我们在物联网方面的综合经验包括早期产品的部署和测试、网络设计、实施、培训和排错。这段经历让我们能够以务实的态度来撰写这个主题，并提炼出构成这个主题的基本要素。本书包含了从技术角度和从商业角度理解物联网所需要的核心元素。

本书分3部分对物联网的基础知识进行了介绍。第1部分对物联网进行概述，并且从设计角度讲解读者需要了解的内容。第2部分介绍物联网的技术基础，包括物联网相关的技术和协议。最后，第3部分则会介绍一些常见的行业用例，以便读者了解物联网在现实世界中的应用方法。

从业者要想在物联网领域获得成功，就必须对物联网的原理和用例拥有基本的理解。本书会按照顺序对这些知识进行介绍，因此本书不仅是非常好的物联网学习资源，同时也可以在读将来遇到具体的物联网问题时，为读者提供参考。

本书读者对象

本书的目标读者是那些正在寻找一本权威、详尽的物联网技术读物的网络专业人士。它主要面向那些在网络技术领域拥有丰富经验，希望掌握物联网基本概念和技术，并且了解如何应用这些概念和技术的读者，从而帮助这些读者达到基本熟练的程度。因此，读者应该基本了解计算机网络的概念，并且熟悉基本的网络术语。本书的读者可以是网络专业的高年级学生，或者担任网络操作员、网络管理员和网络经理等职务的专业人士；还可以是网络设计师或架构师、网络工程师、网络技术人员、网络分析员或网络顾问，以及网络数据库管理员。

本书组织结构

第1部分，物联网简介

本书的第1部分旨在帮助读者理解物联网这个术语。这个词经常被人们误用，但这个词的含义非常丰富。本书的第1部分旨在帮助读者理解到底什么是物联网，同时对智能对象的范围

进行概述，智能对象的范围包括那些以每秒数百次的动作频率进行控制的望远镜镜片，以及每月发送一次生锈信息的传感器。这一部分还会介绍物联网网络是如何设计和构建的。

第1章，“物联网是什么”

本章概述物联网的历史和起源，还探讨运营技术（OT）和信息技术（IT）之间的融合，并会给物联网在一般网络环境中所在的位置提供一个参考模型。

第2章，“物联网网络架构与设计”

大量标准和行业组织定义了物联网的具体架构，其中包括ETSI/oneM2M和物联网世界论坛。本章将对这些架构进行比较，并提出一个简化的模型，以帮助读者理解物联网的关键功能，而不必掌握各个垂直领域中的元素。本章还会介绍核心的物联网功能栈和数据基础设施栈。

第2部分，物联网网络工程

一旦读者理解了物联网的范围和物联网网络的一般原则，第2部分将会带领读者深入了解物联网网络工程技术，其中包括智能对象以及将它们与应用程序连接起来的网络，也包括数据分析和安全技术。这一部分对物联网网络的每一层进行详细介绍，并分析每一层现有的协议（那些已经存在很长时间的协议和正在获得支持的新兴协议）、用例和不同架构（可以定义有效的物联网解决方案）。

第3章，“智能对象：物联网之‘物’”

智能对象有很多不同的种类，从穿戴之物到安装在墙上、窗户、桥梁、火车、汽车或路灯上的对象，不一而足。本章会帮助读者了解不同类型的智能对象，从简单记录信息的智能对象到针对变化因素来执行操作的智能对象。

第4章，“连接智能对象”

部署智能对象之后，它们需要连接到网络。本章会指导读者理解构建物联网网络所需的不同要素，其中包括各类连接技术，如802.15.4、802.15.4g、802.15.4e、1901.2a、802.11ah、LoRaWAN、NB-IoT和其他LTE变体；也包括无线波段及范围、能耗方面的考虑因素，以及物联网网络的拓扑。

第5章，“IP作为物联网网络层”

早期的物联网协议并不依赖于OSI网络层。本章会介绍在物联网网络中已经包含了数百万个传感器时，IP如何成为网络连接的首选协议。本章还会详细介绍如何使用如6LoWPAN、6TiSCH和RPL等增强功能来优化IP协议，从而适应低功耗和有损网络（LLN），因为物联网通常就是在这类网络中运行的。

第6章，“物联网应用协议”

智能对象需要通过网络与应用程序进行通信，以报告环境读数或接收信息、配置和指令。本章会指导读者了解各类通用应用程序协议，其中包括MQTT、CoAP和SCADA，也包括各种基于Web的通用协议。本章还会介绍优化物联网网络应用和通信效率的推荐架构。

第7章，“物联网的数据和分析”

在数据中心或云中的某个地方，来自数百万个传感器的数据会被分析并与来自其他数百万个传感器的数据进行关联。大数据和机器学习是当今世界的关键词。本章会详细解释什么是大数据，以及机器学习的工作原理，并且会介绍各类用来对大量数据进行智能处理和实时分析网络流的工具。

第8章，“物联网安全”

黑客如果攻破了物联网智能对象，就可以深入访问它所在的网络和数据。本章会对IT和OT的安全方案进行解释，并详细介绍如何将安全技术应用于物联网环境当中。本章还会描述能够对物联网基础设施进行正式风险分析的工具。

第3部分，物联网在行业中的应用

一旦读者知道如何构建物联网网络，第3部分就会帮助读者把这些知识应用到正在变革中的关键行业。通过本部分涉及的7个垂直领域，读者会了解如何使用物联网，以及建议使用什么物联网架构来提高这些领域的安全性、操作效率和用户体验。

第9章，“制造业”

只要生产率提高，制造业就有可能发生巨大变化，而物联网给这个世界带来了一场颠覆性的变革。本章会解释在这种环境下制造业的连接和数据的处理，同时也会详细介绍融合型工厂的体系结构及其组件，包括IACS和CPwE。本章还会研究各类过程自动化协议，包括以太网/IP、PROFINET和Modbus/TCP。

第10章，“石油和天然气业”

石油和天然气是现代社会最重要的资源。本章会展示物联网如何在这一垂直领域中得到大规模利用，以提高运营效率。本章还讨论了OT安全这一敏感话题，并为油气领域的物联网提供了架构方面的建议。

第11章，“公用事业”

公用事业公司为我们所处的城市、企业和整个经济提供服务。在这个垂直领域中，物联网可视化和控制能耗方面的功能，对公用事业公司和终端用户都至关重要。本章将通过GridBlocks参考模型、变电站和控制系统，以及FAN GridBlocks来帮助读者了解智能电网系统，以及物联网如何在这个垂直领域中进行使用。

第12章，“智慧互联城市”

智慧互联城市包括道路照明、智能停车、交通优化、垃圾收集和管理、智能环境等。这些不同的用例正在越来越多地整合到城市范围的物联网解决方案当中，这些数据和智能对象具有多种用途。本章会讨论智慧互联城市的各种物联网解决方案。

第13章，“交通运输业”

本章会讨论公路、铁路、公共交通和车队的管理。读者会了解物联网如何通过DSRC和WAVE等协议实现车辆和基础设施之间的通信，以及物联网如何提高交通基础设施的效率和安全性。

第14章，“采矿业”

采矿业常被描述为“运送大量物资的巨大交通工具”。在当今世界中，物联网正在保障安全、提升竞争力方面发挥着越来越大的作用。从自动驾驶的运输工具到雷达制导的350吨铁

锹，本章会向读者展示物联网在采矿中的各种应用。本章还提出了一种架构式物联网战略，用于在不断变化的极端环境中部署智能对象。

第15章，“公共安全”

公共安全组织的首要目标是保证公民、社区和公共空间的安全。这些组织长期处于采用新技术的前沿，物联网已成为它们运营的一个关键组成部分。本章会描述应急响应物联网架构，并详细介绍公共安全运营商如何利用物联网来更好地交换信息，并利用大数据来更快、更有效地应对突发事件。

资源与支持

本书由异步社区出品，社区（<https://www.epubit.com/>）为您提供相关资源和后续服务。

提交勘误

作者和编辑尽最大努力来确保书中内容的准确性，但难免会存在疏漏。欢迎您将发现的问题反馈给我们，帮助我们提升图书的质量。

当您发现错误时，请登录异步社区，按书名搜索，进入本书页面，单击“提交勘误”，输入勘误信息，单击“提交”按钮。本书的作者和编辑会对您提交的勘误进行审核，确认并接受后，您将获赠异步社区的100积分。积分可用于在异步社区兑换优惠券、样书或奖品。

详细信息 写书评 提交勘误

页码: 页内位置 (行数): 勘误印次:

B I U

字数统计

提交

扫码关注本书

扫描下方二维码，您将会在异步社区微信服务号中看到本书信息及相关的服务提示。



与我们联系

我们的联系邮箱是contact@epubit.com.cn。

如果您对本书有任何疑问或建议，请您发邮件给我们，并请在邮件标题中注明本书书名，以便我们更高效地做出反馈。

如果您有兴趣出版图书、录制教学视频，或者参与图书翻译、技术审校等工作，可以发邮件给我们；有意出版图书的作者也可以到异步社区在线投稿（直接访问www.epubit.com/selfpublish/submission即可）。

如果您所在的学校、培训机构或企业，想批量购买本书或异步社区出版的其他图书，也可以发邮件给我们。

如果您在网上发现有针对异步社区出品图书的各种形式的盗版行为，包括对图书全部或部分内容的非授权传播，请您将怀疑有侵权行为的链接发邮件给我们。您的这一举动是对作者权益的保护，也是我们持续为您提供有价值的内容的动力之源。

关于异步社区和异步图书

“异步社区”是人民邮电出版社旗下IT专业图书社区，致力于出版精品IT技术图书和相关学习产品，为作译者提供优质出版服务。异步社区创办于2015年8月，提供大量精品IT技术图书和电子书，以及高品质技术文章和视频课程。更多详情请访问异步社区官网<https://www.epubit.com>。

“异步图书”是由异步社区编辑团队策划出版的精品IT专业图书的品牌，依托于人民邮电出版社近30年的计算机图书出版积累和专业编辑团队，相关图书在封面上印有异步图书的LOGO。异步图书的出版领域包括软件开发、大数据、AI、测试、前端、网络技术等。



异步社区



微信服务号

第1章 物联网是什么

我们来想象这样一幅场景：万物全都连接到了网络当中，并且和其他人或物进行通信，这一切都是为了通过新的服务来提升我们的生活品质。从自动驾驶的快递送货小飞机，到衣物上安装的身体健康检测仪，你所知道的整个世界都必将经历一场重大的技术变革。这场技术变革的总称就叫作物联网（Internet of Things, IoT）。

IoT的基本前提和基本目标就是“将所有未连之物连接起来”。这也就意味着，所有当前还没有连接到计算机网络（即互联网）中的物品都会被接入进来，以便与其他人或物进行通信与互动。IoT是一个技术过渡阶段，在这个阶段当中，我们可以实现万物的智能化，并且将它们连接到一个智能网络当中，并且由此使用这些设备来认识和控制外在的世界。

当这些智能产品都可以通过网络来远程进行传感和控制时，外在的世界和计算机就可以更加紧密地结合在一起。由此，高级应用的效率、准确性、自动化水平和实现层次都可以迈上一个新的台阶。

物联网的世界广阔而又多元，有些读者甚至会认为它有些复杂，这是因为物联网包含了大量的构成元素和不同的协议。IoT不是一个单一的技术领域，读者不妨将其视为各类概念、协议和技术的总和，而这些概念、协议和技术都不时依赖于某一个行业。IoT的各个组成部分虽然会给人们的生产力和自动化水平带来诸多助益，但也会给人们带来很多的挑战。比如，将大量设备和海量待处理数据连接到网络当中，这本身就是一项不小的挑战。

本章的目的是在一个更高的层级上对物联网及其相关的组成部分进行定义。了解这类信息可以帮助读者深入掌握本书接下来的各章中与物联网有关的话题。本章会对下列内容进行讲解。

■ 物联网的起源：本节的重点在于强调物联网在互联网发展过程中所占据的位置。

■ 物联网与数字化：本节会详细介绍物联网和数字化这两个概念的差异，同时通过定义一个框架，帮助读者更好地理解它们之间的关系。

■ 物联网的影响：本节会与读者分享几个高度概括化的场景和案例，以便向读者阐释IoT会给我们的世界带来怎样的影响。

■ IT与OT的融合：本节旨在探索物联网是如何实现信息技术（Information Technology，IT）和运营技术（Operational Technology，OT）之间的融合的。

■ 物联网的挑战：本节会简单概述迁移到物联网世界所面临的难题。

1.1 物联网的起源

人们常说物联网始自于2008年到2009年之间。在这段时间里，连接到互联网中的设备数量超过了全球的人口数量。随着连接到互联网中的“物”比与“人”越来越多，一个新的时代就此诞生，这就是物联网的时代。

创造了“物联网”这一措辞的人被公认为是Kevin Ashton。当他1999年供职于宝洁公司时，他曾经使用这个词来解释一个新的观点，这个观点与如何将公司的供应链连接到互联网有关。

Kevin后来提到，“物联网”一词所涉及的范围现在已经超越了计算机这个领域。他曾经这样说道：“在20世纪，计算机只是没有感知功能的大脑，它们只知道我们告诉它们的信息。”计算机依靠人类通过打字、条形码等方式来输入信息。物联网正在改变这种传统的模式；而到了21世纪，计算机正在自己感知这个世界。

越来越多的人承认，互联网会是一场重大的技术变革，但它的范围有多广，重要性有多大呢？它又在互联网的演变过程中占据了什么样的位置？

互联网的演化可以分为4个阶段，如图1-1所示。其中每个阶段都对我们的社会和生活带来了深远的影响。表1-1对这4个阶段进行了深入的解释。

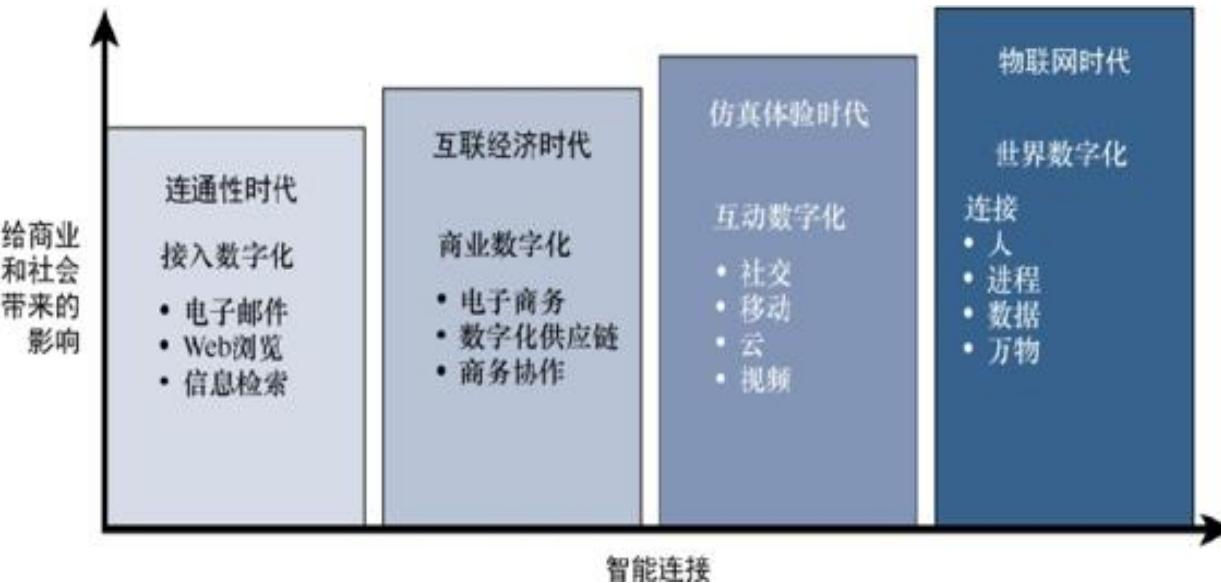


图1-1 互联网的演化阶段

表1-1 互联网的演化阶段

互联网的发展阶段	定义
连通性时代 (接入数字化)	在这个阶段，人们可以通过电子邮件、Web 服务和信息检索来更加轻松地访问信息
互联经济时代 (商业数字化)	在这个阶段，除了电子商业和供应链的改善之外，人们可以通过协作的方式提升商务流程的效率
仿真体验时代 (互动数字化)	在这个阶段，互联网的体验中进一步包含了大量的视频和社交媒体，而且人们可以通过移动端进行连接。越来越多的应用迁移到了云端
物联网时代 (世界数字化)	在这个阶段，网络将我们身边的物品和设备连接了起来，以便给人们带来新的服务和体验。一切未连之物都在接入当中

这个演化过程中的每个阶段都是建立在前一个阶段的基础之上的。而商业、政府和社会都会在接下来的一个阶段中收获更多实惠。

第一个阶段，即连通性时代，始自20世纪90年代中期。如果读者年龄不大，对那个时代的记忆恐怕已经淡忘。甚至，有些读者很难去想象一个尚未像我们今天一样建立广泛互联的时代。最初，电子邮件和接入互联网都是大学和企业才能享有的奢侈专利。普通人上网需要连接调制解调器进行拨号，哪怕是最为简单的网络连接在当时看来也不啻一个小小的奇迹。

虽然连通性和网络的速度不断拓展，网络依然达到饱和，建立连接也不再成为最主要的挑战。于是，人们关注的内容也就变成了如何利用连通性来提升效率和效益。这个拐点以互联网进入到第二个阶段为标志，这个阶段称为互联经济时代。

在互联经济时代，电子商务和建立供应链的数字化连接成为了人们追逐的目标，这些问题在过去100年间曾经是困扰人类的一大难题。厂商和供应商都能够与制造商更加紧密地联系起来，在线购物经历了巨大的增长。这个时代的受害者是传统的实体店零售商。随着供应商、厂商和消费者之间的联系变得更加直接，经济本身也变得更加数字化了。

第三个阶段，即仿真体验时代，以社交媒体、在线协作的涌现和各类设备广泛支持移动性为标志。从手机到平板电脑再到笔记本电脑和台式机，连通性已经无处不在。无处不在的连通性则让通信、协作和社交媒体能够通过各类渠道（包括电子邮件、短信、语音和视频）建立起来。从本质上说，人与人之间的互通也已经实现了数字化。

最后一个阶段就是物联网时代。无论各类关于物联网的访谈和报道是如何谈及物联网的，我们都在很多方面仍然处于这个阶段的起步状态。考虑到99%的“物”仍未联网，我们就可以想象出目前我们在这个演化阶段的目的。在这个阶段中，设备与物品都会和其他人与物连接在一起。商业和社会已经进入了这条轨道，它们正在体验数据和知识的大幅增加。接下来，这个阶段会让人们获得此前人类未尝掌握的信息，同时还会带来自动化水平和流程效益的增长。物联网终将以一种全新的、激动人心的方式改变整个世界，一如互联网发展过程中的前几个阶段那样。

1.2 物联网与数字化

物联网与数字化（digitization）是人们常常替换使用的两个术语。在大多数语境中，这样替换表达无伤大雅，但这两个术语之间仍然存在着一些不容小觑的差异。

概括地说，物联网强调“物”的连网，比如将物品和设备连接到计算机网络（如互联网）中。物联网这个词的表意在业内已经达成了一致。然而，数字化对于不同的人可能有不同的含义，但这个词的含义中通常包括将“物”与它们生成的数据连接起来，以及由此获得的商业洞见。

例如，在一个部署了WiFi地点追踪的商厦中，“物”就是WiFi设备。WiFi位置追踪只是通过追踪用户手机连接到哪个商家的WiFi网络，来判断用户正在哪个商家选购的功能。将WiFi设备或“物”连接到互联网的价值显而易见，这种做法也会得到顾客的欢迎，而实时追

踪WiFi客户端的位置也可以给商厦和店家带来商业利益。这可以帮助商家判断出顾客喜欢聚集在哪里，以及它们在商厦不同区域或者不同商家处停留了多久。分析这些数据可以改变商家打广告的位置、展示商品的方式、判断应该在哪里安何种类型的店面、这些店面的租金应该收取多少，甚至应该在那里部署保安等。

注释：在过去很多年中，万物互联（Internet of Everything, IoE）这个词得到了广泛的使用。时间久了，IoE这个词也就逐渐被“数字化”这个术语所取代。虽然技术术语都会随着时间发生变化，但IoE和数字化这两个术语大致是指同一个概念。物联网始终属于这两个术语的范畴，但物联网的概念是IoE和数字化这两个概念的子集，了解这一点十分重要。

用最直白的方式说，数字化就是将信息用数字的格式进行表达。在过去几十年里，人们曾经用不同的形式实现过数字化。比如，整个摄影行业现在就已经数字化了。这些年来，无论是作为一台独立的设备，还是作为安装在智能手机中的一个部件，几乎每个人都已经拥有了数码相机。几乎没人还会购买胶卷，再把胶卷拿去照相馆冲洗。仅仅就拍摄图片这个角度来看，摄影行业的数字化已经彻底改变了我们的生活方式。

其他数字化的例子包括音像租赁领域和运输领域。在过去，人们会去音像店租赁或者购买电影的影碟或者DVD光盘。随着数字化时代的到来，几乎人人都在拍摄自己的视频内容，购买电影的方式也变成了在线下载文件。

运输领域中的出租车服务目前正在经历数字化变革。诸如Uber和Lyft这样的业务都在使用数字技术让人们通过手机App实现搭车。在这个过程中，App可以提供关于车辆、司机和费用的信息。乘客接下来只需要使用App进行付费。这种数字化趋势给传统出租车行业带来的打击是毁灭性的。

在物联网的语境下，数字化将连网之物与数据和商业流程结合在了一起，让网络变得更加紧密也更有价值。关于物联网，人们常常想到的例子是智能家居，以及诸如Nest这类颇受用户喜爱的产品。通过

Nest，传感器可以判断出住户期待的气温设置，也可以将传感器与其他智能设备（如烟雾报警器、监控摄像头和各类第三方设备）连接在一起。在过去，这些设备以及它们提供的功能都是独立进行管理和控制的，它们无法提供当下这种一体化的体验。说到数字化和物联网提升网络智能连接的关联性和价值，提升我们生活水准的这个话题，Nest的例子只是冰山一角。

今天，很多企业都将数字化视为让自己的公司在业内脱颖而出的方式，而物联网则是数字化的一项重大赋能因素。智能设备和连通性的普及都在推动数字化趋势的发展，而这只是很多企业、国家和政府张开双臂拥抱这种趋势的原因之一。

1.3 物联网的影响

如果对物联网的潜在影响进行推测，结果往往会给人带来深刻印象。今时今日，约140亿或约0.06%的“物”业已联网。Cisco公司预计，到2020年，这个数字会到达500亿。英国的一项报告中推测的数字甚至更高，联网物的数量可能会达到千亿的数量级。Cisco进一步预计，这些新的连接会带来19万亿美元的利润增长和成本削减。图1-2提供了一个图表来展示联网设备数量的增加趋势。

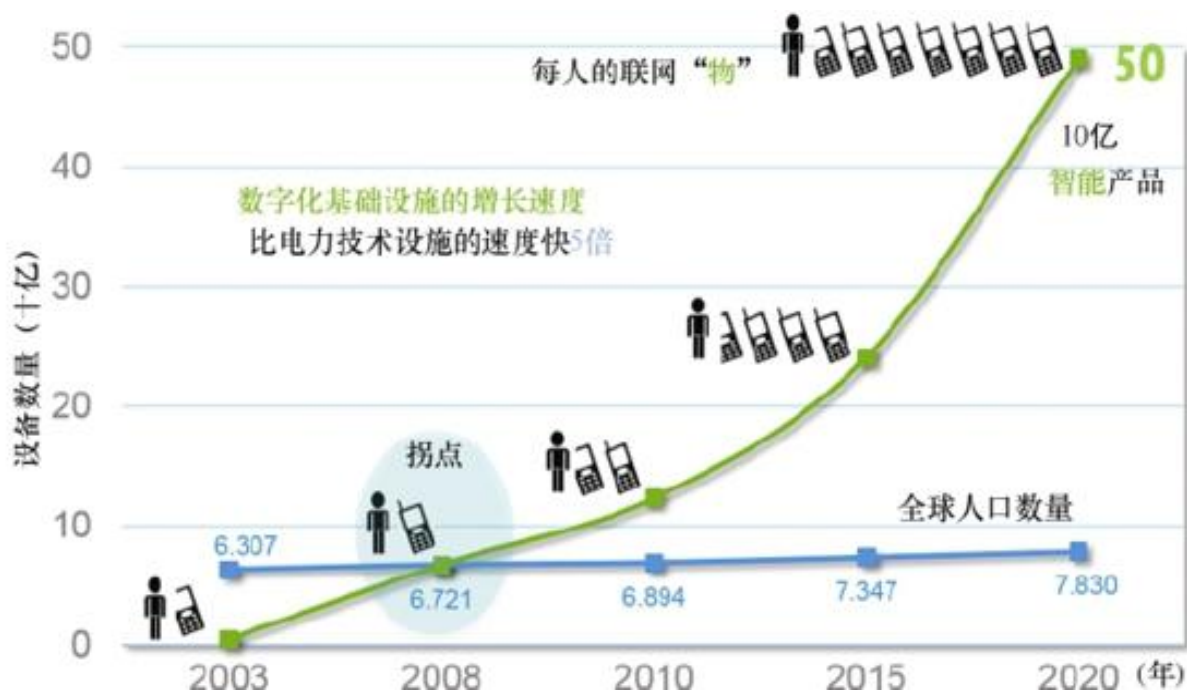


图1-2 连接到互联网设备的数量快速增加

这些数字表示物联网甚至会改变人类和商业与周边环境的交互方式。使用实时连接管理和监测智能设备，让人们利用数据做出决策的能力步入了一个全新的阶段。这可以进一步优化系统和进程，让它们为人们提供新的服务，并且在提升整体生活质量的同时，为人们和商业活动节省更多时间。

下面的示例解释了物联网及其影响带来的一大利好。这些示例对于实际的物联网用例进行了概括，以便清晰地展示出物联网会在未来如何影响人们的日常生活。读者如果希望深入了解物联网的用例，可以参考本书的第3部分。

1.3.1 互联道路

几十年来，人们一直在通过文学作品和电影对自动驾驶汽车进行各式各样的幻想。当这种幻想通过谷歌的自动驾驶汽车这样的知名项目走进人们的现实生活时，物联网仍然是实现全互联交通基础设施的关键一环。

物联网可以让自动驾驶汽车与车辆周围的交通系统进行双向数据交换，从而更好地与周围的环境进行互动，同时依然向乘客提供重要的数据。自动驾驶汽车必须与其他交通传感器之间建立不间断的、可靠的通信数据信息，才能完全发挥这类车辆的潜力。所谓互联道路（connected roadway）就是指驾驶员和无人驾驶车辆能够与周围交通基础设施充分集成的道路环境。图1-3所示为谷歌设计的自动驾驶汽车。



图1-3 谷歌的自动驾驶汽车

汽车中已经拥有了一些基本的传感器。它们负责检测油压、胎压、温度和其他工作环境条件，提供与车辆的核心功能有关的其他数据。方向盘背后的驾驶员可以在使用方向盘、踏板等设备驾驶车辆的同时浏览这些数据。人们之所以需要这些传感信息和控制信息，理由是显而易见的。驾驶员在集中注意力安全驾驶车辆的同时，必须能够理解、处理这些信息，并且使用这些信息来作出重要的判断。而物联网正是在很大程度上复制了这个概念。

今天，我们看到装备有成千上万个传感器的车辆被制造了出来，这些传感器负责测量的内容从油耗到车辆的位置，再到家人乘车时观看的娱乐节目，凡此种种不一而足。就在各大汽车制造商努力尝试重新定义驾驶体验的同时，这些传感器也开始支持IP功能，让它们能够轻松与汽车内外的其他系统进行通信。此外，新研发出来的传感器和

通信技术，开始让汽车有能力与其他汽车、交通信号灯、校园区域及交通基础设施中的其他组成成分之间进行“交流”。我们也开始日渐体验到一个真正全互联的交通解决方案。

大多数互联道路解决方案的侧重点，都是希望解决当今交通所面临的各类挑战。这些挑战可以按照表1-2所示分为3大类。

表1-2 当前被互联道路技术解决的挑战

挑战	支持数据
安全性	根据美国交通部的数据，仅 2012 年一年就发生了 560 万起车祸。这些事故共导致 33000 人丧生。物联网和互联汽车技术的采用可以让驾驶员通过工具预测潜在的交通事故，并由此显著减少每年因交通事故丧生的人数
移动性	在世界范围内，有超过 10 亿车辆在道路上驾驶。互联车辆移动性应用可以让系统管理员和驾驶员根据更加全面的信息作出决策，减少因交通问题导致的延时 每年，人们因交通阻塞而被浪费掉的时长长达 55 亿小时，减少交通延迟从未像今天这样重要。此外，与公共交通工具、应急车辆和交通管理设施之间的通信可以优化车辆的选路，这可以进一步减少潜在的延时
环境	根据美国公共运输协会（American Public Transportation Association）的数据，每年公共交通系统可以通过减少私家车的里程数，共计减少 1620 万公吨的二氧化碳（CO ₂ ）排放。互联车辆环境应用可以让所有交通参与者掌握选择“绿色”交通方式的实时信息

通过解决表1-2中所述的这些挑战，互联道路可以给设备带来诸多利好。这些利好因素包括减少交通拥堵和城市拥堵，减少因交通事故造成伤亡的人数，减少应急车辆的响应时间，减少汽车的尾气排放。

例如，通过将车辆连接到物联网当中，一种称为十字路口移动协助（Intersection Movement Assist, IMA）的概念就有可能落地。这种应用可以在车辆进入十字路口的时机不安全，极可能造成撞车的情况下（例如另一辆车通过停车标记闯入十字路口，或者偏离了正常行驶线路），向驾驶员进行告警（或者在自动驾驶车辆中触发相应操作）。由于汽车和道路基础设施之间的通信系统，这类场景可以迅速而又安全地得到解决。图1-4所示为IMA的图形化表示。



图1-4 十字路口移动协助的应用

IMA是我们将物联网与传统车辆和自动驾驶汽车进行集成之后，有可能得到的众多道路交通解决方案之一。其他解决方案包括自动车辆追踪、货物管理和道路天气通信。

通过自动车辆追踪，人们可以用车辆的位置来通告车辆抵达的时间、防止车辆失窃，或者提供高速公路协助。货物管理功能可以在车辆在途时提供精确的货物位置信息，这些通告提示信息可以发送给调度人员，车辆的选路也可以针对道路拥堵情况和天气情况进行优化。道路天气通信功能可以使用传感器和卫星、道路和桥梁发送的数据，来向车辆进行危险条件告警，或者针对当前道路提供天气信息。

当今，一般的机动车会使用百万条以上的代码，这些数据仅仅是冰山一角。随着汽车越来越深入地连接到网络，并且也越来越有能力针对自己的位置、性能、驾驶行为等因素生成连续的信息，一辆车能够生成的信息会达到令人不可思议的数量级。据估计，一辆能够完全接入网络的车辆可以每小时生成25GB的数据，其中大部分数据都会被发送到云端。说得更清楚一些，这相当于每小时向云端上传 10 多部高清电影——这说的可是我们的家用汽车！这个数量乘以每辆车每年的驾驶时长，再乘以上路的车辆数，每年生成的数据会以泽字节

（zettabyte）计（即每年百万拍字节[petabyte]）。图1-5展示了一辆联网车辆上有可能安装的传感器类型和连接。

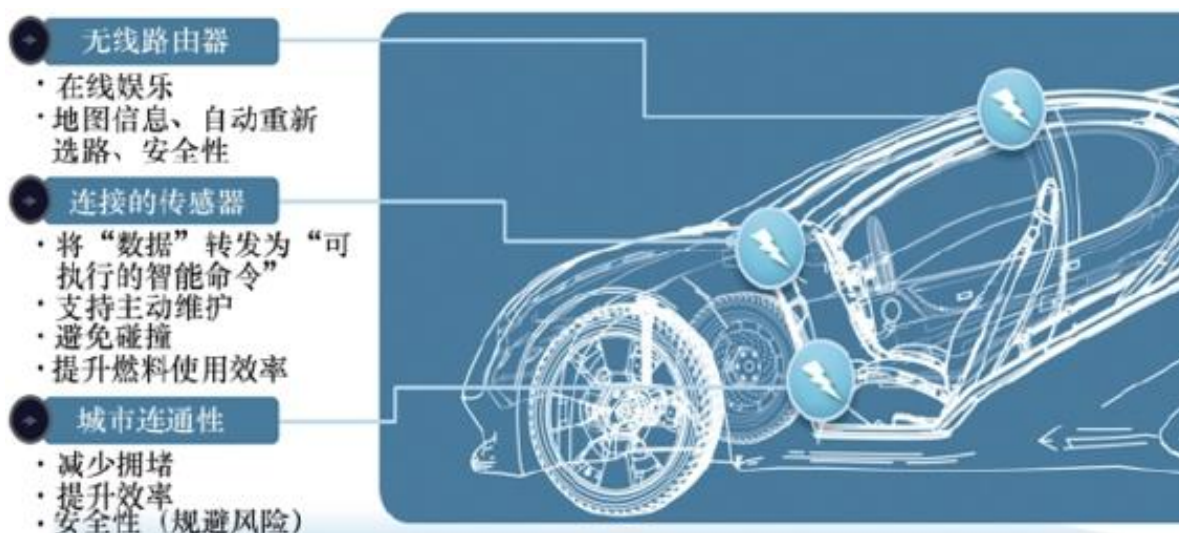


图1-5 联网车辆

互联道路可能经历的另一项重大突破在于，汽车生成的数据可能会被第三方使用。显然，我们的车辆生成的数据需要用一种安全可靠的方式来进行处理，这也就意味着网络的安全性必须得到保障，它必须能够对驾驶员和车辆进行身份认证和信息验证，它还必须拥有很高的可用性。但谁又会使用这些数据呢？车辆数据对很多感兴趣的机构来说都很有价值。比如，轮胎企业可以实时收集到它们的产品在各类环境中的使用寿命数据。汽车厂商可以通过传感器的数据，更好地掌握汽车的驾驶方式，以及当一些零部件出现故障时，汽车是否会发生故障——这些信息可以帮助汽车制造商在未来设计出更好的车辆。在自动驾驶汽车问世之后，这类信息就格外重要，因为这类汽车的驾驶方式显然会与传统家用汽车存在巨大的区别。

在未来，汽车传感器可以与第三方的应用（如GPS/地图）进行互动，这可以让汽车能够动态重新计算道路以便规避拥堵、事故和其他道路风险。同样，基于互联网的娱乐信息（包括音乐、影片和其他流媒体信息或者下载的文档）都可以针对每个人进行定制，让人们的旅程更加惬意。

这些数据也可以用来针对用户推送有针对性的广告。GPS导航系统会与传感器和寻路应用进行更加深入的集成，车辆可能会有能力针对每个人定义不同的推荐道路方案。例如，车主特别青睐某家咖啡厅，那么导航系统就可以通过基于云的数据连接器，提供通过该咖啡厅的推荐道路方案。

所有这些与数据有关的机会都会催生同一项新兴技术：物联网数据代理商。试想，一辆汽车生成了大量不同类型的数据，各方又都对这些数据抱有兴趣。这就会带来一个巨大的商机。很有可能，汽车和驾驶员生成的数据会成为一项有利可图的交易品。在数据从汽车传输到云端时，它会到达云端的一个初始位置，这些数据会在那里进行分类并且有选择地销售给不同的数据代理。例如，轮胎企业可能会付费购买与轮胎有关的传感器所提供的信息，但它们不会获得其他的信息。当信息代理商成为一个历史比较悠久的行业时，用来（在一个安全可靠的环境中）对汽车提供的数据进行汇总和分类的技术也会快速发展，这类技术也会在未来很多年间成为物联网行业的核心技术。

互联道路可能会成为发明创造的最大增长点之一。机动车，以及机动车行驶的道路在过去一个世纪中都曾经发生了惊天动地的变化，但未来的变化一样会激动人心。仅在过去几年中，我们已经看到世界各地的高速公路系统采用了复杂的传感器系统，这些传感器系统可以检测到地震、车祸、恶劣天气、交通拥堵等。道路光纤传感技术的最新发展变化在于，道路现在不仅能够记录行驶的汽车数量，还能够记录它们的速度和类型。由于上文已经讨论过的很多原因，互联车辆与道路会有限采用物联网技术。读者如果希望阅读针对物联网用例和交通行业架构的深入探讨，可以阅读本书的第13章。

1.3.2 互联工厂

很多年来，传统的工厂已经因为生产环境“无连接”而占尽劣势，这种劣势至少也是因为信息被“严格控制在”企业商业系统、供应链、客户和合作伙伴之间而造成的。这类传统工厂的管理人员基本是“两眼一抹黑”，他们对企业的运作缺乏了解。这里的运作包括厂

房车间、前台的运作和在独立仓库中供应方的运作。由于缺乏了解，修复各类宕机事故和质量问题，以及找出制造缺陷的根源，对于这类传统工厂往往并非易事。

当今工厂环境中的制造业面临的挑战包括以下几点：

- 需加速推出新的产品和服务，以便抓住客户和市场机会；
- 提升工厂的生产力、质量和运行时间，同时降低生产成本；
- 缓解计划外的宕机时间（这段时间平均消耗至少5%的生产力）；
- 保护工厂免遭网络攻击的威胁；
- 减少布线和重布线的功能（这类成本最多可能占部署总成本的60%）；
- 提升工人的生产率和安全性。

火上浇油的是，这些挑战往往需要在生产业务的各个级别上进行解决。例如，执行管理人员希望有新的方式能够降低生产成本，以便平衡能源和材料成本的增加。产品开发将市场视为第一要务。厂房的经理则把自己的全部注意力都放在了工厂的生产效率和操作的灵活性上。控制与自动化部门则负责管理工厂的网络系统、控制系统和应用，因此需要深入了解这些系统。

世界各地的工业类企业都在给工厂重新配备新的技术和架构，以便解决这些问题，同时提升生产的灵活性和效率。这些科技进步让企业的总体设备效率、供应链响应能力和客户满意度都迈上一个新的台阶。将这些基于工厂的操作技术和架构与国际互联网进行融合，这个趋势刚刚显现出来，这种趋势就称为互联工厂。

正如我们在前文中谈到的互联道路那样，工厂车间的地板上已经部署了大量基本的传感器。不过，随着物联网时代的到来，这些传感

器不仅增加了科技含量，而且可以建立更高级别的连通性。它们更加智能，能够实现数据通信，这种通信主要是使用IP协议通过以太网架构建立起来的。

除了传感器之外，车间地板上的设备也变得更加智能了，它们可以传输和接收大量的实时信息和诊断数据。以太网连接变得无处不在，它们不再仅仅停留在工厂的主控制器和机器人之间。此外，更多支持IP协议的设备（如监控摄像头、诊断智能对象，甚至个人移动设备）都加入到了工业生产环境中。

例如，一台熔炼设备从矿石中提取金属。这台设备使用加热和化学物质来分解矿石，留下纯金属。上述这个过程分成很多步骤，但所有的数据和控制系统需要在车间中的很多控制间中访问。所以，操作人员必须走到控制间（往往在数百米开外）中来查看数据，对生产操作进行调整。大量的操作时间往往就浪费在了往返于操作间的路途之中。而在物联网和互联工厂的解决方案中，人们可以通过真正的“人机连接”，让传感器数据直接通过移动设备传输给车间中的操作人员。往返于控制间和车间的时间也被节省了下来。此外，由于操作人员能够实时收到数据，他们也就可以更加迅速地做出决策，这样可以提升生产效率，弥补生产中的质量问题。

实时定位系统（Real-Time Location System, RTLS）是互联工厂解决方案的另一个应用示例。这种系统可以通过粘贴在任何材料上的小型WiFi RFID标签来提供该材料的实时位置和状态信息。这些标签可以让工厂追踪生产的情况。这些物联网传感器让流水线上的各个部件和材料能够与网络进行“交流”。如果人们能够对流水线上的产品实时进行跟踪，也就可以调节流水线的生产速度来实现既定的生产目标，人们也可以轻松判断出在产品生产的各个环节中，工作人员的工作效率。生产环节中的瓶颈和产品的质量问题的同样会被迅速定位出来。

当我们都把物联网看作是升级版的互联网时，我们也同样可以将其视为是工业领域的升级版。在2016年的世界经济论坛中，人们将互联网的发展和物联网的影响称为“第四次工业革命”。第一次工业革

命诞生于18世纪晚期的欧洲，这次工业革命以人们将蒸汽和水力应用于机械化生产作为标志。第二次工业革命发端于19世纪70年代早期，终止于20世纪初，这次工业革命见证了电力网和大规模生产技术的采用。第三次革命始自20世纪60年代末/70年代初，人们自此将计算机和电子设备应用到了工业生产领域和其他工业化系统当中。我们现在正在经历的是第四次工业革命，物联网正是这场工业革命的驱动力。图1-6总结了这四次工业革命，它们分别称为工业1.0版到工业4.0版。

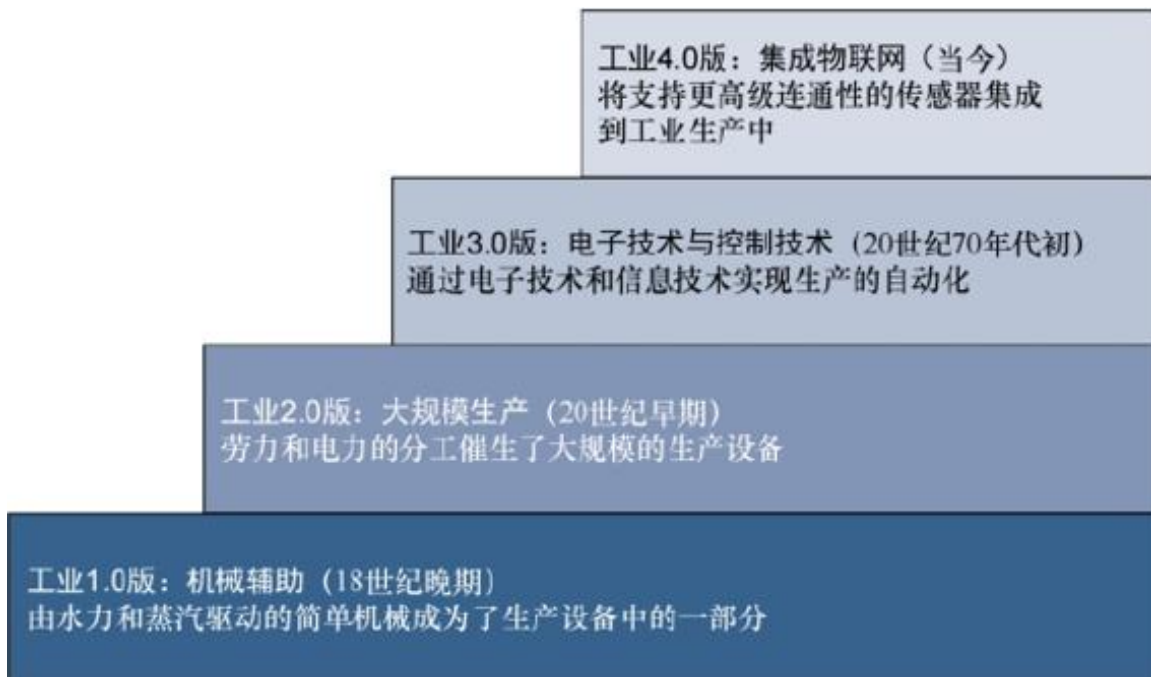


图1-6 四次工业革命

工业4.0版的物联网潮流将工业生产从纯粹的自动流水线组装模式转变为了由能够相互通信的智能机械进行工业化生产。工业生产领域的物联网将智能生产带到了工厂环境中。这始自于将传感器、执行器和控制器置入一切与生产有关的环节当中。网络连接将这些装置连接在了一起，以便人与机器能够共同分析数据，做出智能决策。最终，这种生产方式会让机器具备预见故障和自动恢复的能力，于是整个世界也就不需要人类的监测和干预了。

1.3.3 智能互联楼宇

物联网会施加重大影响的另一个领域是智能互联楼宇。在过去几十年时间里，楼宇的架构变得越来越复杂，其中包含了一层又一层的系统。这使得楼宇中的建筑结构、机械结构、电力供应系统和IT系统之间的关系变得前所未有的复杂。时间一久，这些用以支持楼宇环境的功能网络演变成了一个复杂的系统。不过，在大多数情况下，这些系统都是独立安装和管理的，它们相互之间并没有太多交集。

楼宇的功能在于给工作人员提供一个舒适、高效而又安全的工作环境。工作区域应该采光良好，同时温度适宜。为了让工作人员感到更加舒适，火警系统和灭火系统都应该善加管理，门和物理安全报警系统也是一样。随着现代化楼宇中智能系统的普及，这些功能都得到了提升，但这些系统中，大多数系统目前仍然是独立于其他系统的，它们也不会考虑人们目前处于楼宇中的哪些区域，以及每个区域中分别有多少人。不过，很多楼宇目前都在开始部署传感器来检测住户的位置。当很多人在一个房间中移动时，移动检测住户传感器可以提供准确的检测，并且在人们全都离开这间房间的时候将灯关掉。可是，如果传感器没有检测到房间中的某个人，又会出现什么情况呢？想让一个非智能传感器将房间的灯关闭却无计可施，这实在让人哭笑不得。

同理，人们也经常通过传感器来控制暖气系统、通风系统和空调系统（HVAC）。温度传感器遍布于楼宇的各个位置，它们的作用是影响楼宇管理系统（BMS）对房间中气流的控制。

智能楼宇的另一个有趣之处在于，它们可以降低管理成本，同时让楼宇的管理更加轻松。试想，大量成本都被花在了管理这些复杂的楼宇结构上，何况很多人都把自己的工作时间花在了大楼里，管理人员势必对于高效低价的楼宇管理方式更感兴趣。你一定听到过人们抱怨自己的工作空间不够大，抱怨管理员人员没有很好地利用办公室环境。当这些人去找管理层申请改变办公环境的布局（比如增加办公区域）时，管理人员往往会要求他们证明自己的要求是合理的。然而，办公环境未被有效利用，这充其量只能是人们的一种直观感受。如果将智能楼宇和住户检测技术结合起来，人们就可以对数据进行分析（见本书第7章）。这样一来，通过展示楼宇布局的使用率来证明当前

的布局不合理，这也就容易多了。同样，这栋建筑的管理人员也可以使用这种方式来判断这栋楼的哪些区域没有得到高效的使用，然后使用这些信息来改善空间的使用效率。通过这种方式，我们也就进入到了由物联网引领的建筑自动化时代。

虽然管理建筑系统的技术解决方案不一而足，但直到最近，这些解决方案仍然都依赖于一个独立的覆盖网络，每个网络都专用于解决一项专门的任务。为了将这些系统连接到同一个框架中，人们设计了楼宇自动化系统（Building Automation System, BAS）来将HVAC、照明、火警、检测和访问控制系统置于同一个管理系统中。这些系统可能都支持将很多不同类型的传感器和连接到BAS当中。我们要如何把这些系统连接在一起，以便通过一种统一的方式来对整栋大楼进行管理呢？这个问题涉及物联网所面临的最大挑战之一，即物联网系统的异构性。对这个问题的讨论会贯穿整本图书。

在将这些异构系统连接在一起之前，这些系统需要汇集在网络层，并且支持一个能够集成应用层的公共服务层。融合网络的价值在很多文档中都被充份论证过了。比如，在2000年初，Cisco和很多其他的企业就曾呼吁将语音和视频集成到IP网络中，彼时已经有很多应用都在共享IP网络了。由于经济规模和管理效率都从这项倡议中获益良多，VoIP和协作技术业已成为了一项通用标准。不过，将IP网络与楼宇的通用服务框架相结合，这个速度就要慢得多了。

例如，建筑自动化系统实际采用的通信协议称为BACnet（建筑自动化与控制网络）。简言之，BACnet协议定义了一系列能够让建筑中的设备（如HVAC、照明系统、访问控制系统、火警系统）通过以太网通信的一系列服务。楼宇可以通过同一台以太网交换机来同时提供IT通信和BACnet连接。这种标准化方式也给人们使用（由IT部门管理的）网关设备作为结点来连接IP网络保留了可能性。此外，根据BACnet/IP的定义，它们都支持建筑网络中的“物”通过IP来相互通信，所以它们也都支持将建筑管理系统连接为同一个网络。图1-7展示了建筑协议与IP之间的会话。

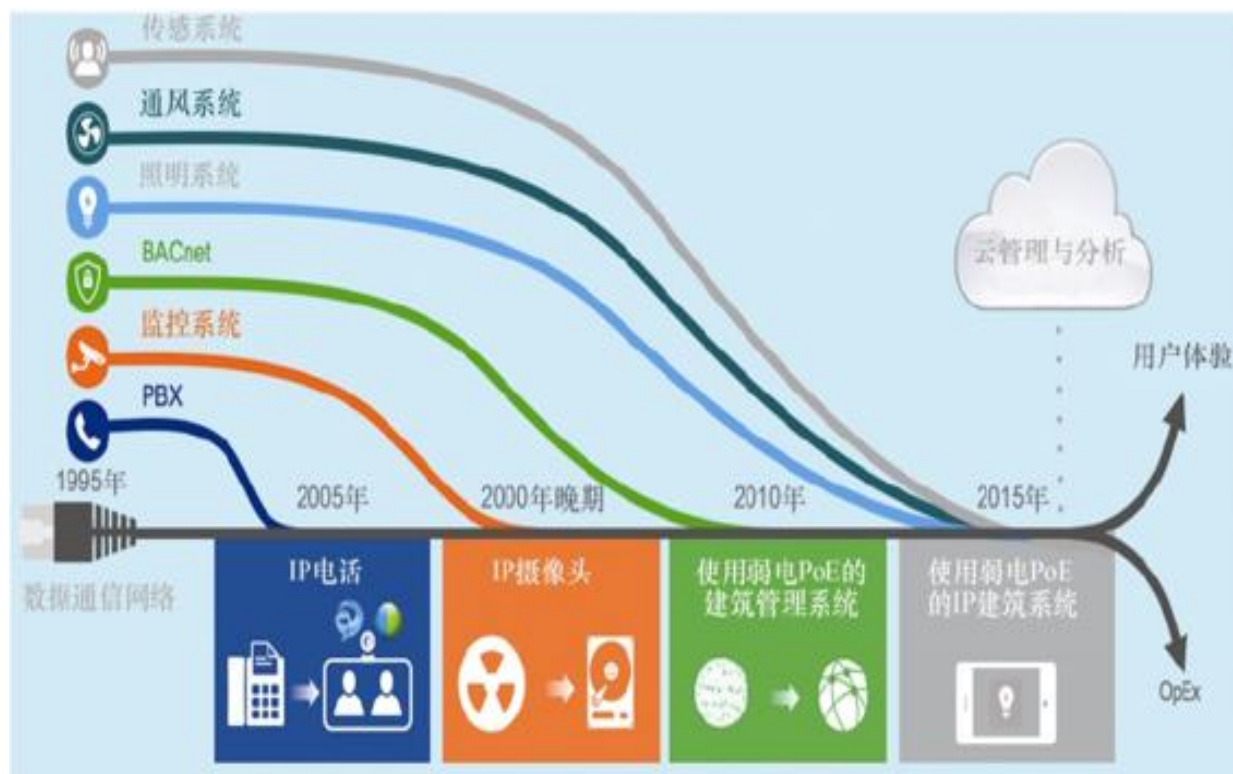


图1-7 建筑技术与IP的融合

物联网技术的另一大前景就在智能互联楼宇领域。当前，这种技术的一大应用示例就是“数字天花板”。数字天花板并不只是一个照明控制系统。这种技术包含了楼宇中很多不同的网络（其中包括照明系统、HVAC、电动窗帘、闭路电视和安保系统），并且它将这些网络都组合到了IP网络当中。图1-8所示为数字天花板的框架结构。



图1-8 数字天花板的框架结构

数字天花板技术的核心是照明系统。读者大概也体会到了，照明市场目前正在经历向LED照明的重大转折期。与传统的照明方式相比，LED能耗更低，使用寿命更长。LED产品的低能耗需求使得这类照明产品能够支持PoE（以太网接口供电），这也就使它们能够直接连接到标准的网络交换机上。

在一个数字天花板环境中，每个照明设施都直接通过网络相连，它们通过相同的基础设施提供控制与电能。照明领域过渡到LED照明意味着人们现在可以在一个融合网络中包含照明系统，让照明系统和其他由IT网络管理的系统一道成为楼宇管理系统的一个组成部分，这个管理系统可以支持语音、视频和其他的数据应用。

下一次，当你抬起头仰望办公楼的天花板时，别忘了数一数灯的数量。灯的数量完全可以远远超过物理接线端口的数量。显然，为了让网络能够支持大量的以太网端口和更多的IP地址，整个网络都需要重新进行设计。同时，这样的环境也要求我们在天花板上部署一个静

音的、无风扇的、支持PoE的交换机。这也就是说，在进行长期商业案例规划时，采用节能的LED照明技术，而不再安装传统的日光灯或卤素灯泡十分重要，因为这样做几乎不会增加在网络上的前期投资。在人们翻新楼宇或者建造新的建筑之后，采用数字天花板的商业案例就会显得更为重要。在这类商业案例中，在天花板中使用CAT 6/5e线缆连接照明设施与在天花板上布满电线来连接所有照明设备相比，前一种方式显然会大大削减成本。

在天花板上安装支持PoE的LED照明设施能够节省成本，这一点毋庸置疑。然而，在每一个会有人经过的地方，都在天花板上安装支持IP功能的传感器，这样做可以带来前所未有的机遇。比如，大多数天花板上的照明设施都支持住户传感器。这类传感器可以支持高分辨率的数据采集，采集来的数据可以用于控制灯的开关，这些数据也可以与其他分析数据结合起来，来控制其他系统，比如HVAC和安防系统。与用来检测移动之物的传感器不同，现代的照明传感器可以集成到大量的住户传感技术当中，包括低功耗蓝牙（BLE）和WiFi。这里面的科学原理十分简单：因为现在人人都会随身携带一台支持BLE和WiFi的智能设备，而这些传感器只需要检测BLE或WiFi信号就可以了。当一个人走近一盏灯时，他的位置就会被检测出来，而无线系统可以发送信息，让HVAC系统实时控制进入那个区域的气流，在最大程度上增加办公人员的舒适度。图1-9所示为一个数字天花板灯上安装的住户传感器。



图1-9 一个携带住户传感器的LED数字天花板照明灯

读者可以想象一下物联网智能照明系统给工作环境带来的变化。它不仅可以根据住户的实际位置和建筑的使用率来优化照明效果，还可以让人们更加准确地控制温度，管理烟雾与火灾检测装置，以及管理视频摄像头和楼宇的访问控制系统。物联网可以让所有这些系统接入同一个网络，这不仅可以节省安装时间，而且可以节省安装这些系统的成本。

1.3.4 智能生物

在想到物联网时，人们首先想到的东西往往是那些死气沉沉的互联装置和互联设备。不过，物联网也可以将活生生的东西连接到互联网当中。人们可以将传感器安装在动物甚至昆虫身上，这就像我们在机器上安装传感器一样简单，但它带来的好处同样十分惊人。

在动物身上应用物联网技术的最知名的应用方法，我们称之为“互联奶牛”。一家名为Sparkd的德国企业发明了一种传感器，这种传感器可以安装在奶牛的耳朵上。它可以检测奶牛的各类健康状况，以及奶牛的位置，并且通过无线的方式将这些数据传输给奶农以供分析。

这些传感器每年可以产生约200MB的数据。显然，这类环境必须有网络设备来与传感器建立连接，并且存储这些信息。然而，一旦采集到这些数据，奶农就完全掌握了牛群的动向，以及每一头奶牛的相关数据。人们可以了解到环境因素会如何影响牛群，改变牛群的食物摄入规律。这可以让人们在看到牛群减少食物摄入时，就提前检测到奶牛的疾病，而不必等到出现症状才发现这一点。这些传感器甚至可以提前检测到奶牛是否已经怀孕。

另一个在有机物上应用物联网的方式，是将传感器安装在蟑螂身上。虽然很多人听到有关蟑螂的话题多少都会感到有些不适，但是“支持物联网的蟑螂”可以在灾害环境中挽救很多人的生命。

北卡罗莱纳州立大学的研究人员希望通过研究马达加斯加蟑螂来帮助应急人员在灾害发生时救助幸存者。如图1-10所示，研究人员将一个电子“背包”安装在了一只蟑螂的后背上。蟑螂身上的这个背包可以通过蟑螂身体中的某些部分与蟑螂建立通信。如果有弱电脉冲发往一侧的天线，蟑螂就会向另一侧移动，因为它们可以让蟑螂认为它在前进的方向遇到了障碍物。蟑螂下腹部的尾须是它的感知器官，它可以通过空气流动察觉到危险。当背包刺激这个尾须时，蟑螂就会前进，因为它会认为天敌正在靠近。

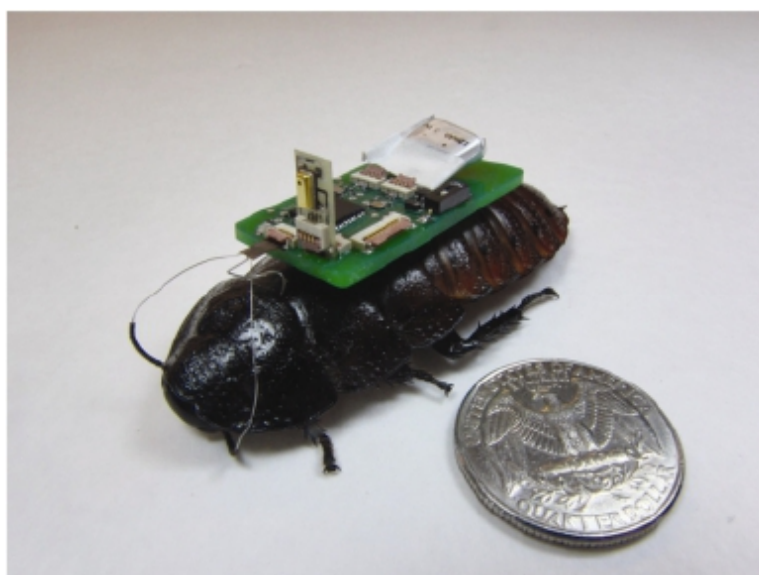


图1-10 支持物联网的蟑螂可以帮助人们在灾害发生时寻找幸存者

电子背包使用无线的方式与控制器进行通信，而且可以远程进行“控制”。想象一下，在灾难发生之后，比如在一场地震之后，有一队这样的蟑螂在倒塌的大楼中搜寻幸存者。蟑螂天然就会在封闭环境中围绕着各种障碍物移动。人们已经测试过在灾害区域培育蟑螂；这就像让狗在后院范围内活动的那道看不见的篱笆墙。用这种方式利用蟑螂可以对救援人员无法进入的区域绘制地形图，这有助于救援人员搜寻幸存者。

为了帮助找寻倒塌大楼中困住的幸存者，电子背包上会安装一个单向麦克风，其目的在于检测声音和声音的来源。人们可以通过软件来对声音进行分析，确保这是由人类发出的声音，而不是由一个漏水

的管子之类的东西发出的声音。接下来，人们就可以派蟑螂向发出声音的地方前进，因为那里可能有人被困。此外，麦克风也可以让救援人员听到检测到的声音。

这些案例显示了物联网不仅仅是安装传感器这么简单，它还可以让原本没有生命的“东西”变得智能起来。而那些有生命的“东西”也可以连接到互联网中，这些连接都可以带来重要的改变。

1.4 IT与OT的融合

不久之前，信息技术（IT）和运营技术（OT）还不存在太多的交集。IT可以让人们与互联网，以及相关的数据和信息系统之间建立连接，它强调要保护一个机构发送的数据流。OT则会对物理操作系统中的设备和流程进行监测和控制。这里所说的系统包括流水线、电网、制造设备、道路系统等。一般来说，IT不会介入OT的工业生产和流通环境当中。

从类别上说，IT机构负责管理企业的信息系统，比如电子邮件、文件和打印服务、数据库等。而OT则负责管理工业环境中设备与流程的运行，比如工业机械、计量表、执行器、配电自动化设备、SCADA（监督控制与数据收集）系统等。过去，OT使用的是专用网络，它有一套专用的协议来连接上述设备，而这些网络是与IT网络完全分离的。

OT的管理是企业的命脉。比如，如果在一个工厂中，连接机器的网络出现了故障，那么这些机器就无法正常工作，生产也要就此停滞，这有可能会给企业带来数百万美元的经济损失。然而，如果（IT部门负责管理的）电子邮件服务器出现了故障，几个小时无法访问，或许有人会大发雷霆，但这种情况不太可能会给企业带来相同数量级的经济损失。表1-3介绍了IT和OT网络的一些区别，以及它们各自面临的挑战。

表1-3 运营技术（OT）和信息技术（IT）之间的比较

标准	工业 OT 网络	企业 IT 网络
运行原则	确保业务不间断运行	以安全的方式管理计算机、数据和员工通信系统
优先级	1. 可用性 2. 完整性 3. 安全性	1. 安全性 2. 完整性 3. 可用性
数据类型	监测数据、控制数据和监督数据	语音数据、视频数据、交易数据和批量数据
安全性	控制对设备的物理访问	设备和用户需要向网络提供身份认证
故障的后果	OT 网络的故障会直接导致经济损失	是否导致经济损失取决于 IT 网络所在的领域，但有可能存在替代方案
网络升级 (软硬件)	只能在运营维护窗口进行升级	往往需要在员工不在现场期间规划一个通信中断窗口；造成的影响不大
安全漏洞	低：OT 网络是隔离的，而且使用的往往是私有协议	高：需要不断给主机打补丁，网络会连接到互联网，因此需要提供有效保护

随着物联网和标准协议（如IPv6）的涌现，IT和OT世界正在融合。说得更准确一点就是，OT正在开始采用IT组织的那一套网络协议、技术、传输机制和方法，而IT组织也在开始对OT的运营需求提供支持。当IT和OT开始使用同一个网络、协议和流程时，就会产生规模经济的效应。这种融合不仅会减少搭建基础设施所需的经费，也会让网络变得更容易操作。因为开放标准十分灵活性，所以新的技术也很容易被采纳并且出现增长。

不过，正如表1-3所示的那样，将IT和OT融合到一个网络中的趋势仍然面临很多挑战。这两种组织仍然存在着最基本的文化差异和优先级差异。物联网的发展正在迫使这些组织相互合作，而在过去，它们远比现在更加独立。比如，当OT机构发现，IT部门可以不考虑工业生产的需求，自行规划在周末关闭网络以便对软件进行升级时，OT机构就会大惑不解。同理，IT部门也无法理解OT部署的那些私有或订制系统与解决方案。

让我们以在一个网络中部署服务质量（QoS）技术为例。在IT部门部署QoS时，按照最高优先级处理语音和视频流量几乎是一项普适法则。但是，当OT系统共享同一个网络时，OT从业会认为实时OT流量应

该被赋予比语音流量更高的优先级，因为OT网络的任何故障都会导致直接的经济损失。

随着OT和IT的融合，两类系统都会进步。OT看上去会更接近IT技术，因为它们也会采用诸如以太网和IP协议这样的公共标准。同时，IT也会看上去更像是OT的业务伙伴，因为IT从业者也会更了解OT的工业产品和操作需求。

IT与OT相结合可以让商业环境变得更加高效，利润也更高，因为这种环境可以降低网络的宕机时间，可以通过规模经济降低成本，可以减少企业的库存，优化商品的运输时间。如果人们能够正确地处理IT/OT之间的融合，物联网就会获得双方组织的支持。这可以“让两类网络都获益良多”。人们会看到各类工业控制系统都工作在一个开放的、高度集成的、安全的技术环境之上。

1.5 物联网的挑战

物联网的未来为我们描绘了一幅生动的图景，但我们同时也面临了重大的挑战。物联网的很多环节已经成为现实，但物联网必须攻克很多障碍，才能真正走进各行各业和我们生活的每一个角落。表1-4重点介绍了物联网当前面临的最大挑战和问题。

表1-4 物联网的挑战

挑战	描述
扩展性	IT 网络的规模或许相当之大，但 OT 的规模比 IT 还要大很多个数量级。例如，亚洲的一个大型电力企业开始在其电网中部署基于 IPv6 的智能电表。这个电力企业拥有数万员工（这些员工可以视为网络中的 IP 节点），而这个电力公司在所服务区域要部署的电表数量可能多达数千万个。这意味着这个电力企业的网络范围增加了 1000 倍！第 5 章会深入介绍如何使用新的设计方法将 IPv6 网络扩展到上百万台设备上
安全性	随着越来越多的“物”连接到了其他的人与“物”，物联网时代的安全性问题也正在变得愈发复杂。安全攻击的目标大大扩展，如果一台设备遭到入侵，它的连通性就会成为一个焦点。因为攻击者可以利用他们入侵的设备作为跳板，攻击其他的设备和系统。物联网安全问题同样涉及物联网的每一个角落。要想进一步了解关于物联网安全的问题，可以参考第 8 章

续表

挑战	描述
私密性	随着我们周围的传感器数量越来越多，这些传感器所采集的数据会越来越具体地涉及每一个人和他的行动。这些被采集的数据包括健康信息、购物模式，以及在某家商店购买的产品。这些数据对于商家而言显然价值连城。各类组织机构现在都在讨论谁应该掌握这些数据，以及人们如何控制是否共享这些数据、与谁共享这些数据
大数据与数据分析	物联网与大量传感器会创建出海量的待处理数据。如果能够通过高效的方式处理这些数据，就会给我们提供价值连城的信息。与此相关的挑战在于，如何及时地评估从不同数据源、以不同形式采集到的海量数据。读者可以阅读本书的第 7 章，进一步了解物联网在大数据层面面临的挑战
互操作性	物联网也和其他新兴技术一样，面临着众多协议和架构大量涌入市场，需要对它们进行标准化的问题。在这些协议和架构中，一部分是私有技术，另一部分则是公共技术。最新的物联网标准正在尽量尝试简化这个问题，但仍然有大量与物联网相关的协议和实现有待标准化。本书的重点就是其中的那些著名的协议和架构（尤其是那些公开的、基于标准的实现方式）。读者可以阅读本书的第 2 章、第 4 章和第 6 章，深入了解构成物联网的各个协议

1.6 小结

本章对物联网进行了入门介绍，回答了“什么是物联网”的问题。物联网的宗旨是连接未连之物，让智能产品能够与其他人、物或者系统进行通信。物联网的最终结果是创建一个能够更好地控制外在世界，同时实现更多高级应用的智能网络。

本章也对物联网的历史发展进行了阐述，指出当前的物联网这一概念是互联网发展的下一个阶段。在这一章中，我们从一定的高度详细介绍了物联网的一些用例，由此解释了物联网对我们的影响，以及它有可能如何改变我们的世界。

本章介绍了大量物联网的相关概念和术语，包括物联网与数字化这两个概念的差异、IT与OT的融合。在最后一节中，我们详细说明了物联网所面临的挑战。

在阅读本章之后，读者应该能够清楚地理解物联网这种理念。此外，本章也希望能够为读者深入学习此后各章打下基础。

第2章 物联网网络架构与设计

我们来想象这样一幅场景：你决定建一座房子，你把车开到建材市场，想要搞清楚要用到哪些材料。接下来，你买了木材、钉子和螺丝钉、用于地基的水泥搀和料、屋顶材料等。过一阵，一辆卡车把你购买的所有这些材料送到了要盖房子的地方。你坐在未来的草坪上，盯着这一大堆建筑材料，完全不知道该如何下手。这时候，你意识到缺了点什么：没有给新房子设计建筑方案！问题来了，在你找一位建筑师聊聊之前，看来建新房子的计划只能推迟下去了。

每一位建筑都明白这样一点，哪怕最简单的建筑项目都需要进行精心的设计，而且所有建筑都要符合一定的建筑标准。如果建筑项目更复杂一点的话，那么“要对这个项目进行详细的规划”就已经不是一个好点子了，这是法律规范。

要想顺利完成一个建筑项目，人们需要付出大量时间和精力对项目的每一个步骤进行从地基到房顶的通盘设计。在这个设计方案中，必须包含供电、给排水、供暖和安全系统的详细设计规划。所有建筑项目中都必须包含完善的建筑蓝图（以及支持这份蓝图的必备工程技术原理），无论是简单的项目，还是复杂的项目。同理，如果没有精心的设计方案、完善的安全策略，以及严格遵循设计方案进行施工的计划，人们也不应该搭建计算机网络。如果人们没有按照完善的网络设计原则来规划网络，那么这样搭建出来的网络往往就会面临诸多问题，包括很难进行扩展、管理，无法适应需求变化，甚至在发生故障时难以排错等。

大多数CIO和CTO都能理解这一点，即网络是业务的关键。如果网络出现故障，企业运作有可能会受到严重的影响。恰如人们在设计房屋时，需要考虑房屋在（如地址、飓风等）灾害条件下的承重水准一样，信息技术（IT）系统也需要在设计时将承受“网络灾害”的能力考虑进来，这里所说的网络灾害包括DDoS（分布式拒绝服务攻击）攻

击、未来的网络扩展需求、网络中断，甚至人为错误导致的问题。为了解决这些问题，在过去20年间，网络设计的技巧在各类IT组织中获得了空前的影响力。实际上，对于很多企业而言，监督网络架构的职责往往是由IT和OT组织中担任最资深职位的人物来负责履行的。比如，企业总架构师（Chief Enterprise Architect, CEA）这个职位近年来备受关注，因为这个职位的职责往往相当于CTO，而且在很多情况下，CEA的直接上级就是CEO。

企业IT网络架构在过去20年间成熟了许多，而且这种网络架构往往也很容易理解。不过，物联网网络架构的原则是全新的，需要人们从一种全新的角度来看待它。尽管IT架构和物联网架构这二者之间确实存在着一些相似之处，但在大部分领域，物联网系统所面临的挑战和需求都与传统IT网络存在巨大差异，读者务必注意到这一点。这两种架构在术语层面也存在区别，因为物联网网络属于OT，它也负责管理操作系统的状态。而IT网络则主要关注传输数据流的基础设施，无论这些设备传输的数据属于什么类型。

本章会介绍物联网所面临的一些挑战，以及这些挑战对这种新型网络架构所构成的影响。本章会介绍以下内容。

- 新型网络架构背后的驱动力：OT网络促进了核心工业运营方式的发展。这类网络有自己的特点和限制，因为传统的IT网络架构很难对其提供支持。

- 比较物联网的架构：各类机构（包括ETSI和物联网世界论坛）已经为物联网发布了很多不同的架构。本节会对这些架构进行讨论和比较。

- 简化的物联网架构：虽然物联网有很多不同的架构，但本节会提供一个简化版的模型，以便为读者学习本书后面的内容打下基础。

- 核心物联网功能协议栈：物联网的设计方案必须能够对它的这些特殊需求和限制条件提供支持。本节会介绍从传感器到应用层的完整的物联网堆栈。

■ 物联网数据管理与计算堆栈：本节会介绍关于数据管理的内容，包括存储、物联网的计算资源模型，这会涉及边缘、雾和云计算。

2.1 新型网络架构背后的驱动力

本章开篇提到的使用建筑蓝图来建造房屋与设计网络的方式如出一辙。现在，请想象一位毕生都在建筑居民楼的经验丰富的建筑师。这位建筑师是这个领域的专家，他十分了解如何才能让自己设计的房屋外观靓丽、功能完善、适宜居住，同时符合当地政府制订的强制规范。有一天，这位建筑师接到了一个新的项目：建一个大型体育馆，这个体育馆应该成为这座城市的地标建筑，负责承接一系列的体育赛事、演唱会和群众性活动，这个场馆需要能够容纳60000人以上。

虽然这位建筑师在建造住宅楼方面经验丰富，但他的这些技能显然无法满足这个项目的需要。这个体育馆不仅规模比住宅楼大很多个数量级，功能与住宅楼全然不同，而且它的使用损耗也和住宅楼不在一个级别。所以，这位建筑师需要使用一种新的建筑设计方式来设计和建筑这座体育场馆。

IT与OT之间的差异就类似于建造住宅楼和建造体育馆之间的差异。IT的传统网络架构已经为我们服务了很多年，但它们无法很好地适应物联网提出的复杂需求。第1章曾经介绍了IT与OT之间的一些区别，以及物联网所提出的一些挑战。这些区别与挑战都在从根本上驱动着网络架构向一种全新的物联网系统架构演化。

IT与OT之间最主要的区别在于数据。其中，IT系统主要关注的是如何给诸如电子邮件、Web应用、数据库、CRM系统这样的业务应用提供可靠的、连续的支持。而物联网的关注对象则是那些由传感器创建的数据，以及如何使用这些数据。所以，物联网架构的核心就是如何传输、采集和分析这些数据，并且最终使用这些数据来达到最终的目的。

表2-1对IT和OT网络之间的区别进行了详细的比较，该表主要关注的是物联网那些正在驱动网络架构发展变化的需求，以及人们需要针对这些需求对网络架构做出哪些调整。

表2-1 物联网架构的驱动力

挑战	描述	需要物联网架构做出的变化
规模	物联网终端（传感器）的规模远比传统网络的规模要大	IPv4 地址空间已经耗竭,它无法满足物联网提出的扩展性需求。这种规模只有通过 IPv6 才能实现。而 IT 网络会继续通过 NAT（网络地址转换）这类的技术来延续对 IPv4 的使用
安全性	物联网设备（尤其是无线传感器网络中的物联网设备）往往在物理层面暴露在外部世界当中	物联网的每个环节都需要安全性保护。每个物联网的端点设备都必须处于整体安全策略的保护之下,它们必须支持设备级认证和链路加密技术。它们还必须能够通过某种零接触部署模型就轻松实现部署
电力、CPU、内存和链路速率给设备和网络带来的限制	由于规模巨大,距离更远,这类网络往往面临比较多的限制,更容易丢包,而且只能支持很低的数据传输速率（几十 bit/s 到数百 kbit/s）	新型的“最后一公里”无线技术必须能够长距离支持一部分物联网设备。网络也会面临一些限制,这表示人们需要对传统的网络层传输机制进行一些修改
生成大量的数据	传感器每天都会创建大量数据,这会造成网络瓶颈,降低云的数据分析性能	数据分析功能必须分布在物联网的各个部分,从网络边缘到云都需要能够对数据进行分析。而在传统 IT 网络中,往往只有云会执行数据分析和运行应用
支持传统设备	物联网中往往会连接一系列新型的、支持 IP 技术的端点设备,以及大量传统的、不支持 IP 功能的设备,后一类设备需要通过串行线缆和私有协议来完成通信	数字化改造是一个长期的功能,可能需要很多年的时间才能完成。物联网需要支持协议转换和/或隧道机制。通过这些机制,物联网就可以让传统协议运行在标准协议（如以太网协议和 IP 协议）之上
实时分析数据的需求	传统 IT 网络对数据执行的是预订批处理,而物联网数据则需要进行实时处理和响应	分析软件需要部署在更靠近网络边缘的位置,这些软件必须支持实时数据流分析。传统 IT 分析软件更适合在事件发生后执行批处理分析

下文会对驱动物联网架构做出变化的需求进行更加深入的解释。

2.1.1 规模

传统IT网络的规模大约包含数千台设备（一般为打印机、移动无线设备、笔记本电脑、服务器等）。传统的三层园区网模型很好理解，这类模型包含接入层、分布层和核心层（还有诸如WAN、WiFi、数据中心网络等一些组成部分）。但想象一下，如果将一个数千端点的网络扩展为数百万端点的规模，又会发生什么呢？有多少IT工程师设计过可以支持数百万个可路由端点的网络？此前恐怕只有一级服务提供商网络可以达到这种规模。物联网引入了一种模型，中等规模的车间、工厂、交通系统或者城市都可以支持这种规模的网络。鉴于物联网的规模比较庞大，IPv6无疑就是物联网网络层的不二之选。

2.1.2 安全性

人们常说，如果第三次世界大战开战，这会是一场网络空间的战争。我们也都见证了利用网络设备的弱点发起的恶意攻击，比如Stuxnet蠕虫就是针对西门子的PLC（可编程逻辑控制器）系统的恶意程序。

几年来，网络攻击的频率和影响与日俱增。保护企业数据免遭入侵和窃取已经成为了IT部门的主要任务之一。IT部门在保护服务器、应用和网络方面已经走得很远，它们部署了深度防御模型，用多层安全模型来保护企业网络的价值。不过，无论人们做出多大的努力来保护网络和数据，黑客仍然可以设法侵入到这些可靠的网络当中。在IT网络中，第一道防线往往是位于网络边缘的防火墙。人们显然不可能把重要的IT端点部署到防火墙外面让感兴趣的人随便参观。但物联网的端点设备则往往处于无线传感器网络当中，这些网络使用的往往是无需授权的频谱，人们不仅可以使使用频谱分析仪看到这些网络，而且还可以从物理上接入并且被人们广泛使用。

虽然越来越多的OT系统连接到了IP网络当中，它们的功能也与日俱增，随之增加的是这类系统的漏洞。比如，在2015年12月23日下午3点半，乌克兰电网经历了一场出乎意料的网络攻击，大约 22.5 万名用户受到了这场网络攻击的影响。这可不是由一个机会主义组织发起

的简单网络攻击，这是一场复杂的、精心策划的针对乌克兰电网SCADA系统的网络攻击，被攻击的系统负责管理电网自动化设备的通信。

传统的IT安全模型并不是为了保护高度分散的物联网系统免遭新型网络攻击而生的。物联网系统需要拥有一致的认证、加密和入侵防御机制，这些机制能够理解工业协议的运作方式，而且能够对那些向重要设备发起的攻击做出反应。要想尽可能提升物联网的安全性，物联网系统必须：

- 能够识别所有接入物联网服务的实体（即网关、端点设备、家庭网络、漫游网络、服务平台），并且对它们进行身份认证；

- 确保端点设备与后端应用之间传输的所有用户数据都经过了加密；

- 符合当地的数据保护法规，让所有数据都受到保护并且是以安全的方式进行存储的；

- 使用了一个物联网连通性管理平台，同时建立了符合规则的安全策略，这样一来，如果物联网所连接的设备被检测出了异常行为，网络就会立刻采取相应的动作；

- 通过整体的、网络级的方式来提供安全性保障。

读者可以阅读第8章进一步了解关于物联网安全的内容。

2.1.3 设备与网络的限制

大多数IT传感器的功能都是单一的，它们往往体积不大，价格低廉。这也就是说，它们的功能、CPU和内存并不强大，而且只有在发生重要的情况时才传输数据。由于这些设备数量庞大，而且往往部署在那些范围广大、不受控制的环境当中，所以为它们提供连接的网络也往往存在比较大的数据损耗，支持的数据传输速率不高。这与IT网络所面临的情况完全不同，IT网络的连接速率可达数Gbit/s，它连接的

端点设备往往也都装备了强大的CPU。如果IT网络的性能不足，解决方法也很简单，把它升级成一个更高速的网络就可以了。如果一个VLAN中连接了太多设备，这种设计方案会对网络的性能造成负面影响，只需要再创建一个新的VLAN，然后就可以继续根据需要扩展网络了。然而，这种方法无法解决物联网系统所存在的天然限制条件。物联网需要使用新的连接技术，这类技术可以满足扩展性的需求，突破网络性能的限制。读者可以阅读第5章进一步了解设备与网络的限制。

2.1.4 数据

物联网设备会创建出海量的数据。一般来说，大多数IT机构都不关心网络中的设备产生的那些乱七八糟的“闲言碎语”。但在物联网环境中，数据就是金子，因为数据是企业提供新的物联网服务、提升客户体验、降低运营成本、创作企业商机的载体。虽然物联网生成的大多数数据同样杂乱无章，但人们可以通过分析这些数据所获取到的信息来优化工作流程，设计全新的商业模式。想象这样一种场景：一座智慧城市里安装了几百个智能路灯，所有这些智能路灯都连接到同一个物联网当中。虽然人们对于这个照明网络与控制中心之间传输的大多数信息都不会抱有太多兴趣，但这个数据中心的模式可以帮助人们预测出什么时候应该替换这些路灯，以及这些路灯应该在什么时候打开或者熄灭，以减少运营成本。然而，当所有这些数据都融合在一个网络当中时，人们就会很难高效地管理和分析这些数据。所以，物联网系统不同于IT网络，物联网需要合理分配在这个架构中传输的数据数量，这既包括过滤和减少去往上游的数据，也包括在必要情况下对设备提供极速响应。

2.1.5 支持传统设备

让IT网络支持传统设备有时并不复杂。如果有人的计算机或者操作系统已经过时，升级一下自己的设备就可以了。如果有人使用的手机还在执行一种过时的WiFi标准（比如802.11b或者802.11g），IT人员只需要拒绝这种人接入无线网络，通过这种方式强制进行升级就可

以了。在OT系统中，终端设备可能会在网络中连接相当长的一段时间（有时可能会连接数十年）。随着物联网的部署，物联网需要能够支持网络中当前连接的这些过时设备，同时也能支持那些带有全新功能的设备。在很多情况下，传统设备就是不支持IP协议的。比如，一家工厂可能只需要每20年（甚至更长时间）升级一次设备。它根本不想为了获取更多数据，或者为了更好地控制设备，就斥资数百上千万美元去升级设备。不过，这种传统机器设备可能都会支持一些古老的协议（比如串行接口），并且都会使用RS-232接口连接网络。在这种情况下，物联网必须能够对一些协议进行转换，或者使用网关设备来将传统的端点设备连接到物联网中。第6章会深入介绍传统物联网协议的转换。

2.2 比较物联网的架构

本书之前提到的那些物联网系统提出的挑战与需求已经催生了一整套全新的网络体系结构。在过去很多年中，人们已经设计了大量的标准和框架来解决大规模设计物联网所面临的诸多挑战。

所有这些框架都有一个基本需求，那就是要支持数据、流程以及终端设备执行的功能。其中最著名的两个框架就是由oneM2M和物联网世界论坛（IoTWF）定义的框架，下面我们来对这两个框架进行深入介绍。

2.2.1 oneM2M物联网标准化框架

在将机器对机器（M2M）的通信进行标准化的过程中，欧洲电信标准化研究院（European Telecommunications Standards Institute, ETSI）在2008年创建了M2M技术委员会。建立这个委员会的目的是创建一个通用架构来加速人们采用M2M应用和M2M设备。后来，这个委员会的范围扩展到了物联网领域。

其他相关组织也开始着手创建类似的M2M架构，指定一种通用的M2M标准也显得必不可少。在意识到这种需求之后，2012年，ETSI和另外13家成员机构发起了oneM2M（即同一个M2M）的全球倡议，这个倡议的目的旨在提升M2M通信系统和物联网的效率。oneM2M的目的是创建一个通用的服务层，这一层可以直接嵌入到设备当中，让设备可以与应用服务器之间进行通信。oneM2M的框架主要关注的是物联网的服务、应用和平台，这其中包括智能测量应用、智能电网、智慧城市自动化、电子健康应用和互联汽车。

设计一个物联网架构所面临的最大挑战在于调和设备、软件和接入方式的异构性。oneM2M开发出了一种横向的平台架构，并且由此制定出了让设备能够在物联网堆栈的各个层面上实现互操作的标准。例如，用户可能希望将自己的HVAC系统与办公室中的各个无线温度传感器连接起来，实现HVAC系统的智能温控。用户可以决定部署使用LoRaWAN技术的传感器（在第4章介绍）。这里的问题在于，LoRaWAN网络与HVAC和BMC运行的BACnet系统是两种完全不同的系统，它们之间本身不存在连接点。这时，oneM2M通用服务架构就有用武之地了。oneM2M的横向框架和RESTful API可以让LoRaWAN系统通过一个物联网与楼宇的管理系统实现互操作，这就通过一种统一的方式提升了物联网的通信范围，解决了网络异构性的问题。

图2-1所示为oneM2M定义的物联网架构。

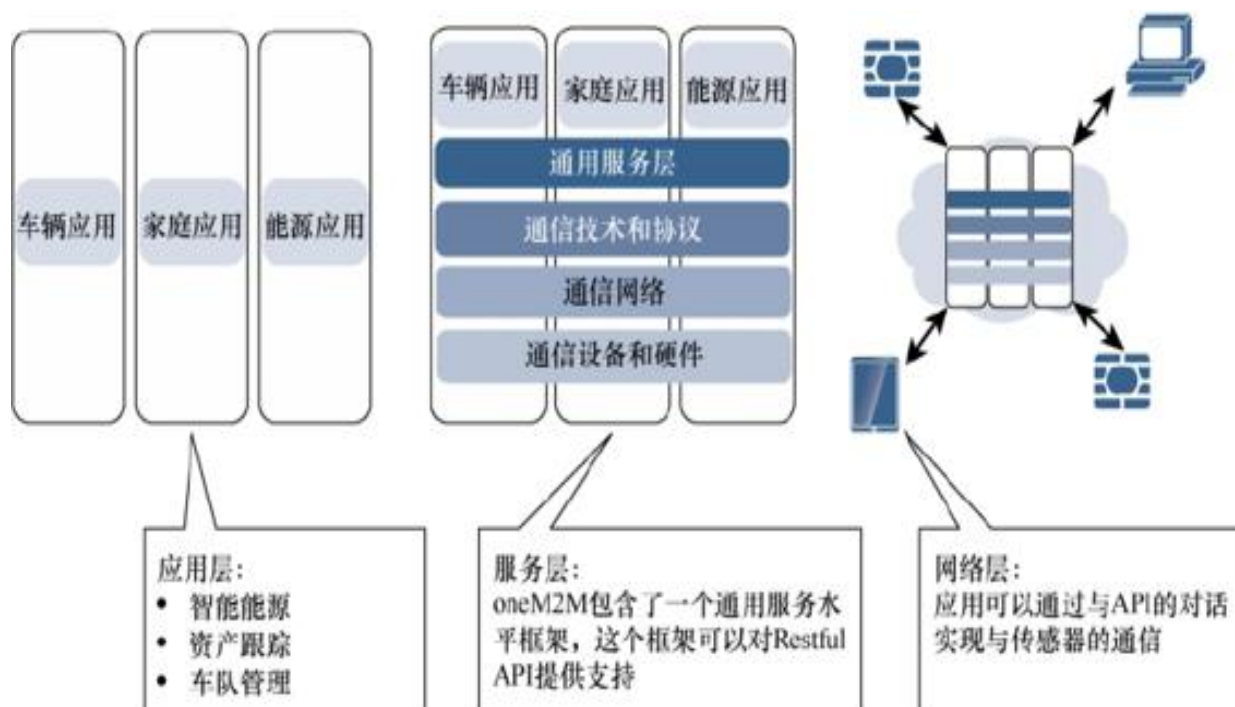


图2-1 oneM2M物联网架构的核心元素

oneM2M架构将物联网功能分为了三大区域：应用层、服务层和网络层。虽然这个架构乍看之下简单而又通俗，但是它的表意十分丰富，而且这个架构可以让不同设备通过对IT友好的API来实现互操作，同时还可以支持大量的物联网技术。下面我们来依次看一看这三层。

■ 应用层：oneM2M架构主要关注的是设备与应用之间的连通。这一层不仅包含了应用层协议，而且尝试对与业务智能（BI）系统互动的北向API的定义进行标准化。应用程序往往是特定于行业的，它们有自己的数据模型集，因此显示为垂直实体。

■ 服务层：这一层是横跨纵向工业应用的横向框架。在这一层中，横向的模块包含了物联网应用所连接的物理网络、底层的管理协议和硬件。服务层的实例包括通过蜂窝网络建立的回程通信、MPLS网络、VPN等。在这些之上的是通用服务层。这一层添加了API和支持第三方服务与应用的中件件。oneM2M的目的之一就是“开发技术标准，让这些技术标准满足嵌入在各类软硬件节点中的通用M2M服务层所提出的需求，并且让本地网络中的设备与位于云或数据中心中的M2M应用服务器建立大量连接。”所以，oneM2M的一项关键目标就是吸引并且主

动争取那些从事M2M相关领域的组织，这里所说的相关领域包括信息技术与智能传输、医疗卫生、电力、工业自动化和智能家庭应用等领域。

■ 网络层：这是物联网设备与端点设备之间的通信层。它包含了设备本身，以及设备所连接的通信网络。这种通信架构具体包括无线连接接口（如IEEE 802.15.4）和无线点到多点系统（如IEEE 801.11ah）。同时，它还包括有限设备连接（如IEEE 1901输电线通信）。第4章会对这些连接技术进行详细介绍。

在很多情况下，智能设备（还有那些不怎么智能的设备）之间会相互通信。在有一些情况下，机器与机器间的通信并不重要，在物联网应用领域中，设备有时只需要通过一个场域网络（Field Area Network, FAN）来使用为这种环境定制的App进行通信。因此，设备的通信域中要包含网关设备，它负责连接设备与核心网络之间的通信，并且充当设备与网络域之间的分界点。

oneM2M发布的技术标准和技术报告涵盖了物联网功能架构和其他方面有关的信息，可通过oneM2M官网进行查询。

2.2.2 物联网世界论坛（IoTWF）标准化框架

2014年，IoTWF架构委员会（由Cisco、IBM、Rockwell和其他机构领导）发布了一个7层物联网架构参考模型。尽管物联网已经有很多参考模型了，但是这个由物联网世界论坛推出的参考模型为人们使用物联网提供了一个更加清晰简洁的视角，这个模型包含了边缘计算、数据存储和访问。它从技术的角度为物联网的虚拟化提供了一个简洁的方式。这7层中的每一层都分为很多具体的功能，安全性贯穿了整个模型的各层。图2-2详细描述了IoTWF发布的物联网参考模型。



图2-2 物联网世界论坛发布的物联网参考模型

如图2-2所示，物联网参考模型定义了一系列的分层，以及如何对从中心（中心可能是云服务或者专用的数据中心网络）到边缘（包括传感器、设备、机器，以及其他类型的智能终端节点）的数据流进行控制。总体来说，数据是从自下而上穿越这个模型各层的，即从边缘一路向北流向中心。通过这个参考模型，我们可以：

- 将物联网面临的问题分为很多个部分；
- 判断出各层需要使用的技术，以及它们之间的相互关系；
- 定义一个系统，让不同厂商可以提供系统中的不同组件；
- 获得一个定义接口的流程，实现异构网络的互操作；
- 定义一个分层的安全模型，应用于参考模型各层之间的过渡点上。

接下来，我们会对物联网参考模型的7层进行更加详细的说明。

1. 第1层：物理设备与控制器层

物联网参考模型的第1层就是物理设备与控制器层。这一层就是物联网中的“物”所在的哪一层，这些“物”包括各类端点设备和那些接收与发送信息的传感器。这些“物”的体积从微型传感器到工厂中的巨型设备不等。它们的主要功能就是收集数据，并且通过网络进行查询和/或控制。

2. 第2层：连接层

物联网参考模型的第2层关注的是连通性。这一层最重要的功能是对数据进行可靠和及时的传输。说得再准确一点，这一层包括在第1层设备与网络之间传输数据，以及在网络和发生在第3层（边缘计算层）的信息处理进程之间传输。

读者也许已经注意到，连接层中包含了所有物联网中的网络连接元素，它并没有真正地区分“最后一公里”网络（即传感器/端点与物联网网关之间的网络，本章稍后会进行讨论）、网关和回程网。连接层的功能如图2-3所示。



图2-3 物联网参考模型中连接层的功能

3. 第3层：边缘计算层

边缘计算是第3层的功能。边缘计算往往被称为“雾”层。关于这一层，我们会在2.5.1节详细介绍。这一层强调的是减少数据量，并且将数据转换为有利于存储和有利于上层进行处理的格式。这个参考模型的一大基本原则在于，针对信息的处理应该尽可能早，尽可能接近网络的边缘。图2-4展示了由物联网参考模型第3层进行处理的功能。

第3层还有另一项重要的功能，那就是对数据进行分析，判断是不是要对其进行过滤，或者在发送给上层之前进行汇总。通过在这一层对数据的格式重新进行设置，同时对数据进行解码，其他系统在处理数据时就会变得更加轻松。因此，第3层的一大核心功能就是对数据进行评估，判断数据是否超出了预定义的门限值，是否需要针对这些数据采取某些行动或者发出某种告警。

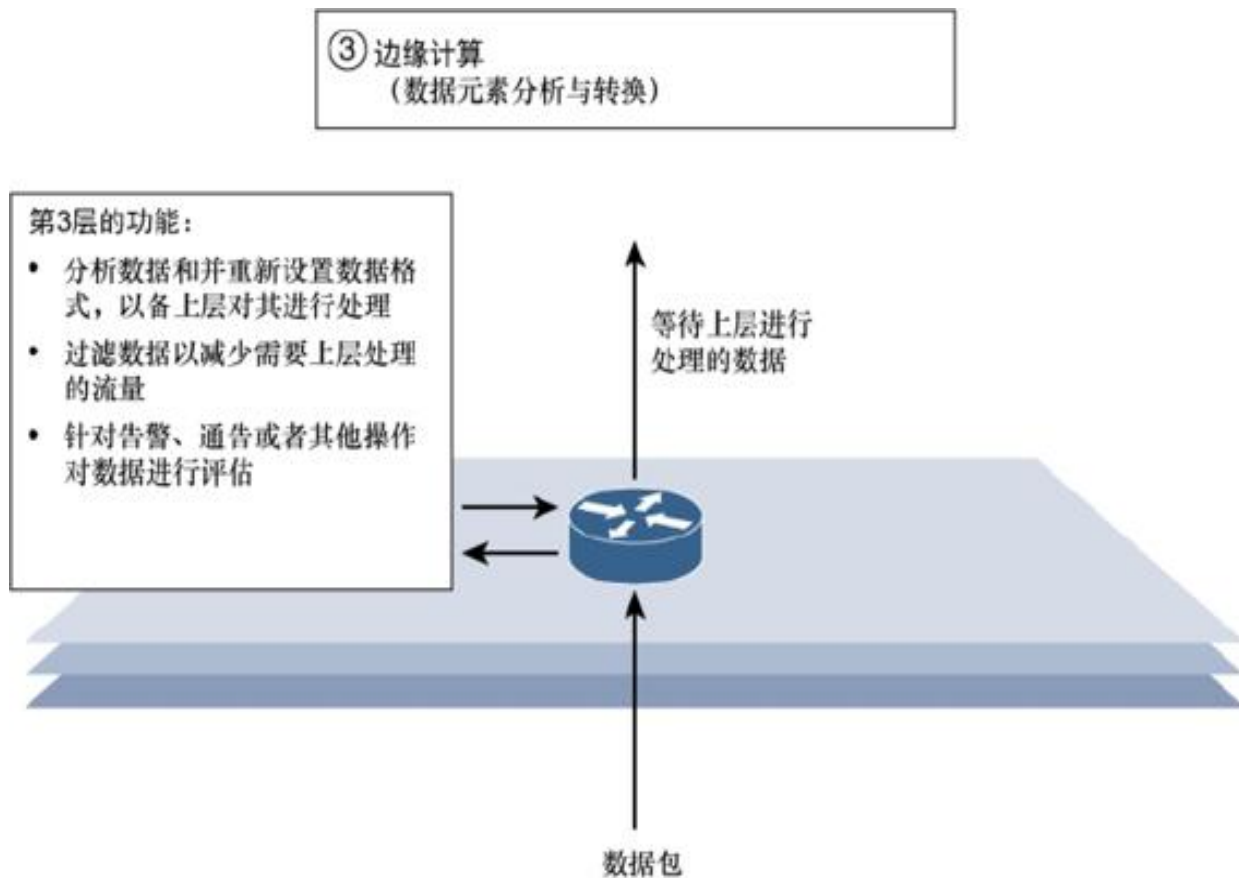


图2-4 物联网参考模型第3层的功能

4. 上层：第4~7层

上层负责处理那些由底层生成的物联网数据。为求完整，表 2-2 对物联网参考模型第4~7层的功能进行了总结。

表2-2 IoTWF参考模型第4~7层功能的总结

物联网参考模型各层	功能
第4层：数据汇集层	收集数据并且对数据进行存储，以备应用在必要时使用这些数据。将描述事件的数据转化为基于查询的信息
第5层：数据抽象层	调和各类不同的数据格式，确保各种不同的源所提供的数据能够使用相同的方式表意。确保数据集是完整的，将数据统一存储在相同位置，或者通过虚拟化技术将数据存储在不同空间中
第6层：应用层	使用软件应用来读取数据。这些应用可能会对数据进行监测、控制，或者基于对数据的分析结果来提供报告
第7层：协作与进程层	使用和共享应用信息。物联网信息的协作与通信往往分为很多个步骤，这也是物联网之所以如此重要的原因。这一层可以改变商业流程，落实物联网带来的优势

5. IT与OT在物联网参考模型中的职责

将物联网架构按照这种方式进行虚拟化可以得到一个有趣的结果，那就是人们可以开始沿着IT和OT两条线来分别组织它们的职责。图2-5显示了在物联网参考模型框架中，IT和OT之间的分界点。



图2-5 物联网参考模型中IT与OT的分隔

如图2-5所示，物联网系统需要穿越很多位于功能层之上的边界。这个协议栈最底部往往是OT的领域。对于诸如油气这样的行业，最底层中会包含与输油管、钻井平台、炼油设备相连的那些传感器和设备。这个协议栈的最上层是IT领域，其中包含了诸如服务器、数据库和应用这些组成成分，所有这些组件都运行在一个由IT控制的网络中。在过去，OT和IT相互之间往往十分独立，彼此之间并没有什么数据需要通信。物联网则正在改变这种情况。

在底层，也就是OT的分层中，设备会以各自的速率创建实时数据。有时，它们每天都会生成海量的数据。这不仅会导致物联网需要传输大量数据，而且，如此之多的数据也意味着上层应用必须能够按照要求的速率来处理规模如此庞大的数据。为了满足这种需求，物联网协议栈中必须有某些位置可以缓冲或者存储这些数据。按照协议栈的方式将管理数据的功能分配到协议栈的各层中，就可以让上4层的应用按照它们自己的速率来处理数据了。

因此，靠近边缘的那些实时“动态数据”必须进行汇总和存储，让它们成为“静止数据”，以便IT层中的应用来处理它们。IT和OT组

织需要共同完成整个的数据管理工作。

2.2.3 其他的物联网参考模型

除了本章前文中介绍的两个物联网参考模型之外，还有一些其他的参考模型。这些模型是由不同的组织机构提出的，它们往往是针对某些特定领域或者物联网应用量身定制的。表2-3对这些物联网参考模型进行了着重介绍。

表2-3 其他物联网参考模型

物联网参考模型	描述
普度模型的控制分层结构	普度模型的控制分层结构是一个通用的、很容易理解的模型，它将设备分为了不同的层级和功能。ISA-95 以这个模型作为控制分层结构的基础和 IEC-62443（之前的 ISA-99）网络安全标准。这个模型是各行各业诸多物联网相关模型和标准的基础。普度模型的物联网应用会在第 9 章和第 10 章详细介绍

续表

物联网参考模型	描述
工业互联网联盟（IIC）提出的工业互联网参考架构（IIRA）	IIRA 是一个针对工业互联网系统（IIS）提出的基于标准的开放架构。为了实现价值的最大化，IIRA 具有广阔的行业适应性，可以驱动设备之间实现互操作，移植可应用技术，促进技术与标准的发展创新。这个架构的描述信息比较笼统，通过高度抽象的描述，可以支持必要的行业功能。IIRA 对当时很容易理解的用例进行了提炼和抽象，从中总结出了以下列的特征、特性和模式。这些用例中绝大多数都是 IIC 中定义的用例
物联网架构（IoT-A）	IoT-A 创建了一个物联网架构的参考模型，定义了一系列初始的重要模块，这些模块是促进新兴物联网发展的基石。IoT-A 使用一个实验环境，并通过模拟的方式按自顶向下的顺序对物联网架构的设计原则和指导方针进行了理论演绎。同时，IoT-A 还为了探索选择不同架构设计方案所得到的结果，而将这个实验环境的原形创建了出来

2.3 简化的物联网架构

虽然本章之前提到的几种模型彼此之间存在着巨大的差异，但它们都用不同的方式对物联网进行了分层，也都在某种程度上将技术和标准的开发工作限制在某一层或某一个领域。这些模型的共同之处在于，它们都认识到了物联网端点设备与数据传输网络之间需要进行互联，而这类网络中传输的数据最终会被各种不同的应用所使用——无论这些应用位于数据中心、云，还是位于协议栈的各个管理端点当中。

本书并不打算为其中任何一种物联网架构背书。实际上，由于不同行业使用物联网的方式不同，部署的协议各异，它们采用的物联网架构也应该有所区分，而上文中的每种架构都在解决物联网异构性的问题上存在着自己的优势。所以，本书只介绍那些大多数物联网系统都会使用的基本构造模块，其目的在于帮助读者理解物联网的设计方案。这个框架包含了两个相互平行的协议栈：物联网数据管理和计算协议栈、核心物联网功能协议栈。虽然这个框架将物联网的结构分为了2个三层的协议栈，但这绝不表示这个模型缺少开发复杂物联网战略所必要的技术细节。我们这样做的目的在于将物联网框架简化为最基本的构造模块，然后再以这个简化的框架为基础，解释各行各业物联网用例中的那些核心设计原则和部署原则。在这个框架中，包含了更加复杂模型的所有分层，我们只是为了便于读者理解，而将那些分层按照功能模块进行了组合。图2-6所示为本书要进行介绍的简化版物联网模型。

几乎所有机构发布的物联网模型中都包括了核心层，它们的核心层与图2-6左侧的协议栈类似。核心层中包括互联之“物”、通信网络和应用。不过，图2-6所示的框架与那些模型的不同之处在于，这个框架将核心物联网和数据管理分成了两个相互平行的协议栈，让读者能够更加清晰地看出物联网这个复杂系统中，各层网络和应用所对应的功能。这种分隔可以让读者更加清晰地看懂各层的功能。

将核心物联网功能堆栈分为三层的目的在于将物联网架构简化为最基本的构造模块。当然，这个简单的架构需要进行扩展。物联网架构的网络通信层包含了大量的详细内容和海量的技术。试想，物联网中会有多少迥异的物联网传感器，以各自不同的方式连接进来。网络通信层需要将这些元素全部统一起来，为它们提供网关和回程技术，并且最终将它们生成的数据发送给中心站点以备分析和处理。

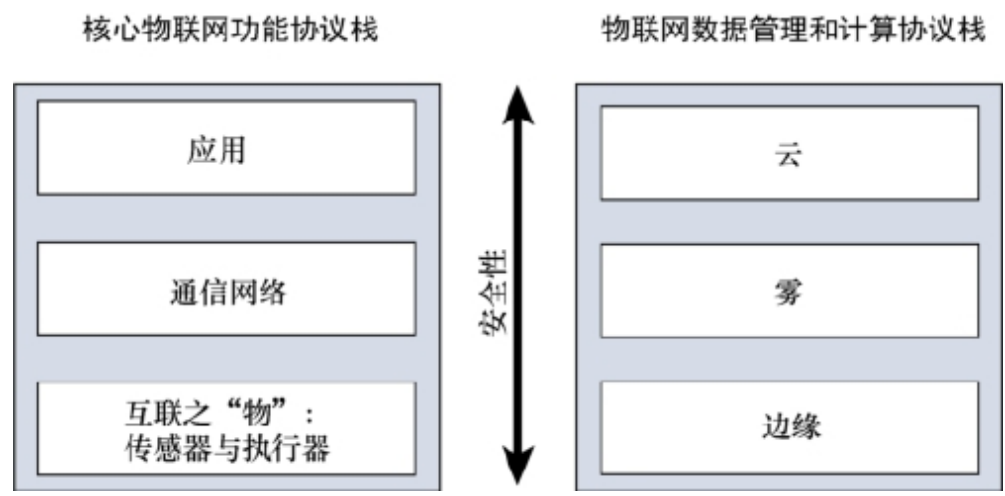


图2-6 简化的物联网架构

物联网中使用的很多“最后一公里”技术都是为了满足端点设备的这类连接需求，这些技术在IT领域中都不常见。不过，在网关和数据中心之间的网络中包含的多为传统技术，也就是IT专业人士耳熟能详的那些技术，包括隧道技术、VPN技术、基于IP的服务质量（QoS）技术、传统三层路由协议（如BGP和IP-PIM）和诸如加密、ACL（访问控制列表）、防火墙这类的安全功能。

与大多数IT网络不同，物联网的应用和分析层未必只存在于数据中心或者云中。由于物联网所面临的特殊挑战和需求，应用和数据管理往往都需要分布在整个架构的各层当中，让物联网系统能够在多点采集数据、分析数据，并且执行智能控制。在本书的模型中，数据管理是与核心物联网功能协议栈的三层相平行的另一个协议栈。数据管理协议栈的三层为边缘层（即传感器自身的数据管理）、雾层（即在网关和传输网络中的数据管理）和云层（即云或中心站点数据中心的

数据管理）。物联网数据管理和计算协议栈会在本章稍后进行详细的介绍。图2-7所示为本书介绍的物联网架构扩展后的视图。

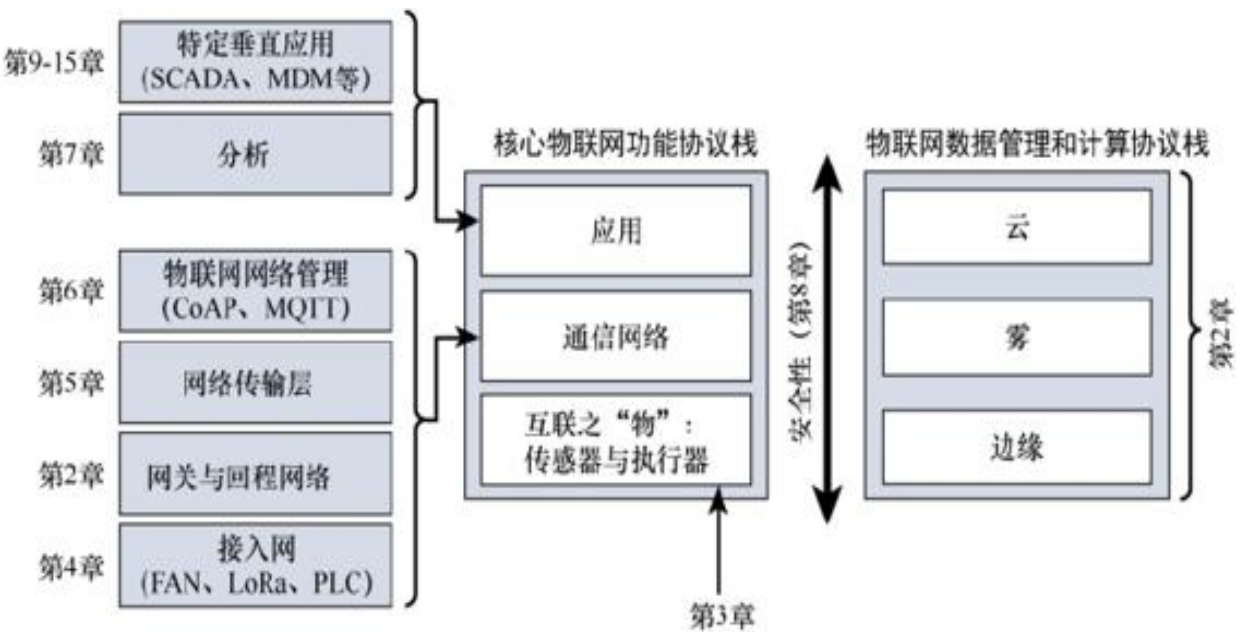


图2-7 简化的物联网架构扩展后的视图

如图2-7所示，核心物联网功能协议栈可以扩展出很多子层，这些子层中包含了更加详细和具体的网络功能。比如，通信层可以分为4个子层：接入网、网关与回程网络、IP传输，以及操作与管理子层。

物联网的应用与传统企业网的应用之间存在着不小的差异。物联网的应用层不仅使用业务应用，也包含大数据分析的部分，因为物联网不仅控制物联网设备，同时也包括对这些设备所产生的数据进行分析，并从中得到重要的知识，这个概念会贯穿本书全篇。所以，应用层往往既包括分析组件，也包含特定行业的物联网控制系统组件。

读者会发现整个架构的中心是安全性，无论从网络连接的角度来看还是从数据管理的角度来看都是如此。本书第2部分会讨论每一层中的安全性问题。第8章还会专门讨论保护物联网系统的话题。第3部分会介绍如何将第1部分和第2部分的内容应用到各个行业中。第3部分中的每一章会对分别探讨一个特定行业中的物联网安全问题。

图2-7所示的框架反映了整本书的脉络。为了帮助读者厘清本书的叙事逻辑，我们在协议栈中的每一层边上都标记了本书会在哪一章对这一层展开介绍。

本章的剩余部分会对这个模型中的每一层进行概括性的介绍，为读者深入学习第2部分中各章所包含的各个技术打下基础。本章的后文还可以帮助读者理解这些技术将如何应用到第3部分所要介绍的各行各业当中。

2.4 核心物联网功能协议栈

物联网是围绕着那些能够执行某些功能，并且提供互联服务的“物”或者智能对象来展开的。这些对象之所以是“智能的”，是因为它们可以通过一系列背景信息和人们配置的目标来执行相应的操作。这些操作可以是由它们独立完成的（也就是说智能对象不需要依靠外部系统来完成这些操作）。然而，在大多数情况下，“物”都需要与外部系统进行互动，来保护智能对象收集到的信息，与其他智能对象交互信息，或者与管理平台之间进行交互。在这些情况下，人们可以使用管理平台来处理那些从智能对象那里收集到的信息，并且使用管理平台来指导这些智能对象的操作。从架构的角度来看，物联网要想正常工作，需要很多组件共同协作。

■ 互联之“物”层：在这一层中，物理设备需要部署在某个环境中，并且能够提供所需的信息。这些设备需要克服环境的限制。

■ 通信网络层：当智能对象不能独立完成工作时，它们就需要与外部系统之间进行通信。在很多情况下，这些通信都是使用无线技术来完成的。这一层包括4个子层：

■ 接入网络子层：物联网的“最后一公里”就是接入网。接入网往往是由诸如802.11ad、802.15.4g和LoRa这类无线技术构成的。连接到这些接入网中的传感器也有可能是通过有线方式连接的。

■ **网关与回程网络子层：**一个常见的通信系统中会在一个区域中包含大量的智能对象，这些对象都围绕一台网关设备。网络设备直接与智能对象进行通信。网关设备的作用是将收集到的信息通过某种范围更广的介质（称为回程）转发给头端工作站，这些信息就是在这些前端工作站中进行处理的。这些信息交换是第7层（即应用层）的功能，这也就是为何这类对象称为网关。在IP网络中，网关同样负责将数据包从一个IP网络转发到另一个IP网络，因此它充当的就是路由器的角色。

■ **网络传输子层：**要想成功建立通信，人们必须通过实施网络层协议和传输层协议（如IP和UDP）来支持大量设备建立连接，同时对它们使用的媒介提供支持。

■ **物联网管理子层：**网络中还必须有其他协议来支持前端应用与传感器之间交互数据，这些应用包括CoAP和MQTT。

■ **应用层与分析层：**在上层，应用需要处理收集到的数据，它们不止需要在必要时控制智能对象，还要根据收集到的信息来做出智能决策，并且指导“物”或其他系统来适应分析出的情况，并且修改它们的行为或者参数。

下文会对上面提到的元素进行分析，以帮助读者构建自己的物联网。

2.4.1 第1层：互联之“物”层

大多数物联网都始于那些需要连接的对象或“物”。第3章会深入介绍关于智能对象的内容。从架构的角度来看，正是各类智能对象大异其趣的类型、形状和需求，催生了大量的物联网协议和架构。对智能对象进行分类的方式不胜枚举。下面是架构化的分类方法。

■ **电池电源或连接中取电：**这种分类方式根据对象是自带电源，还是通过外部电源不间断供电来进行判断。电池供电的智能物比通过

电线供电的对象移动起来更加方便。但电池供电限制了设备每次可以使用的时长，以及对象可以消耗的总能源，因此这类对象的传输范围和移动频率也会受到限制。

■ **移动还是静态：**这种分类方式是根据“物”是移动的还是长期处于同一位置来进行判断的。传感器可能是移动的，因为它会从一个对象移动到另一个对象（例如，黏度传感器就需要在化工厂中从一堆化学原料移动到另一堆化学原料），或者因为传感器本身是附着在一个移动物上的（比如那些安装在仓库或者工厂车间货物上的位置传感器）。“物”的移动频率也各不相同（从偶尔移动到始终在移动）。移动的范围（是几厘米还是几公里）往往可以决定这个“物”的供电方式。

■ **报告频率是低是高：**这种分类方式是根据对象报告被监测参数的频率来判断的。一个锈蚀传感器可能每个月才会报告一次数值，而移动传感器则可能会每秒报告数百次速度参数。高频传感器消耗的能量也更高，这也会限制它们的供电方式（因此也会限制这类对象的移动性）和传输范围。

■ **数据是简单还是丰富：**这种分类方式是根据每次报告时，传感器提供的数据量是大是小来判断的。某个环境中的湿度传感器每次只需要（使用二进制）报告一个（范围在0~255的）当日指数，而一个引擎传感器则可能需要报告上百个参数，从温度到压力、气流速度、压缩速度、碳指数等。数据量越大，消耗的能量也越高。这种分类方式往往需要和前面的分类方式相结合，判断对象的数据吞吐量（是低吞吐量还是高吞吐量）。读者应该记住一点，即吞吐量是一个复合参数。中等吞吐量的对象既有可能是那种以较高频率发送简单数据的对象（此时数据流的结构看上去是连续的），也有可能是那种以较低频率发送复杂数据的对象（此时数据流的结构看上去则是断续的）。

■ **报告范围：**这种分类方式是根据网关的距离来判断的。比如，健康手环与手机的通信过程中，健康手环最多距离手机也只有几米的距离。我们在这里假设用户的手机需要在视线范围之内，以便查看屏幕上的报告数据。如果手机距离很远，说明用户没有在使用手机，那

么手环报告给手机的那些数据也就没有什么价值了。然而，沥青路上安装的湿度传感器可能需要与数百米甚至数公里之外的人进行通信。

■ 每单元的对象密度：这种分类方式是根据给定区域内连接在相同网关上的智能对象数量来进行判断的（往往是拥有相同通信需求的智能对象数量）。一条石油管线可能需要每几公里才在重要位置上安装一个传感器。但是像惠普天文台的SETI巨型望远镜这样的天文望远镜可能需要在很小的一片区域中安装成百上千个镜片，其中每个镜片上都带有多个陀螺仪、重力传感器和震动传感器。

从网络架构的角度来看，人们首先应该判断出应该使用哪些技术来实现智能对象之间的通信。判断的结果取决于智能“物”属于哪一类。不过，有些领域（如制造业和电力行业）可能会包含很多类的智能“物”，每一种智能“物”所匹配的需求也各不相同。图2-8显示了一些同时匹配不同移动性和吞吐量需求的应用。

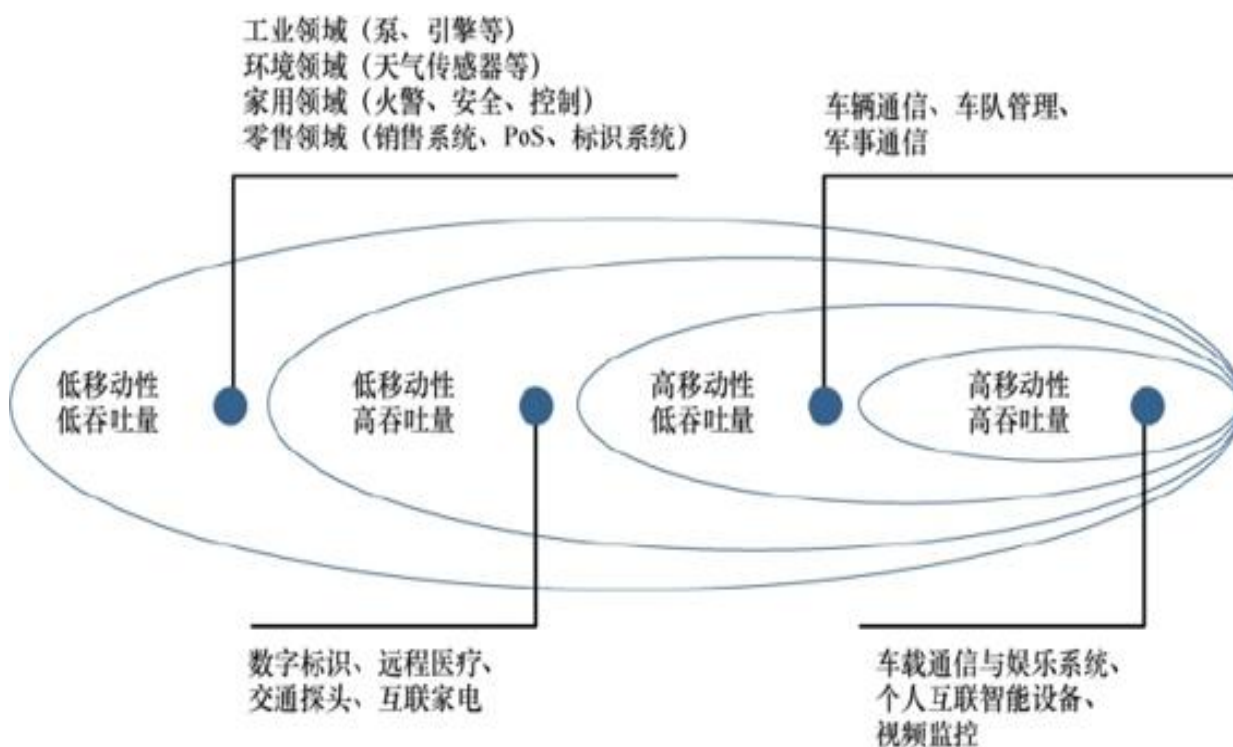


图2-8 根据移动性和吞吐量进行分类的传感器应用示例

上述这些（用来分类智能“物”的）类别会对其他参数造成影响，也可以相互影响。比如，电池供电的移动对象（比如心率监测仪）往往尺寸比较小，而小型传感器很容易移动或者集成到它所在的环境当中。同时，小型高移动性智能对象不太可能需要使用大型天线，也不可能需要大量供电。这些限制条件又会限制它们的数据传输范围，因此也会对它们支持的网络协议提出限制。数据的重要性可能也会影响到传感器的尺寸和架构。比如，沥青路上的湿度传感器有一个月没有发送报告，这导致的结果可能只是系统上亮起了更换传感器（或者传感器电池）的提示灯。一个多镜陀螺仪超过100ms没有传输报告，则可能导致整个系统无法稳定工作，或者根本无法工作。这些传感器或者需要连续供电（导致移动性受限），或者需要比较容易更换电池（导致传输距离受限）。而设计物联网的第一步，就是判断移动性和数据传输（包括有多少数据、传输频率是多久一次）的需求。

2.4.2 第2层：通信网络层

在了解了智能对象的尺寸与它的数据传输功能（包括传输范围、数据量和频率、传感器密度与移动性）有关这一点之后，我们就可以准备将智能对象连接起来建立通信了。

物联网环境中使用的计算资源和网络资源与IT环境中的资源截然不同。显然，没人会忽略IT和OT所使用的设备存在巨大的体积差异这一点，而导致这种差异的原因是这些设备所部署的环境。还有一种差异没有体积差异那么明显，那就是这两类设备在操作方式上的差异。读者必须理解它们在操作方式的差异，才能正确地处理和保护这些设备资源。

温度差异很容易理解。造成这种差异的原因包括外部天气因素和内部操作环境因素。远程的外部站点范围很广，那些采矿或者管线设备，有些需要忍受阿拉伯半岛的炙热，有些则需要面临阿拉斯加北坡的严寒。炼钢炉边上的控制设备显然需要具备强大的耐热性，而食物冷藏环境中的设备则刚好相反。在有些情况下，控制设备必须经历极端环境的巨大波动。采用相同部署方式的设备可能会经历迥然不同的

极端环境。比如，一部分加州德哈查比（Tehachapi）的风力发电场位于莫哈韦沙漠（Mojave Desert）中，另一部分则建造在海拔1800米的崇山之中。可以想见，这个巨大的温度差异势必要求其中的一部分硬件能够承受这类极端环境的考验。

湿度的波动也可能会给一个系统的长期稳定工作带来影响。位于尼日尔河三角洲地带的钻井头需要经历的环境与阿拉伯沙漠中部的钻井头势必截然不同。在有些条件下，系统甚至可能需要直接与液体接触，就像那些户外无线设备或者部署在海底的设备一样。

还有一种差异来自于力和运动所造成的极端条件，虽然这种极端条件看上去并不那么明显。根据部署环境的不同，人们对于设备承受震动的需求也有差异。有时，人们关注的是设备能否承受低振幅的连续震动（比如服装制造厂中的流水线设备）。有时，人们关注的则是设备是否能够承受突如其来的增压或减压，这就像是人们会在地震中经历的峰值地面加速度这样的震动——高速铁路或者重载运土设备上的移动系统就需要能够承受这样的震动。

固体颗粒也有可能对设备造成影响。大多数IT环境都要处理严重积尘的问题，这个问题是由IT设备冷却风扇造成的。在缺乏有效控制的IT环境中，灰尘大量聚集会导致严重的问题。对付这些灰尘的有效手段是使用无风扇的冷却系统，这类系统会增加散热的表面积，用散热片散热的方法也是这样。

在有些场所，设备可能会遭到腐蚀，而腐蚀性材料会给电力或通信线路的连接造成不良影响。此外，这些材料可能会附着在散热表面上，从而降低设备的散热效率。

在有些环境中，人们关心的并不是环境有可能会给设备造成什么样的影响，而是设备会对环境造成什么破坏。比如，在存在挥发性气体的场所，设计标准中一定包含了设备必须抑制火花这项要求。

IT和OT设备之间还有另一种差异，这种差异和（采取不同安装方式或执行不同工业功能的）设备的外部连接方式有关。在OT和IT环境

中，设备的安装环境完全不同。诚然，有些工业环境中也具备机架安装环境，但这类环境还是多存在于IT部署环境之中。在工业环境下，大多数计算和通信设备都位于在一个封闭空间（比如一个控制间）中，它们需要在这个空间中被垂直安装在一个DIN（德国标准化研究所）导轨内。另有一些环境则需要将设备水平安装在一面墙上。

工业计算系统与大多数IT系统不同，它们往往需要通过一个报警信道来与外部相互传输状态信息，或者接收输入信息。指示灯可能会从远处显示处理设备的状态，而这个设备也可能会接收输入信息，并且在系统内部执行某些操作。

OT系统中的供电与标准IT设备的供电之间同样存在一定的差别。工业计算设备的功率变化往往更大。在很多环境中，这些设备使用的都是直流电源。很多工业系统十分重要，因此这些设备往往自身配备有冗余电源。这些设备通常都不使用外来的电源（尤其是那些非设备原装的电源），因为外来电源很可能会被人不小心拔出。在一些电力环境中，系统必须能够在短时间断电的情况下继续工作。

1. 接入网子层

人们所选择的物联网技术与这种技术支持的拓扑类型之间存在着直接的关系。每种技术都天然支持一些用例（例如可以连接哪些组件、连接在哪里、传输多少数据、传输数据的间隔时间是多长、传输距离有多远）。这些用例决定了这个物联网中的设备最适合工作在哪些频段、哪种数据帧结构与这种数据包的模式（数据包大小和通信的间隔时间）最为匹配，以及这种用例中最典型的拓扑是什么。

物联网仍然在以惊人的速度发展，读者在未来可能会遇到大量应用和特殊的物联网用例。但无论哪种应用和用例都需要使用一种接入技术来连接设备。物联网常常会借用那些现成的接入技术，而被借技术的特征则或多或少与物联网在该用例中的需求存在共通之处。固然有些接入技术是专为物联网的用例而设计的，但大多数接入技术都不是这样。

判断使用哪种接入技术的一大重要参数是智能对象和信息采集设备的范围。图2-9列出了读者在物联网环境中有可能遇到的一部分接入技术，以及它们的预期数据传输距离。

可以看出，图2-9中的区域表示的是一种包含关系。比如，蜂窝网络旨在实现5公里范围之外的传输，但是蜂窝网的传输也可以在更短的距离之内实现（如100米）。相对而言，ZigBee旨在实现数十米范围之内的高效传输，那我们就不能指望用ZigBee来实现10公里范围的传输。

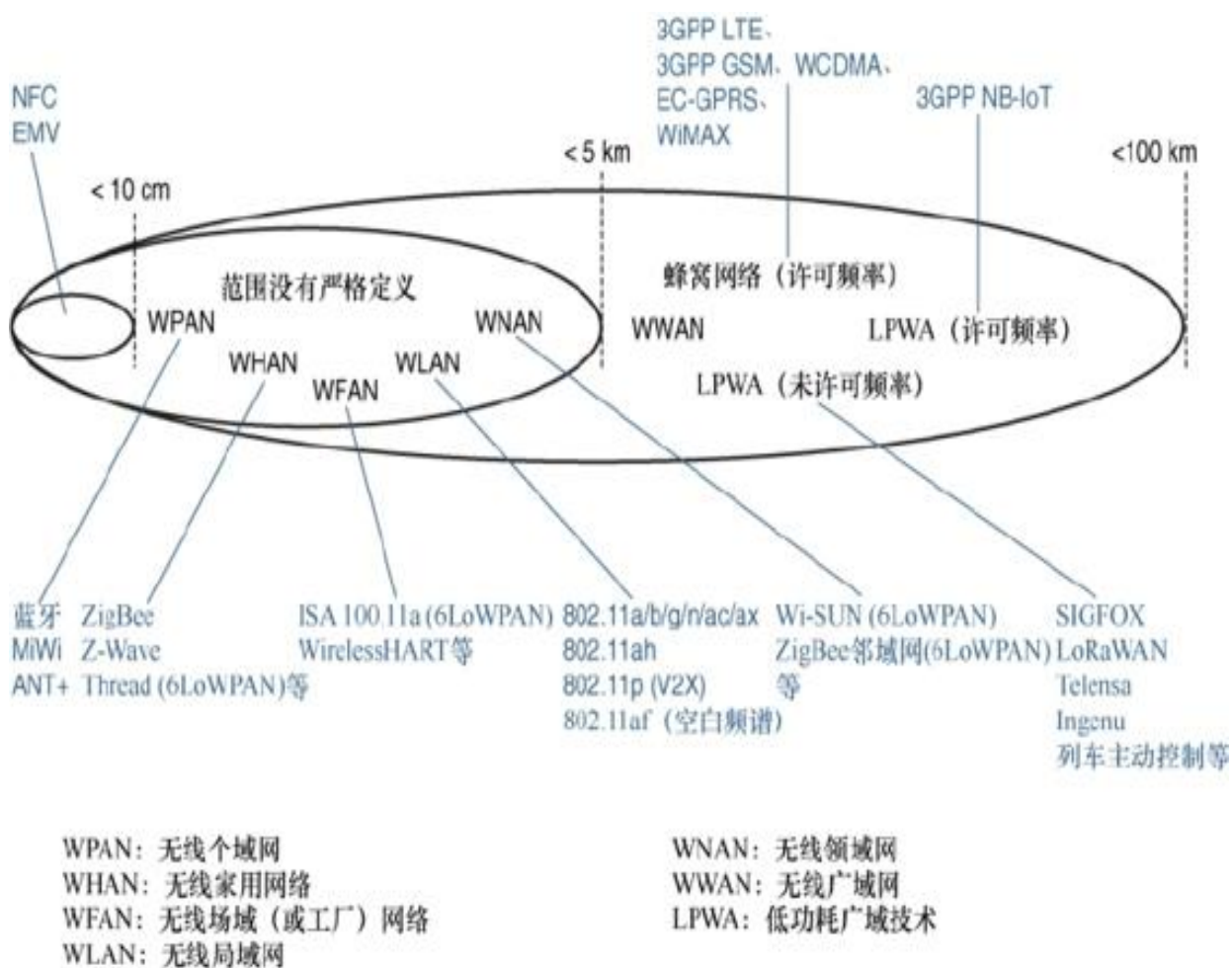


图2-9 接入技术与距离

根据不同技术预计的传输范围，我们可以用不同的名称来对这些技术进行归类，这些名称可以说明在这个范围内收集数据的环境以及垂直位置。常见的分组方式如下所示。

■ PAN（个域网）：范围仅数米。这是围绕着一个人身边的个人空间。这个范围的常见无线技术为蓝牙。

■ HAN（家用网络）：范围为数十米。在这个范围内，常见的物联网无线技术包括ZigBee和低功耗蓝牙（BLE）。

■ NAN（领域网）：范围为几百米。NAN往往用来在几座楼宇之间收集数据。

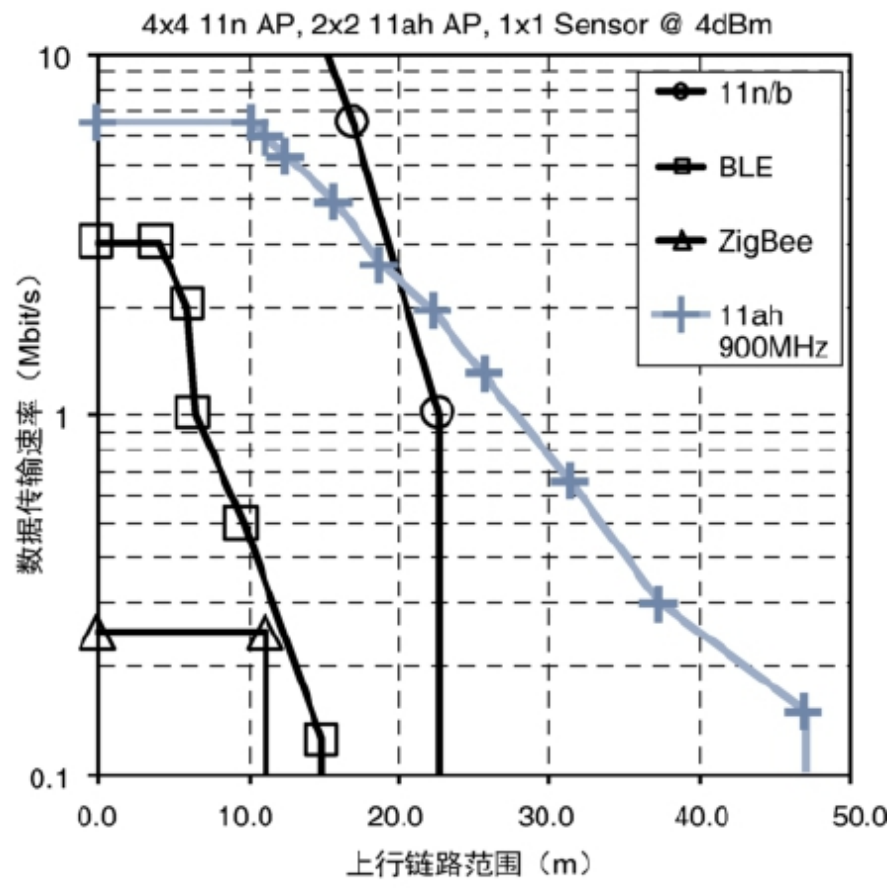
■ FAN（场域网）：范围从几十米到几百米不等。FAN一般指大于几栋楼宇的户外区域。FNA往往可以视为是一个“开放区域”（因此属于非安全区域，而且也不受控制）。FAN时常可以视为是一组HAN，或者一组更小的户外区域单元。在交流当中，FAN和NAN有时可以替换使用。在大多数情况下，垂直环境就足以清晰地判断这个网络属于哪种分类了。

■ LAN（局域网）：范围最大为100米。这个概念在网络领域相当常见。因此当我们在IoT中使用标准网络技术（如以太网或者IEEE 802.11）的时候，这个概念也十分常用。其他网络分类技术（如MAN[城域网，范围为数公里]和WAN[广域网，超过数公里范围的网络]）也在IoT环境中十分常用。

读者应该注意，在IoT网络中，对于所有这些区域都可以加上一个字母前缀“W”来表示在这个空间中使用的是无线网络连接。例如，HomePlug是一种HAN环境中的有限网络技术，但是如果在这个范围内使用的是无线技术（如ZigBee），则我们一般用WHAN（无线家用网络）来表示HAN。

距离相似并不代表使用的协议和技术特征相近。每项协议都会在特定频率（或带宽）上使用一个特定数据帧结构和传输方式。由于不同技术的特征各不相同，因此它们之间也会存在很多差异。比如，图2-10中展示了范围在WHAN到WLAN之间的4项技术，并且比较了这些技术各个应用环境中的吞吐量和范围。图2-10假设传感器使用了相同的数据帧大小、传输功率和天线增益。随着距离的增加，不同技术吞吐

量降低的斜率存在巨大差异。当传感器与接收器之间的距离增加时，这种差异限制了每种技术可以实现的数据吞吐量。



模拟环境：1%PER，4dB NF，32字节，D-NLOS衰减，室内到室外PL模型。900MHz具有12dB的传播增益。

传感器天线增益：11ah (-6.5dB) 和11n (-4dB) 。AP天线增益=2dB。

*BT远程增加125kbit/s和500kbit/s模式

图2-10 4种从WHAN到WLAN技术的范围与吞吐量对应关系

增加吞吐量和可达距离往往会增加能耗。因此，在判断了物联网设备的需求（即移动性和数据传输需求）之后，下一步是根据传输距离和吞吐量来判断该设备在一个数据收集单元中部署的目标数量。直接选择范围最长、吞吐量最高的技术固然很有吸引力，但技术的成本也是一个应该考量的因素。图2-11包含了常见物联网接入技术的成本、覆盖范围、能耗和标准的可用带宽。

在指定时间范围内携带的数据量，以及相关的能耗（这些因素会影响该技术的移动性和范围）决定了无线单元的大小和结构。



图2-11 各类常见的“最后一公里”技术在范围、成本、能耗和带宽方面的对比

传输距离类似并不带表拓扑结构类似。有些技术可以提供更加灵活的连接结构，以便增加通信的可能性。

■ 点到点拓扑：这类拓扑可以让一个节点与另一个节点之间实现通信。这种拓扑的结构最为严格，所以在IoT连接中并不常用，因为这种拓扑结构表示一个物联网设备只能与一台网关进行通信。不过，有很多技术会因为物联网设备要与网关单独建立会话，而被人们称为“点到点”技术。在这种情况下，“点到点”这个概念往往是指通信结构而不是物理拓扑的结构。

■ 点到多点拓扑：这类拓扑支持一个节点与多个不同的节点进行通信。一个或者多个网关需要与大量物联网设备进行通信的大多数IoT技术都属于这一类。不过，根据各个通信节点支持的不同特性，也有很多子类需要考虑。IoT网络的一种特性在于有些节点（如传感器）同时支持数据收集和转发功能，而另一些节点（如某些网关）则会收集

智能设备的数据，让传感器执行某些操作，并且连接其他网络或者网关。因此，有些技术会依照设备执行的（协议）功能来对节点进行分类。

根据功能来分类技术的例子是IEEE 802.15.4，这项技术会在第4章进行深入介绍。虽然本节仅以802.15.4为例，但是同样的原则也适用于很多其他的技术。使用IEEE 802.15.4的技术往往会依赖终端设备（传感器）收集数据和将数据传输给收集方的这个概念。传感器需要体积小，而且一般需要有比较强的移动性。在移动的时候，这些传感器一般就需要使用电池来维持运作。

要想建立一个网络，设备就需要与另一台设备之间建立连接。当两台设备都完全实现了协议栈功能时，它们就可以建立起一个对等体到对等体的网络。不过，在很多环境中，都是由其中一台设备来从另一台设备那里收集数据。例如，在一栋楼中，温度传感器可能会部署在这栋楼的每个房间当中，或者房子的每个区域当中，它们可以与中央节点进行通信，并且由中央节点将温度显示出来，同时控制这栋楼的温度。一个房间中的传感器并不需要与另一个房间中的传感器进行通信。在这种环境中，控制点会部署在房间的中央。这就会构成一个星型拓扑，中央节点处于这个拓扑的中心（hub），其他传感器则充当拓扑的分支（spoke）。

在这样的环境当中，中央节点可以负责整个网络的协调工作，负责向各个传感器传输信号，并且与它们建立连接。在IEEE 802.15.4标准中，中央节点称为整个网络的协调器（coordinator）。在这类部署环境中，每个传感器都只会与协调器之间建立主/从式的通信关系。传感器可以只具有协议栈中的一部分特定的功能（与协调器进行通信）。这类设备称为简化功能设备（RFD，Reduced-Function Device）。RFD不能充当协调器，也不能直接与另一台RFD进行通信。

能够实现完整网络功能的协调器则称为完整功能设备（FFD，Full-Function Device）。FFD可以与另一台或者多台FFD直接进行通信，建立多条对等体到对等体的连接。当每个FFD都有一条去往另一个FFD的专门路径时，这类拓扑称为集群树拓扑。集群树中的FFD可能会

连接RFD，这样就会形成一个集群星型拓扑。图2-12所示为这种类型的拓扑。

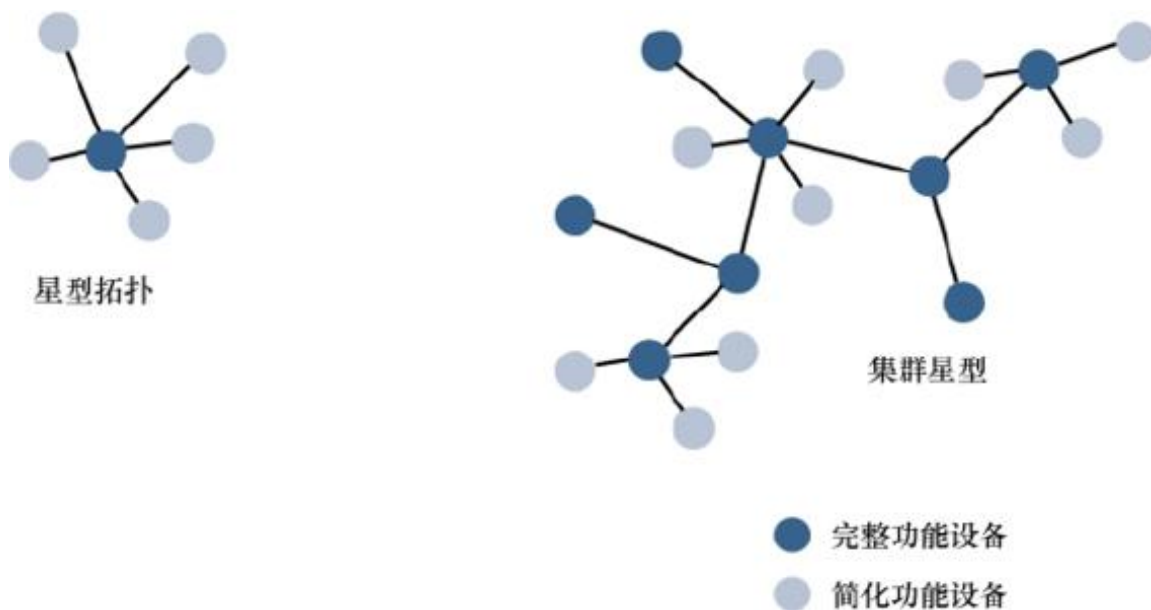


图2-12 星型与集群星型拓扑

其他点到多点拓扑都支持一个节点拥有多条去往另一个节点的路径，这样建立起来的拓扑是互联拓扑。这种冗余性表示每个节点都可以与多台节点进行通信。这种通信结构可以实现节点间直接的信息交互（接收方直接读取接收到的信息），或者可以扩展通信链路的范围。在这类环境中，中间节点可以充当两个节点之间的中继设备。这里的两个节点无法直接成功地实现通信，而又不违背物理层协议在能耗和射频调制方面的限制。扩展范围往往需要以牺牲通信速率为代价（因为中间节点需要花时间来中继其他节点的消息）。实施互联拓扑的典型技术为WiFi互联。

互联网络的另一个属性在于它的冗余性。任何一个节点的消失都不一定会导致网络通信的中断。数据有可能依然可以通过其他节点到达预期的目的地。

图2-13所示为一个互联拓扑。节点A和节点D由于距离过远，所以无法直接进行通信。在这种情况下，通信可以通过节点B或者节点C来进行中继。节点B可以充当主中继设备。但节点B消失并不会导致节点A

与节点D之间的通信出现中断。在这种环境中，通信会通过节点C重新路由过去。

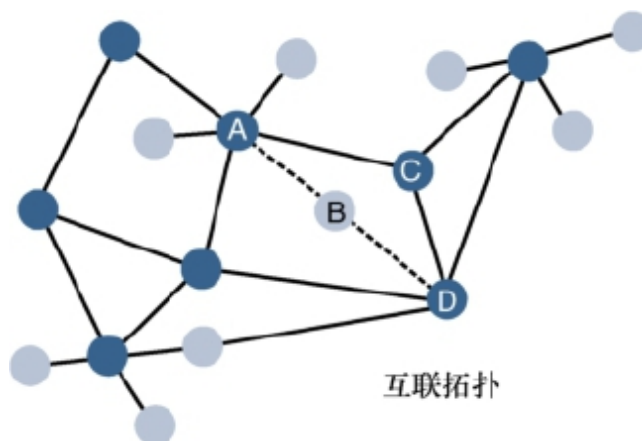


图2-13 互联拓扑

注释：图2-13显示的是一个部分互联拓扑，在这类拓扑环境中，一个节点可以与一个以上的节点进行通信，但并不是每个节点都可以直接与所有其他节点进行通信。在全互联拓扑中，每个节点都可以与其他所有节点进行通信。在图2-13所示的拓扑中一共有17个节点，如果采用全互联拓扑就意味着每个节点都要建立16条连接（即与所有其他节点建立连接）。全互联结构的高昂价格世人皆知（因为每个节点都需要与其他节点之间维护一条连接）。在互联网环境中，全互联的部署方式并不常见。在大多数情况下，信息需要传输给一个目的设备，而不是直接分发给所有其他的节点。全互联拓扑也会限制节点之间的可接受距离（因为每一个节点都必须在搜其他节点的范围之内）。

注释：不要把拓扑和范围这两个概念搞混。拓扑描述的是节点的组织方式，而范围则与频率或者操作、信令结构，以及可用带宽有关。比如，IEEE 802.15.4和LoRaWAN使用的都是星型拓扑，但是IEEE 802.15.4的范围是几十米，而LoRaWAN则可以在数公里的范围内成功传输信令。带宽和信令结构（调制方式）的区别是很大的。读者可以通过图2-11来对比各个常见IoT接入技术的使用环境和实施时应该考虑的因素（范围、成本、可用带宽）。本书会在第4章中详细描述IEEE 802.15.4、LTE、LoRaWAN和其他完备的物联网技术。但读者也要切记，很多一开始并不是给物联网设计的技术也可以最终运用于某些特定的应用。比如，在标准的物联网无线技术的范围无法实现通信时，

远端站点可能需要利用卫星来进行通信。同样，物联网中采用的技术可能会随着时间的推移而变化，可能会随着用户使用环境而变化，也可能会随着新技术的日趋成熟，以及其他因素而变化。在本世纪头几年，移动设备大行其道导致的数据流激增，引发了（LTE）蜂窝网络通信标准的更新换代。而这种更新换代则让LTE可以迅速发展，成为了FAN的一项主流连接技术。

2. 网关与回程子层

从一台物联网设备那里收集到的数据可能需要转发给中心站点，让中心站点来处理这些数据。由于这类站点往往与物联网设备处于不同的地理位置，所以通过接入技术直接从传感器那里接收到的数据需要转发给另一个媒介（回程）并且传输到中心站点。网关负责处理媒介间的通信。

在大多数情况下，物联网设备都是有限区域内的固定或者移动设备，而网关往往是固定设备。不过，有些物联网技术并不会采用这个模型。例如，专用短程通信（DSRC）支持从车辆到车辆和车辆与基础设施之间的通信。在这个模型中，物联网设备与网关之间的相对位置就是固定的。车内会包含多个传感器和一个网关。传感器与网关之间的通信可能会采用有线或者无线技术。传感器也有可能与道路基础设施进行集成，通过一种有线或者无线技术连接到道路一端的网关。无线技术（DSRC工作在5GHz以上的范围）会用于车辆之间的回程通信、对等体间通信，或者互联通信。

在DSRC环境中，整个“传感器区域”都会沿着网关进行移动，但互联网连接的原则仍然保持不变。DSRC可以通信的范围是有限的。同样，对于所有其他DSRC架构而言，回程技术的选择都取决于通信距离，以及需要转发的数据总量。当物联网设备的操作是由本地站点控制时，当整个环境都是稳定的情况下（例如，工厂或者油气田），我们可以使用以太网作为回程技术。在不稳定或者多变的环境中（例如露天矿环境），无法安全地铺设线缆，这时就应该使用无线技术。在这类环境中，WiFi是最常用的技术，而且传感器区域和操作中心之间

也会间隔很多跳。在多变的环境中，互联拓扑是常用的拓扑，因为互联拓扑的通信结构更加灵活。

不过，吞吐量不仅会随着距离的增加而减小，也会随着跳数的增加而减少。在典型的WiFi互联网络中，每增加一跳，吞吐量都会减半。有些技术（如802.11ah）则会为了适应物联网环境而以低频率实施WiFi（低于1GHz而不采用典型WiFi的2.4 GHz/5 GHz），这样做的目的是为了增加传输范围（最远可达2公里）。如果超出了这个范围，则需要使用其他技术。

WiMAX（802.16）就是长距离技术的一例。WiMAX可以以最高70Mbit/s的速率实现范围最远50公里的通信。显然，最远距离和最大速率不可得兼。我们可以认为70Mbit/s速率的通信只能在较短范围内建立起来，而最大范围内的速率只能达到2~3 Mbit/s。802.16d（也称为固定WiMAX）描述了回程的实现方式。此后，这个技术发布了修订版本（802.16.1），但大多数WiMAX网络仍然在实施802.16d的变种。802.16可以在无需许可频率上工作，但它的回程功能往往会部署在更可靠的许可频率上，这样来自其他系统的干扰才能更加可控。

鉴于许可频率表示需要支付使用费用，因此在类似的范围中，其他蜂窝技术也已经成长为了很有竞争力的回程技术解决方案。选择WiMAX还是蜂窝技术取决于垂直面和位置（本地优先级、本地成本）。第4章会深入介绍这里最常用的协议，表2-4从架构的角度对主要的解决方案进行了比较。

表2-4 WiMAX和蜂窝技术在架构方面需要考虑的因素

技术	类型与范围	架构特征
以太网	有线，最大 100 米	需要给每个传感器/传感器组部署一条线缆，适合稳定环境中在固定位置部署传感器；范围不大，链路相当可靠
WiFi (2.4 GHz 和 5GHz)	无线，100 米（多点）到数公里（点到点）	可以将大量客户端（数量一般不超过 200 个）连接到一个 AP；范围不大，适合客户端电源问题很好解决的环境（即有连续电源或者客户端电池很容易充电的环境）；可用带宽高，但有可能遭遇来自其他系统的干扰；AP 需要用线缆连接
802.11ah (HaloW、1 GHz WiFi)	无线，1.5 公里（多点）到 10 公里（点到点）	可以将大量客户端（数量可达 6000 个）连接到一个 AP；范围比传统 WiFi 大；带宽有限；不常用；成本相对较高
WiMAX (802.16)	无线，数公里（“最后一公里”），最高可达 50 公里（回程）	可以连接大量客户端；在（收费的）许可频率上可用带宽高；在无须经许可证的频率上带宽较低，且有可能受到来自其他系统的干扰；采用率因位置而异
蜂窝网络 (如 LTE)	无线，数公里	可以连接大量客户端；可用带宽高；工作在许可频率上（不会受到干扰，频率需要拥有许可）

3. 网络传输子层

上一节介绍了分层的通信架构，在这种架构中大量物联网设备都会向网关发送报告，而网关会将报告的数据通过另一个媒介发送给一台中央站点。不过，实际的实施方案往往都很灵活，会有多条通信路径。比如能源网的物联网环境。一栋住宅中的电表可能会通过无线技术将能耗情况发送给一台网关。这个区域的其他住宅（NAN）也会将相同的报告信息发送给一台或者多台网关。这个环境中要传输的数据量不大，而且时间间隔巨大（比如每小时只发送4次报告）。因此，这是一个低移动性、低吞吐量类型的数据结构，传输距离最大在1公里左右。有很多技术（如802.11ah、802.15.4或LPWA）都可以用来在这个

区域进行数据收集。其他社区可能也会用类似的方式来建立连接，这样也就连接形成了一个FAN。

例如，电力公司的前端应用服务器可能是分区的，网关可能会将数据通过某种有线或者无线回程技术进行发送。这类结构看上去就是分层的。不过在实际使用当中，这类物联网系统可能会产生更多的上游报告数据。如果网络的能耗变得很高，那么电力公司的前端应用服务器可能就要求住宅的电表以更短的时间间隔来按需提供报告了，这样才能满足能耗的需求。从标准的垂直推送模型来看，这种传输结构其实已经发生了变化，成为了双向传输（即成为下游收集模型而不是上游推送模型）。

配电自动化（DA）也可以让电表与邻居的电表或者配电网中的其他设备进行通信。通过这样的通信，能耗的负载分担结构就可以得到优化。比如说，房子里面的空调可以有节奏地以某个时间间隔来向房子里面输送新风。通过DA，当一栋房子的系统暂停的时候，邻居的AC就会启动；通过这种方式，两栋楼里面的空气都可以保持新鲜，而网络中的能耗也可以保持稳定，流量并不会因为随机的起始点和停止点而时大时小。这里必须再次强调，传输模型是变化的。从垂直的结构来看，这种网络结构正在变成互联结构，对等体与对等体之间会有多组信息交互路径。

同样，房子中的智能电表可能会与房间中的设备进行通信，来判断这些设备的类型和耗能。通过这种方式，房子里面的洗衣机可以在其他系统（比如电灯）能耗较低的时间启动，而家庭影院则一直可以获得电源，只要房主需要就可以使用。一旦系统学习到了这栋房子的能耗模式，那么系统就可以以某个时间间隔来给机动车充电，这样既可以过夜充电，也不会造成能耗高峰。在这些功能出现的时候，传输模型还会再次发生变化。互联系统可能会出现在整个房屋的范围内。此时比较常见的情况是，系统会建立部分互联，让一些中央节点连接到其他多个节点。数据可能会在本地流动，或者由一个中央应用进行编排，来协调多个房屋的能耗计划。

在这类智能系统中，汽车的充电系统会连接到用户的能源账户。当车主将车辆连接到一个公共充电站的时候，这辆车就会登录到这个系统中，让系统识别自己的身份并且连接到用户账户。中央系统会以一定的时间间隔来查询所有的充电站来更新状态。在这种传输模型中，这种传输结构会在一定程度上失去自己的垂直结构，因为用户可能会从任何位置发起连接。在一个被管理环境中，前端系统需要对电表中的软件进行更新，就像设备厂商可能需要更新烤箱或者洗衣机上的智能能耗软件一样。这样一来，我们就从一个自底向上的数据传输流作为起点，实现了一个自顶向下的数据流。

因此，这种通信结构可能会包含一个对等体到对等体（比如电表对电表）、点到点（电表到前端站点）、点到多点（网关或者前端站点到多个电表）、单播与组播通信（向一个或多个系统提供软件更新）。在一个多租户环境（如电力和天然气消耗管理环境）中，不同的系统可能会使用相同的通信路径。这种通信会通过多个媒介进行传输（比如房屋中的电线，或者某种短距离的无线系统，如室内WiFi和/或ZigBee）：一个用来连接网关的较长距离的无线系统；另一个用于实现回程传输的无线或者有线介质。

为了实现这样的通信结构，我们就需要实施具有某种特征的网络协议。这种协议需要是一种开放的、标准化的协议，这样才能满足多个行业和各类不同的媒介。扩展性（让一个网络可以部署成千上万直至上百万个传感器）和安全性同样是最为常见的需求。本书会在第5章对IP网络的优势进行介绍。

IP协议非常灵活，这个协议能够内嵌到许多差异巨大的设备当中，能够通过很多大不相同的媒介（包括低功率、有损和低带宽网络）来交换信息。例如，RFC 2464描述了IPv6数据包是如何封装在以太网数据帧当中，并且用于IEEE 802.11 WiFi的。同样，IETF 6LoWPAN工作组也描述了如何通过有损网络来高效地传输IPv6数据包，这就给IPv6建立了一个“适应层”，这类技术主要用于互联网环境。第4章会详细介绍6LoWPAN及其功能。

最后，我们可以利用在IP之上的传输层协议（UDP和TCP）来判断是由网络来控制数据包传输（通过TCP），还是让应用来执行控制任务（通过UDP）。与TCP相比，UDP是一个非常轻量级同时也非常快速的协议。但是这个协议并不给数据包传输提供任何保障。TCP和UDP可以使用TLS/SSL（TCP）或者DTLS（UDP）来提供保护。第6章会对TCP和UDP在物联网环境中的使用进行详细的介绍。

4. 物联网管理子层

IP、TCP和UDP都可以给物联网环境提供连通性。上层协议需要负责处理物联网设备和其他系统之间的数据传输。人们可以利用或者定义很多协议来解决物联网的数据通信问题。其中有些网络使用的是推送模型（即传感器以一定的时间间隔或者在触发的情况下发送报告），有些网络使用的则是收集模型（即应用通过网络向传感器发送查询），同时人们也可以使用混合的方式。

按照IP的逻辑，有些物联网实施者建议在数据传输阶段使用HTTP。毕竟，HTTP天然拥有客户端和服务器的组件。传感器可以使用客户端来向物联网中央应用（即服务器）来建立连接，然后才能进行交换数据。我们可以在一些物联网应用中找到HTTP，但HTTP总是属于一种胖协议，它的初衷并不是在一个受限制、低内存、低带宽、高丢包率的环境中使用。除了这些限制条件之外，也有人提议用其他Web协议来用于物联网环境。其中一个示例就是WebSocket。WebSocket是HTML5规范中的一部分，它可以通过一条连接来建立一个简单的双向连接。有些互联网解决方案会使用WebSocket来管理物联网设备与外部应用之间的连接。WebSocket经常会和其他协议结合起来使用（如MQTT，这个协议会在后文进行介绍），以便解决那些物联网环境中存在的典型通信问题。

通过“复用一些常见方法”的这种方式，人们创建出了XMPP（可扩展消息和表示协议）。XMPP是基于即时消息和表示的一种协议。它可以在两个或两个以上的系统之间交换数据，同时可以维护表示和联系人列表。此外，这种协议也可以处理发布/订阅的需求，因此这个协

议很适合用来向多台设备发布信息。XMPP的限制在于它依赖TCP协议，因此XMPP可能会强制订阅方来维护与其他系统之间的开放会话，这会给那些本身内存不高的物联网设备带来问题。

为了解决Web协议带来的限制，IETF CoRE（Constrained Restful Environments）工作组创建了一项新的协议：CoAP（受限应用协议）。CoAP使用了一些与HTTP类似的方式（如Get、Post、Put和Delete），但是CoAP采用了更短的列表，这样可以限制头部的长度。CoAP也会基于UDP运行（而HTTP一般会使用TCP作为传输层协议）。CoAP也加入了一个HTTP并不具备但是对物联网相当重要的特性：观察（observation）。观察可以让状态的变化按照流的方式传播，而不需要接收方去查询状态的变化。

在中高层使用的另一项常见的物联网协议是消息队列遥测传输（MQTT）。MQTT使用的是一个基于代理的（broker-based）架构。传感器可以设置为MQTT的发布方（负责发布信息），需要接收这类信息的应用可以设置为MQTT订阅方，而所有的中间系统都可以设置为代理，在发布方和订阅方之间传递信息。MQTT会以TCP作为传输协议。依赖TCP的结果是，MQTT客户端往往会始终让自己与代理之间的连接处于开放状态。对于那些丢包率高或者计算资源有限的环境中，这可能会成为一个限制因素。

第6章会详细介绍各类物联网应用协议，包括CoAP和MQTT。从架构的角度来看，我们需要首先判断出应用协议的需求。使用TCP作为传输层协议表示设备需要与端点之间维护会话。可靠性的优势需要以“为了感知会话而消耗大量内存和处理资源”为代价。使用UDP作为传输协议会把控制的任务留给上层协议。在此之外，我们需要判断各类（需要拥有不同优先级的）消息对QoS提出的需求。最后，我们需要评估物联网应用的安全协议，在安全性的需求与由此带来的开销之间进行平衡。第8章会介绍如何从物联网的角度来对安全性进行评估。

2.4.3 第三层：应用与分析层

一旦连接到网络，物联网设备就会与其他系统之间交换信息。一旦这个物联网的传感器数量增加，物联网的功能就会在那些（利用了物联网设备之间交换的数据的）应用中体现出来。

1. 分析与控制应用

很多应用都可以增加物联网网络的效率。每个应用都会收集数据，并且根据这些数据的分析结果来提供一系列的功能。我们很难对这些特性进行比较。第7章会深入分析各类应用。从架构的角度来看，我们可以采用下面这种基本的分类方式。

■ 分析型应用：这类应用会从多个物联网设备那里收集数据，处理收集到的数据，并且显示处理的结果。显示的信息可能涉及物联网的方方面面，从历史报告、统计数据到各个系统的状态趋势，不一而足。这里最关键的地方在于，应用处理这些数据是为了展示网络的一副完整的视图，这个视图不是只查看某一台物联网设备显示出来的信息就可以了解到的。

■ 控制型应用：这类应用可以控制物联网设备的行为，或者与物联网设备相关的某个对象的行为。例如，一个压力传感器可能会与一台泵连接在一起。当与泵连接的传感器检测到压力下降的时候，控制应用就会增加泵的速率。控制型应用十分适合控制物联网中一些复杂的领域，也就是按照那些很难编程到某一个物联网设备中的逻辑来执行控制的领域。这里所说的“很难编程到某一个物联网设备中”，有可能是因为要配置的变更过于复杂，无法由某一台本地设备执行，也有可能是因为要配置的变更必须依赖于其他物联网设备的参数才能执行。控制系统架构的一个示例是SCADA。SCADA是一种访问远程系统并且发送控制信息的通用方式。SCADA得到广泛应用的一大环境，是控制和监控配电网的远程终端装置（RTU）。

很多高级物联网应用中同时包含了分析和控制模块。在大多数环境中，数据都是从智能设备中收集过来，然后在分析模块中进行处理的。处理的结果可能会修改智能设备或者（与智能设备有关的）系统

的操作。控制模块会发送修改设备操作的控制信息。在评估物联网数据和分析型应用的时候，我们需要判断在这个用例中控制部分需要具备的相对深度，并且将这一点和提供的分析类型进行匹配。

2. 数据与网络分析

“分析”是一个通用术语，描述的是让收集到的信息能够表意的信息处理过程。在物联网领域，分析功能可以分为下面几种类型。

■ **数据分析：**这一类分析是处理由物联网设备收集到的数据，并且将它进行组合，以便提供一个与这个物联网系统相关的智能视图。在最基本的层面，当一个重量传感器检测到商场里的一个货架已空时，通过一个面板就可以显示出告警信息。在一个比较复杂的环境中，通过数以千计的传感器收集到的温度、压力、风力、湿度和灯光强度等信息，都可以汇总到一起，然后通过处理来判断发生了风暴的可能性，以及风暴可能的路径。在这种情况下，数据处理可能会非常复杂，需要通过复杂的算法来组合各类不断变化的数值。数据分析也可以监测物联网系统本身。例如，工厂中的一台机器或者机器人可以将关于动态的数据报告出去。这类数据可以由分析型应用来报告移动速度的下降，而这类数据可以作为该机器人部件需要维修的指示信息。

■ **网络分析：**大多数物联网系统都是围绕着连接网络的智能设备构建起来的。连接断开或者连接效率下降都有可能会导致系统的整体效率受到影响。这种连接断开造成的影响可能相当之大。比如，露天矿区会使用无线网络来自动驾驶翻斗车。如果连接长时间断开，有可能造成矿区事故或者给矿区的工作效率造成影响（因为在连接断开的时候，自动驾驶的翻斗车一般都会停止工作）。在一个比较小的范围中，连接断开表示数据分析平台不会再接收到数据了，系统也不会继续对物联网系统进行智能分析。于是，控制模块也就无法再去修改物联网设备的行为了。

大多数分析应用都会同时使用数据分析和网络分析模块。在构建一个物联网系统的时候，我们需要分别评估使用这两种模块的必要性。对于互联系统而言，网络分析是必要的，但分析的深度则取决于具体的用例。如果物联网设备只是偶尔需要报告状态，我们并不需要立刻针对报告采取行为，那么基本的连接视图就已经很足够了。如果需要中央应用在几乎是实时的连接系统中执行操作，那就需要执行具体分析和网络性能趋势判断。

与网络分析相比，数据分析空间广阔，而且灰色区域巨大（关于需求的灰色区域）。基本的系统分析可以提供系统状态分析和状态趋势分析的视图。更高级的系统可以优化收集到的数据，并且显示一些关于系统的其他信息。收集和处理的数据类型因具体使用环境的不同而存在巨大的差异。

3. 数据分析与商业利益

毫无疑问，数据分析是物联网的价值可以充分发挥出来的一个领域。几乎所有设备都可以连接到网络中，每个设备上都可以安装上各类不同的传感器。收集和解释这些设备产生的数据可以让物联网的价值充分展现出来。

从架构的角度来看，我们可以定义静态的物联网，也就是定义一个清晰的检测与分析对象列表。这类静态系统在工业环境中非常常见。在这类环境中，物联网的目的是对操作状态提供一个清晰的视图。不过，我们也可以采用更加智能的架构，即使用一个开放的系统，这个系统足够灵活，以便人们可以在未来向系统中添加新的传感器，并且上游操作和下游操作都可以实现。这种灵活性让人们可以对当前部署的传感器执行一些其他的处理，同时可以更加深入并且更加高效地与物联网所连接的设备进行互操作。这种增强的数据处理能力，可以给商业带来更多新的价值，这些价值甚至有可能是人们在这个系统部署之初始料未及的。

灵活的控制应用可以以Cisco Jasper为例。Cisco Jasper可以给物联网的管理和盈利提供一个一键式的、基于云的平台。设想一下人们在整个城市中部署的自动贩卖机。在最基本的层面上，这些自动贩卖机可能是彼此互联的，人们可以部署传感器让自动贩卖机可以在出现错误状态的时候发送报告。当出现这类状态的时候，修理员就可以去现场解决这个问题了。这类告警可以节省人们的时间，避免维修团队在或许只有一台设备出现故障时，必须去依次查看每一台设备。

这个告警系统或许也可以缩短从系统出现错误状态到维修团队到达现场之间的时间。对于静态平台而言，能否满足这类环境的需求受限于告警的类型。对于一个像Cisco Jasper这样的灵活平台而言，人们可以随时不断开发新的应用。例如，人们可以改进机器传感器，让传感器在每当设备卖出一件商品的时候就发送报告。接下来，人们可以对中心应用进行增强，让它们可以处理这类信息，并且分析出最畅销的商品、商品销量最高的地点和销量最高的时间。设备的这种全新视图可以让我们优化在各个区域中销售的商品。人们可以根据时间、季节或者地点（以及其他系统可以分析的参数）来实施系统。简而言之，设计开放的系统可以给新的应用敞开大门。

4. 智能服务

使用物联网来增强操作水准的功能往往被人们称为“智能服务”。这个词是一个通用术语。这个词非常常用，但是人们经常把它的表意进行延伸，表示某种可以提供额外智能的服务。

基本上，智能服务都会使用物联网，而且智能服务的目的都是为了提升效率。比如，人们可以在设备上安装传感器来确保设备的工作符合规范或者安全性方面的标准。这里所说的效率可以体现为很多不同的形式，包括在危险地带部署用来判断是否有人闯入的传感器，到在货车上安装超出最大重量的检测装置都属于这一类。

智能服务也可以通过检测设备的输出、速率或者评估其他使用数据，来测量设备的效率。整个操作都可以通过物联网来进行优化。比如在医院中，现场（presence）和移动传感器可以用来评估大堂中的访客数量，并且根据评估的结果来对人员进行引流。同样的做法也可以应用在商店环境中，这样可以检测出有些客人在货架前停留的时间比其他客人停留的时间更长。这时，系统可以安排人员来给这位客人提供帮助。在工厂楼层中，系统可以分析人员和设备的移动来优化生产流程。

智能服务可以集成到一个物联网系统当中。例如，我们可以在一个灯泡中集成传感器。而这个传感器可以根据房间中是否有人来开关电灯。更加智能的系统甚至可以与房屋中的其他系统进行通信，学习人们的移动模式，对人们是否会出现现在一个房间中做出预判，以便在有人进入房间之前就点亮电灯。如果系统还可以更加智能一些，那么它就可以使用智能传感器通过分析各类参数来判断人们的心情，并且根据不同的心情点亮不同颜色的灯泡来适应人们不同的心理需求，以便给人们营造一个更加轻松或者更加活力四射的环境。

在这里，灯泡只是一个简单的例子。人们可以让物联网与房间中的其他系统进行连接来协调这个网络的效率。比如，房屋的入口告警系统或者温度系统可以与灯泡中的人员检测器进行协作，按照检测器检测到的数据来变化状态。如果告警系统检测到的是熟悉的人员，那么告警系统就可以禁用这个区域的移动告警。温度系统可以根据房屋中有人的情形，或者根据被检测人的个人偏好来调整房屋的温度。

这种效率也可以扩展到比房屋更大的系统中。比如，智能电网应用可以协调不同房屋之间的能源消耗情形，来规划对电网的能源需求。在本书中，我们曾经提到过，洗衣机可以在夜间启动，因为夜间人们对温控（制冷制热）的能耗需求最低。此外，一栋楼的空调耗能也可以与邻居的空调耗能进行协调，一栋房子中的洗衣机也可以与这种房子里面其他的用电器，乃至与周边住宅的用电器进行协调，让这个社区对于电网的能源需求变得更加稳定平缓。

效率同样适用于M2M通信。在采矿环境中，车辆可以通过通信，协调钻机、铲土机、推土机和翻斗车的操作。协调的结果包括在推土机需要的时候，就会有翻斗车就位。在智慧城市中，机动车之间是可以相互通信的。当公共交通系统可以检测到或者预测出道路发生拥堵的情况时，系统可以临时让公交车换另一条路行驶，也可以根据交通状况和乘客数量来安排某条公交线路的公交车数量。这种根据情况调度公交车的做法既可以是临时的决策，也可以是根据趋势学习到的某种固定的调度方法。

本书第3部分会深入介绍物联网改变某个特定行业的案例。读者可以通过这些内容反复领会这一概念：设计开放的物联网系统可以让系统的效率随着时间不断改善。物联网环境中的新应用以及新技术会在未来几年不断涌现出来。在搭建物联网系统的时候，我们应该保证这个系统是开放的，让新的物联网设备和更多流量可以接入这个系统中来。

2.5 物联网数据管理与计算堆栈

本书前两章的一大核心概念在于，物联网网络的巨大规模会从根本上催生新的架构。比如，图1-2介绍了连接到互联网当中的“物”正在呈指数递增。Cisco预测，到2020年，连接到各类IP网络的设备数量会超过500亿台。显然，传统IT网络并没有给如此庞大数量的设备留出足够的空间。不过，在网络架构之上，我们也要考虑一下这些设备所生成的数据。如果设备的数量已经超出了传统的数量，那么这些设备生成的数据量也必然值得严肃对待。

事实上，物联网传感器生成的数据才是搭建物联网系统时最大的挑战。在最新的IT网络中，发端于一台计算机或者一台服务器的数据往往是由客户端/服务器这种通信模型产生的，这类数据可以满足应用的需求。在传感器网络中，绝大部分数据都是非结构化的，这些数据本身几乎没有任何用处。比如，一个智能电表生成的大部分数据都是轮询数据；通信系统只需要判断这个电表与网络之间的连接是不是正

常就可以了。这个数据本身用处着实不大。智能电表的真正价值在于那些电表管理系统（MMS）读取到的那部分测量数据。不过，如果我们从另一个角度来看待那些原始的轮询数据，这些信息可能就会非常重要。比如，一家公用事业单位可能有上百万门电表，这些电表覆盖了这家公司提供服务的整个区域。如果智能电网覆盖的整个区段都显示与电表的连接断开，那我们就可以对这些数据进行分析，并且将这些数据和其他数据源（如天气预报和电网的电力需求）结合起来，依此判断这次故障的成因。这类信息可以帮助人们判断，电表连接中断是不是表示真的存在电力损失，还是说电网中出现了其他问题。此外，分析这类数据可以帮助这家公用事业单位发现服务中断的原因，并且迅速修复故障。

在大多数情况下，数据处理的进程都是在物联网设备之外执行的。数据处理的天然位置是在云端完成。智能设备需要连接到云，数据需要以集中式的方式进行处理。这个模型的一大优势就是简单。物联网设备只需要连接到一个中央的云应用即可。应用可以看到全部的物联网节点，而且可以处理所有我们在今天或者未来需要进行的数据分析。

不过，这个模型也有缺陷。当数据量增大，连网之“物”种类增加，且人们对效率的要求进一步提升时，就会出现新的需求，而这些新的需求往往会要求执行数据分析的位置更加贴近物联网系统。这里所说的需求如下所示。

■ **最小化延迟：**各类工业系统中，在诸如防止流水线停顿或者恢复电力服务这类场合中，毫秒级的差异都是很重要的。在距离数据收集设备很近的位置分析数据，可以让整个系统免遭级联系统故障。

■ **节省系统带宽：**海上石油钻机每周可以产生500GB的数据。商用喷气机每30分钟的航程就可以产生10TB的数据。把如此海量的数据从上百万台边缘设备传输到云端是不切实际的，也是完全没有必要的，因为很多重要的分析其实根本用不到云级别的处理与存储资源。

■ 增加本地效率：在自然条件差异巨大的广大地理范围内收集和保护数据有可能用处并不大。一个区域中的条件会触发本地设备做出某种响应，这种响应和上百公里之外另一个自然条件下的站点所做出的响应是相互独立的。如果以提升效率作为出发点的话，我们其实不必在同一个系统中分析这两个区域。

因此，在设计的时候，一项重要的考量因素在于如何设计出一个物联网，以高效的方式管理如此海量的数据，这样数据才能迅速得到分析，而分析的结果也能够直接作用于商业利益。物联网设备所生成的海量数据可以轻而易举地让数据中心或者云中的前端系统难以为继。例如，一个中等规模的智能电表网络包含100万台电表，这样一个网络每天可以生成近10亿个数据点（包括读表和其他控制数据），由此产生的数据量将达1TB之多。对于一个无法实时分析和储存如此海量数据的IT机构而言，这会造成巨大的问题。

庞大的数据量也会给带宽管理带来难题。随着大量物联网数据开始涌入数据中心，网络真的能够支持如此庞大的流量吗？应用服务器能够正确接收、存储和分析如此庞大的进站数据吗？我们将这种情况称为物联网系统生成的数据和管理应用处理数据的能力存在“阻抗失配”。

如图2-14所示，传统IT系统中的数据管理是非常简单的。端点设备（笔记本电脑、打印机、IP电话等）通过IP核心网络与数据中心或者云端的服务器进行通信。数据一般会储存在数据中心的数据库中，而接入层到核心层之间的物理链路一般都拥有高带宽，因此访问IT数据的速度也是很快的。

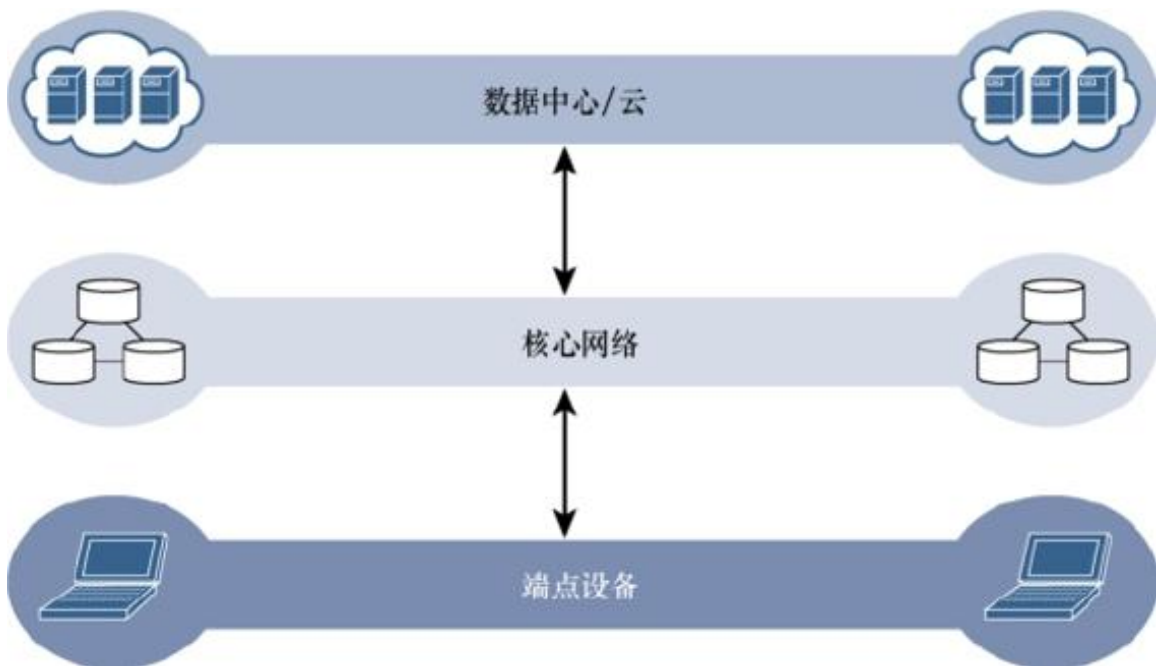


图2-14 传统IT的云计算模型

物联网系统的工作方式与此不同。很多与数据相关的问题都需要得到解决。

■ “最后一公里”物联网的带宽是很低的。在处理成千上万台设备的时候，每台设备可用的带宽可能只有几十kbit/s，甚至更低。

■ 延迟可能非常高。除了处理延迟（以毫秒为单位）之外，大型物联网往往会引入数百毫秒甚至数秒的延迟。

■ 从网关的回程路径有可能并不可靠，这条路径往往需要依靠3G/LTE甚至卫星链路来建立连接。如果必须借助逐字节的数据使用模型，回程链路有可能价值非常昂贵。

■ 通过回程链路传输的数据量可能非常高，其中有很多数据或许价值不大（比如普通的轮询消息）。

■ 大数据越来越大。在云中存储和分析所有传感器的数据是不现实的。设备产生的数据量极大，执行实时数据分析和响应早已成为天方夜谭。

2.5.1 雾运算

解决前面这种问题的方法是在整个物联网系统中分发数据管理，越贴近IP网络边缘越好。物联网中最有名的边缘服务是雾运算。任何具有计算、存储和网络连接功能的设备都可以是一个雾节点。雾节点包括控制器、交换机、路由器、内嵌的服务器和物联网网关。在贴近物联网数据连接的位置对这些数据进行分析可以降低延迟，不让大量网络流量流向核心网络，让敏感数据停留在本地网络当中。

注释：雾的概念最初是由Cisco公司的Flavio Bonomi和Rodolfo Milito提出的。在物联网环境中，雾得名于云端的计算。正如空中会有云层一样，雾存在于贴近地面的位置。同样，雾计算的目的是让资源尽可能接近地面——物联网设备。这里有一点值得一提，那就是“雾”这个词最初是由Ginny Nichols（也就是Rodolfo的夫人）提出的。虽然这位女士的工作领域并不与物联网直接相关，但是她对于自己丈夫工作的领域相当了解，能够迅速对云计算和边缘计算做出比较。有一天，她就建议直接把边缘叫作“雾层”。雾由此得名。

这种结构的一大优势在于，雾节点可以汇聚智能设备（如分析设备），并且从最近的节点执行控制，因此雾节点比受限网络的性能更优。从某种意义上讲，这给传统IT计算模型中引入了一个新的层级，也就是人们所说的“雾层”。图2-15显示了物联网数据管理与计算堆栈中雾层的部署方式。

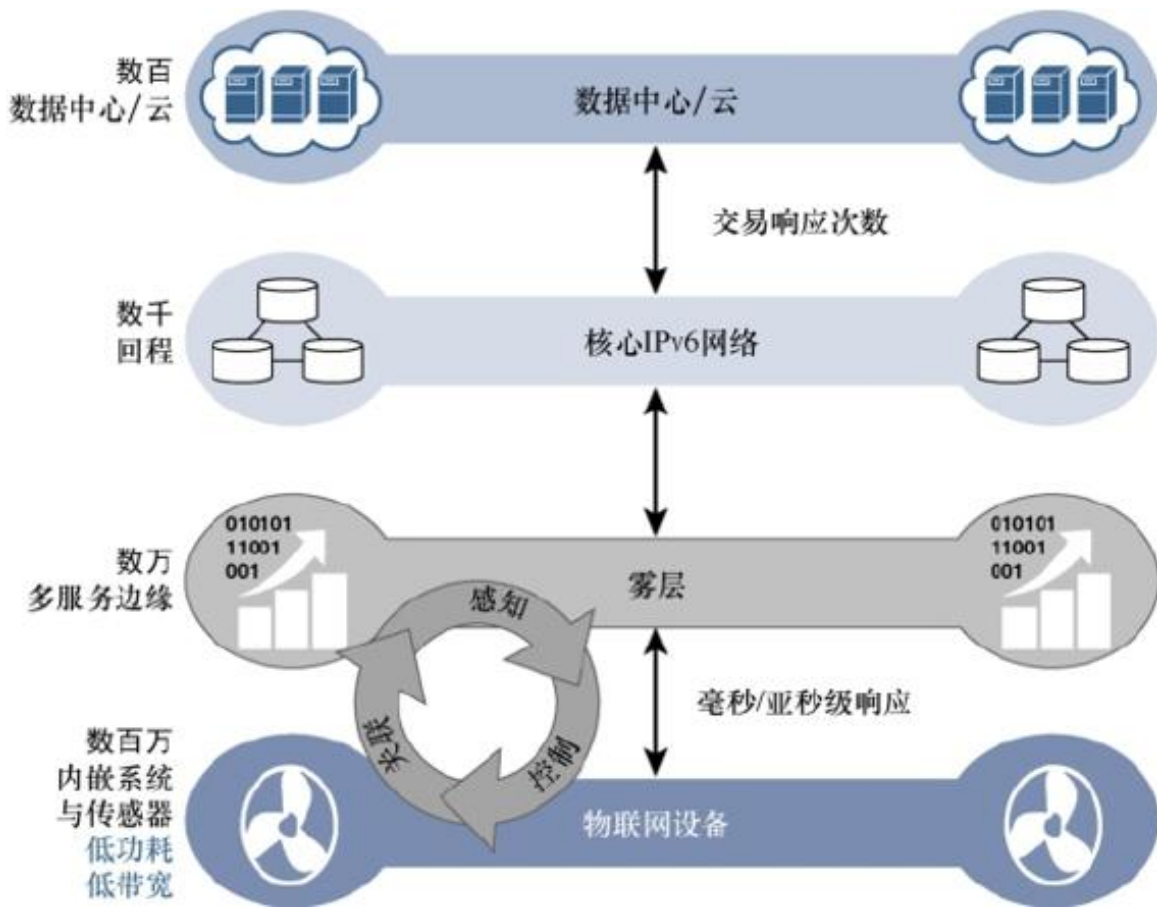


图2-15 包含雾计算的物联网数据管理和计算堆栈

雾服务一般会在非常接近边缘设备的地方完成，执行的位置会尽可能接近物联网端点。这样做的一大好处在于，雾节点可以感知到其管理的传感器所处的环境，因为节点在地理位置上非常接近传感器。例如，在一个石油井架上的一台雾路由器会负责管理这个位置之内的所有传感器的活动。由于这个雾节点可以对井架上所有传感器发来的信息进行分析，因此它可以对它接收到的消息执行情境分析，甚至可以只把相关信息通过回程网络发送给云。通过这种方式，雾节点可以执行分布式分析，这可以大大减少发送给上游网络的数据。因此，这对于云端的应用服务器和分析服务器非常重要。

此外，雾节点能够感受环境，因此可以对物联网中的事件快速做出响应，其响应的速度远比传统IT计算模型的响应速度要快得多，后者的延迟和响应时间要长很多。因此，雾层可以提供分布式的边缘控

制环路功能，在边缘对设备进行实时的监测、控制和分析，而不需要与云端的中心分析与应用服务器进行通信。

这种模型的价值不言自明。比如，一个露天矿区的大卡车上所安装的胎压传感器有可能会全天不间断地报告它的测量结果。但一辆卡车的胎压变化往往都是微乎其微的，大部分情况下都并不会超出危险范围，因此不断将报告发送给云毫无必要。所以，我们真的需要没完没了地把这些数据通过（很可能是）天价的回程连接发回云端吗？如果在卡车上安装一个雾节点，我们就可以不必迅速测量所有轮胎的胎压，我们也可以将这些数据与引擎、液压等系统中其他传感器发来的信息结合起来。通过这种方式，雾节点只有在卡车真的出现了问题，而且这些问题会对整个系统构成影响的情况下，才会把数据发送给上游。

物联网雾计算可以预处理数据，并且将数据与其他输入信息进行关联，来生成相关的信息。接下来，物联网应用可以用这些信息作为实时、可操作的信息。从长期来看，人们可以用这些数据来深入了解网络和系统的活动，以便制定出更有预见性的策略、处理和响应方式。

雾应用的多样性毫不逊于物联网本身的多样性。通过雾节点，通信中的数据量就可以减少。人们可以监测或者分析从连网之“物”发送过来的实时数据，然后据此来执行操作（比如锁门、修改某台设备的设置、执行火车制动、把摄像头拉近、在读到压力时即打开阀门、创建一个柱状图，或者给技术人员发送一条告警信息，让他们进行维修）。

雾计算的具体特征如下所示。

■ 可感知环境位置且延迟低：雾节点的位置会尽可能贴近物联网节点，其目的是为了实现在分布式计算。

■ 在地理上更加分散：雾节点的目标服务与应用需要采用分布式的部署方式，这一点与更加集中化的云部署方式形成了鲜明对比。

■ 部署在接近物联网节点附近：雾节点往往部署在存在大量物联网节点的环境中。例如，在计量系统部署环境中，每台网关路由器往往连接有3000~4000个节点，而网关路由器则会在这个环境中充当雾计算节点。

■ 雾与物联网节点之间使用无线通信：虽然雾计算也可以连接有线节点，但是在处理大量端点设备的情况下，雾的优势才最为明显，而无线接入是实现扩展规模的最简单方式。

■ 用于实现实时的信息交互：重要的雾应用都包含了实时交互这一特点，而不是执行批处理。在雾节点预处理数据可以让上层应用只对一部分数据执行批处理。

2.5.2 边缘运算

雾计算解决方案已经为许多行业所接纳，人们在开发分布式应用与分析工具方面也越来越积极。雾节点在网络中的天然位置就是位于那些距离物联网端点最近的设备中，而这些雾节点往往遍布于整个物联网网络中。不过，在最近几年，物联网计算的概念已经被推广到边缘之外。在有些情况下，雾节点就直接位于传感器和物联网设备当中。

注释：边缘计算有也称为“薄雾”计算。如果云彩是在天上，雾处于距离地面比较近的位置，那么薄雾实际上就是在地面上。因此，薄雾计算的概念也把雾扩展到了更远的位置，也就是直接部署在物联网端点设备当中。

物联网设备和传感器上的资源往往比较有限，不过所有设备的计算能力已经今非昔比。至少有些新的物联网端点有足够的计算资源可以执行低级别的分析和过滤功能，来帮助这些设备做出决策。我们可以以一个消防栓上安装的水力传感器为例。配电网中某个导电柱上安装的雾节点可能掌握本地范围内所有消防栓的信息，而每个消防栓上的节点都能够发现水压低于警戒线的情况，并且能够快速发出故障告警。雾节点的视野更广，它们能够判断出问题是只影响一个局部，还

是正在对整个区域构成威胁。部署智能电表也是这种情况。有计算功能的边缘电表可以相互通信，这样配电网中一小部分设备之间就可以共享信息，以便监测本地电力质量与耗电情况，这些设备可以将那些有可能只与电网中一小块区域有关的事件通知给雾节点。这类模型都可以保障电能可以以最高质量传输给用户。

2.5.3 边缘、雾和云的层级

边缘或者雾运算绝不会取代云，这一点我们必须强调。不仅如此，云和雾互为表里，很多使用环境都要求云和雾之间能够通力协作。恰如对于一个国家而言，地方法院并不会取代最高法院，边缘和雾运算层只会作为过滤、分析和管理数据端点的第一道防线。这种结构可以节省云上的资源，防止每个节点每天都向云发起查询。

这种模型建议网络、计算和数据存储资源采用一种层级化的结构。只要有必要，每一层都会对数据进行收集、分析和响应，这取决于每一层资源的性能。由于数据需要发送给云端，延迟会越来越高。分层的好处在于，对从最接近端点设备的资源来对事件做出响应是速度最快的，因此分层可以带来直接的好处，同时云端仍然有更加强大的计算资源可供调用。

这里有一点值得注意：物联网设备的异构性也意味着边缘和雾运算资源是异构的。鉴于云资源是同质的，人们常常认为在很多情况下，边缘和雾资源会使用不同的操作系统、拥有不同的CPU和数据存储功能，并且拥有不同的能耗特征。因此，边缘和雾需要有一个抽象层，让应用之间可以相互通信。这个抽象层需要包含一个常见的API集，来以一种标准化的方式监测、提供和控制物理资源。这个抽象层也需要拥有某种机制来支持虚拟化，能够在一个物理设备上运行多种操作系统或者服务容器，以便在物联网系统中支持多租户，实现应用一致性。诸如oneM2M这样的组定义了通用通信服务框架的概念，这一点在前面已经介绍过了。图2-16显示了物联网环境中，边缘、雾和云计算的分层结构。

从架构的角度来看，距离网络边缘最近的雾节点会从物联网设备那里接收到数据。接下来，雾物联网应用会将不同类型的数据转发给最优的地点进行分析。

■ 对时间最敏感的数据会在距离生成数据的“物”最近的边缘或者雾节点上进行分析。

■ 可以等待数秒或者数分钟的数据会被转发给汇集节点来执行分析和操作。

■ 对时间不那么敏感的数据会被转发给云来执行历史分析、大数据分析，并且进行长期储存。例如，每成千上万个雾节点都会周期性地向云发送数据汇总，供云执行历史分析和存储。

总之，在构建一个物联网的时候，我们应该考虑要进行分析的数据流，以及数据对时间的敏感程度。搞清楚这些因素可以帮助我们判断只使用云计算是否足以满足需求，抑或部署边缘或者雾运算可以进一步提升系统的效率。雾运算可以让人们对事件掌握更多信息，而且能够更快做出响应，因为雾运算可以消除掉把数据发送回云执行分析的需要。借助雾运算，人们不必增加昂贵的带宽，可以减少核心网络的流量。雾运算可以保护敏感的物联网数据，因为借助雾运算，这些数据可以直接在企业内部进行分析。

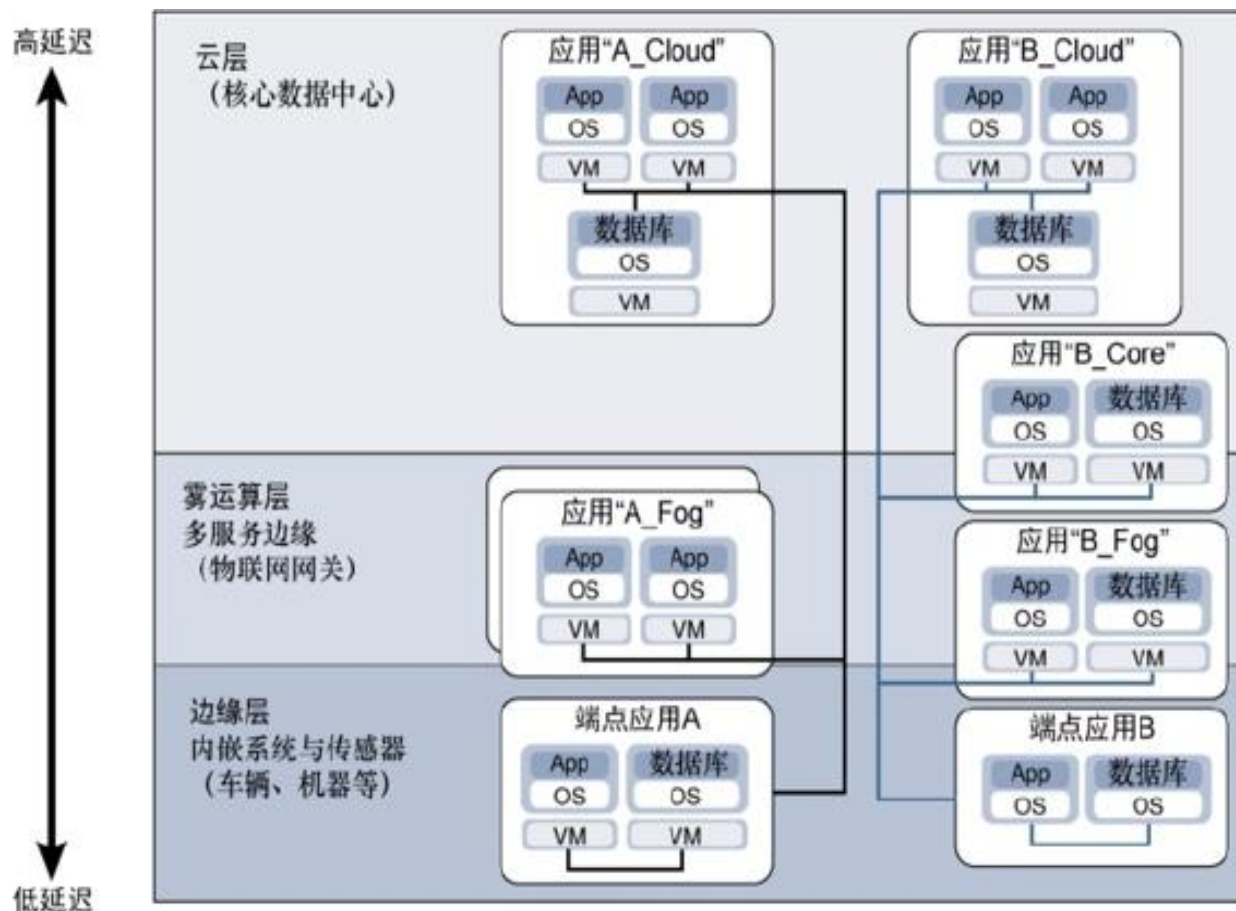


图2-16 物联网系统上的分布式计算与数据管理

2.6 小结

物联网系统的需求催生了新的网络架构，这个新的架构解决了扩展性方面的问题，解除了很多束缚，从数据管理的角度重新审视了物联网。很多专用于物联网的参考模型由此诞生，包括oneM2M物联网模型，以及物联网世界论坛的物联网参考模型。这些模型的共性在于物联网设备之间的互动、连接这些设备的网络，以及管理这些端点的应用。

本书呈现了物联网的框架，这个框架使用了很多模型的不同方面，将这些模型应用到了各个专门的领域和不同的环境中。本章根据这些架构中所包含的共同概念向读者呈现出了一个模型。所有架构都

把物联网分层分为了一个简化的架构，这个架构中包含有两个相互平行的堆栈：核心物联网功能协议栈和物联网数据管理与计算协议栈。这个架构就是本书后续章节的结构。

核心物联网功能协议栈分为三层：物联网传感器与执行器、网络组件，以及应用与分析层。网络组件和应用层都包含了很多子层，它们分别对应物联网系统中的不同部分。

物联网数据管理与计算协议栈负责处理如何以及在何处过滤、汇总、存储和分析数据。在传统IT模型中，这些操作都发生在云端或者数据中心当中。不过，由于物联网的独特需求，数据管理需要分配到尽可能接近边缘的位置，包括边缘和雾层。

第3章 智能对象：物联网之“物”

想象一下在第1章中强调的支持物联网连接的车辆和道路，这种通过物联网连接的车辆有一个令人印象深刻的传感器生态系统，它提供了可以被各种系统智能使用的大量数据，并提供了汽车本身以及与外部其他车辆共享的服务、连接的道路基础设施，甚至一整套基于云数据的诊断和消费者服务。从方向盘后面看，车里几乎所有的东西都可以检查（感知）和控制。汽车里装满了各种各样的传感器（例如，温度、位置[GPS]、压力、速度），这些都意味着要提供丰富的有价值的相关数据，以提高安全性，简化车辆维护，提升驾驶员的经验。

这些传感器是物联网网络的基本构件。事实上，它们是智能对象中的基本元素——物联网中的“物”。智能对象是任何包含嵌入式技术的物理对象，它们通过相互联系与周围的环境进行有意义的互动，并且相互之间或与外部代理之间能够通信。

本章详细分析了智能对象及其体系结构。它还阐述了它们在物联网网络中的设计限制和作用。具体来说，本章会介绍以下内容。

- 传感器、执行器和智能对象：本节定义了传感器、执行器和智能对象，并描述它们如何成为物联网的基本构件网络。

- 传感器网络：本节介绍了设计、采用和部署传感器网络所面临的挑战。

3.1 传感器、执行器和智能对象

下文描述了传感器和执行器的性能、特征和功能，还详细说明了经济和技术状况如何影响了物联网的蓬勃发展。最后，还介绍了如何

将这些基本功能元素结合在一起形成智能对象，这些对象又连接在一起形成传感器和执行器网络，最终使大多数物联网用例成为可能。

3.1.1 传感器

传感器就像它的名字所示：感知。更确切地说，是一个传感器测量一些物理量，并将测量读数转换成数字表示。该数字表示通常传递给另一个设备，转换为可由智能设备或人类使用的有用数据。

自然地，我们可以运用人类的 5 种感官来了解周围所处的环境。人类的感官并不是各自为政、独立运作的。相反，它们互相补充，一起计算，让人类大脑做出明智的决策。大脑是最终的决策者，它经常使用多个感官输入源来验证事件并补偿“不完整”的信息。

传感器并不局限类人的感官数据。它们可以衡量任何有价值的东西测量。事实上，它们能够提供非常广泛丰富的频谱和多样化的测量数据，精度远超人类感官；传感器提供超人的感觉能力。这个额外的数据维度使我们的物质世界成为了非常宝贵的信息资源库。传感器可以很容易地嵌入在任何可以通过有线或无线网络轻松连接到互联网的物理对象中。由于这些传感器具有多维感知能力且相互连接的主机物理对象与外部系统通信，因此它们可以解释环境并做出智能决策。以这种方式连接传感装置，能够引领物联网世界和全新的商业智能范式。

有无数不同的传感器可用来测量这个物理世界中几乎所有的东西。我们有许多方法可以将传感器分组，集合到不同的类别中，具体如下。

■ 有源或无源：有源或无源的分类依据是传感器会产生能量输出并需要外部电源（有源），还是只接收能量，通常不需要外部电源（无源）。

■ 侵入性或非侵入性：根据传感器是属于它所测量的环境一部分（侵入性）还是属于外部环境（非侵入性）来分类。

■ 接触或无接触：可以根据是否需要与被测对象进行身体接触（接触）或不接触（无接触）来分类。

■ 绝对或相对：可以根据其测量的是绝对尺度（绝对）还是具有固定或可变参考值的差异（相对）来分类。

■ 应用领域：可以根据特定的行业或所应用的垂直领域进行分类。

■ 传感器如何测量：可以根据用于测量感官输入（如热电、电化学、压阻、光学、电学、流体力学、光弹性等）的物理机制来分类。

■ 传感器测量对象：可以根据其应用程序或测量的物理变量来分类。

注意，上述分类方式并不详尽，还有许多其他的传感器分类和分类方案，包括基于材料、成本、设计和其他因素的方案。如本书所述，对于传感器在物联网网络中的实际应用，最有用的分类方案是简单地根据传感器所测量的物理现象进行分类。这种分类如表 3-1所示。

表3-1 传感器类型

传感器种类	描述	案例
位置传感器	位置传感器测量物体的位置；位置测量可以用绝对值（绝对位置传感器）表示，也可以用相对量（位移传感器）表示。位置传感器可以是线性的、角度的或多轴的	电位计、倾角计、近程传感器
空间占用和运动传感器	空间占用传感器检测监视区域内的人和动物的存在，而运动传感器检测人和物体的运动。两者的区别在于，即使在一个人静止的时候，空间占用传感器也会产生信号，而运动传感器则不会	电子眼、雷达
速度和加速度传感器	速度传感器可以是线性的，也可以是角度的，用来指示物体沿直线运动的速度或旋转的速度；加速度传感器则用来测量速度的变化。	加速度仪、陀螺仪
力传感器	力传感器检测是否施加了物理力以及力的大小是否超过阈值	测力计、黏度传感器、触觉传感器（接触式传感器）
压力传感器	压力传感器与力传感器有关，用来测量液体或气体施加的力。压力是用单位面积上的力来测量的	气压计、波尔登管式压力计、压力计
流量传感器	流量传感器检测流体的流速，测量流体在给定时间内通过一个系统的体积（质量流量）或速率（流速）	风速计、质量流量传感器、水表
声学传感器	测量声音级别，并将信息转换成数字信号或模拟数据信号	麦克风、地震检波器、水下听器
湿度传感器	湿度传感器检测空气或物体中的湿度（水蒸气的数量）；湿度水平可以通过多种方式测量：绝对湿度、相对湿度、质量比等	湿度计、湿敏电阻土壤湿度传感器
光传感器	光传感器检测光的存在（可见或不可见）	红外传感器、光电探测器、火焰检测器
辐射传感器	辐射传感器探测环境中的辐射；辐射可以通过闪烁或电离探测来探测	盖革-米勒计数器、闪烁器中子探测器
温度传感器	温度传感器测量系统中存在的冷热量，大致可以分为两种类型：接触型和非接触型。接触型温度传感器需要与被感知对象进行物理接触；非接触型传感器不需要物理接触，因为它们通过对流和辐射测量温度	温度计、量热仪、水温表
化学传感器	化学传感器测量系统中化学物质的浓度；当受到混合化学物质的影响时，化学传感器通常对目标化学物质是有选择性的（例如，二氧化碳传感器只感知二氧化碳）	酒精分析仪、嗅觉测量器、烟雾探测器
生物传感器	生物传感器检测各种生物元素，如生物体、组织、细胞、酶、抗体和核酸	血液生物传感器、脉搏血氧仪、心电图仪

传感器有各种形状和大小，如表3-1所示，可以测量所有类型的物理条件。一个凸显传感器和物联网力量的有吸引力的用例是在精准农业（有时称为智慧农业）领域，该领域利用各种技术进步来提高传统农业的效率、可持续性和盈利能力。这包括使用全球定位系统和卫星航空图像来确定田间的生存能力；用于高精度种植、收割、灌溉等的机器人；使用实时分析和人工智能来预测最佳作物产量、天气影响和土壤质量。

精准农业最重要的影响之一是处理传感器测量的各种土壤特性。这些包括实时测量土壤质量、pH水平、盐分、毒性水平、灌溉规划所需的水分水平、施肥规划所需的营养水平等。所有这些详细的传感器数据都可以进行分析，为提高生产力和作物产量提供非常有价值和可操作的见解。图3-1显示了生物可降解的无源微传感器，用于测量土壤、作物和条件。这些传感器由北达科他州立大学（NDSU）开发，可以直接种植在土壤中，并留在土壤中进行生物降解，而不会对土壤质量造成任何危害。

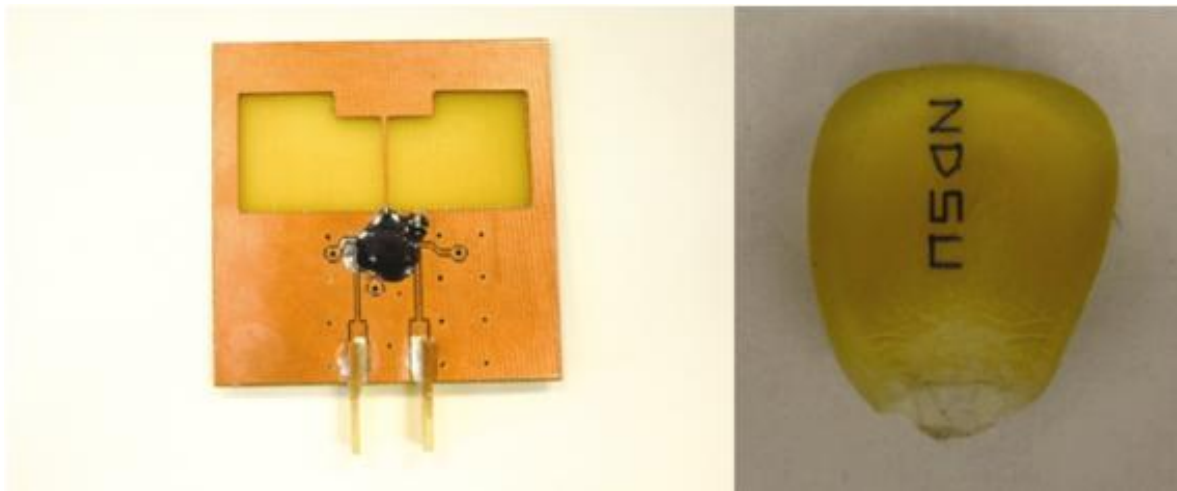


图3-1 北达科他州立大学为智慧农业开发的生物降解传感器

物联网（IoT）乃至联网传感器，已被反复列入少数将改变全球经济、塑造未来的新兴革命技术之列。传感器的大量推广是这一现象的主要驱动力，这在很大程度上得益于较小的尺寸、小巧的外形以及更低的成本。这些因素使得在所有类型的物体中增加传感器密度的经济和技术可行性成为可能。对于传感器部署来说，最重要的加速器可能

是移动电话。智能手机每年的销量超过10亿部，每一部手机都有10多个传感器（见图3-2），而且这个数字还在逐年增长。想象一下将传感器扩展到几乎所有技术、行业和垂直领域的指数效应。例如，有可能有数百个传感器的智能家庭，每辆有100多个传感器的智能汽车，以及有成千上万个连接传感器的城市，这样的例子不胜枚举。

令人着迷的是，万亿传感器经济即将到来。图3-3显示了过去几年的爆炸性同比增长，以及对未来几年传感器数量的一些大胆预测。在传感器行业，人们坚信这个数字将在未来几年超过一万亿。事实上，传感器行业的许多大型参与者已经联合起来组成行业联盟，例如TSensor 峰会，已经为万亿传感器经济创建战略和路线图。万亿传感器经济的规模将是前所未有的，难以想象的，它将永远改变世界。这就是物联网的力量。



图3-2 智能手机中的传感器

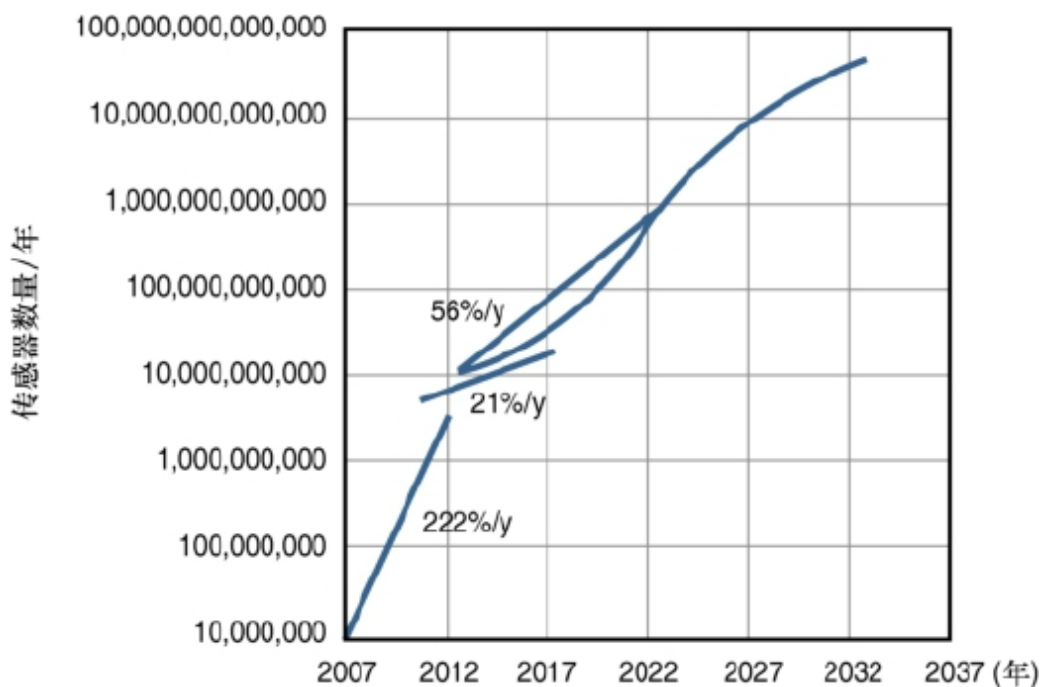


图3-3 传感器数量的增长和预测

3.1.2 执行器

执行器是传感器的自然补充。图3-4展示了这两种器件的对称性和互补性。上一节讲到，传感器是为了感知和测量物理世界中任何可测量的变量而设计的。它们将测量值（通常是模拟值）转换为电信号或数字表示，可以由智能代理（设备或人）使用。另一方面，执行器接收某种类型的控制信号（通常是电信号或数字命令）来触发物理效应，通常是某种类型的运动、力等。

上一节将传感器和人类感官进行了比较。这种比较可以扩展到执行器上，如图3-5所示。人类用5种感官来感知和测量环境。感觉器官将这些感觉信息转换成神经系统发送给大脑进行处理的电脉冲。同样，物联网传感器是感知和测量物理世界的设备，（通常）将测量结果作为电信号发送给某种类型的微处理器或微控制器进行额外处理。人类大脑发出运动功能和运动的信号，神经系统将这些信息传送到肌肉系统的适当部位。相应地，处理器可以向执行器发送电信号，执行器将信号转换为某种类型的运动（线性、旋转等）或有用的工作，这

些工作可以改变或对物理世界产生可测量的影响。传感器、执行器和处理器之间的这种交互作用以及生物系统中的类似功能是各种技术领域的基础，包括机器人技术和生物识别技术。

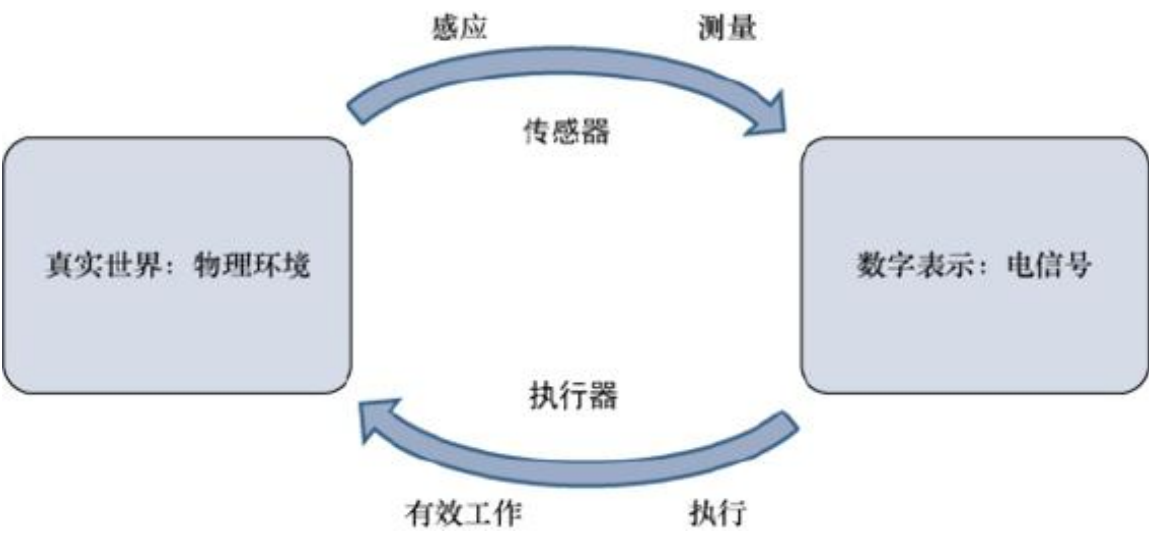


图3-4 传感器和执行器如何与物理世界交互

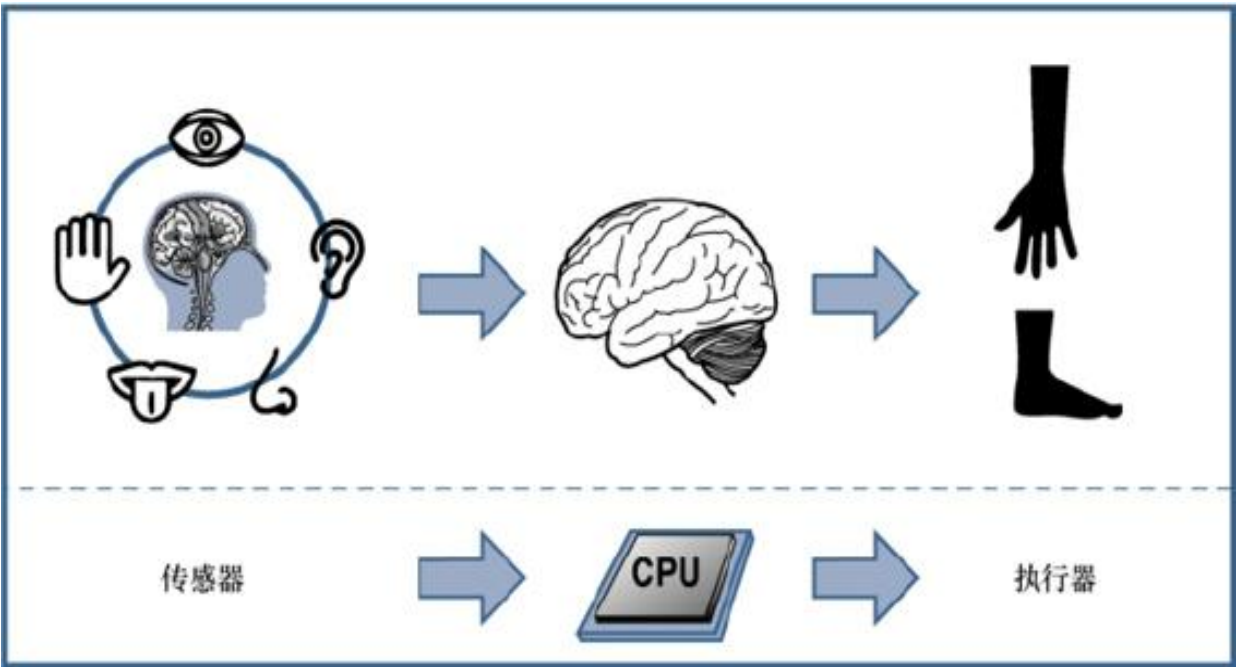


图3-5 传感器和执行器功能与人类的比较

就像传感器一样，执行器在功能、尺寸、设计等方面也有很大的差异。以下是一些常见的分类方法。

■ 运动类型：执行器可以根据其产生的运动类型进行分类（例如，线性、旋转、一/二/三轴）。

■ 功率：执行器可根据输出功率（如大功率、低功耗、微功耗）进行分类。

■ 二进制或连续数据流：执行器可以根据稳定状态输出的数量进行分类。

■ 应用领域：执行器可以根据所应用的具体行业或垂直领域进行分类。

■ 能量类型：执行器可以根据其能量类型进行分类。

考虑到执行器的多样性，对执行器进行分类是相当复杂的，因此下文的分类方案并不详尽。最常用的分类是基于能量类型。表3-2显示了按能量类型分类的执行器，以及每种类型的一些示例。尽管表3-2不详尽，但它提供了一个相当全面的概述，强调了执行器的功能和设计的多样性。

表3-2 按能量类型分类的执行器

种类	示例
机械执行器	杠杆、螺旋千斤顶、手动曲柄
电子执行器	生物晶体管、二极管、晶闸管
机电集成型执行器	交流电机、直流电机、步进电机
电磁执行器	电磁铁、线性螺线管
液压和气动执行器	液压缸、气动缸、活塞、压力控制阀、空气马达
智能材料执行器 (包括热致动器和磁性致动器)	形状记忆合金 (SMA)、离子交换液、限磁材料、 双金属片、压电双晶片
微型或纳米执行器	静电电机、微阀、梳状驱动器

传感器提供信息，而执行器实施行动。物联网最有趣的用例是传感器和执行器以智能、战略和互补的方式协同工作。这种强大的组合可以用来解决日常问题，只需将传感器提供的数据提升到可执行的洞察力，这些洞察力可以由产生工作的执行器执行。

我们可以基于上一节的精准农业示例来演示执行器如何补充和增强纯传感器的解决方案。例如，用于评估土壤质量的智能传感器（测量各种土壤、温度和植物特性）可以与控制水、杀虫剂、化肥、除草剂等的电动或气动阀执行器连接。以温度、pH、土壤/空气湿度、营养水平等良好的传感器读数为基础，来智能触发高精度执行器，提供高度优化的定制环境专用解决方案，这才是真正的智慧农业。

3.1.3 微机电系统（MEMS）

传感器和执行器技术最具有意义的进步之一是它们的组装和部署方式。微机电系统有时简单地称为微型机器，可以在非常小的（毫米或更小的）尺度上集成和组合机电元件，例如传感器和执行器。这项技术的关键之一是一种类似于用于微电子集成电路的微制造技术。这种方法允许以非常低的成本进行大规模生产。MEMS具有体积小、成本低和大规模生产的能力，这使得MEMS成为众多物联网应用程序的一个有吸引力的选择。

MEMS设备已经广泛应用于各种不同的应用中，并且可以在非常熟悉的日常设备中找到。例如，喷墨打印机使用微型泵MEMS。智能手机也使用MEMS技术，比如加速度计和陀螺仪。事实上，汽车是最早借助安全气囊加速度计将微机电系统（MEMS）引入大众市场的产品之一。

图3-6显示了一个扭转棘轮执行器（TRA），是由桑迪亚国家实验室开发的可以替代微型引擎的一个低压替代品。

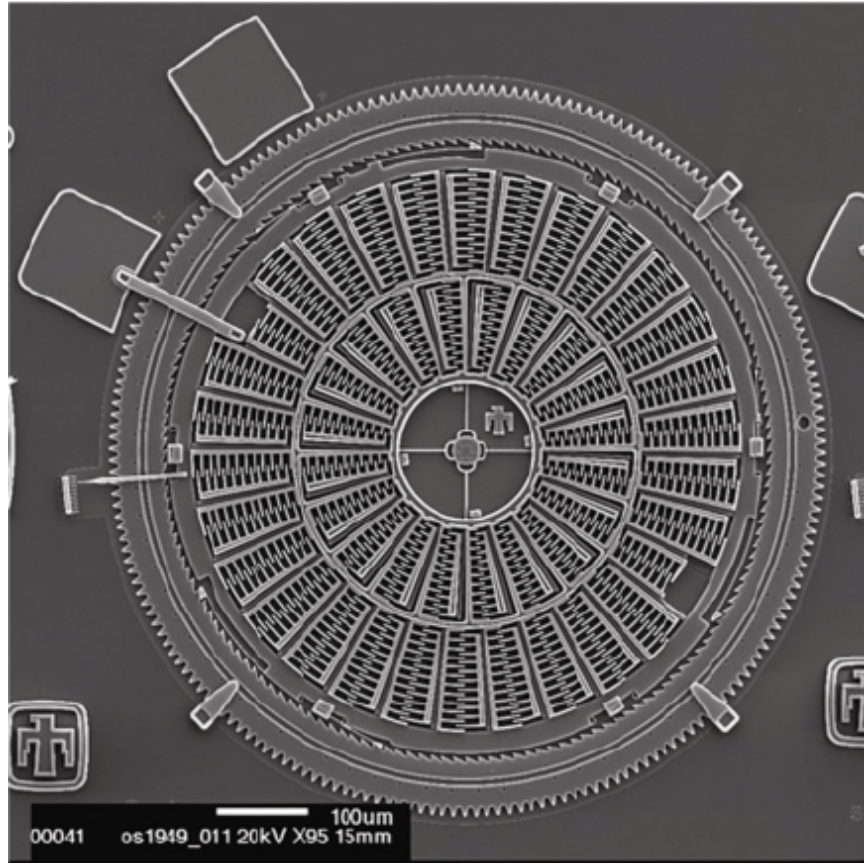


图3-6 扭转棘轮执行器（TRA）MEMS

如图3-6所示，该MEMS只有几百微米宽；需要扫描电子显微镜来显示图中可见的细节。微尺度传感器和执行器在日常物体中具有极大的可嵌入性，这是物联网的一个显著特点。基于这一原因，物联网有望引发MEMS技术和制造业的重大进步，并随着它们的广泛商业化，渗透到所有行业和垂直领域。

3.1.4 智能对象

简单地说，智能对象是物联网的基石。它们将日常物体转化为智能物体的网络，这些智能物体能够以一种有意义的方式从它们的环境中学习并与之交互。物联网中智能对象的真正力量来自于它们之间的互联，而不是被孤立的单独对象，这一点怎么强调都不为过。这种通过网络进行通信的能力具有倍增效应，并允许不同智能对象之间具有非常复杂的关联和交互。例如，回想一下前面描述的智能农业传感

器。如果一个传感器是一个独立的设备，它只是简单地测量土壤湿度，这很有趣也很有用，但它不是革命性的。如果把同一个传感器连接成智能网络的一部分，这个智能网络能够与执行器智能协调，根据传感器读数按需触发灌溉系统，我们就有了更强大的东西。进一步扩展，假设协调的传感器/执行器集与其他传感器/执行器集合智能地互连，从而进一步协调施肥、虫害控制等，甚至与智能后端通信来计算潜在的作物产量。现在，这看起来像是一个完整的系统，开始释放物联网的力量，并提供我们所期待的人工智能自动化，这是一项革命性的技术。

1. 智能对象：定义

从历史上看，由于智能对象有多种不同的解释，因此其定义一直比较模糊。更令人困惑的是，尽管智能对象在语义上存在一些差异，但它经常与智能传感器、智能设备、物联网设备、智能设备、物、智能物、智能节点、智能物、泛在物、智能产品等术语互换使用。为了澄清其中的一些困惑，我们在这里提供了在本书中使用的智能对象的定义。正如本书所描述的，智能对象是至少具有以下4个定义特征的设备（见图3-7）。

■ **处理单元：**智能对象具有某种类型的处理单元，用于获取数据，处理和分析传感器接收到的传感信息，协调控制信号到任意执行器，控制智能对象上的各种功能，包括通信和电力系统。根据不同应用程序的特定处理需求，所使用的特定处理单元类型可能会有很大差异。最常见的是微控制器，因为它具有体积小、灵活性强、编程简单、无处不在、低功耗、低成本等特性。

■ **传感器和/或执行器：**智能对象能够通过传感器和执行器与物理世界交互。如前几节所述，传感器学习并测量其环境，而执行器能够在物理世界中产生一些变化。智能对象不需要同时包含传感器和执行器。事实上，一个智能对象可以包含一个或多个传感器和/或执行器，这取决于应用程序。

■ **通信设备：**通信单元负责将智能对象与其他智能对象和外部世界（通过网络）连接起来。用于智能对象的通信设备可以是有线的，也可以是无线的。绝大多数情况下，在物联网网络中，智能对象通过无线连接的原因有很多，包括成本、有限的基础设施可用性以及易于部署等。智能对象有无数不同的通信协议。事实上，本书的大部分内容都是关于智能对象如何在物联网网络中通信的，尤其是第4章、第5章和第6章。因此，本章只提供一个高级概览，有关这个主题的细节请参阅其他各章。

■ **电源：**智能对象有需要供电的组件。有趣的是，最显著的功耗通常来自智能对象的通信单元。与其他三个智能对象构建块一样，不同的应用程序对电源的需求也有很大差异。通常，智能对象的能力有限，部署时间很长，并且不容易访问。这种因素组合起来，特别是当智能对象依赖于电池电源时，意味着电源效率、智能的电源管理、睡眠模式、超低功耗硬件等是关键的设计元素。对于长期部署的智能对象，出于所有实用目的，都是不可接近的，电力通常通过太阳能、压电材料等获得，或者以混合方式获得，也可以使用基础设施的电力。

2. 智能对象的发展趋势

如定义所示，智能对象的关键特征可能是可变性。它们在功能、技术需求、体积、部署条件等方面差异很大。然而，我们可以从最近和计划的未来智能对象部署中推断出某些重要的宏观趋势。当然，这些并不适用于所有智能对象，因为总会有依赖于应用程序的可变性，但这些都是影响物联网的广义概括和趋势。

■ **体积正在减小：**如前所述，在MEMS中，体积有不断减小的明显趋势。有些智能物体很小，甚至肉眼都看不见。这种缩小的体积使智能对象更容易嵌入到日常对象中。

■ **功耗正在下降：**智能对象的不同硬件组件持续地消耗更少的功耗。对于很多无源传感器来说尤其如此。一些使用电池供电的传感器在不更换电池的情况下可以使用10年或更长时间。

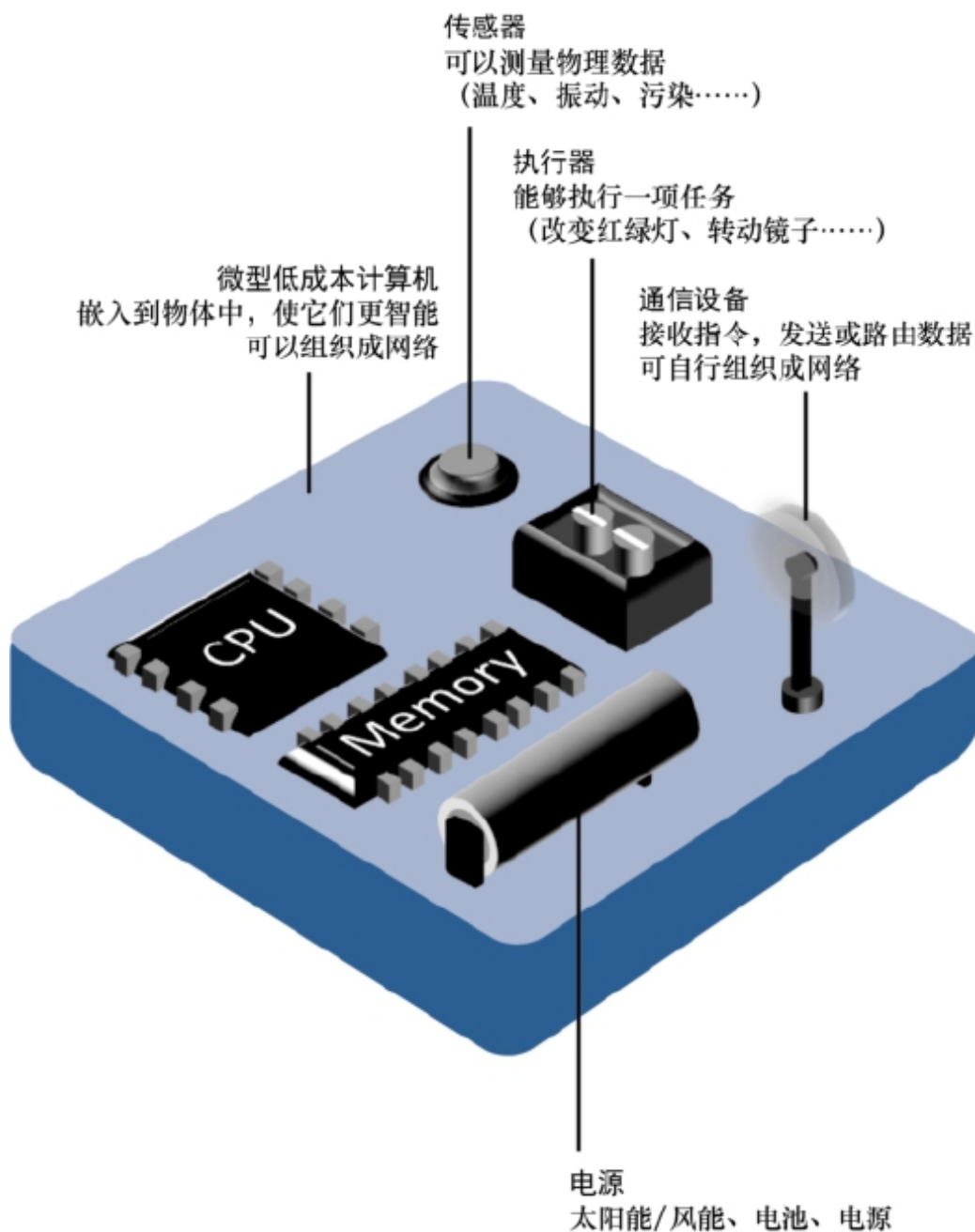


图3-7 智能对象的特征

■ 处理能力正在增加：处理器越来越小，性能越来越强大。对于智能对象来说，这是一个关键的进步，因为它们变得越来越复杂和越来越相关。

■ 通信能力正在提高：无线速度不断提高并不令人惊讶，但它们的范围也在扩大。物联网正在推动越来越多的专用通信协议的发展，

这些协议涵盖了更多多样化的用例和环境。

■ 通信正日益标准化：业界大力推动为物联网通信协议开发开放标准。此外，有越来越多的开源力量来推进物联网的发展。

智能对象的这些趋势开始描绘出一幅画面：越来越复杂的设备能够以更高的效率执行越来越复杂的任务。这里的一个关键支持因素是系统内相互连接的智能对象之间以及系统与外部实体（例如边缘计算、云）之间的通信得以提升。当智能对象在传感器/执行器网络中协同工作时，物联网的力量才真正得到释放。

3.2 传感器网络

顾名思义，传感器/执行器网络（SANET）是一个传感器网络，可以感知、测量环境和/或在环境中运行的执行器。SANET中的传感器和/或执行器能够以有效的方式进行通信和合作。有效和协调的沟通与合作是一个突出的挑战，主要是因为SANET中的传感器和执行器多种多样、结构不同而且受限于资源。

SANET可以提供高度协调的感知和驱动能力。智能家居就是一种SANET，它体现了分布式传感器和执行器之间的这种协调。

例如，智能家居可以有温度传感器，这些温度传感器与供暖、通风和空调（HVAC）执行器有策略地联网。当传感器检测到指定的温度时，可以触发执行器采取行动，并根据需要对房屋进行加热或制冷。

虽然这些网络理论上可以有有线或无线的方式连接，但SANET通常出现在“现实世界”中，这意味着它们需要极高的部署灵活性。例如，智能家居温度传感器需要安装在整个家居的战略位置，包括HVAC入口和出口点。

以下是无线解决方案的一些优点和缺点。

优点：

- 更大的部署灵活性（特别是在极端环境或难以到达的地方）；
- 能够更简单地扩展到大量节点；
- 实现成本降低；
- 更容易长期维护；
- 可以毫不费力地引入新的传感器/执行器节点；
- 更好地处理动态/快速拓扑更改。

缺点：

- 不太安全（例如，AP被劫持）；
- 通常传输速度较低；
- 更大程度的环境影响。

无线技术不仅具有更大的灵活性，而且在非常广泛的范围内（甚至在非常苛刻的条件下），它也是一种越来越便宜和可靠的技术。这些特性是无线SANET成为物联网网络技术的关键原因。

注释：从术语的角度来看，无线SANET通常被称为无线传感器和执行器网络（WSAN）。由于许多物联网部署绝大多数是传感器，因此WSAN通常也可称为无线传感器网络（WSN）并与之互用。在本书中，我们通常将WSAN称为WSN，并知道执行器通常是无线网络的一部分。

3.2.1 无线传感器网络（WSN）

无线传感器网络由无线连接的智能物体组成，这些智能物体有时被称为微节点。无线传感器网络无需考虑基础设施，这对于灵活部署

来说无疑是一个强大的优势，但对于这些无线连接的智能对象，需要考虑各种设计限制。图3-8说明了WSN中通常涉及的一些假设和限制。

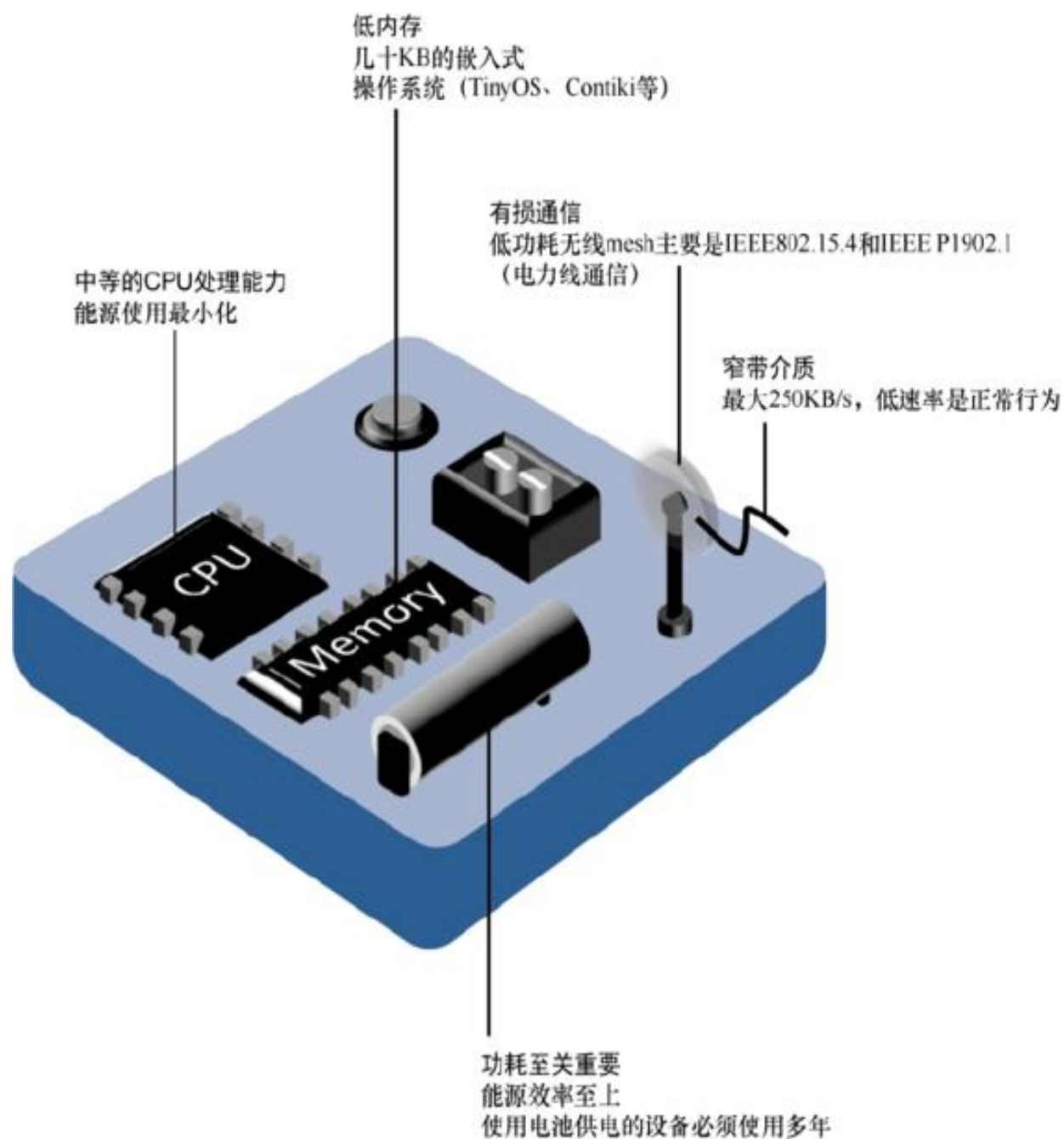


图3-8 无线智能对象的设计缺陷

以下是WSN中智能对象的一些重要限制：

- 有限的处理能力；

- 有限的内存;
- 有损的沟通;
- 有限的传输速度;
- 有限功率。

这些限制极大地影响了WSN的设计、部署和使用。单个传感器节点通常非常有限，这是它们经常大量部署的原因之一。随着传感器节点的成本不断下降，部署高冗余传感器的能力变得越来越可行。由于许多传感器非常便宜，而且准确性也差一些，因此通过冗余部署智能对象可提高精度。

注释：具有有限处理、内存、电源等功能的智能对象经常被称为约束节点。第5章将更详细地讨论约束节点。

如此大量的传感器需要引入智能对象的层次结构。除了其他组织优势外，这种层次结构还可以将彼此接近的传感器节点的类似读数聚合起来。图3-9显示了WSN中此类数据聚合功能的一个示例，其中来自温度传感器逻辑组的温度读数聚合为平均温度读数。

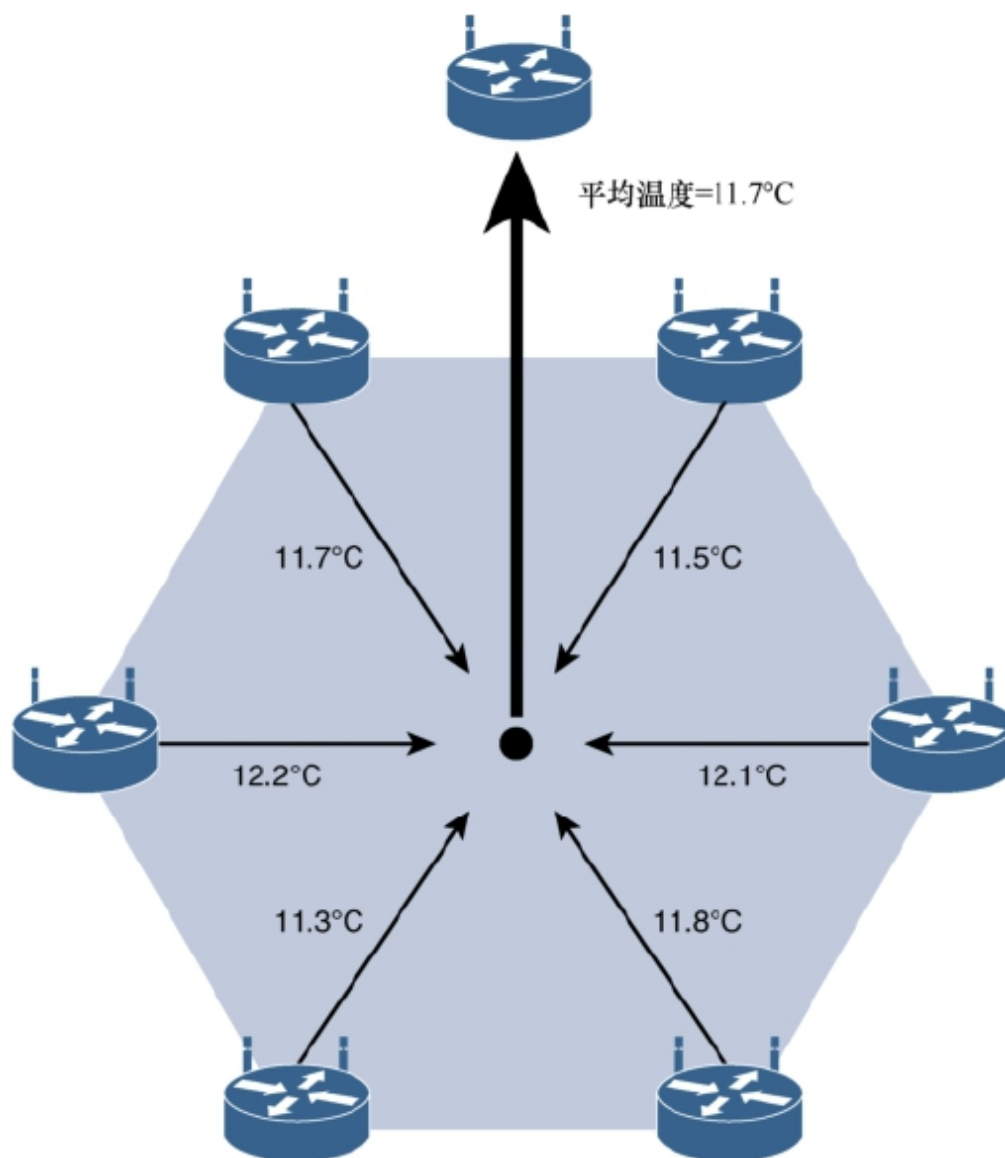


图3-9 无线传感器网络中的数据聚合

这些数据聚合技术有助于减少部署了大量智能对象的WSN中的总通信量（和能耗）。这种在网络边缘的数据聚合是通过雾计算和薄雾计算实现的，后两者可以用来交付众多物联网用例所需的规模和性能。虽然在某些情况下，传感器会不断地传输它们的测量数据，但通常情况并非如此。无线连接的智能对象通常具有以下两种通信模式。

■ **事件驱动：**只有当智能设备检测到特定的事件或预先设定的阈值时，才会触发感知信息的传输。

■ 周期性：感知信息的传递只在周期性的时间间隔内发生。

使用哪种通信方案在很大程度上取决于具体的应用。例如，在一些医疗用例中，传感器定期发送术后生命体征，如体温或血压读数。在其他医疗用例中，只有在测量到某些非常低或非常高的读数时，才触发发送相同的血压或温度读数。

随着无线传感器网络中的智能对象越来越多，产生了这样一种趋势，即自主性水平越来越高。例如，手工配置潜在的数千个智能对象是不切实际和笨拙的，因此WSN中的智能对象通常是在后台由物联网管理平台进行自配置或自动化的。同样，在大规模无线传感器网络的众多节点之间建立内聚通信也需要额外的自治功能，这些节点通常是临时部署，不考虑节点的均匀分布和/或密度。例如，“智能尘埃”应用的趋势越来越明显，其中非常小的传感器节点（即MEMS）分散在一个地理区域内，用于检测振动、温度、湿度等。这种技术实际上具有无限的能力，如军事（例如，探测敌军移动）、环境（例如，探测地震或森林火灾）和工业（例如，探测制造异常和资产跟踪）。将无线智能对象的SCAD联网需要一定程度的自组织，以便这些节点能够自主地聚集在一起，形成具有共同目的的真正网络。这种自组织能力能够适应和演化WSN的逻辑拓扑结构，从而优化通信（节点之间以及集中式无线控制器之间的通信），简化新智能对象的引入，提高可靠性和对服务的访问。

部署大量低成本无线智能对象的额外优势是可以提供容错、可靠性，以及延长WSN寿命，特别是在智能对象电池寿命有限的情况下。自治技术，如自我修复、自我保护和自我优化，经常用来代表一个整体的WSN系统执行这些功能。物联网应用往往是关键任务，在大规模的WSN中，即使环境突然发生变化，无线通信暂时丢失，或者有限数量的节点的电池电量耗尽或功能不正常，整个系统都不会出现故障。

3.2.2 无线传感器网络的通信协议

传感器和执行器的类型有成千上万种。更复杂的是，WSN正变得越来越异构，交互也越来越复杂。这种异质性表现在许多方面。例如，WSN网络正经历着从主要由单一类型传感器组成的同构无线网络到由多种类型的传感器组成的网络的转变。这些传感器甚至可以是许多廉价传感器和昂贵传感器（用于特定的高精度功能）的混合。无线传感器网络也正在从单用途网络向更灵活的多用途网络发展，可以在任何给定时间为多个不同的应用程序使用特定的传感器类型。假设一个WSN有多种类型的传感器，其中一种是温度传感器，可以灵活地同时用于环境应用、天气应用和智能农业应用。

在这样一个异构的环境中，通过受限的设备与复杂的交互进行协调通信是一个相当大的挑战。控制无线传感器网络通信的协议必须处理无线传感器网络固有的定义特征及其内部受限的设备。例如，任何通信协议都必须能够扩展到大量节点。同样，在选择通信协议时，必须仔细考虑特定应用程序的需求，并考虑通信协议在功耗、最大传输速度、范围、包丢失容忍度、拓扑优化、安全性等方面所提供的任何折衷。无线传感器网络通常部署在恶劣和不可预测的环境中，这一事实增加了另一个需要考虑的变量，因为显然不是所有的通信协议都设计得同样坚固。除了上述技术功能之外，它们还必须根据需要启用上一节中提到的自治技术（例如，自组织、自修复、自配置）。

无线传感器网络与其环境进行交互。传感器通常产生大量需要处理的传感和测量数据。这些数据可以由无线传感器网络的节点进行本地处理，也可以在物联网网络中跨零个或多个层次进行处理（详见第2章）。通信协议需要促进传感器节点之间以及从传感器节点到可选网关、边缘计算或集中式云计算之间的数据流的路由和消息处理。因此，无线传感器网络的物联网通信协议横跨整个协议栈。最终，它们被用来为各种物联网智能服务提供一个平台。

与任何其他网络应用程序一样，为了在多厂商环境中进行互操作，这些通信协议必须标准化。这是物联网的关键依赖，也是最重要的成功因素之一。物联网是影响所有垂直领域和行业的罕见技术之一，这意味着通信协议的标准化是一项复杂的任务，需要跨栈的多层协议定义，以及跨多个标准开发组织的大量协调。

最近，人们集中精力对物联网的通信协议进行标准化，但与任何重大技术的采用一样，市场也出现了一些分化。虽然没有单一的协议解决方案，但围绕几个关键通信协议的市场融合已经开始显现。我们不在此处花时间讨论这些特定的协议及其详细的操作，因为本书的大部分内容都专门讨论这些协议，包括第4章～第6章。

3.3 小结

无线传感器和执行器网络是一种独特的计算平台，可以高度分布并部署在传统计算平台通常无法实现的独特环境中。这提供了与这些环境交互和影响的独特优势和机会。这是物联网的基础，它开启了一个充满可能性的世界，在日常物品中嵌入传感器和/或执行器，并将它们联网，使复杂而协调良好的自动化成为可能，从而改善和简化我们的生活。

本章介绍了物联网的基本组成部分。它包括传感器的描述和实际示例，以及它们如何能够测量所处的环境。本章同样讨论了执行器，执行器以一种互补的方式使用环境传感信息来对其周围环境起作用。本章还重点介绍了最近的制造趋势（如MEMS），这使得传感器和执行器更小，更可嵌入到日常物品中。本章还讨论了智能对象，这些对象通常是高度受限的设备，具有传感器和/或执行器，以及非常有限的功率、传输和计算能力。

正如本章所讨论的，我们通过联接智能对象来释放物联网的力量。本章讨论了传感器和执行器网络（SANET），并给出了无线传感器网络（WSN）的泛在用例的细节。本章讨论的最后一个主题是WSAN的通信协议，它将为下一章关于连接智能对象的内容做好准备。

第4章 连接智能对象

物联网设备和传感器必须连接到网络，以便利用它们的数据。除了组成物联网的各种传感器、执行器和智能对象之外，还有许多不同的协议用于连接它们。本章将介绍智能对象连接所用的技术的重要特征和通信标准，以及当前部署的一些主要技术。

本章分为两节。4.1节描述了在选择和处理连接智能对象时应该考虑的特性和属性。根据在对传感器进行分析时所采用的标准，用于连接传感器的各种技术可能会有很大的不同。4.1节将仔细研究这些标准。

- 覆盖范围：讨论信号传播和距离的重要性。

- 频段：描述已授权和未授权的频段，包括亚GHz频率。

- 功耗：讨论与电池供电的设备相比，连接到稳定电源的设备需要考虑的问题。

- 拓扑结构：重点介绍连接多个智能对象时可能支持的各种布局。

- 受限设备：从连接的角度详细说明某些智能对象的限制。

- 受限节点网络：重点介绍连接智能对象的网络时经常遇到的挑战。

4.2节深入介绍了连接智能对象时需要考虑的一些技术。目前，连接智能对象的技术数量相当广泛，但你应该期待进行整合，某些协议最终会在各种物联网细分市场中战胜其他协议。

本节有意将传感器连接技术的讨论限制在物联网市场最有前景的技术上，其他技术在适用时将在上下文中提到。以下小节介绍连接智

能对象的技术。

■ IEEE 802.15.4：重点介绍IEEE 802.15.4，这是一种早期用于连接智能对象的基本无线协议。

■ IEEE 802.15.4g 和 IEEE 802.15.4e：讨论针对公用事业和智慧城市部署的802.15.4的改进。

■ IEEE 1901.2a：讨论IEEE 1901.2a，这是一种通过电力线连接智能对象的技术。

■ IEEE 802.11ah：讨论IEEE 802.11ah，这是一种基于著名的802.11 WiFi标准的技术，专门针对智能对象。

■ LoRaWAN：LoRaWAN是一种可扩展的技术，适用于无授权频段中长距离、低功耗的要求。

■ NB-IoT和其他LTE变体：讨论NB-IoT和其他LTE变体，这些变体通常是希望在授权频段中连接更远距离智能对象的移动服务提供商的选择。

本章涵盖了相当多的物联网基础技术，对于真正理解智能对象如何处理网络之间的数据传输至关重要。建议读者特别注意这里讨论的协议和技术，因为它们在本书的许多其他章节中都得到了应用和引用。

4.1 通信标准

在连接“物”的世界中，有大量有线和无线接入技术可供使用或正在开发中。在回顾这些接入技术之前，讨论一下在评估各种用例和系统解决方案时使用的标准是很重要的。

无线通信在智能对象相互连接的世界中非常流行，主要是因为它简化了部署，并允许智能对象移动，在不丢失连接的情况下改变位

置。下文在讨论各种标准时考虑到了这一点。此外，在适用时还会提到有线连接注意事项。

4.1.1 覆盖范围

信号需要传播多远？也就是说，所选的无线技术的覆盖范围是什么？室内部署和室外部署应该区别对待吗？通常在讨论有线和无线接入技术时，首先要问的问题就是这些。

回答这类问题最简单的方法是对这些技术进行分类，如图4-1所示，将它们划分为以下范围。

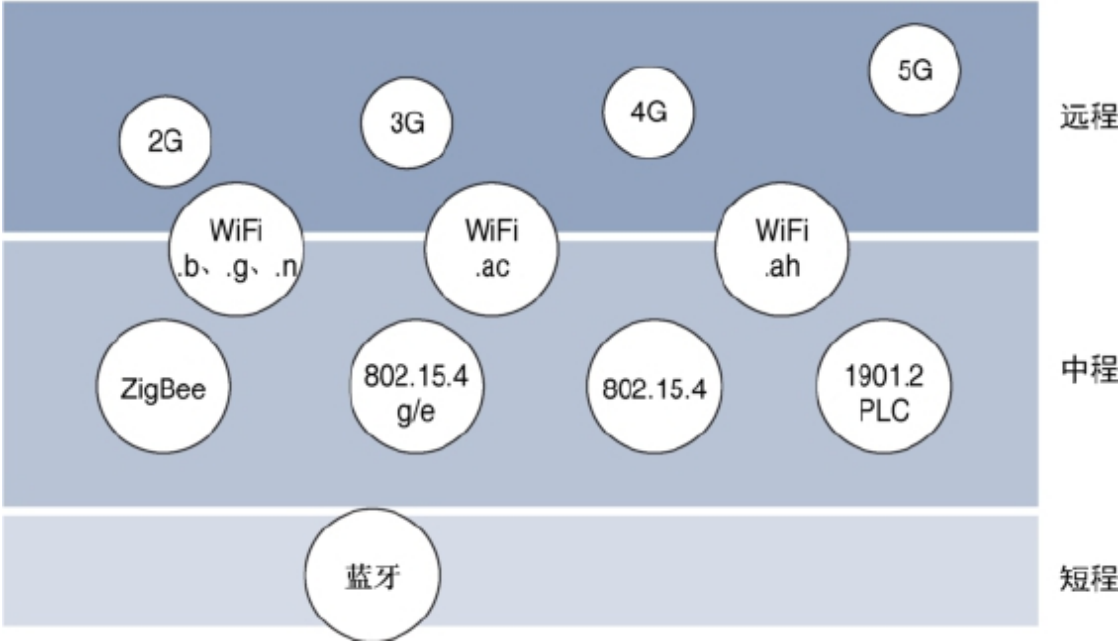


图4-1 无线接入分类

注释：图4-1聚焦于本章讨论的物联网技术。为了避免在讨论当今市场上众多物联网技术时造成太多混淆，本章只讨论那些应用广泛且稳定的技术。

■ 短程：典型的有线示例是串行电缆。无线短程技术通常被认为是串行电缆的替代品，两个设备之间的最远通信距离可达10米。短程无线技术的例子有IEEE 802.15.1蓝牙和IEEE 802.15.7可见光通信

（VLC）。这些短程通信方法只存在于少数物联网安装中。在某些情况下，它们还不够成熟，无法用于生产部署。

■ 中程：这一范围是物联网接入技术的主要范畴。在几十米到几百米的范围内，有许多规范和实现。两个设备之间的最大距离一般小于1公里，但只要无线电信号在适用规范的范围内发射和接收，RF技术就没有实际定义的最远距离。中程无线技术的例子包括IEEE 802.11 WiFi、IEEE 802.15.4和802.15.4g WPAN。根据物理介质特性，IEEE 802.3以太网和IEEE 1901.2窄带电力线通信（PLC）等有线技术也可分为中程技术（本章后面将更详细地讨论刚才提到的所有中程协议）。

■ 远程：两台设备之间超过1公里的距离时需要远程技术。无线的示例有蜂窝（2G、3G、4G）和一些户外IEEE 802.11 WiFi及低功耗广域（LPWA）技术的应用。LPWA通信能够在不消耗大量电力的情况下进行大面积的通信。因此，这些技术是采用电池供电的物联网传感器的理想选择（本章稍后将更详细地讨论LPWA和刚才提到的其他示例）。IEEE 802.3光纤通信和IEEE 1901宽带电力线通信主要应用于工业网络中，属于长距离通信，但并不属于真正的物联网接入技术。

对于无线部署，以规范或产品描述表示的最大覆盖范围通常由最优估计条件得出。在现实世界中，规划者应该使用适当的工具进行适当的无线电规划，然后进行现场无线勘查以便更好地了解给定地区的实际情况。此外，还需要考虑环境因素，如干扰和噪声，以及特定的产品特性，如天线设计和发射功率，最后，规划者应该了解该领域潜在的场景和拓扑变化，例如新建筑可能会干扰信号传输。

4.1.2 频段

无线电频段由国家和/或组织管理，如国际电信联盟（ITU）和联邦通信委员会（FCC）。这些组织定义了各种频段的规则和传输要求。例如，频段的一部分被分配给各种类型的远程通信中，如无线电广播、电视、军事等。

在世界范围内，各种通信用途的频段通常被视为一种关键资源。例如，可以通过检查移动运营商为蜂窝频段许可证支付的成本来了解这些频率的价值。

就物联网接入技术来说，无线通信使用的频段分为许可频段和未经许可频段。许可频段一般适用于物联网远程接入技术，并分配给服务提供商、公共服务（例如，紧急救援、军方）、广播公司和公用事业公司部署的通信基础设施。

对于希望利用许可频段的物联网接入基础设施，一个重要的考虑因素是，用户在连接物联网设备时必须订阅服务。这增加了部署大量传感器和其他物联网设备的复杂性，但由于服务是付费的，因此网络运营商可以保证在目标区域独自使用频率，可以提供更好的服务保证。

在许可频段中部署大量设备时存在一些固有的复杂性，不过这些复杂性的处理已经出现了改进。由于物联网平台的发展，例如Cisco Jasper控制中心的出现，大量设备的自动配置、部署和管理变得容易得多。通常用于物联网接入的许可频段包括蜂窝网络、WiMAX和窄带物联网（NB-IoT）技术。

注释：许可频段中存在例外。例如，数字增强无绳电信（DECT）无线技术在以1.9 GHz为核心的许可频段运行，但不收取使用费。因此，DECT超低能耗（ULE）被定义为许可频段中的物联网无线通信标准，但它不需要服务提供商。

国际电联还为无线电频段的工业、科学和医学（ISM）部分定义了未经许可的频段。这些频率用于许多短程设备（SRD）的通信技术中。“未经许可”意味着在ISM频段中没有为设备通信提供任何保证或保护。对于物联网接入，以下是最著名的ISM频段。

- 2.4 GHz频段采用IEEE 802.11b/g/n WiFi。

- IEEE 802.15.1蓝牙。

- IEEE 802.15.4 WPAN。

注释：IEEE 802.15.1 蓝牙较小的覆盖范围限制了其在大多数物联网部署中的实用性。

未经许可的频段（例如ISM频率范围内的频段）并非不受监管。每个已分配的频段都有国家和区域规定（与许可频段相同）。这些规定要求设备的传输功率、占空比和停留时间、信道带宽和信道跳变等参数符合要求。

未经许可的频段通常比许可频段更容易部署，因为它不需要服务提供者。然而，它可能会受到更多的干扰，因为其他设备可能在某个特定区域竞争相同的频率。这成为物联网部署决策的一个关键因素。物联网基础设施是应该利用专用网络的未经许可频段，还是依赖于服务提供商的许可频段？在回答这个问题时，各种LPWA技术正变得越来越重要。除满足低功耗要求外，LPWA通信还能够覆盖长距离通信，而在过去，这需要提供商为蜂窝设备提供许可频段。

ISM频段内的一些通信在亚GHz范围内运行。亚GHz频段被IEEE 802.15.4、802.15.4g和802.11ah等协议以及LoRa和Sigfox等LPWA技术使用（本章稍后将更详细地讨论这些技术）。

传输频率直接影响信号的传播方式以及实际的最大范围（本章前面讨论了范围及其对物联网接入的重要性）。无论是室内部署还是室外部署，亚GHz频段都允许设备之间有更大的距离。与2.4 GHz ISM频段相比，这些频段具有更好的穿透建筑基础设施或绕过障碍物的能力，同时传输功率保持在规定范围内。

亚GHz频段的缺点是，与高频段相比，其数据传输速率较低。然而，大多数物联网传感器不需要高速率来发送数据。因此，对于IoT传感器部署，低传输速度的亚GHz技术通常不是问题。

例如，在大多数欧洲国家，169MHz频段通常被认为最适合无线水气计量应用。这是因为它的信号能够穿透深层建筑地下室。此外，该频率的低数据速率与需要传输的低数据量相匹配。

ISM频段定义了几个亚GHz范围，主要集中在169MHz、433MHz、868MHz和915MHz。然而，大多数物联网接入技术往往集中在868MHz和915MHz附近的两个亚GHz频段。这些主要频段在世界各地普遍存在，几乎适用于所有国家/地区。

注释：国家/地区也可指定其他非许可频段。例如，中国大陆地区已经按照LoRaWAN 1.0规范和IEEE 802.15.4g标准提供了779~787 MHz频段。

欧洲邮电管理委员会（CEPT）在欧洲无线电通信委员会（ERC）Recommendation 70-03中规定了868MHz频段。CEPT成立于1959年，是欧洲国家电信和邮政组织的协调机构。欧洲国家一般将Recommendation 70-03应用于其国家电信法规，但868MHz的定义也适用于欧洲以外的地区和国家。例如，印度、中东、非洲和俄罗斯采纳了CEPT的定义，其中一些国家作了小的修改。Recommendation 70-03主要描述了863~870MHz频段的使用、允许的发射功率或EIRP（等效全向辐射功率）和占空比（即设备在传输中处于活动状态的时间百分比）。EIRP是天线在最大增益方向上产生峰值功率密度时所需发射的功率量。868MHz频段适用于IEEE 802.15.4、802.15.4g、802.11ah、LoRaWAN等物联网接入技术（本章稍后将介绍这些协议）。

注释：在最新版本的ERC Recommendation 70-03（2015年5月起）中，CEPT引入了新的870~876MHz频段。该频段与物联网无线接入解决方案有关。然而，将其应用于国家的法规中仍然是一个正在进行的过程。IEEE 802.15.4v草案和Wi-SUN 1.0区域PHY层参数中引用了这个新频段（本章稍后将讨论Wi-SUN 1.0）。

北美地区主要使用的未经许可亚GHz频段是以915MHz为中心的902~928 MHz频段，符合FCC规定（FCC 15.247部分）。世界上不符合CEPT ERC Recommendation 70-03的国家通常认可在其国家规定中使用902~928 MHz范围或其子集。例如，巴西的ANATEL监管机构定义了902~907.5和915~928 MHz范围的使用（ANATEL506），日本的ARIB监管机构规定了920~928 MHz范围（ARIB-T108），澳大利亚的ACMA提供了915~928 MHz范围的建议。如前所述，即使这些频段是未经许可的，

它们也会受到监管。监管机构会记录参数，如通道带宽、通道跳变、传输功率或EIRP以及驻留时间。

综上所述，在实施或部署物联网智能对象时，我们应该考虑到一个国家/地区的频率和相应的法规，优化运行在未经许可频段上的智能对象硬件，以支持全球两个主要的亚 GHz频率：868 MHz和915 MHz。然而，发射功率、天线和EIRP等参数的设计必须符合各国家/地区法规的要求。

4.1.3 能耗

虽然物联网设备的定义非常广泛，但在供电节点和电池供电节点之间有明确的界限。供电节点与电源直接连接，通信通常不受功耗标准的限制。然而，电源的可用性限制了电源节点部署的便利性，这使得移动性更加复杂。

电池供电的节点为物联网设备带来了更大的灵活性。这些节点通常根据电池的使用寿命进行分类。比如水表或煤气表的节点是否需要10~15年的电池寿命？5~7年的电池续航时间是否足够智能泊车传感器等设备使用？当重新铺设街道路面时，它们的电池可以更换，或者设备可以更换。对于定期保养的设备，可选择使用寿命为2~3年的电池。

物联网无线接入技术必须解决电池供电节点低功耗和连通性的需求。这导致了一种新的无线环境的进化，称为低功耗广域网络（LPWA）。显然，任何无线技术都可以使用电池来运行。然而在现实中，如果每个月都必须更换数百个电池，则无法进行任何操作部署。

由供电节点组成的有线物联网接入技术也不例外。在通过PLC部署智能电表的情况下，电表上的无线接口不能消耗5~10W的电力，否则需要部署的电表数将高达2000万部，这将要消耗100~200MW的能源用于通信。

4.1.4 拓扑结构

在可用于连接物联网设备的接入技术中，有3种主要的拓扑方案占主导地位：星型、网状和点对点。对于远程和短程技术，星形拓扑结构非常流行，如蜂窝网络、LPWA和蓝牙网络。星型拓扑使用单个中央基站或控制器来与端点通信。

对于中程技术，星型、点对点或网状拓扑都比较常见，如图4-2所示。点对点拓扑允许任何设备与任何其他设备通信，只要它们在彼此的通信范围内。显然，点对点拓扑依赖于多个全功能设备。点对点拓扑支持更复杂的结构，比如网状拓扑。

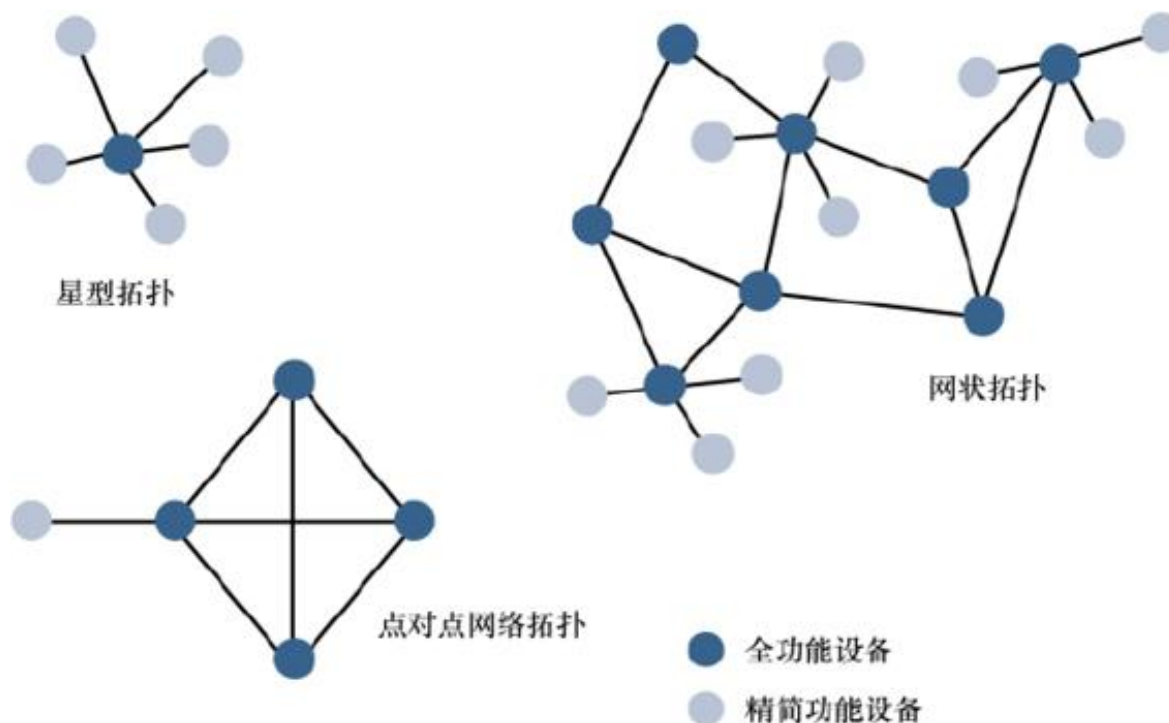


图4-2 星型、点对点和网状拓扑

例如，室内WiFi部署主要是一组节点围绕接入点（AP）来形成星型拓扑结构。而户外WiFi可以由AP主干的网状拓扑组成，节点以星型拓扑连接到AP。同样，IEEE 802.15.4和802.15.4g，甚至有线的IEEE 1901.2a PLC一般都采用网状拓扑结构来部署。网状拓扑有助于处理低

传输功率、寻求更大的总距离，以及通过中间节点为其他节点中继流量来解决通信覆盖的问题。

网状拓扑要求在每个中间节点上实现称为mesh-under的第2层转发协议或称为mesh-over的第3层转发协议（更多信息请参见第5章）。正如在第2章讨论的，中间节点或全功能设备（FFD）只是连接其他节点的节点。一个不互连或不中继其他节点的流量的节点称为叶节点，或精简功能设备（RFD）（本章稍后还将介绍关于全功能和精简功能设备的更多信息）。

尽管网状拓扑能够很好地用于供电节点，但针对电池供电节点进行实施时需要适当的优化。电池供电的节点通常处于“休眠模式”，以在不传输时保持电池寿命。在网状拓扑的情况下，电池供电的节点要么作为叶子节点，要么在用作中间节点时作为“最后的资源路径”来转发流量。否则，电池寿命将大大缩短。对于电池供电的节点，拓扑类型和节点在拓扑中的角色（例如，作为中间节点或叶子节点）是成功实施的重要因素。

4.1.5 受限设备

互联网工程任务组（IETF）在RFC 7228中承认已部署了不同类别的物联网设备。虽然对物联网节点进行分类是一项艰巨的任务，但随着计算、内存、存储、电源和网络的不断发展和改进，RFC 7228给出了一些受限节点的定义。这些定义有助于区分受限节点和不受限节点，例如服务器、台式机或便携式计算机以及功能强大的移动设备（如智能手机）。

受限节点具有影响其网络特性集和功能的有限资源。因此，某些类别的物联网节点无法实现IP堆栈。根据RFC 7228，受限节点可以细分为表4-1中定义的类。

表4-1 RFC 7228所定义的受限节点的类

分类	定义
类别 0	这类节点受到严重限制，内存不足 10KB，闪存处理和存储能力不足 100KB。这些节点通常由电池供电。它们没有直接实现 IP 堆栈和相关安全机制所需的资源。类别 0 节点的一个示例是一个按钮，它在改变状态时发送一个字节的的信息。这个类特别适用于新的未经许可的 LPWA 无线技术
类别 1	虽然处理和代码空间大于类别 0，但是类别 1 的处理和代码空间（大约 10KB RAM 和大约 100KB Flash）仍然低于完整 IP 堆栈实现的预期。它们无法轻松地与使用完整 IP 堆栈的节点通信。但是，这些节点可以实现专为受限节点设计的优化堆栈，比如受限应用协议（CoAP）。这允许类别 1 节点无须网关即可与网络进行有意义的对话，并为必要的安全功能提供支持。环境传感器是类别 1 节点的一个示例
类别 2	类别 2 节点的特征是在嵌入式设备上运行完整的 IP 堆栈实现。它们包含超过 50KB 的内存和 250KB 的闪存，因此可以完全集成到 IP 网络中。智能电表就是类别 2 节点的一个例子

4.1.6 受限节点网络

虽然一些物联网接入技术（例如WiFi和蜂窝网络）适用于笔记本电脑、智能手机和一些物联网设备，但还有一些物联网接入技术更适合于连接受限节点。典型的示例有IEEE 802.15.4和802.15.4g RF、IEEE 1901.2a PLC、LPWA和IEEE 802.11ah接入技术（本章稍后将更详细地讨论这些技术）。

受限节点网络通常被称为低功耗有损网络（LLN）（有关LLN的更多详细信息，请参见第5章）。低功耗指的是节点必须满足来自电源和电池供电的受限节点的需求。有损网络表明，由于恶劣的无线环境，网络性能可能会受到干扰和变化的影响。可以用于受限节点网络的第1层和第2层协议必须根据以下特征来评估用例适用性：数据速率和吞吐量、延迟和可靠性、开销和负载。

1. 数据速率和吞吐量

物联网接入技术提供的数据速率从100bit/s（采用Sigfox等协议）到每秒数十兆比特（采用LTE和IEEE 802.11ac等技术）不等（本章稍后将讨论Sigfox、LTE和IEEE 802.11ac）。然而，实际的吞吐量要比数据速率低（有时甚至比数据速率低得多）。因此，理解特定技术的带宽需求、针对给定用例的适用性、容量规划规则和预期的实际吞吐量对于正确的网络设计和成功的设备部署非常重要。

即使不是专门为物联网设计的技术，例如蜂窝网络和WiFi，也可以很好地匹配高带宽要求的物联网应用。例如，涉及视频分析的节点需要高数据速率。这些节点位于零售、机场和智慧城市环境中，用于检测事件和驱动操作。由于这些类型的物联网端点在计算或网络带宽方面不受限制，设计指南往往侧重于应用程序需求，如延迟和可靠性（本章稍后将更详细地讨论延迟和可靠性）。

短程技术还可以提供中到高的数据速率，这些速率具有足够的吞吐量来连接几个端点。例如，现在出现在可穿戴设备上的蓝牙传感器就属于这一类。在这种情况下，解决方案更多地关注内存占用和电池寿命，而不是数据速率。

为受限节点开发的物联网接入技术针对低功耗进行了优化，但在数据速率方面依然受限，数据速率取决于选择的频段和吞吐量。

数据速率范围为 100bit/s~1Mbit/s，这可能使我们回想起带宽是一种稀缺资源的年代。我们通常需要一些专业知识来了解如何设计这样的网络。如今，这种专业知识对LPWA网络很有帮助，因为在设计LPWA网络时是假定每天或每个端点的消息是定量的，而不仅是有一个纯粹的带宽使用限制。此外，在接入网状拓扑时，应用程序的行为（如轮询的频率）会对设计产生影响，因为所有设备共享受限的带宽容量。

在讨论LLN中的数据速率和带宽时，必须包括应用程序所看到的实际吞吐量。尽管对于每天只发送一条消息的受限节点来说，实际吞吐量可能并不重要，但是对于实现IP堆栈的受限设备来说，实际吞吐量

非常重要。在这种情况下，即使节点在给定时间获得了整个受限网络，其吞吐量在数据速率中的占比也不大。

以一个IEEE 802.15.4g子网为例，它在915MHz频段以150kbit/s实现2FSK调制（IEEE 802.15.4g协议将在本章后面详细介绍）。为了覆盖传输距离的边界，提升无线信号质量，将启用前向纠错（FEC），将数据速率从150kbit/s降低到75kbit/s。如果现在添加协议堆栈开销、双向通信处理、可变的数据负载大小，则最终的最大吞吐量为30~40kbit/s。这必须被视为最佳值，因为同时通信的设备数量、拓扑结构和控制平面开销也会影响吞吐量。

物联网设备的另一个特点是，大多数设备会发起通信。流向应用服务器的上游流量通常比来自应用服务器的下游流量更常见。理解这种行为也有助于部署不对称的物联网接入技术（如蜂窝网络），因为上游带宽必须被视为分析网络容量的一个关键参数。

2. 延迟和可靠性

与吞吐量需求非常相似，选择接入技术时应该了解物联网应用程序的延迟预期。对于无线网络尤其如此，在无线网络中，由于干扰、冲突和噪声而造成的数据包丢失和重传属于正常现象。

在受限网络上，延迟可能从几毫秒到几秒不等，应用程序和协议栈必须处理这些范围广泛的值。例如，强烈建议将传输层的UDP用于通过LLN通信的IP端点。在网状拓扑的情况下，如果网络内的两个设备之间需要通信，转发路径可能需要进行路由优化，而这可以使用IPv6 RPL协议（有关RPL的更多信息，请参见第5章）。

注释：当延迟问题较严重时，应该考虑紧急接入技术，如确定性以太网或IEEE 802.15.4e的时隙信道跳变（Time-Slotted Channel Hopping, TSCH）模式。然而，其中一些解决方案还不够成熟，无法用于生产部署（有关TSCH的更多信息，请参见第5章。本章稍后将讨论802.15.4e协议）。

3. 开销和载荷

在考虑受限接入网络技术时，重要的是考虑应用程序所需的MAC载荷大小。此外，我们应该了解针对IP的任何要求。IPv6 MTU的最小值应为1280字节。因此，具有较小MTU的链路层接入协议必须考虑IPv6载荷的分片。

注释：在物联网设备上使用IP是一个公开讨论的话题。本章前面提到，IETF承认存在不同种类的物联网设备。对于更为受限的设备类别，如类别0和类别1设备，通常不可能实现一个完整的IP堆栈，也不是最优的。

对于属于LLN定义但能够传输IP的技术，如IEEE 802.15.4和802.15.4g、IEEE 1901.2和IEEE 802.11ah，第一层或第二层分片功能和/或IP优化非常重要（本章后面将介绍IEEE 802.14和802.15.4g、IEEE 1901.2和IEEE 802.11ah协议）。例如，IEEE 802.15.4的载荷大小为127字节，需要一个IPv6载荷，其最小MTU为1280字节（有关IPv6分片的更多信息，请参见第5章）。另一方面，IEEE 802.15.4g支持最多2048字节的载荷，放宽了对IPv6最小MTU为1280字节的支持。

大多数LPWA技术都提供有较小的载荷。定义这些较小的载荷是为了应对低数据速率和空中传输时间或物联网节点和传感器的工作周期要求。例如，取决于自适应数据速率（ADR），使用LoRaWAN技术的载荷可能只有19字节，也可能多达250字节。虽然这并不排除使用IPv6/6LoWPAN载荷（正如在一些端点实现中可以看到的那样），但是这些类型的协议更适合于类别0和类别1节点，如RFC 7228中定义的那样（LoRaWAN和ADR将在本章后面详细讨论。RFC 7228及其定义的节点类别在本章的前面已经介绍过）。

综上所述，上述通信标准对于理解物联网接入技术、它们的特点以及何时最适用是至关重要的。这些标准包括无线覆盖的范围、频段、功耗、网络拓扑、受限设备和/或网络的存在以及数据吞吐量。

从网络工程师的角度来看，我们必须确保在开发一个体系结构时对特定的接入技术进行了适当的抽象。对于受限的网络节点尤其如此，在这些节点上，我们对协议和解决方案的选择通常是有限的。下一节将介绍专用于受限网络的物联网接入技术。

4.2 物联网接入技术

上一节描述了帮助读者评估物联网受限网络技术标准，以便进行适当的设计和操作。本节对主要的物联网接入技术进行概述。这里强调的技术是那些被认为具有广大市场且接受度高的技术。因此，我们应该对它们有基本的了解，因为它们是许多物联网通信的基础。

注释：请记住，今天市场上的物联网技术比我们在这里讨论的要多得多。本章的重点是那些应用广泛且稳定的技术。

对于本章讨论的每一种物联网接入技术，有一个通用的信息集。具体来说，每种物联网接入技术都要解决以下问题。

- 标准化和联盟：维护技术协议的标准组织。
- 物理层：有线或无线方式及相关频率。
- MAC层：媒体访问控制（MAC）层面的考虑事项，该层将物理层与数据链路控制连接起来。
- 拓扑：技术支持的拓扑结构。
- 安全性：技术的安全方面。
- 竞争性技术：其他类似的技术，可能用于替代给定技术。

虽然建议读者熟悉这些协议及其功能，但是读者可能会发现，关于这些技术的许多信息更适合用作参考资料。当遇到这些协议时，读者可以使用本章作为重要细节的有用的概述和快速摘要。

4.2.1 IEEE 802.15.4

IEEE 802.15.4是一种无线接入技术，适用于低成本、低数据速率的由电池供电或运行的设备。除了低成本和提供合理的电池寿命外，这种接入技术还支持使用紧凑的协议栈轻松安装，同时保持简单和灵活的特性。若干网络通信栈（包括确定性通信栈）和概要文件利用该技术为消费者和企业市场中的许多物联网用例提供了支持。IEEE 802.15.4通常用于下列部署类型：

- 家居及楼宇自动化；
- 汽车网络；
- 工业无线传感器网络；
- 交互式玩具和遥控器。

IEEE 802.15.4的弊端主要集中在其MAC可靠性、无限延迟、易受干扰和多径衰减的影响。可靠性和延迟的缺点通常与载波侦听多路访问/冲突避免（CSMA/CA）算法有关。CSMA/CA是一种接入方法，在此方法中，设备“侦听”以确保在开始自己的传输之前没有其他设备在传输。如果另一个设备正在传输，在“侦听”再次发生之前会有一个等待时间（通常是随机的）。由于IEEE 802.15.4缺乏跳频技术，因此会导致干扰和多径衰减。IEEE 802.15.4的后续版本开始解决这些问题。有关更多信息，请参阅4.2.2节。

注释：大多数形式的无线通信都不同程度地受到多径衰减的影响。多径衰减是指由于不同的信号路径和反射，信号的多个副本在不同时间点到达接收机。改变频率的能力可以减轻多径衰减的影响。

1. 标准化和联盟

IEEE 802.15.4或IEEE 802.15任务组4定义了用于无线个域网（WPAN）的低数据速率PHY和MAC层规范。多年来，该标准经过不断发

展，成为一种众所周知的解决方案，适用于具有低数据速率、低复杂度，且电池寿命可持续数月甚至数年的无线设备。

自2003年以来，IEEE已经发布了IEEE 802.15.4规范的多个版本，每个版本都标有发布年份。例如，IEEE 802.15.4-2003于2003年发布，802.15.4-2006于2006年发布，802.15.4-2011和802.15.4-2015分别于2011年和2015年发布。较新的版本通常会取代旧版本，集成附录，并为以前的版本添加功能或说明。

虽然IEEE 802.15.4本身没有联盟或推广机构，但IEEE802.15.4 PHY和MAC层是多个网络协议栈的基础。这些协议栈在物理层和链路层使用802.15.4，但上层不同。这些协议栈通过各种组织单独推广，并且通常是商业化的。表4-2中列出了一些基于802.15.4的著名协议栈。

表4-2 使用IEEE 802.15.4的协议栈

协议	描述
ZigBee	通过 ZigBee 联盟推广，ZigBee 定义了上层组件（通过应用程序的网络）以及应用程序配置文件。通用配置文件包括楼宇自动化、家庭自动化和医疗保健。ZigBee 还定义了设备对象功能，例如设备角色、设备发现、网络连接和安全性。ZigBee 将在下一节中详细讨论
6LoWPAN	6LoWPAN 是由 IETF 6LoWPAN 工作组定义的 IPv6 适配层，描述了如何通过 IEEE 802.15.4 层传输 IPv6 数据包。RFC 记录了报头压缩和 IPv6 增强功能，以应对 IEEE 802.15.4 的具体细节（有关 6LoWPAN 的更多信息，请参阅第 5 章）
ZigBee IP	ZigBee IP 是 ZigBee 协议栈的改进，采用 6LoWPAN 适配层、IPv6 网络层和 RPL 路由协议。此外，它还改善了 IP 安全性。ZigBee IP 将在本章后面详细讨论
ISA100.11a	ISA100.11a 由国际自动化学会（ISA）作为“工业自动化无线系统：过程控制及相关应用”开发的。它基于 IEEE 802.15.4-2006，规范于 2010 年发布，后被采纳为 IEC 62734。网络和传输层基于 IETF 6LoWPAN、IPv6 和 UDP 标准
WirelessHART	由 HART 通信基金会推动的 WirelessHART 是一个协议栈，提供时间同步、自组织和自我修复的网状结构，在 2.4 GHz 频段上利用 IEEE 802.15.4-2006
Thread	Thread 构建于 IETF 6LoWPAN/IPv6 之上，是一个协议栈，是用于连接和控制家居产品的安全可靠的网状网络

由于其历史相对较长，ZigBee 是表 4-2 中列出的最有名的协议之一。此外，随着 Zigbee IP 的发布，ZigBee 不断发展，并且证明 IEEE 802.15.4 可以应用于 PHY 和 MAC 层，独立于上面的协议层。因此，后续章节将更详细地讨论 Zigbee 和 Zigbee IP。

ZigBee

基于 20 世纪 90 年代末 ZigBee 风格网络的思想，第一个 ZigBee 规范在 2004 年得到批准，就在 2003 年 IEEE 802.15.4 规范发布后不久。虽然 ZigBee 没有像 RFC 那样作为一个典型的标准发布，但它在最初发布时仍然获得了 100 多家公司的行业支持。这种行业支持已经发展到 ZigBee 联盟成员的 400 多家公司。与 WiFi 联盟类似，Zigbee 联盟是一个行业组织，旨在认证供应商之间的交互操作性，致力于推动和发展 Zigbee，使其成为互联智能对象的物联网解决方案。

ZigBee解决方案针对具有低带宽和低功耗需求的智能对象和传感器。此外，符合ZigBee标准并经ZigBee联盟认证的产品应该可以交互操作，即使产品是由不同的供应商制造的。

Zigbee规范已经过多次修订。在2006年的修订版中，引入了多组命令和消息类型，并在2007年（称为Zigbee pro）迭代中增加了数量，以实现设备的不同功能，例如计量、温度或照明控制。这些命令和消息类型集称为集群。最终，这些来自不同功能域或库的集群构成了Zigbee应用程序配置文件的构建块。实现预定义的Zigbee应用程序配置文件（如家庭自动化或智能能源）的供应商可以确保其产品之间的互操作性。

ZigBee最知名的主要领域包括商业、零售、家庭应用和智能能源的自动化。在工业和商业自动化领域，基于ZigBee的设备可以处理各种功能，从测量温度和湿度到跟踪资产。对于家庭自动化，ZigBee可以控制照明、恒温器和安全功能。ZigBee Smart Energy汇集了各种可互操作的产品，例如智能电表，可以监控和控制电力和水等公用事业的使用和交付。这些ZigBee产品由公用事业提供商控制，可以帮助协调家庭和企业与公用事业提供商本身之间的使用，以提供更高效的运营。

传统的ZigBee堆栈如图4-3所示。如前所述，ZigBee在较低的PHY和MAC层使用IEEE 802.15.4标准（本章后面将详细介绍802.15.4 PHY和MAC层）。ZigBee指定位于较低层之上的网络和安全层以及应用程序支持层。

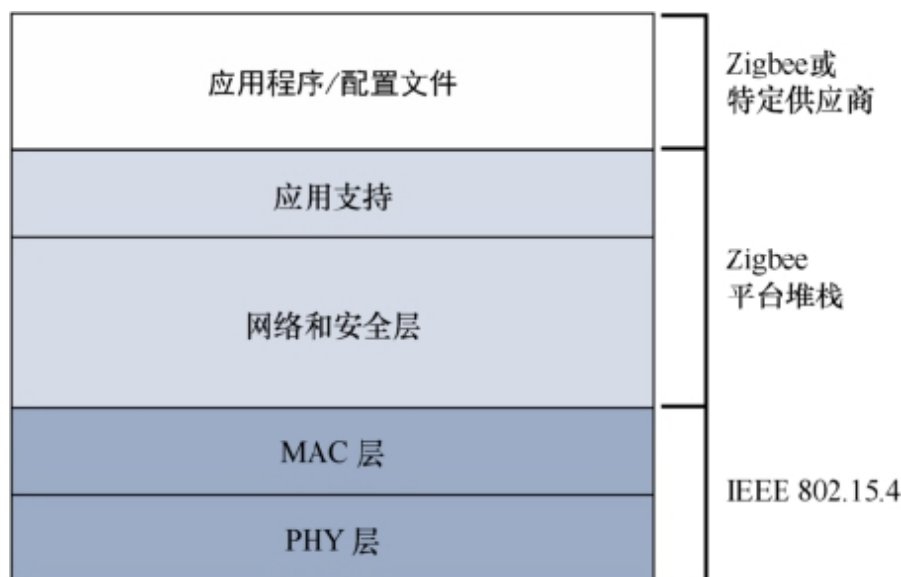


图4-3 高级ZigBee协议栈

ZigBee网络和安全层提供了网络启动、配置、路由和安全通信机制。这包括在经常变化的拓扑结构中计算路由路径、发现邻居以及在设备首次加入时管理路由表。网络层还负责形成适当的拓扑结构，该拓扑结构通常是网状的，但也可以是星型或树状拓扑。从安全角度来看，ZigBee利用802.15.4在MAC层实现安全性，使用带有128位密钥的高级加密标准（AES），并在网络和应用层提供安全性。

注释：ZigBee使用网状网络上的Ad hoc按需距离矢量（AODV）路由。有趣的是，这种路由算法在需要路由之前不会发送消息。假设路由的下一跳不在其路由表中，则网络节点广播路由连接请求。这会导致与路由相关的流量突发，但是在比较各种响应之后，将确定具有最低跳数的路径用于连接。该过程与标准企业路由协议完全不同，后者通常以某种方式学习整个网络拓扑，然后存储合并完整的路由表。

图4-3中的应用程序支持层将处理ZigBee设备联网的堆栈的下半部分与更高层应用程序连接起来。ZigBee为某些行业预定义了许多应用程序配置文件，供应商可以选择在该层创建自己的自定义应用程序配置文件。如前所述，家庭自动化和智能能源是两个流行的应用程序配置文件的示例。

ZigBee是建立在IEEE 802.15.4基础上的最著名的协议之一。在802.15.4 PHY和MAC层之上，ZigBee指定了自己的网络和安全层以及应用程序配置文件。虽然这种结构为拥有ZigBee联盟成员资格的供应商提供了相当程度的互操作性，但它没有提供与其他物联网解决方案的互操作性。然而，随着ZigBee IP的发布，这种情况已经开始发生变化，接下来将对此进行讨论。

ZigBee IP

随着ZigBee IP的引入，IEEE 802.15.4的支持仍在继续，但现在网络和传输层已经支持IP和TCP/UDP协议以及各种其他开放标准。现在，ZigBee特定层仅位于应用程序协议堆栈的顶部。

创建ZigBee IP是为了接受来自IETF关于LLN工作的开放标准，例如IPv6、6LoWPAN和RPL（这些IETF标准将在第5章中讨论）。它们在连接智能对象时提供低带宽、低功耗和经济高效的通信。

ZigBee IP是ZigBee联盟Smart Energy(SE) Profile 2.0规范的重要组成部分。SE 2.0面向智能计量和住宅能源管理系统。事实上，ZigBee IP是专为SE 2.0设计的，但不仅限于此用例。需要基于标准的IoT堆栈的任何其他应用程序都可以使用Zigbee IP。ZigBee IP堆栈如图4-4所示。

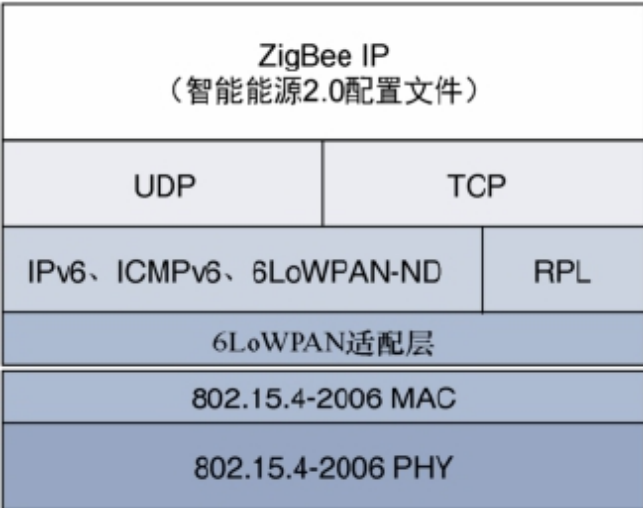


图4-4 ZigBee IP协议栈

与上一节中讨论的传统ZigBee不同，ZigBee IP支持6LoWPAN作为适配层（6LoWPAN协议将在第5章中介绍）。因为ZigBee IP利用网状覆盖或路由转发方法来转发数据包，所以不需要6LoWPAN网状寻址报头。ZigBee IP需要支持6LoWPAN的分片和报头压缩方案。

在网络层，所有ZigBee IP节点都支持IPv6、ICMPv6和6LoWPAN邻居发现（Neighbourhood Discovery, ND），并利用RPL在网状网络上进行分组路由。IPv6和RPL将在第5章中详细讨论。ZigBee IP还同时支持TCP和UDP，以提供面向连接和无连接的服务。

如读者所见，ZigBee IP是一个引人注目的协议栈产品，因为它基于应用层下每层的当前IoT标准。这为ZigBee IP在几乎任何802.15.4网络上与其他基于这些开放式IoT标准的解决方案进行集成和交互操作提供了机会。后文将深入探讨802.15.4及其PHY和MAC层。

2. 物理层

802.15.4标准支持大量PHY选项，频率范围从2.4 GHz到ISM频段的亚GHz（本章前面讨论过ISM频段）。最初的IEEE 802.15.4-2003标准仅基于直接序列扩频（DSSS）调制规定了三种PHY选项。DSSS是一种调制技术，其中信号有意地在频域中扩展，从而产生更大的带宽。最初的物理层传输选项如下：

- 2.4 GHz，16通道，数据速率为250 kbit/s；
- 915 MHz，10通道，数据速率为40 kbit/s；
- 868 MHz，1通道，数据速率为20 kbit/s。

读者应该注意到只有2.4 GHz频段在全球范围内运行。915 MHz频段主要在北美和南美运行，868 MHz频率在欧洲、中东和非洲使用。IEEE 802.15.4-2006、802.15.4-2011和IEEE 802.15.4-2015引入了以下这些PHY通信选项。

■ OQPSK PHY：采用偏移正交相移键控（OQPSK）调制。OQPSK是一种调制技术，它使用由相位变化发出信号的4个唯一比特值。在相移期间存在的偏移功能使数据传输更可靠。

■ PSK PHY：采用二进制相移键控（BPSK）调制。BPSK指定两个唯一的相移作为其数据编码方案。

■ ASK PHY：并行序列扩频（PSSS）PHY，采用幅移键控（ASK）和BPSK调制。PSSS是一种高级的编码方案，与DSSS相比，可提供更大的范围、吞吐量、数据速率和信号完整性。ASK使用振幅偏移而不是相移来发送不同比特值的信号。

这些改进将868 MHz和915 MHz的最大数据速率分别提高到100kbit/s和250kbit/s。868 MHz的支持增强至3个信道，而其他IEEE 802.15.4研究组则为新频段编写了附录。例如，IEEE 802.15.4c研究组创建了314~316 MHz、430~434 MHz和779~787 MHz频段供中国使用。

图4-5显示了802.15.4物理层的帧。此帧的同步标头由前导码和帧开始定界符字段组成。前导码字段是32位4字节（用于并行构造）模式，用于标识帧的开始并用于同步数据传输。帧开始定界符字段通知接收方帧内容在该字节之后立即开始。

图4-5中PHY帧的PHY报头部分只是一个帧长度值。它使接收方了解802.15.4 PHY的PHY服务数据单元（PSDU）部分中预期的总数据量。PSDU表示数据字段或载荷。

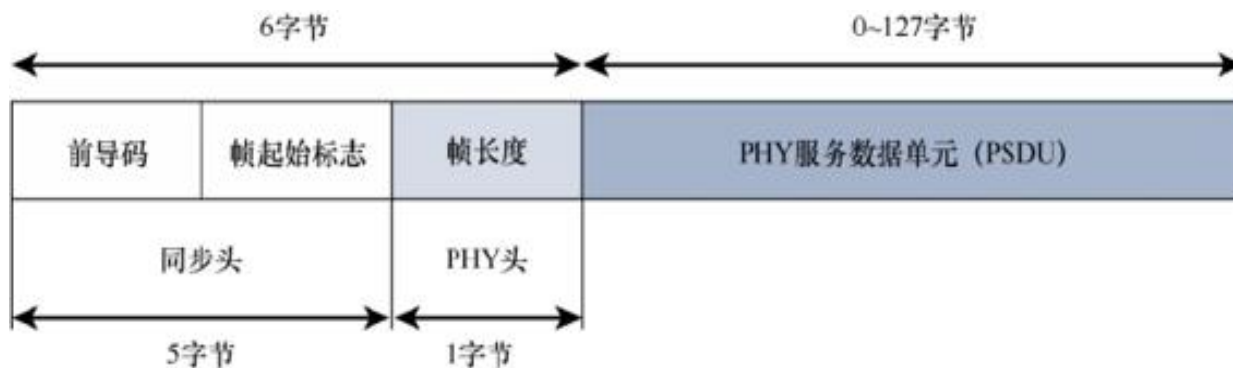


图4-5 IEEE 802.15.4 PHY格式

注释：IEEE 802.15.4 PSDU最大为127字节，这明显小于其他上层协议的最低MTU设置，例如IPv6，其最小MTU设置为1280字节。因此，IPv6数据包的分片必须发生在数据链路层，以便通过IEEE 802.15.4帧传输更大的IPv6数据包（有关详细信息，请参阅第5章）。

多年来，由于不同工作组对802.15.4的各种版本和附录进行了修改，可能会使其难以理解。因此，读者应该注意802.15.4特定设备支持哪些版本。在提供有关物理层实现的详细信息时，产品和解决方案必须参考适当的IEEE 802.15.4规范、频段、调制和数据速率。

3. MAC层

IEEE 802.15.4 MAC层通过定义同一区域中的设备如何共享分配的频率来管理对PHY信道的访问。该层同时还协调数据帧的调度和路由。802.15.4 MAC层执行以下任务：

- 作为设备的网络信标协调器（新设备使用信标加入802.15.4网络）；
- 设备的PAN关联和解除关联；
- 设备安全；
- 两个对等MAC实体之间的可靠链路通信。

MAC层通过使用各种预定义的帧类型来实现这些任务。实际上，802.15.4中指定了4种类型的MAC帧。

- 数据帧：处理所有数据传输。
- 信标帧：用于从PAN协调器传输信标。
- 确认帧：确认帧的成功接收。

■ MAC命令帧：负责设备之间的控制通信。

这4种802.15.4 MAC帧类型中的每一种都遵循图4-6中所示的帧格式。在图4-6中，请注意MAC帧作为PHY载荷进行传输。802.15.4 MAC帧可以分解为MAC报头、MAC载荷和MAC帧尾字段。

MAC报头字段由帧控制、序列号和寻址字段组成。帧控制字段定义诸如帧类型、寻址模式和其他控制标志之类的属性。序列号字段指示帧的序列标识符。寻址字段指示源和目标PAN标识符字段以及源地址和目标地址字段。

注释：802.15.4报头的帧控制部分中是安全启用（Security Enabled）字段。当该字段设置为0时，帧格式与图4-6匹配。从802.15.4-2006规范开始，当该字段设置为值1时，辅助安全报头字段将添加到802.15.4帧，如图4-8所示。

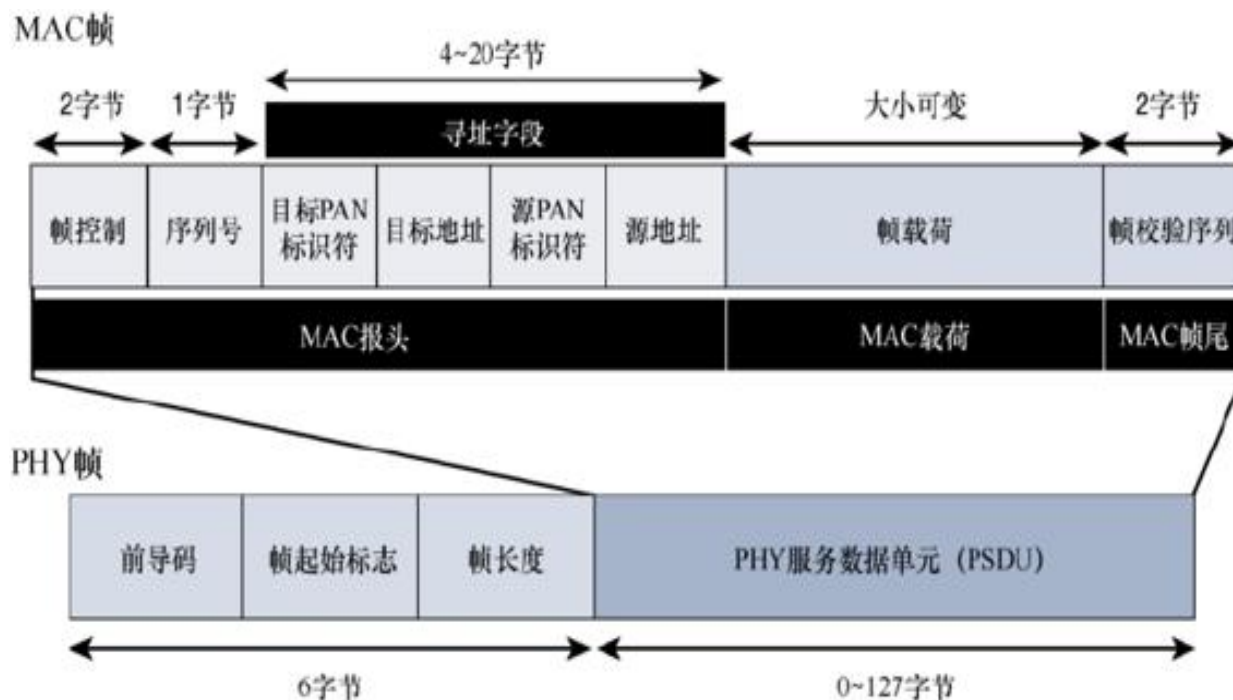


图4-6 IEEE 802.15.4 MAC格式

MAC载荷字段因帧类型而异。例如，信标帧具有与信标相关的特定字段和载荷，而MAC命令帧具有不同的字段。MAC尾帧字段只是一个帧

校验序列（FCS）。FCS是基于帧中数据的计算，接收方使用该数据来确认帧中数据的完整性。

MAC帧

IEEE 802.15.4要求所有设备都支持基于EUI-64的唯一64位扩展MAC地址。但是，由于最大载荷为127字节，因此802.15.4还定义了如何为设备分配16位“短地址”。

该短地址是PAN的本地地址，并且与64位扩展MAC地址相比，大大减少了帧开销。但是，这个短地址的使用可能仅限于特定的上层协议栈。

4. 拓扑

基于IEEE 802.15.4的网络可以构建为星型、点对点或网状拓扑。网状网络将许多节点连接在一起。如果尝试直接通信，则超出范围的节点可以利用中间节点来传输通信。

请注意，每个802.15.4 PAN都应使用唯一ID进行设置。同一802.15.4网络中的所有节点都应使用相同的PAN ID。图4-7所示为PAN ID为1的802.15.4网状网络示例。

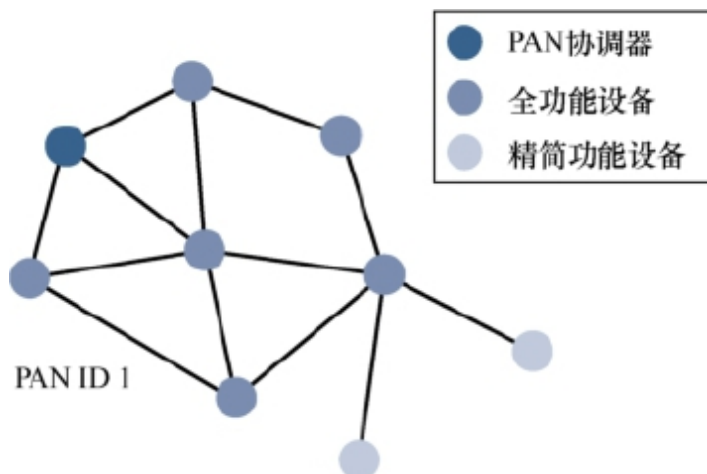


图4-7 802.15.4网状网络示例拓扑

如本章前面所述，IEEE 802.15.4中定义了全功能设备（FFD）和精简功能设备（RFD）。需要至少一个充当PAN协调器的FFD来提供允许其他设备关联并形成单元或PAN的服务。请注意，图4-7中使用PAN ID 1标识了一个PAN协调器。FFD设备可以与任何其他设备通信，而RFD设备只能与FFD设备通信。

IEEE 802.15.4规范没有在MAC层中为网状拓扑定义路径选择。此功能可以在第2层完成，称为mesh-under。通常这基于专有解决方案。或者，路由功能可以使用路由协议在第3层发生，例如用于低功率和有损网络（RPL）的IPv6路由协议。这称为mesh-over（要了解有关mesh-under、mesh-over和RPL的更多信息，请参阅第5章）。

5. 安全

IEEE 802.15.4规范使用具有128位密钥长度的高级加密标准（AES）作为保护其数据的基本加密算法。AES是由美国国家标准技术研究院于2001年建立的一种分组密码，这意味着它可以在固定大小的数据块上运行。

美国政府对AES的使用及其在私营部门的广泛采用，使其成为对称密钥加密中最常用的算法之一（对称密钥意味着相同的密钥同时用于数据的加密和解密）。

除加密数据外，802.15.4中的AES还负责验证发送的数据。这是通过消息完整性代码（MIC）实现的，该代码使用用于加密的相同AES密钥计算整个帧。

为802.15.4启用这些安全特性会稍微改变帧格式，并消耗一些载荷。在802.15.4报头的帧控制部分使用“安全启用”字段是启用AES加密的第一步。该字段是为安全起见而设置为1的一个位。设置好这个位之后，通过从载荷字段中借用一些字节，即可在源地址字段之后创建一个名为“辅助安全报头”的字段。图4-8显示了高层的IEEE 802.15.4帧格式，其中设置了安全启用位和辅助安全报头字段。

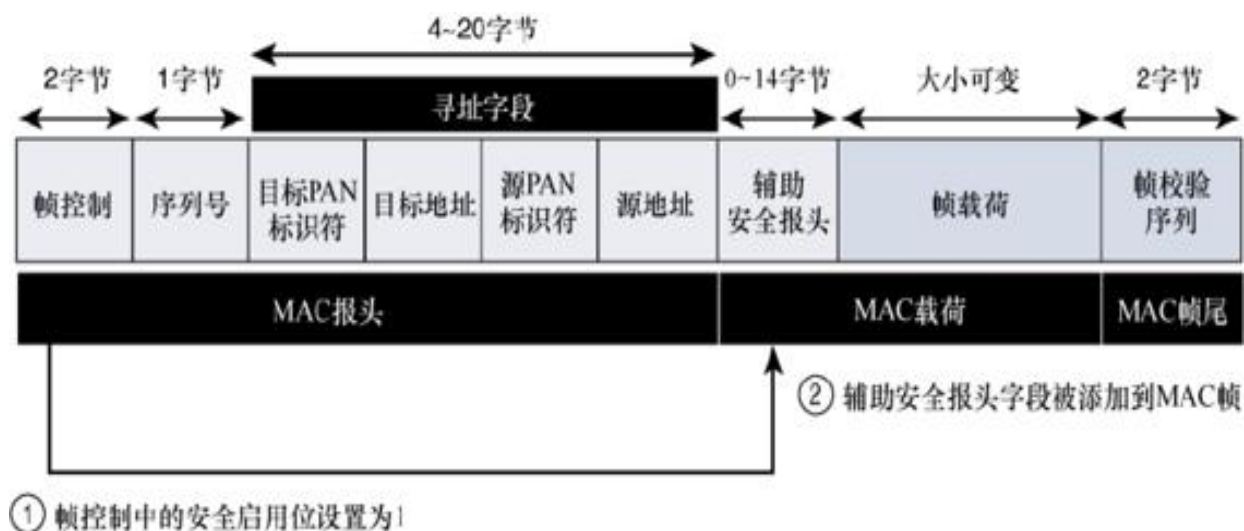


图4-8 带有辅助安全报头字段的帧格式，适用于802.15.4-2006及其以后的版本

6. 竞争性技术

如表4-2所示，IEEE 802.15.4 PHY层和MAC层是在各种物联网接入环境中相互竞争的几种网络配置文件的基础。这些不同的供应商和组织在802.15.4内核的基础上构建上层协议栈。它们根据这些上层的特性和功能进行竞争和区分。

DASH7是一项具有竞争力的无线技术，它在PHY层和MAC层方面与其他技术不同。DASH7最初基于ISO18000-7标准，定位于工业通信，而IEEE 802.15.4则更通用。DASH7通常用于有源射频识别（RFID）实现中，多年来一直被美国军方使用，主要用于物流目的。有源RFID利用由电池供电的标签在物体上产生的无线电波来实现连续跟踪。

目前的DASH7技术提供低功耗、紧凑的协议栈、长达1公里的范围和AES加密，而且定义了433MHz、868MHz和915MHz的频率，支持高达166.667 kbit/s的数据速率和最大载荷256字节。

DASH7由DASH7联盟进行推广，该联盟已将该协议从其活跃的RFID市场发展成为一项针对商业市场的无线传感器网络技术。

7. IEEE 802.15.4总结

IEEE 802.15.4无线PHY层和MAC层是成熟的规范，是各种行业标准和产品的基础（见表4-2）。PHY层提供的最高速度可达250kbit/s，但这取决于调制和频率。用于802.15.4的MAC层是健壮的，并且能够实现在PHY层上传输和接收数据。具体来说，MAC层处理设备与PAN之间的关联和分离、设备之间的可靠通信、安全性以及各种拓扑结构的形成。

802.15.4中使用的拓扑包括星型、点对点和簇树，这些形成网状网络。从安全的角度来看，802.15.4使用AES加密来实现安全通信，并提供数据完整性。

IEEE 802.15.4的主要竞争对手是DASH7，这是另一种相对较好的无线技术。然而，IEEE 802.15.4在市场上具有优势，因为其PHY层和MAC层应用于所有供应商和机构。随着802.15.4的不断发展，IPv6标准将在网络层得到更广泛的应用。对于低功耗、低数据速率、低复杂度的物联网传感器部署，IEEE 802.15.4标准值得高度重视。

4.2.2 IEEE 802.15.4g和IEEE 802.15.4e

IEEE经常对核心802.15.4规范进行修订，然后将其集成到核心规范的下一个版本中。当进行这些修改时，会在版本名称后面附加一个小写字母。其中两个例子是802.15.4e-2012和802.15.4g-2012，它们都与物联网主题特别相关。这两个修订版都集成在IEEE 802.15.4-2015中，但通常以其修订名称来引用。

IEEE 802.15.4e修订版对802.15.4-2011扩展了MAC层特性集，弥补了与802.15.4相关的缺点，包括MAC可靠性、无限延迟和多径衰减。除对MAC层进行一般增强外，IEEE 802.15.4e还进行了改进，以更好地处理某些应用领域，如工厂和流程自动化以及智能电网。智能电网通过连接智能设备和通信设备，与电网和公用事业基础设施的现代化相关联。IEEE 802.15.4e-2012增强了IEEE 802.15.4 MAC层在帧格式、

安全性、可靠性机制、跳频等方面的能力。IEEE 802.15.4e中引入的特定MAC层增强将在本章后面详细介绍。

IEEE 802.15.4g-2012也是对IEEE 802.15.4-2011标准的修订，与802.15.4e-2012一样，它已完全集成到核心IEEE 802.15.4-2015规范中。该规范的重点是智能电网，或者更具体地说，是智能公用事业网络通信。802.15.4g旨在为场域网（FAN）优化大型户外无线网状网络。此外还引入了新的PHY定义，以及支持其实现所需的一些MAC修改。该技术适用于物联网的以下用例。

■ 用于远程监控与控制的配电自动化和工业监控与数据采集（SCADA）环境（SCADA在第6章中有更详细的介绍）。

■ 公共照明。

■ 智慧城市中的环境无线传感器。

■ 电动汽车充电站。

■ 智能停车计时收费表。

■ 微型电网。

■ 可再生能源。

注释：IEEE通过修改继续改进802.15.4规范。例如，IEEE 802.15.4u为印度定义了PHY层特性（865~867 MHz）。同时，IEEE 802.15.4v定义了SUN PHY的变化，规定了欧洲的870~876 MHz和915~921 MHz频段、墨西哥的902~928 MHz频段、巴西的902~907.5 MHz和915~928 MHz频段、澳大利亚/新西兰915~928 MHz频段，以及亚洲区域的IEEE 802.15.4-2015频段。

1. 标准化和联盟

因为 802.15.4g-2012 和 802.15.4e-2012 只是对 IEEE 802.15.4-2011 的简单修订，所以同一个 IEEE 802.15 Task Group 4 标准组织的作者负责维护并将它们集成到核心规范的下一个版本中。然而，802.15.4g-2012 和 802.15.4e-2012 提供的附加功能和选项导致用户要求的设备和混合供应商之间的交互性更难实现。

为了保证交互性，Wi-SUN 联盟成立（SUN 代表智能公用事业网络）。该组织不是一个标准组织，而是一个行业联盟，为智能公用事业和相关网络定义通信配置文件。这些配置文件基于开放标准，例如 802.15.4g-2012、802.15.4e-2012、IPv6、6LoWPAN 和用于 FAN 配置文件的 UDP（有关 6LoWPAN 的更多信息，请参见第 5 章）。此外，Wi-SUN 还提供了一个测试和认证程序，以进一步确保交互性。

Wi-SUN 联盟的功能与 WiFi 联盟和 WiMAX 论坛相同。每个组织都有一个相关的标准机构和一个商业名称，如表 4-3 所示。

表 4-3 一些通用 IEEE 标准的行业联盟

商用名称/商标	行业组织	标准机构
WiFi	WiFi 联盟	IEEE 802.11 Wireless LAN
WiMAX	WiMAX 论坛	IEEE 802.16 Wireless MAN
Wi-SUN	Wi-SUN 联盟	IEEE 802.15.4g Wireless SUN

2. 物理层

在 IEEE 802.15.4g-2012 中，SUN PHY 的原始 IEEE 802.15.4 最大 PSDU 或 127 字节的负载增加到 2047 字节。这为许多上层协议中更大的数据包提供了更好的匹配。例如，默认的 IPv6 MTU 设置为 1280 字节。当 IPv6 数据包通过 IEEE 802.15.4g MAC 帧传输时，第 2 层不再需要分片。此外，在 IEEE 802.15.4g 中，通过将 CRC 从 16 位扩展至 32 位，改进了错误保护。

如IEEE 802.15.4g-2012所述，SUN PHY支持169MHz~2.4 GHz频段的多种数据速率。这些频段包含在不同国家和地区指定的未经许可的ISM频段内。在这些频段内，必须使用以下至少一种符合IEEE 802.15.4g的物理层机制将数据调制到频率上。

■ 多速率、多区域频移键控（MR-FSK）：由于传输信号的封装是恒定的，因此具有良好的传输功率效率。

■ 多速率和多区域正交频分复用（MR-OFDM）：提供较高的数据速率，但对于低成本和低功耗设备来说可能过于复杂。

■ 多速率、多区域偏移正交相移键控（MR-O QPSK）：与IEEE 802.15.4-2006 O-QPSK物理层具有相同的特性，使得多模式系统更经济，更易于设计。

根据频段和调制方式的不同，可以提高数据速率和增加信道数量来实现信道跳频。例如，对于美国使用的902~928 MHz ISM频段，MR-FSK提供50 kbit/s、150 kbit/s或200 kbit/s的数据传输速率。相同频率的MR-OFDM允许高达800 kbit/s，其他频率提供了各自的设置。

因此，产品和解决方案在提供有关PHY层实现的详细信息时，必须参考适当的IEEE 802.15.4规范、频段、调制和数据速率。这很重要，因为支持新的物理层机制（如MR-OFDM）的芯片组的可用性可能会限制增强数据速率的实现。我们应该寻求Wi-SUN联盟来缓解这些问题，并在实现、交互性和认证方面提供一定的一致性。例如，Wi-SUN PHY工作组发布了一个区域性频段规范，描述了不同国家和地区的信息。

3. MAC层

IEEE 802.15.4e-2012修订版不适用于PHY层，但适用于MAC层。该修订版通过各种功能增强了MAC层，可以根据标准的各种实现选择性地启用这些功能。事实上，如果交互性是“必须具备的”，那么就有必

要使用Wi-SUN等组织定义的配置文件。以下是IEEE 802.15.4e-2012提出的对MAC层的一些主要增强。

■ **时隙跳频 (Time-Slotted Channel Hopping, TSCH)**：TSCH是IEEE 802.15.4e-2012 MAC操作模式，用于保证媒体访问和信道多样性。跳频利用不同的信道在不同的时间进行传输。TSCH将时间划分为固定的时间段或“时隙”，这些时间段或时隙提供有保证的带宽和可预测的延迟。在一个时隙中，可以传输一个数据包及其确认，这增加了网络容量，因为多个节点可以在同一个时隙中使用不同的信道进行通信。许多时隙被定义为“时隙帧”，它们定期重复以提供“有保证的访问”。发射器和接收器通过全局时隙计数器和全局信道跳频序列列表的组合，就信道和信道间的切换时序达成一致，在每个节点上计算以确定每个时隙的信道。TSCH增强了噪声环境中的稳健性，并与其他无线技术更平稳地共存，特别是在工业用例中。

注释：虽然802.15.4e-2012支持TSCH，但是由于行业标准化了TSCH的实现方式，因此该特性的实现可能会有所不同。TSCH的实现与IETF 6TiSCH工作组标准化工作紧密相关，后者为TSCH定义了一个调度算法。有关6TiSCH的更多信息，请参见第5章。

■ **信息元素**：信息元素（IE）允许在MAC层以可扩展的方式交换信息，可以作为报头IE（标准化）和/或载荷IE（私有）。IE字段以标签、长度、值（TLV）格式指定，允许帧携带额外的元数据来支持MAC层服务。这些服务可能包括IEEE 802.15.9密钥管理、用于广播和单播调度定时信息的Wi-SUN 1.0 IE，以及用于6TiSCH体系结构的跳频同步信息。

■ **增强信标（EB）**：EB扩展了IEEE 802.15.4信标的灵活性，允许构建特定于应用程序的信标内容。这是通过在EB框架中包含相关的IE来实现的。在EB中可以找到的一些IE包括网络度量、跳频广播调度和PAN信息版本。

■ **增强信标请求（EBR）**：与增强信标相似，EBR也使用了IE。EBR中的IE允许发送方有选择地指定信息请求。然后信标响应被限制在

EBR中所请求的范围内。例如，设备可以查询允许新设备加入的PAN或支持特定MAC/PHY功能集的PAN。

■ 增强确认：增强确认帧允许为被确认帧集成帧计数器。该特性有助于防止在欺骗确认帧时发生的某些攻击。

802.15.4e-2012 MAC修订版通常与802.15.4g-2012物理层相结合。图4-9详细说明了这种帧格式。注意，802.15.4g-2012 PHY与图4-5中的802.15.4 PHY相似。两者的主要区别在于载荷大小，802.15.4g支持2047字节，而802.15.4只支持127字节。

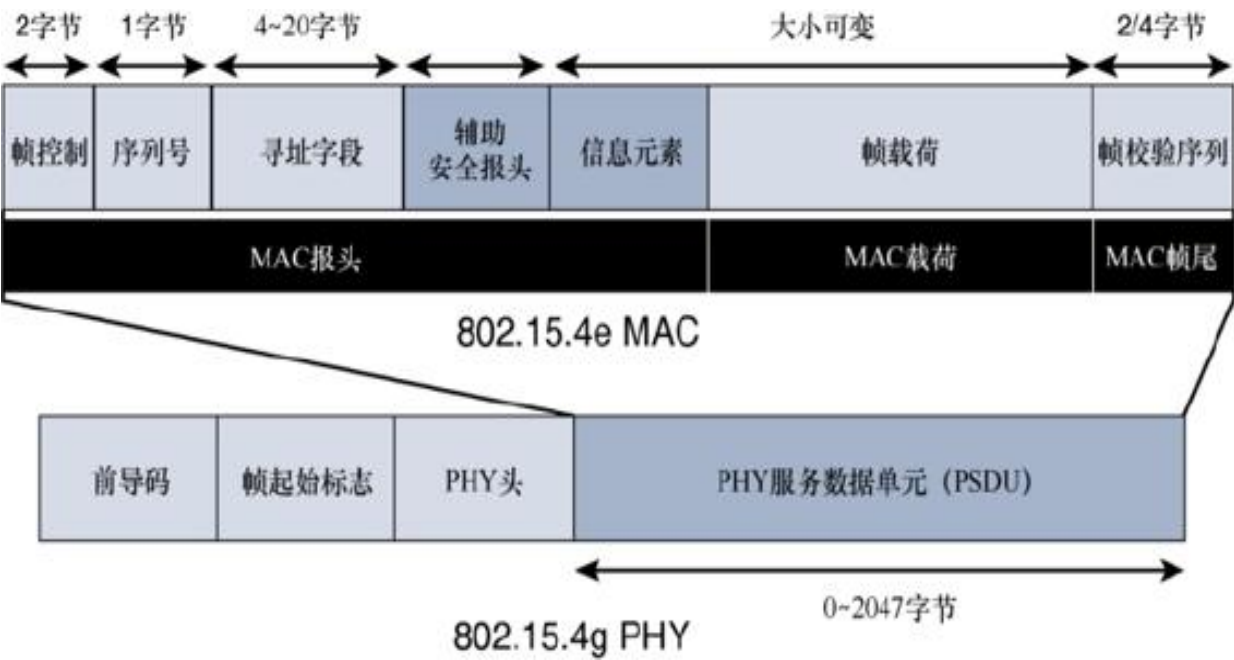


图4-9 IEEE 802.15.4g/e MAC帧格式

802.15.4e MAC类似于图4-6中的802.15.4 MAC。图4-9中IEEE 802.15.4e报头中显示的主要变化是存在辅助安全报头和信息元素字段。辅助安全报头用于对数据帧进行加密。从802.15.4-2006规范开始，802.15.4e-2012和802.15.4都支持这个字段，如图4-8所示。正如本节前面所讨论的，IE字段包含一个或多个信息元素，允许在MAC层交换额外的信息。

4. 拓扑

IEEE 802.15.4g-2012的部署大多基于网状拓扑。这是因为网状拓扑通常是应用802.15.4g-2012的工业和智慧城市地区用例的最佳选择。网状拓扑允许在城市或农村地区进行部署，从而扩大节点之间的距离，以便转发其他节点的流量。考虑到应用该技术的用例，供电节点一直是该技术实现的首选目标。为了支持长生命周期的电池供电节点，则需要对第2层转发或第3层路由的协议的实现进行优化。这提供了额外的复杂性，但是为了处理休眠的电池供电节点，这是必要的。

5. 安全

IEEE 802.15.4g和802.15.4e都继承了IEEE 802.15.4-2006规范的安全属性。因此，AES使用128位密钥提供加密。除了最初在802.15.4-2006中定义的辅助安全报头字段外，安全确认和安全增强信标字段保证了MAC层的安全性。图4-10显示了与IEEE 802.15.4e MAC帧相关联的安全性的高级概览。

图4-10中的完整帧通过帧末的MIC进行身份验证。MIC是根据帧内容计算的唯一值（本章前面更详细地讨论了MIC）。图4-10中所示的安全报头字段由辅助安全字段和一个或多个信息元素字段组成。信息元素字段的集成允许采用附加的安全功能，比如IEEE 802.15.9密钥管理协议（KMP）规范。KMP提供了一种建立密钥的方法来实现健壮的数据报安全性。如果没有密钥管理支持，通常会导致弱密钥，从而使安全系统容易受到攻击。

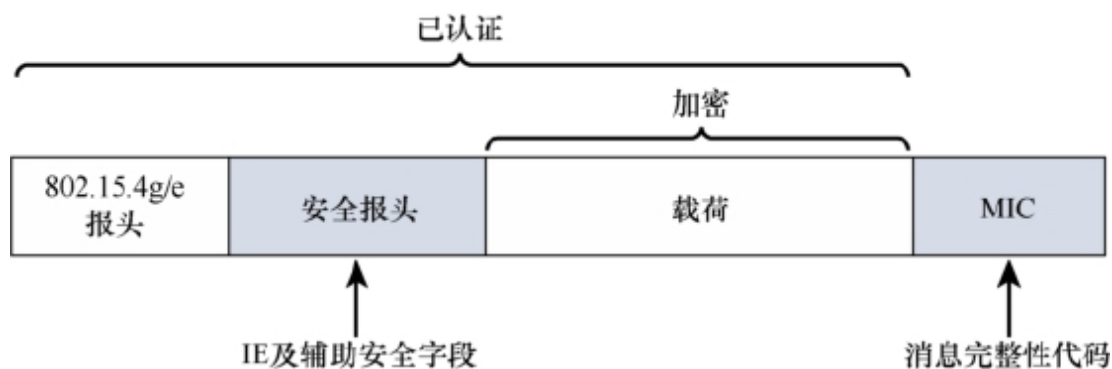


图4-10 IEEE 802.15.4g/e MAC层的安全架构

6. 竞争性技术

IEEE 802.15.4g和802.15.4e的竞争技术与IEEE 802.15.4的技术（如DASH7）是并行的。本章前面讨论了DASH7。在许多方面，802.15.4及其上层各种不同的协议（见表4-2）也可以视为竞争对手。IEEE 802.15.4已经很好地建立起来，并且已经部署在许多场景中（主要是在室内）。

7. IEEE 802.15.4g和802.15.4e小结

IEEE 802.15.4g和802.15.4e只是IEEE 802.15.4标准的修订。它们是集成到IEEE 802.15.4-2015中的成熟规范，已经成功地部署在实际场景中，并且支持数百万个端点。IEEE 802.15.4g主要针对PHY层进行改进，IEEE 802.15.4e主要针对MAC层。这些改进克服了IEEE 802.15.4的许多缺点，如延迟和易受多径衰减的影响。此外，这些修订中的条款使它们更适合处理智能电网/公用事业和智能城市领域的独特部署模式。

Wi-SUN联盟是一个重要的行业联盟，为行业实现提供交互性和认证。联盟利用802.15.4g作为基础，发布了一些配置文件，比如FAN配置文件，以帮助促进该技术的应用，同时保证供应商之间的交互性。我们应该会发现802.15.4g和802.15.4e的应用会越来越多，尤其是在物联网的智能电网和智慧城市领域，它们已经被广泛采用。

4.2.3 IEEE 1901.2a

虽然大多数受限网络技术都与无线有关，但IEEE 1901.2a-2013是一种有线技术，是对原有IEEE 1901.2规范的更新。这是窄带电力线通信（NB-PLC）的标准。NB-PLC在用于输送电力的电线上，利用窄带频段实现低功耗、远程、抗干扰能力。NB-PLC经常出现在以下用例中。

■ **智能计量：**NB-PLC可用于电表、燃气表、水表等公用事业仪表的自动抄表。在欧洲尤其如此，PLC是公用事业公司部署智能电表解决方案的首选技术。

■ **配电自动化：**可采用NB-PLC进行配电自动化，包括对电网中所有设备的监控。

■ **公共照明：**NB-PLC的一个常见用途是公共照明——在城市、街道、高速公路和公园等公共区域的公共照明。

■ **电动汽车充电站：**NB-PLC 可用于电动汽车充电站，对电动汽车的电池进行充电。

■ **微电网：**NB-PLC可用于微电网，以及与传统电网断开连接并独立运行的地方电网。

■ **可再生能源：**NB-PLC可用于太阳能、风能、水力发电、地热能等可再生能源领域。所有这些用例都需要直接连接到电网。因此，在已有的电网连接上传输物联网数据是有意义的。

尽管存在多种PLC标准，但IEEE 1901.2a的形成是由于缺乏500 kHz以下的低频PLC解决方案而造成的。IEEE 1901.2a规定了交流电和直流电的使用。在室内和室外环境中都支持低压和中压线路，以及几公里的距离。数据速率可以扩展到500kbit/s。IEEE 1901.2a PHY层和MAC层可以在端点上与IEEE 802.15.4g/e结合，为某些用例提供双PHY层解决方案。

1. 标准化和联盟

第一代NB-PLC实现在欧洲引起了公用事业公司的极大兴趣，但其可靠性差、吞吐量低（每秒几百位到最多2kbit/s），也缺乏可管理性，交互性也不好。这使得一些组织（包括标准机构和联盟）为新一代NB-PLC技术开发了自己的规范。最新的NB-PLC标准基于正交频分复用（OFDM），然而，来自不同厂商的不同标准相互竞争，形成了一个

分散的市场。OFDM在多个载波频率上对数字数据进行编码，这提供了几个并行流，很少受到铜线高频衰减和窄带干扰的影响。

IEEE 1901.2工作组于2013年11月发布了IEEE 1901.2a规范。IEEE 1901.2工作组最初利用G3-PLC（现在的ITU G.9903）和PRIME（现在的ITU G.9904）工作组所做的工作，只研究独立于上层的NB-PLC PHY和MAC层（由IEEE章程定义，由其他IEEE标准完成）的标准化。这与G.9903和G.9904不同，G.9903和G.9904是为单个用例、智能电表开发的，专注于运行智能电表的特定应用协议。

IEEE 1901.2a标准确实与其他IEEE工作组的最新开发成果有一些一致性。例如，使用802.15.4e信息元素字段可以简化对IEEE 802.15.9密钥管理的支持。此外，当在端点上结合IEEE 802.15.4g/e时，双PHY层方法是可行的。

HomePlug联盟是推动PLC技术推广和认证的主要行业组织之一，IEEE 1901.2a是其HomePlug Netricity计划的一部分。2016年，HomePlug联盟决定将其宽带电力线网络技术向更广泛的受众开放，公开其技术规范，还与其他联盟开展合作，继续进行工作。

HomePlug联盟已经与Wi-SUN联盟达成了一项联络协议，目标是实现同时支持无线和电力线连接的混合智能电网网络。

2. 物理层

NB-PLC适用于3~500kHz的频段。与无线亚GHz频段一样，区域规则和定义也适用于NB-PLC。IEEE 1901.2工作组对世界所有地区提供综合支持，以便制定一个全球标准。规范包括支持CENELEC A和B频段、美国FCC-Low和FCC-above-CENELEC频段，以及日本ARIB频段。CENELEC是法语Comite Europeen de Normalisation Electrotechnique（欧洲电工标准化委员会）的缩写。该组织负责欧洲电气工程领域的标准化工作。CENELEC A和B频段分别为9~95kHz和95~125kHz。FCC（联邦通信委员会）是一个美国政府组织，管理无线电广播、电视、电线、卫

星和电缆的州际和国际通信。FCC-Low频段为37.5~117.1875kHz，CENELEC以上频段为154.6875~487.5 kHz。CENELEC以上的频段，由于具有较高的吞吐量和较低的干扰，可能成为最有用的频率。

图4-11为NB-PLC的不同频段。请注意，最著名的频段由CENELEC和FCC监管，但日本无线工业及商贸联合会（ARIB）频段也在其中。两个ARIB频段分别为ARIB 1（37.5~117.1875 kHz）和ARIB 2（154.6875~403.125 kHz）。

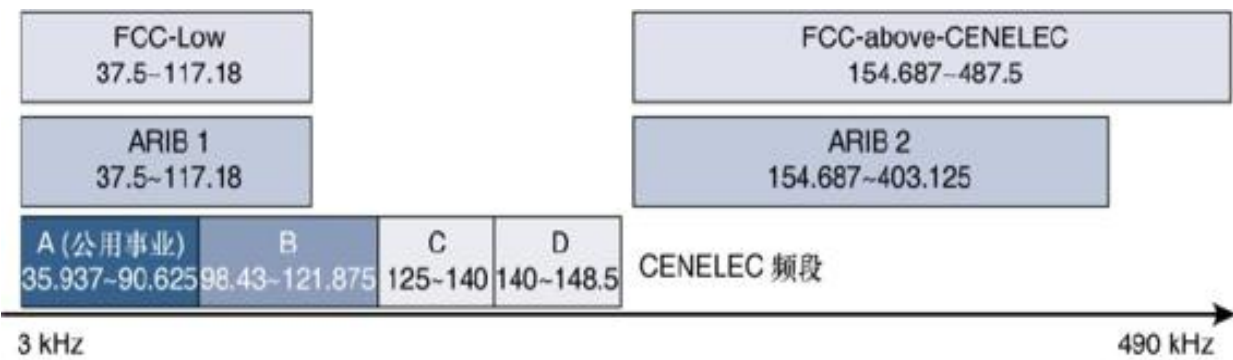


图4-11 NB-PLC频段

IEEE 1901.2规范以OFDM为基础，充分利用了以前开发的其他NB-PLC OFDM技术。因此，IEEE 1901.2a支持最大的编码集，并且实现了健壮性和吞吐量。该标准包括音调映射和调制，如稳健调制（ROBO）、差分二进制相移键控（DBPSK）、差分正交相移键控（DQPSK）、针对所有频带的差分8点相移键控（D8PSK），以及可选的针对某些频带的16正交幅度调制（16QAM）。

ROBO模式在多个载波上传输冗余信息，DBPSK、DQPSK和D8PSK都是相移键控的变体，其中信号的相位被改变为二进制数据传输的信号。ROBO使用QPSK调制，其吞吐量依赖于编码在流中重复的程度。例如，标准ROBO使用4次重复编码，而超级ROBO使用6次重复编码。

在IEEE 1901.2a中，数据吞吐率能够根据调制类型和音调映射发生动态变化。对于CENELEC A频段，数据速率范围从4.5kbit/s（ROBO模式）到46kbit/s（D8PSK调制）。对于高于CENELEC的FCC频率，吞吐量从21kbit/s（ROBO模式）到最大值234kbit/s（使用D8PSK）不等。

IEEE 802.15.4g/e和IEEE1901.2a之间的一个主要区别是，在IEEE1901.2a规范中，物理层完全集成了不同类型的调制和音调映射。IEEE 802.15.4g/e并没有真正定义多物理层管理算法。在IEEE 1901.2a中，物理层载荷大小可以根据信道条件动态变化，从而实现MAC子层分割。如果MAC载荷过大，无法容纳在一个PHY服务数据单元（PSDU）中，则将MAC载荷划分为更小的段。MAC载荷分段是通过将MAC载荷根据PSDU大小划分为多个较小的数据量（段）来完成的。在分段时可能需要向最后一个载荷段添加填充字节，以便最终的MPDU能填满PSDU。所有形式的寻址（单播和广播）都要进行分段。

3. MAC层

IEEE 1901.2a的MAC帧格式基于IEEE 802.15.4 MAC帧，但集成了最新的IEEE 802.15.4e-2012修订版，支持关键特性（有关802.15.4 MAC帧格式的更多信息，请见图4-6。有关802.15.4e MAC帧格式，请见图4-9）。从802.15.4e引入IEEE 1901.2a的关键组件之一是信息元素。在IE的支持下，还支持其他功能，如IEEE 802.15.9密钥管理协议和SSID。图4-12概述了IEEE1901.2的通用MAC帧格式。注意，帧中每个字段上方的数值表示以字节为单位的字段大小。

3	2	1	0/2	0/2/8	0/2	0/2/8	0/5/6/ 10/14	变量	大小可变	2
分段 控制	帧控制	序列号	目标 PAN 标识符	目标 地址	源PAN 标识符	源地址	辅助 安全 报头	信息 元素	帧载荷	帧校 验序列
MAC报头 (MHR)								MAC协议数据单元 (MPDU) 载荷		AC帧尾 (MFR)

图4-12 IEEE 1901.2通用MAC帧格式

如图4-12所示，IEEE 1901.2有一个分段控制字段。这是一个新的字段，之前在讨论802.15.4和802.15.4e的MAC框架时没有出现过。该字段处理大于MAC协议数据单元（MPDU）所能承载的上层数据包的

段。其余字段在本章前面讨论过，如图4-6、图4-8和图4-9所示。如果需要了解关于这些字段的信息，请参考这些图。

4. 拓扑

IEEE 1901.2a的用例和部署拓扑被绑定到物理电力线上。与无线技术相同，信号传播受到噪声、干扰、失真和衰减等因素的限制。这些因素随着距离的增加而变得更加普遍，因此大多数NB-PLC部署都使用某种网格拓扑结构。在网状网络，设备可以转发其他设备的流量，因此可以将更长的距离进行分段。图4-13突出显示了一个应用于网络的PLC邻域。

IEEE 1901.2a标准提供了运行任何上层协议的灵活性，因此支持IPv6 6LoWPAN和RPL IPv6协议的实现。这些协议允许使用网络层路由在PLC上创建网状网络（有关6LoWPAN和RPL的更多信息，请参见第5章）。

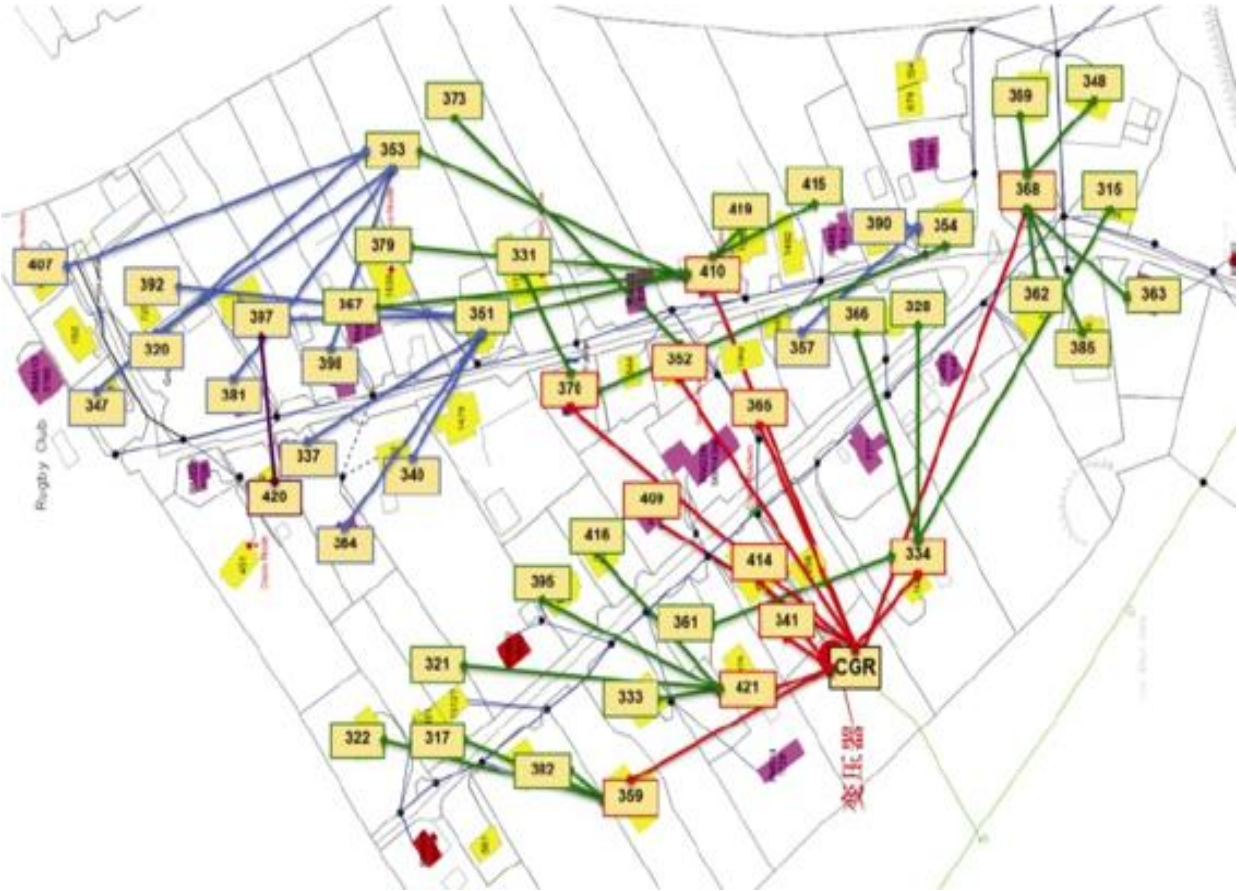


图4-13 NB-PLG的IPv6网络

5. 安全

IEEE 1901.2a安全性提供了与IEEE 802.15.4g类似的特性，使用AES执行加密和身份验证。此外，IEEE 1901.2a在支持IEEE 802.15.9密钥管理协议的能力上与802.15.4g一致。然而，两者之间也存在一些差异。这些差异主要与IEEE 1901.2a的物理层分段能力有关，具体如下。

- 帧控制字段中的安全启用位应该在所有携带加密帧段的MAC帧中设置。安全启用位如图4-8所示。

- 如果需要数据加密，应该在数据包分段之前进行。在包加密期间，段控制字段不应该包含在加密算法的输入中。

■ 在接收端，数据解密是在数据包重组之后完成的。

■ 启用安全性后，MAC载荷由加密的载荷和用于非分段载荷的消息完整性代码（MIC）身份验证标记组成。如果载荷是分段的，MIC仅是最后一个分组（段）的一部分。MIC身份验证仅使用携带第一个分段的帧的MHR中的信息来计算。

6. 竞争性技术

在NB-PLC领域，有两种技术与IEEE 1901.2a竞争：G3-PLC（现为ITU G.9903）和PRIME（现为ITU G.9904）。这两种技术最初都是为了解决一个用例而开发的：通过CENELECA频段在欧洲部署智能计量。

如前所述，IEEE 1901.2a利用了G3-PLC和PRIME的部分功能，并与它们竞争。更具体地说，G3-PLC非常接近IEEE 1901.2。主要的区别包括G3-PLC要求数据链路层协议选项用于引导和分配设备地址，并且它与IEEE 802.15.4g/e和端到端IPv6模型不兼容。这意味着不支持信息元素，也不支持全局IPv6地址。PRIME更像是一种ATM方法，具有直接运行在第2层之上的第7层协议（即DLMS/COSEM）。若要添加IP支持，则需要添加第3层协议。

在IEEE 1901.2工作组的努力下，G3-PLC和PRIME发布了新版本。这些新版本增加了类似的功能集，比如支持FCC和ARIB频段、PRIME支持ROBO、G3-PLC支持Super-ROBO和16QAM。随着这些竞争性技术的不断发展和相互借鉴，未来某个时刻可能会出现兼容性的趋同。

7. IEEE 1901.2a总结

IEEE 1901.2a是一种开放的物理层和MAC标准方法，使窄带电力线通信成为可能。该标准的用例集依赖于连接设备的物理电力线，并从中获益。

IEEE 1901.2a标准利用了早期的标准G3-PLC（现为ITU G.9903）和PRIME（现为ITU G.9904）。在物理层支持广泛的频率范围，IoT接入技术IEEE 1901.2a还具有基于802.15.4的功能丰富的MAC层。MAC层的灵活性使其能够更好地支持网状拓扑。

HomePlug联盟的Netricity计划和与Wi-SUN联盟的联络协议通过配置文件定义和认证计划为IEEE 1901.2a提供行业支持。然而，IEEE 1901.2a面临来自G3-PLC和PRIME的竞争，因为它们是不不断发展的更成熟的标准。

IEEE 1901.2a的广泛应用依赖于供应商的实现。大多数芯片组支持IEEE 1901.2a、G3-PLC和PRIME，因为它们是3种具有竞争力的基于OFDM的PLC技术。如果期望端到端IP通信或双PHY与IEEE 802.15.4g/e集成，则IEEE 1901.2a将是首选协议。

4.2.4 IEEE 802.11ah

在无约束网络中，IEEE 802.11 WiFi无疑是部署最成功的无线技术。该标准是一项关键的物联网无线接入技术，既可用于连接端点（例如雾计算节点、高数据速率传感器、音频或视频分析设备），也可用于部署WiFi回程基础设施（例如智慧城市、石油和矿业或其他环境中的户外WiFi网络）。然而，WiFi缺乏亚GHz支持，信号的穿透性不好，电池供电节点的功耗较低，也无法支持大量设备。基于这些原因，IEEE 802.11工作组启动了一个名为IEEE 802.11ah的任务组，以制定亚GHz版本的WiFi。IEEE 802.11ah确定了3个主要用例。

■ 覆盖智能电网的传感器和仪表：电表、环境/农业监测、工业过程传感器、室内保健系统和健康传感器、家庭和建筑自动化传感器。

■ 工业传感器和仪表数据的回程聚合：潜在地连接 IEEE 802.15.4g子网。

■ 扩展范围WiFi：当IEEE 802.11a/b/g/n/ac覆盖的距离不够远时，用于户外扩展热点的范围或减轻蜂窝网络的流量。

1. 标准化和联盟

2010年7月，IEEE 802.11工作组决定开发“工业WiFi”，并成立了IEEE 802.11ah工作组。802.11ah规范将在未经许可的亚GHz频段中运行，类似于IEEE 802.15.4和其他LPWA技术。

推动2.4 GHz和5 GHz产品WiFi认证和交互性的行业组织是WiFi联盟。WiFi联盟与Wi-SUN联盟类似。

对于802.11ah标准，联盟定义了一个名为Wi-Fi HaLow的新品牌。HaLow品牌独家覆盖IEEE 802.11ah，用于亚GHz设备的认证。我们可以将Wi-Fi HaLow看作一种商业名称，用于包含IEEE 802.11ah技术的产品。

2. 物理层

IEEE 802.11ah本质上提供了一个额外的802.11物理层，在未经许可的亚GHz频段中运行。例如，许多国家和地区对IEEE 802.11ah使用以下频段：EMEAR使用868~868.6 MHz，北美和亚太地区使用902~928 MHz及其相关子集。

基于OFDM调制，IEEE 802.11ah使用2MHz、4MHz、8MHz或16MHz的信道（对于低带宽传输使用1MHz）。这是IEEE 802.11ac信道的1/10，相应数据速率也是IEEE 802.11ac的1/10。IEEE 802.11ac标准是一种高速无线局域网协议，频率为5GHz，速率可达1 Gbit/s。虽然802.11ah没有达到这个传输速度（因为它使用了802.11ac通道宽度的1/10，其速率为802.11ac的1/10），但它确实为低速率的数据提供了扩展范围。例如，在数据速率为100kbit/s时，IEEE 802.11ah的户外传输范围预计为1公里。

3. MAC层

IEEE 802.11ah MAC层经过优化，支持新的亚GHz WiFi物理层，同时能提供低功耗和支持更多的端点。IEEE 802.11ah为MAC层指定的增强和特性如下所示。

- 设备数量：已扩展到每个接入点可接入8192台设备。

- MAC报头：已被减小，以允许更有效的通信。

- 空数据包（NDP）支持：扩展到多个控制和管理帧。相关信息集中在PHY报头中，避免了与解码MAC报头和数据载荷相关的额外开销。这种变化使控制帧交换效率提高，接收站的功耗更低。

- 分组和分段：使AP能够使用扇区天线，也可以对工作站进行分组（分发组ID）。通过与RAW和TWT相结合，该机制通过限制哪个组、哪个扇区可以在哪个时间窗口内竞争，从而减少了大型单元中与多个客户端之间的争用（下一节将更详细地描述扇区）。

- 受限访问窗口（RAW）：是一种控制算法，当存在多个设备时，可以避免同时传输，并提供对无线网络的公平访问。通过提供对介质更有效的访问，可以为电池供电的设备节省额外的电力，并减少冲突。

- 目标唤醒时间（TWT）：在设备访问网络时通过允许接入点（AP）来定义访问时间，以减少能源消耗。这允许设备进入低功耗状态，直到其TWT时间到来为止。它还降低了在大型单元中与许多客户端发生冲突的可能性。

- 快速帧交换：允许AP和端点在保留的传输机会（TXOP）期间交换帧。这减少了介质上的争用，减少了帧交换的数量以提高信道效率，并通过保持较短的唤醒时间来延长电池寿命。

从上文中可以看出，802.11ah MAC层主要关注功耗和机制，以允许低功耗WiFi站点减少唤醒时间次数，并更有效地运行。这种MAC层是物联网设备的理想层，这些设备常常产生短的、低比特率的传输。

4. 拓扑

IEEE 802.11ah被部署为星型拓扑，它包括一个简单的跳中继操作来扩展其范围。这个中继选项没有跳数限制，但是IEEE 802.11ah任务组的工作是基于两跳的假设。它允许一个802.11ah设备充当中介，并将数据转发给另一个设备。在某些方面，这类似于网状拓扑，需要注意的是处理中继功能的是客户端而不是接入点。

这种中继操作可以与更高的传输速率或调制编码方案（MCS）相结合。这意味着中继设备直接与接入点通信时使用更高的传输速率。当信息通过中继客户端从接入点进一步传输时，传输速率会降低。这确保系统能够在中继设备边缘限制传输速度，使邻近AP的通信不会受到负面影响。

功能分区是一种技术，它将覆盖区域划分为多个扇区，以减少特定扇区中的争用。这种技术对于限制具有许多客户端的单元中的冲突非常有用。当802.11ah接入点的覆盖面积较大，且相邻接入点的干扰存在问题时，通常也需要使用这种技术。分段使用天线阵列和波束形成技术来划分单元覆盖区域。图4-14显示了802.11ah分区的示例。

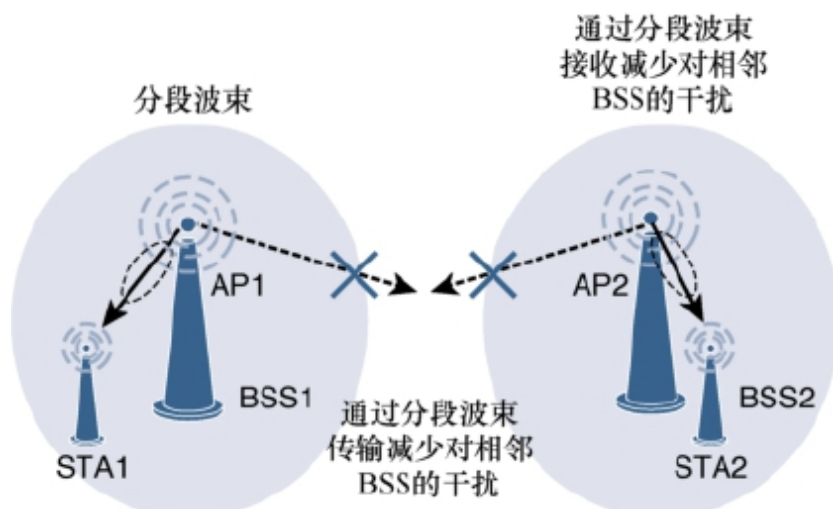


图4-14 IEEE 802.11ah分段

5. 安全

与其他IEEE 802.11规范相比，IEEE 802.11ah没有提供更高的安全性（本章前面讨论了其他IEEE协议）。这些协议包括IEEE 802.15.4、IEEE 802.15.4e和IEEE 1901.2a，它们的安全性也适用于IEEE 802.11ah。

6. 竞争性技术

IEEE 802.11ah的竞争性技术包括IEEE 802.15.4和IEEE 802.15.4e，以及在讨论它们时强调的竞争性技术。有关这些竞争性技术的更多信息，请参阅4.2.1节和4.2.2节。

7. IEEE 802.11ah总结

IEEE 802.11ah接入技术是IEEE 802.11工作组为定义“工业WiFi”而进行的工作。目前，这一标准还处于发展的初期，市场对这一新的WiFi标准会做何反应并不清楚。

该规范提供了比传统WiFi技术更广的范围，并为低功耗设备提供了良好的支持，这些设备需要以较低的速度发送较小的突发数据。同时，它也有能力扩展到更高的速度。

IEEE 802.11ah在2.4GHz与5GHz频段的现有产品和WiFi技术有很大的不同。为了在这个领域获得广泛应用并与类似技术竞争，它将需要一个产品和解决方案的生态系统，这些产品和解决方案可以以较低的成本配置和部署。

4.2.5 LoRaWAN

近年来，一种被称为低功耗广域网络（LPWA）的新型无线技术受到了业界和媒体的广泛关注。LPWA技术特别适用于远程和电池供电的终端，为服务提供商和考虑物联网解决方案的企业提供了新的商业机会。本节将讨论一种称为LoRaWAN的未经许可频段LPWA技术示例，4.2.6节将介绍来自第三代合作项目（3GPP）的许可频段替代方案。

注释：从LPWA的角度来看，其他技术本可以在本书的这一部分介绍，但是目前物联网的无线通信技术仍在不断发展，有很多可供选择的选项。我们选择介绍LoRaWAN，是因为它是为数不多的选择之一，而且它得到了一个由大量公司支持的行业联盟的支持。

1. 标准化和联盟

最初，LoRa是由一家名为Cycleo的法国公司开发的物理层（或者说第一层）调制。后来Cycleo被Semtech收购。通过LoRa联盟的建立，该技术从第一层发展到更广泛的应用领域。

LoRa联盟很快获得了业界的支持，目前已有数百名成员。已发布的LoRaWAN规范是开放的，可以通过LoRa联盟网站访问。

Semtech LoRa作为第一层物理层调制技术可通过多个芯片组供应商获得。为了区别于被称为LoRa的物理层调制，LoRa联盟使用术语

LoRaWAN来指代描述端到端LoRaWAN通信和协议的体系结构及规范。

图 4-15 提供了LoRaWAN层的高级概览。在图 4-15 中， 请注意 Semtech负责物理层， 而LoRa联盟负责MAC层和区域频段。

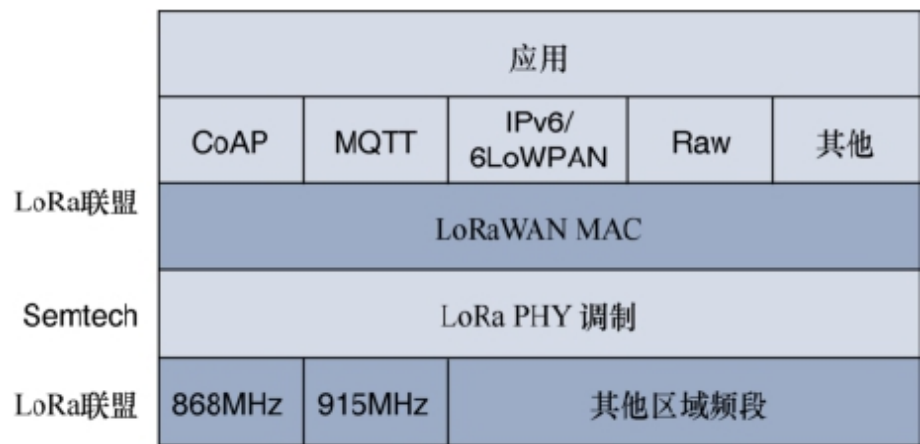


图4-15 LoRaWAN层状图

总的来说，LoRa联盟拥有并管理LoRaWAN体系结构和协议的路线图及技术开发。该联盟还通过其认证和营销委员会处理LoRaWAN端点认证计划和技术推广。

2. 物理层

Semtech LoRa的调制以chirp扩频调制为基础，它会以较低的数据速率来换取接收机的灵敏度，从而显著增加通信距离。此外，它允许在噪声底限以下进行解调，提供对噪声和干扰的稳健性，并管理不同扩频因子对单个信道的占用。这使得LoRa设备能够在多个信道上并行接收信号。

LoRaWAN 1.0.2区域规范描述了使用433 MHz、779~787 MHz、863~870 MHz和902~928 MHz的未经许可的亚GHz频段，以及902~928 MHz带宽子集的区域配置文件。例如，澳大利亚使用915~928 MHz频段，韩国使用920~923 MHz，日本使用920~928 MHz。

注释：Semtech LoRa芯片组支持其他的频段，如169MHz，这些频段不受LoRaWAN规范的支持。LoRA联盟正在考虑开发更多的区域配置文件和频段。

了解LoRa网关对于了解LoRaWAN系统至关重要。LoRa网关被部署为星型网络体系结构的中心枢纽。它使用多个收发器和信道，可以同时解调多个信道，甚至可以同时解调同一信道上的多个信号。LoRa网关充当一个透明的网桥，在端点之间中继数据，端点使用单跳无线连接与一个或多个网关通信。

LoRaWAN的数据速率取决于频段和自适应数据速率（ADR）。ADR是一种为每个端点管理数据速率和无线信号的算法。ADR算法确保数据包以尽可能高的数据速率传输，并且网络性能是最优且可扩展的。靠近网关的端点具有良好的信号值，传输速率最高，这使得无线网络上的传输时间更短，传输功率最低。同时，位于链路预算边缘的端点以最低的数据速率和最高的传输功率进行通信。

注释：LoRaWAN的最佳实践建议对固定端点使用ADR，对移动端点使用固定的数据速率或扩频因子（SF）。当移动终端导致无线环境中的快速变化时，数据速率管理是不实用的。

LoRa的一个重要特性是它能够通过扩频因子处理各种数据速率。具有低扩频因子的设备在通信中实现的距离较短，但传输速度更快，从而缩短了传输时间。

较高的SF提供较慢的传输速率，但在较长的距离实现更高的可靠性。表4-4所示为LoRaWAN数据速率如何随两个主要频段（863~870 MHz和902~928 MHz）的相关扩频因子而变化。

表4-4 LoRaWAN数据速率示例

配置	863~870 MHz(bit/s)	902~928 MHz(bit/s)
LoRa: SF12/125 kHz	250	N/A
LoRa: SF11/125 kHz	440	N/A
LoRa: SF10/125 kHz	980	980
LoRa: SF9/125 kHz	1760	1760
LoRa: SF8/125 kHz	3125	3125
LoRa: SF7/125 kHz	5470	5470
LoRa: SF7/250 kHz	11000	N/A
FSK: 50 kbit/s	50000	N/A

续表

配置	863~870 MHz(bit/s)	902~928 MHz(bit/s)
LoRa: SF12/500 kHz	N/A	980
LoRa: SF11/500 kHz	N/A	1760
LoRa: SF10/500 kHz	N/A	3900
LoRa: SF9/500 kHz	N/A	7000
LoRa: SF8/500 kHz	N/A	12500
LoRa: SF7/500 kHz	N/A	21900

在表4-4中，需要注意SF和数据速率之间的关系。例如，当通道带宽为125 kHz且SF值为12时，数据速率为250 bit/s。但是，当SF减小为7时，数据速率增加至5470 bit/s。

通道带宽值125 kHz、250 kHz和500 kHz在表4-4中列出。增加带宽的效果是，对于相同的扩频因子，可以获得更快的数据速率。

3. MAC层

如前所述，MAC层是在LoRaWAN规范中定义的。该层利用LoRa物理层，并对LoRaWAN端点进行分类，以优化其电池寿命，并确保与LoRaWAN端点的下游通信。LoRaWAN规范记录了3类LoRaWAN设备。

■ A类：该类是默认实现。它针对电池供电的节点进行了优化，允许双向通信，这种情况下给定节点能够接收下游流量。每次传输后都有两个接收窗口可用。

■ B类：在被更好地定义之前，该类在LoRaWAN 1.0.1中被指定为“实验类”。与A类相比，B类节点或端点应该获得额外的接收窗口，但是网关必须通过信标过程进行同步。

■ C类：该类特别适用于供电节点。这种分类使节点在不传输时保持接收窗口打开，从而能够持续监听。

无论是上行链路还是下行链路，LoRaWAN消息都有一个PHY载荷，它由一个1字节的MAC报头、一个可变字节的MAC载荷和一个长度为4字节的MIC组成。MAC载荷大小取决于频段和数据速率，在863~870 MHz频段为59~230字节，在902~928 MHz频段为19~250字节。图4-16显示了高级LoRaWAN MAC帧格式。



图4-16 高级LoRaWAN MAC帧格式

在1.0版本中，LoRaWAN使用了6种MAC消息类型。LoRaWAN设备使用连接请求和连接接受消息进行空中传达（OTA）来激活和连接网络。其他消息类型是未经确认的向上/向下数据和已确认的向上/向下数据。“已确认”消息是必须确认的消息，而“未确认”表示终端设备不需要确认。“向上/向下”只是一个方向符号，用于标识消息是在上行路径还是下行路径中流动。上行链路消息从端点发送到网络服务器，并由一个或多个LoRaWAN网关中继。下行链路消息从网络服务器流

向单个端点，并且仅由一个网关中继。未来版本正在考虑通过LoRaWAN进行多播。

LoRaWAN端点可以通过多种方法进行唯一寻址，包括以下方法。

- 端点可以具有全局终端设备ID或DevEUI，并将其表示为IEEE EUI-64地址。

- 端点可以具有一个全局应用程序ID或AppEUI，表示为IEEE EUI-64地址，该地址唯一地标识应用程序提供商（如终端设备所有者）。

- 在LoRaWAN网络中，端点也可以通过其终端设备地址（称为DevAddr，一个32位地址）来识别。7个最高有效位是网络标识符（NwkID），它标识LoRaWAN网络。25个最低有效位被用作网络地址（NwkAddr）来标识网络中的端点。

注释：LoRa联盟维护一个公司列表，这些公司都已注册了网络标识符（NwkID）。LoRa联盟也分配了新的NwkID。当发布LoRaWAN 1.1规范时，NetID字段将唯一标识网络运营商。该代码也由LoRa联盟管理。NetID中7个最低有效位包含NwkID。DevAddr字段和NetID字段中的NwkID是相同的，因此DevAddr字段中的7个最高有效位必须与NetID的7个最低有效位匹配。

4. 拓扑

LoRaWAN拓扑通常被描述为“星中星”拓扑。如图4-17所示，该基础设施包含通过网关（充当桥接器）交换数据包的端点，以及一个中央LoRaWAN网络服务器。网关使用标准IP连接连接到后端网络，端点直接与一个或多个网关通信。

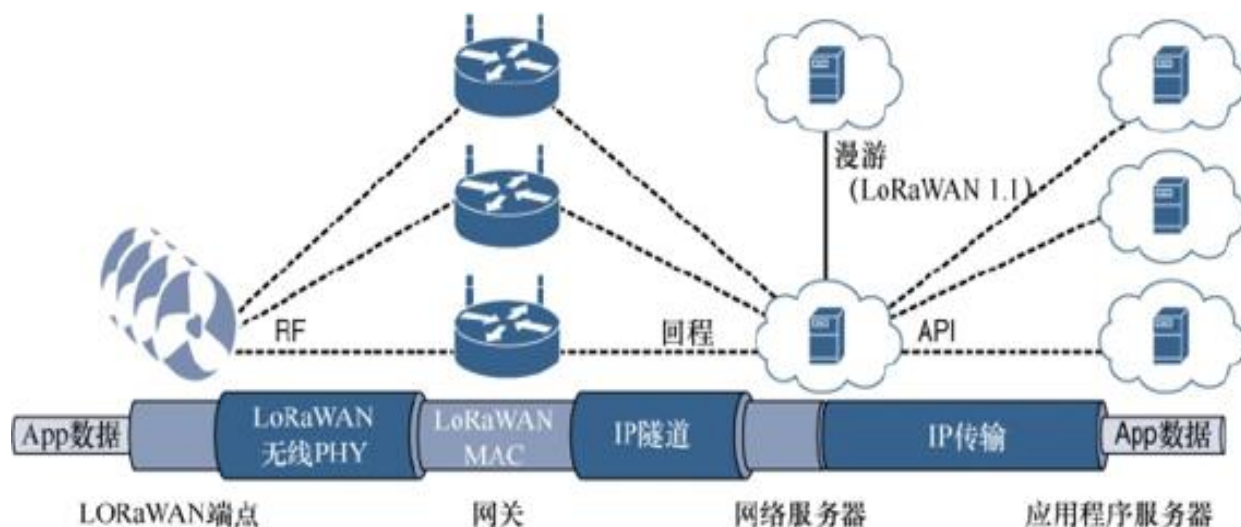


图4-17 LoRaWAN结构

在图4-17中，LoRaWAN端点在一个支持PHY层频段上的LoRaWAN MAC层上传输选定的应用程序数据。应用程序数据包含在上层协议层中。这些上层不属于LoRa联盟的业务范围，但是可以制定和推荐最佳实践。这些上层数据可以是LoRaWAN MAC层上的原始数据，也可以是多个协议中的数据。例如，可以有上层协议，如ZigBee控制层（ZCL）、受限应用程序协议（CoAP）或消息队列遥测传输（MQTT），无论是否有IPv6/6LoWPAN层（第6章讨论了CoAP和MQTT协议）。

图4-17还显示了LoRaWAN网关如何充当端点和网络服务器之间的桥梁。多个网关可以接收和传输相同的数据包。当接收到重复数据包时，网络服务器可以删除重复数据。

注释：LoRa PHY的开发人员Semtech指定了两代LoRaWAN网关。第一代很简单，而第二代（即版本2）增加了一些新特性，比如地理定位。地理定位的工作原理是使版本2的LoRaWAN网关共享一个精确的时间源，然后为每个接收到的LoRa包添加一个高分辨率的时间戳。端点的地理位置可以通过使用时差到达（TDoA）算法来确定。

LoRaWAN网络服务器通过自适应数据速率（ADR）算法管理每个端点的数据速率和射频（RF）。ADR是网络可扩展性、性能和终端电池寿命的关键组成部分。LoRaWAN网络服务器将应用程序数据转发给应用程序服务器，如图4-17所示。

在LoRaWAN规范的未来版本中，网络服务器之间的漫游功能将被添加到LoRaWAN中。这些功能将使移动终端能够在不同的LoRaWAN网络基础设施之间连接和漫游。

5. 安全

LoRaWAN部署中的安全性适用于体系结构的不同组件，如图4-18所示。LoRaWAN端点必须实现两层安全性，保护跨网络的通信和数据隐私。



图4-18 LoRaWAN安全

第一层称为“网络安全”，但应用于MAC层，它保证由LoRaWAN网络服务器对端点进行身份验证。此外，它还通过基于AES执行加密来保

护LoRaWAN包。

每个端点实现一个网络会话密钥（NwkSKey），由其自身和LoRaWAN网络服务器使用。NwkSKey通过计算和检查每个数据消息的MIC，以及加密和解密仅针对MAC的数据消息载荷，来确保数据的完整性。

第二层是应用程序会话密钥（AppSKey），它在端点及其应用程序服务器之间执行加密和解密功能。此外，它计算和检查应用程序级消息完整性代码（如果包括）。这确保LoRaWAN服务提供商在不允许访问应用程序载荷的情况下无法对其进行访问。

端点从应用程序所有者接收AES-128应用程序密钥（AppKey）。此密钥很可能源生自特定应用程序的根密钥，该根密钥由应用程序提供商专有，并且由其控制。

对于生产部署，人们希望LoRaWAN网关也受到保护，以保护LoRaWAN流量以及通过其回程链路进行的网络管理和操作。这可以使用传统的VPN和IPSec技术来实现，这些技术在传统IT部署中具有可扩展性。LoRaWAN联盟正在评估其他安全附加组件，以便将来对规范进行修订。

在将LoRaWAN端点连接到LoRaWAN网络时，必须进行注册并验证。这可以通过以下两种加入（join）机制之一实现。

■ 个性化激活（ABP）：端点不需要运行加入过程，因为它们的个别详细信息（包括DevAddr、NwkSKey和AppSKey会话密钥）已预先配置并存储在终端设备中。相同的信息在LoRaWAN网络服务器中注册。

■ 空中激活（OTAA）：在成功完成加入过程后，允许端点动态地加入到特定的LoRaWAN网络。每次更新会话上下文时都必须执行加入过程。在加入过程中，包括发送和接收MAC层加入请求和加入接受消息，节点与LoRaWAN网络服务器建立凭据，交换其全局唯一的DevEUI、AppEUI和AppKey。然后使用AppKey派生会话NwkSKey和AppSKey密钥。

6. 竞争技术

LPWA解决方案和技术分为未经许可的频段和许可频段。许可频段技术专用于已取得频段牌照的移动服务供应商（下一节将讨论这些技术）。此外，一些技术公司已经瞄准未经许可频段的LPWA市场，与LoRaWAN竞争。LPWA市场正在迅速发展。表4-5评估了两个已知的提供LPWA选项的最佳供应商。

表4-5 未经许可的LPWA技术比较

特点	LoRaWAN	Sigfox	Ingenu Onramp
频段	433 MHz、868 MHz、 902~928 MHz	433 MHz、868 MHz、 902~928 MHz	2.4 GHz
调制	线性调频扩频	超窄带	DSSS
拓扑	星型	星型	星型；树状由 RPMA 扩展器支持
速率	250 bit/s ~ 50 kbit/s (868 MHz) 980 bit/s ~ 21.9 kbit/s (915 MHz)	100 bit/s (868 MHz) 600 bit/s (915 MHz)	6 kbit/s

续表

特点	LoRaWAN	Sigfox	Ingeni Onramp
自适应数据速率	是	否	否
载荷	59~230 B (868 MHz) 19~250 B (915 MHz)	12 B	6 B~10 KB
双向通信	是	部分是	是
地理位置	是 (LoRa GW 版本 2 参考设计)	否	否
漫游	是 (LoRaWAN 1.1)	否	是
规范	LoRa 联盟	私有	私有

表4-5很好地概述了两个最成熟的LoRaWAN竞争对手。如果对部署LPWAN感兴趣，可以进行更深入的研究，以进一步区分这些技术。

7. LoRaWAN小结

LoRaWAN无线技术是为LPWAN开发的，对于在物联网网络上实施许多新设备至关重要。术语LoRa指的是物理层，而LoRaWAN则侧重于体系结构、MAC层以及无缝交互性的统一标准。LoRaWAN由行业组织LoRa联盟来管理。

物理层和MAC层允许LoRaWAN覆盖更远的距离，数据速率可以根据各种不同的因素而变化。LoRaWAN体系结构依赖于网关将端点桥接到网络服务器。从安全角度看，LoRaWAN在两个独立的层提供AES身份验证和加密。

未经许可的LPWA技术为私有企业网络、广播公司、移动和非移动服务提供商实施物联网基础设施、解决方案和用例提供了新的机会。端点生态系统正在迅速发展，必将成为各种LPWA技术和解决方案（包括LoRaWAN）之间的纽带。智慧城市运营商、广播公司、移动和非移动

服务提供商正在解决区域或国家物联网基础设施的需求，这些提供商对于为消费者市场启用用例尤其重要。

随着私营企业考虑开发LPWA网络，它们将受益于私有和公共基础设施之间的漫游能力。LPWA网络可以类似于WiFi基础设施进行部署，并可以与许可频段LPWA选项共存。总的来说，LoRaWAN和其他LPWA技术满足了物联网领域的明确需求，随着越来越多的“物”需要相互连接，这种需求将继续增长。

4.2.6 NB-IoT和其他LTE变体

现有的蜂窝技术，如GPRS、Edge、3G和4G/LTE，并不特别适合于电池供电的设备和专为物联网开发的小型设备。虽然行业参与者一直在开发未经许可频段的LPWA技术，但3GPP和相关供应商一直在致力于发展蜂窝技术，以更好地满足物联网的需求。这项工作始于定义新的LTE设备类别，其目标是既符合特定的物联网需求，如低吞吐量和低功耗，又能降低LTE设备的复杂性和成本。LTE-M工作项目应运而生。

注释：第三代伙伴关系项目（3GPP）是一个标准组织，它将多个电信标准开发组织联合起来，提供一个稳定的环境来生成定义3GPP技术的报告和规范。

由于新的LTE-M设备类别与LPWA的功能还不够接近，2015年3GPP批准了一项提案，旨在将一种名为窄带物联网（NB-IoT）的新窄带无线接入技术标准化。NB-IoT特别针对大量低吞吐量设备、低设备功耗、改善室内覆盖范围、优化网络架构的需求。以下部分将讨论蜂窝技术的发展，以更好地支持移动服务提供商提供的物联网机会。

1. 标准化和联盟

3GPP组织包括多个工作组，它们分别专注于电信的不同方面（例如，无线电、核心、终端等）。许多服务提供商和供应商组成了3GPP，它们在这些领域的合作成果是3GPP规范和相关研究。3GPP中的

工作流程包括从相关供应商接收与LPWA工作授权相关的贡献。然后，根据紧密结合的接入技术，如3G、LTE或GSM，与IoT相关的贡献由3GPP或GSM EDGE无线接入网（GERAN）工作组负责。

移动设备供应商和服务提供商不愿在连接物联网设备的市场中失去领导地位。因此，已经推进了一些中间步骤，最终确定了NB-IoT的目标，并由3GPP记录。与此同时，另一个行业组织GSM协会（GSMA）提出了移动物联网计划，该计划“旨在加速许可频段中LPWA解决方案的商业可用性”。

2. LTE Cat 0

为了更好地支持3GPP中的物联网设备，第一个增强出现在LTE第12版。增加了一个新的用户设备类别（UE）—— Cat 0，其中设备的最大数据速率为1 Mbit/s。一般来说，LTE增强的目标是提高带宽。Cat 0包括网络和终端设备都支持的重要特性。同时，UE仍然可以在现有LTE系统中运行，带宽高达20MHz。这些Cat 0特性如下所示。

■ **节能模式（PSM）：**这种新的设备状态将能耗降至最低。与现有的空闲模式相比，PSM的能耗预计会更低。PSM被定义为类似于“关机”模式，但是设备仍然在网络上注册。通过保持注册状态，设备可以避免重新连接或重新建立网络连接。设备与网络协商空闲时间，之后它将被唤醒。被唤醒时，它启动一个跟踪区域更新（TAU），在此之后，它将在配置的时间内保持可用状态，然后切换回睡眠模式或PSM。TAU是LTE设备用来使网络了解其当前跟踪区域或网络中可以到达的塔群的过程。总体来说，在PSM模式下，设备实际上可以关闭电源，但不会丢失它在网络中的位置。

■ **半双工模式：**由于不需要双工滤波器，这种模式降低了设备实现的成本和复杂性。大多数物联网终端是传感器，它们发送的数据量较小，不需要全双工通信。

注释：最近的LTE芯片组应该支持LTE Cat 0，因为供应商从2015年开始宣传它们的芯片组支持LTE Cat 0。然而，系统应用和市场接受度仍有待证明。

3. LTE-M

继LTE Cat 0之后，下一步是为3GPP LTE第13版引入LTE-M类，使许可频段更支持物联网设备。以下是第13版LTE-M类的主要特点。

- 较低接收带宽：带宽已经从通常的20MHz降低至1.4MHz。这进一步简化了LTE端点。

- 较低的数据速率：LTE-M的数据速率约为200kbit/s，而Cat 0的数据速率为1Mbit/s。

- 半双工模式：与Cat 0一样，LTE-M提供了一种降低节点复杂度和成本的半双工模式。

- 增强的不连续接收（eDRX）：该功能将端点在寻呼周期之间的“休眠”时间从几秒增加到几分钟。寻呼周期是指设备先后两次登入网络的间隔。寻呼周期之间延长的“睡眠”时间显著延长了端点的电池寿命。

LTE-M需要新的芯片组并需要开发额外的软件，预计在2017年进行商业部署。移动运营商预计，基站只需要新的LTE-M软件，无须对硬件再投资。

4. NB-IoT

在认识到新的LTE设备类别的定义不足以支持LPWA物联网需求后，3GPP指定了窄带物联网（NB-IoT）。NB-IoT的工作从参与厂商提出的多个提案开始，包括以下内容：

- 扩展覆盖GSM（EC-GSM），爱立信提案；
- 窄带GSM（N-GSM），诺基亚提案；
- 窄带M2M（NB-M2M），华为/Neul提案；
- 窄带OFDMA（正交频分多址），高通提案；
- 窄带蜂窝物联网（NB-CIoT），NB-M2M和NB-OFDMA联合提案；
- 窄带LTE（NB-LTE），阿尔卡特朗讯、爱立信和诺基亚提案；
- 合作超窄带（C-UNB），Sigfox提案。

上述提案在协议中进行了整合，它以下行链路中的正交频分多址（OFDMA）和上行链路中的两个选项为基础，指定了一个NB-IoT版本。OFDMA是一种调制方案，它为单个用户分配子载波频率的子集。这使得多个用户可以同时传输低速数据。有关上行链路选项的更多信息，请参阅3GPP规范TR 36.802。

NB-IoT有3种运营模式。

- 单机：GSM载波用作NB-IoT载波，这可以重用900 MHz或1800 MHz。

- 带内：LTE载波频段的一部分拿出来供NB-IoT频率使用。服务提供商通常进行这种分配，并相应地配置物联网设备。读者应该知道，如果这些设备必须通过不同的服务提供商在不同的国家或地区部署，除非服务提供商之间进行过协调，并且NB-IoT频段分配是相同的，否则可能会出现问题。

- 保护频段：NB-IoT载波位于LTE或WCDMA频段之间。这需要LTE和NB-IoT频段共存。

在第13版中，3GPP完成了NB-IoT的标准化。除了无线电相关的方面，这项工作还指定了物联网核心的适应性，以支持特定的物联网功

能，包括简化LTE附加过程，从而不需要专用承载信道，而且可以传输非IP数据。3GPP NB-IoT的后续版本将引入额外的特性和功能，如多播，并将向后与第13版兼容。

移动服务提供商将NB-IoT作为目标技术，因为它允许利用许可频段支持LPWA用例。例如，NB-IoT定义为上行链路和下行链路均为200 kHz宽的信道，允许移动服务提供商优化其频段，并提供了GSM、WCDMA和LTE频段的多种部署选项，如图4-19所示。

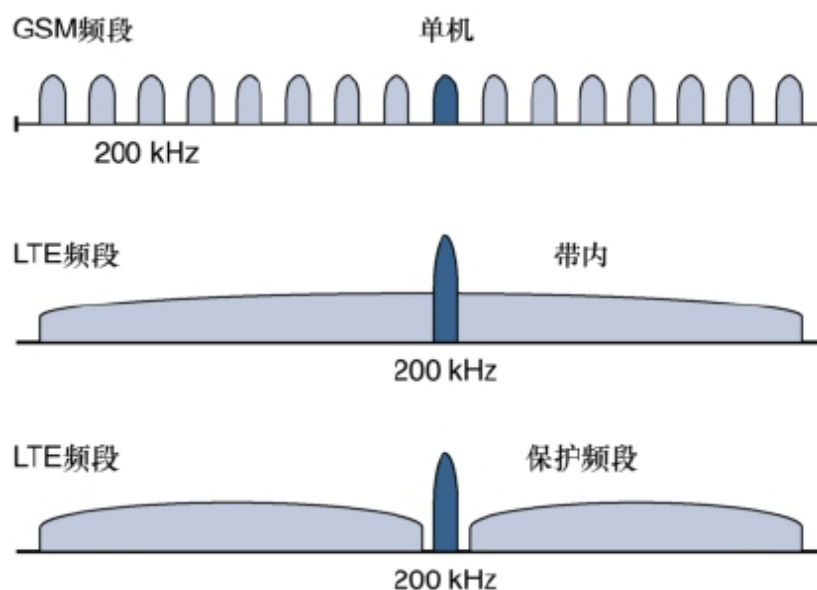


图4-19 NB-IoT部署选项

在LTE网络中，频段资源块被定义为具有180 kHz的有效带宽，而在NB-IoT中，信道或子载波代替了LTE频段资源块。上行链路信道可以是15kHz或3.75 kHz或多频音道（ $n \times 15\text{kHz}$ ， n 最大为12）。在第1层，下行链路的最大传输块大小（TBS）为680比特，上行链路为1000比特。在第2层，分组数据汇聚协议（PDCP）服务数据单元（SDU）最大为1600字节。

NB-IoT采用半双工频分双工（FDD）模式，上行链路的最大数据速率为60kbit/s，下行链路的最大数据速率为30kbit/s。

5. 拓扑

NB-IoT由164 dB的链路预算来定义，将此与许多机器对机器（M2M）服务使用的大小为144 dB的GPRS链路预算进行比较，可以发现额外增加的20 dB链路预算应能保证信号更好地穿透建筑物和地下室，同时达到电池寿命的要求。

6. 竞争技术

在许可频段，预计3GPP NB-IoT在完全可用时将成为大规模应用的LPWA技术。竞争技术主要是未经许可的LPWA技术，如LoRaWAN。许可频段提供商面临的主要挑战是非移动服务提供商有机会在无须购买昂贵频段的情况下，通过提供物联网基础设施来抢占市场份额。

7. NB-IoT和其他LTE版本的小结

对于拥有许可频段的移动服务提供商来说，NB-IoT代表着LPWA技术的未来。与物联网相关的规范必须由3GPP完成并发布，以使供应商、移动服务提供商和应用程序能够成功且广泛地认可该技术。eSIM还在发展之中，尽管没有得到广泛支持，但应该与NB-IoT结合起来，因为管理数百万张SIM卡可能无法被市场接受。eSIM卡在多个运营商之间兼容，并且可重新配置。这意味着它是设备的永久部分，如果设备切换到不同的提供商，它很容易被重写。

4.3 小结

本章讨论了支持物联网智能对象部署的通信标准以及重要的最新技术。4.1节提供了评估智能对象的标准，以及连接需要的条件。这些标准包括传输范围、频段、功耗、拓扑结构以及受限的设备和网络。在处理物联网部署和网络时，评估这些标准至关重要。

4.2节详细讨论了连接传感器的主要技术。虽然有各种各样的技术可以用于此目的，但其中许多技术还处于起步阶段，并将在今后几年内不断发展。本章基于当前的市场趋势、行业支持和市场份额，全面介绍了最有前景的技术。4.2节涉及的技术包括IEEE 802.15.4、IEEE 802.15.4g 和 IEEE 802.15.4e 、 IEEE 1901.2a 、 IEEE 802.11ah 、 LoRaWAN和NB-IoT。读者应该对这些技术有一定的认识和基础知识，因为它们连接物联网智能对象的基础；此外，了解这些技术将为您了解新技术提供基础。表4-6总结并比较了本章讨论的接入技术的一些主要特征。

表4-6 本章讨论的接入技术的主要特点

特点	IEEE 802.15.4	IEEE 802.15.4g 与 IEEE 802.15.4e	IEEE 1901.2a	IEEE 802.11ah	IEEE 802.11ah	NB-IoT
有线或无线	无线	无线	有线	无线	无线	无线
频段	未经许可的 2.4 GHz 和 亚 GHz	未经许可的 2.4 GHz 和亚 GHz	未经许可的 CENELEC A 和 B、 FCC ,ARIB	未经许可的 亚 GHz	未经许可的 亚 GHz	被许可
拓扑	星型、网状	星型、网状	网状	星型	星型	星型
范围	中程	中程	中程	中程	远程	远程
速率	低	低	低	低-高	低	低

第5章 IP作为物联网网络层

第4章介绍了创建物联网网络的重要考虑因素，以及智能对象用于访问和与网络通信的通用协议。第4章主要讨论第1层（PHY）和第2层（MAC）的连接。在本章中，我们向上移动协议栈，讨论网络层连接，通常称为第3层。回顾图2-7中介绍的核心物联网功能栈，本章介绍了作为通信网络层一部分的网络传输层子层。读者也可以让本章与图2-1所示的oneM2M架构的网络层保持一致，或者与图2-3所示的物联网世界论坛架构的连接层保持一致（如果这些模型更可取的话）。

本章由以下部分组成。

■ IP的商业案例：从物联网角度讨论IP的优势，并介绍采用和适应的概念。

■ 优化的需要：将深入探讨在部署IP时受限节点和设备的挑战。本节还将介绍从IPv4到IPv6的迁移及其对物联网的影响。

■ 针对物联网来优化 IP：探讨物联网中使用 IP 的常见协议和技术，包括 6LoWPAN 6TiSCH和RPL。

■ 概要文件和合规性：对一些涉及IP连接和物联网的重要组织和标准机构进行了汇总。本章以前面介绍的许多技术为基础。事实上，这些章节中的协议和技术经常是成对的，在开发时要考虑到这种配对关系。例如，802.15.4和6LoWPAN在许多应用程序中经常成对出现。

本章重点关注IP，IP已成为物联网许多领域的事实标准。在众多标准和行业组织的支持下，IP及其作为物联网网络层传输的角色是读者应该熟悉的基本要素。

5.1 IP的商业案例

流入或流出物联网中“物”的数据流由数据中心服务器使用、控制或监视，这些服务器可以位于云中，也可以位于分布或集中的位置。然后，专用的应用程序在虚拟或传统操作系统或网络边缘平台（例如，雾计算）上运行。这些轻量级应用程序与数据中心服务器通信。因此，将各种物理层和数据链路层组合在一起的系统解决方案需要一种体系结构方法，该方法具有独立于较低层（连接性）和/或较高层（应用程序）的公共层。这就是为什么互联网协议（IP）在20世纪90年代初开始扮演关键的架构角色的原因。IP不仅是IT市场的首选，也是OT环境的首选。

5.1.1 因特网协议的主要优点

传统信息技术（IT）和运营技术（OT）之间的主要区别之一是底层技术和产品的生命周期不同（有关OT和IT的更多信息，请参阅第1章）。一个完整的工业工作流程通常要求平稳的、渐进的、不断发展的步骤，运营本身是组织中最关键的时间和任务因素。

定义一个分层的体系结构是确保结构可以多年使用的一种方法，如已有30年历史的IP体系结构。IP已经在很大程度上证明了其整合小型和大型演进的能力。与此同时，它还能够维持大量设备和用户（比如30亿互联网用户）的运营。

注释：使用互联网协议套件并不意味着运行IP的物联网基础设施必须是开放或可公开访问的网络。实际上，许多现有的关键任务是私有且高度安全的网络，如银行与银行之间的网络、军事和防御网络、公共安全和应急响应网络，使用的都是IP架构。

在评估IP的接纳性和适应性优缺点之前，本节将对物联网的IP套件的关键优势进行简要介绍。

■ 开放的和基于标准的：运营技术通常由供应商作为“交钥匙”特性交付，它们可能通过封闭和专有的网络解决方案优化了通信。物联网创建了一种新的模式，在这种模式中，设备、应用程序和用户可以利用大量的设备和功能，同时保证互换性、交互性、安全性

和管理性。这需要实现、验证和部署基于标准的开放解决方案。尽管许多标准开发组织（SDO）正在研究物联网的定义、框架、应用程序和技术，但没有人质疑Internet工程任务组（IETF）在指定和优化网络层和传输层方面所发挥的作用。IETF是一个开放的标准组织，专注于互联网协议套件及相关互联网技术和协议的开发。

■ 多用途：大量的接入技术可以提供“最后一公里”范围内的连接。附加的协议和技术也用于通过回程链路和数据中心传输物联网数据。即使物理和数据链路层（如以太网、WiFi和蜂窝网络）被广泛采用，但数据通信的历史表明，没有任何一种特定的有线或无线技术符合所有的部署标准。此外，通信技术的发展速度比OT解决方案预期的10~20年的生命周期要快。因此，分层IP架构可以很好地处理任何类型的物理和数据链路层。这使得IP成为一项理想的长期投资，因为这些层上的各种协议可以在部署中随时使用，而无须更改整个解决方案体系结构和数据流。

■ 无处不在：所有最近发布的操作系统，从通用计算机和服务器的轻量级嵌入式系统（TinyOS、Contiki等），都有一个集成的双IP栈（IPv4和IPv6），随着时间的推移，这个栈会得到增强。此外，近年来，许多行业OT解决方案中的物联网应用协议已得以更新，以在IP上运行。虽然到目前为止这些更新主要由IPv4组成，但是最近几个领域的标准化工作正在添加IPv6。事实上，当我们比较各种物联网解决方案和行业垂直领域所支持的协议时，可以发现IP是最普遍的协议。

■ 易于管理和高度安全：通信基础设施需要适当的管理和安全能力。已运行 30 年的IP网络的好处之一是，人们对广泛使用的网络管理和安全协议、机制和工具集有了充分的理解。采用IP网络管理也为OT带来了可操作的业务应用。众所周知的网络和安全工具很容易与IP网络层结合使用。但是，大家应该意识到，尽管IP具有安全性，但在这方面仍然存在真正的挑战。具体来说，业界在保护受限节点，处理遗留OT协议和扩展操作等方面面临挑战。

■ 稳定性和恢复能力：IP已经存在了30年，很明显是一个可行的解决方案。IP拥有一个庞大且完善的知识库，更重要的是，它已经在

金融和国防网络等关键基础设施中使用了多年。此外，IP已被用于语音和视频等关键服务，这些服务已经从封闭的环境过渡到开放的IP标准。最后，它的稳定性和恢复能力得益于由IT专业人员构成的大生态系统，他们可以帮助设计、部署和操作基于IP的解决方案。

■ 消费者市场接受度：在开发面向消费者市场的物联网解决方案和产品时，供应商知道消费者主要通过宽带和移动无线基础设施来访问应用程序和设备。消费者的主要设备包括智能手机、平板电脑和个人电脑。将消费者领域的物联网与这些设备连接起来的通用协议是IP。

■ 创新因素：在过去 20 年，知识产权在很大程度上成为推动创新的一个因素。IP是应用程序的底层协议，应用范围从文件传输和电子邮件到万维网、电子商务、社交网络、移动网络等。即使是最近从PC到移动设备，从大型主机到云服务的计算技术的发展，也完美地展示了IP技术的创新领域。物联网也可以利用IP基础进行创新。

综上所述，IP的应用为物联网提供了坚实的基础，为网络中所有设备提供了安全且可管理的双向数据通信能力。IP协议是一种基于标准的协议，具有普遍性、可扩展性、通用性和稳定性。命名、时间分布、流量优先级分配、隔离等网络服务都是可以利用IP的知名和成熟的技术。在云、集中式或分布式架构中，IP数据流可以根据业务需求进行开发和实现。然而，读者可能想知道IP是否是一个端到端的需求，这将在下一节中讨论。

5.1.2 应用或自适应互联网协议

如何在数据中心、云服务和托管物联网应用的运营中心中实现IP，这似乎是显而易见的，但在“最后一公里”采用IP则更加复杂，往往会让端到端运行IP更加困难。

如果从总体上了解IT网络中IP应用的历史趋势，我们可以对IP在“最后一公里”中的应用应该如何展开有一些深刻的见解。在IPv4

被广泛接受并部署到IT网络之前，许多不同的协议栈与IP重叠。例如，X.25/X.75被服务提供商标准化和推广，而计算机制造商实现了其专有协议，如SNA、DECnet、IPX和AppleTalk。这种网络层协议的扩展需要多协议路由器来处理。

除IP外，是否使用多种网络层协议常常是计算机网络专家之间的一个争论点。通常会建议使用两种模式，即自适应或应用。

■ 自适应意味着必须实现应用程序分层网关（ALG），以确保非IP层和IP层之间的转换。

■ 应用涉及将所有非IP层替换为对应的IP层，从而简化部署模型和操作。

类似的转变正在物联网以及使用IP连接的“最后一公里”中发生。虽然IP正在慢慢变得更加普遍，但是仍然经常使用替代协议栈。我们来看几个不同行业的示例，以了解IP自适应和应用目前是如何应用于物联网“最后一公里”连接的。

在工业和制造业领域，IP应用已经成为一种趋势。这个领域的解决方案和产品生命周期超过10年，并且已经开发了许多用于串行通信的协议。虽然在初始版本中没有规定对IP和以太网提供支持，但是这些串行通信协议的最新规范集成了以太网和IPv4。

监视控制和数据采集（SCADA）应用程序是垂直市场部署的典型示例，它们同时运行IP自适应模式和应用模式。在许多现代工业的核心，SCADA是一种用于远程监控和控制设备的自动化控制系统。利用IP自适应模式的实现将SCADA设备通过串行接口连接到网关隧道或转换流量。在IP应用模式下，SCADA设备通过以太网连接到交换机和路由器，转发其IPv4流量。有关SCADA的更多信息，请参见第6章。

另一个示例是ZigBee解决方案，它在设备和ZigBee网关之间运行一个非IP堆栈，ZigBee网关将流量转发到应用服务器。有关ZigBee的更多信息，请参见第4章。ZigBee网关通常充当ZigBee和IP协议栈之间的转换器。

正如这些示例所强调的，IP自适应与应用模式仍然需要对物联网使用的特定“最后一公里”技术进行调查。在试图确定哪个模式最适合“最后一公里”连接时，应该考虑以下因素。

■ **双向与单向数据流：**虽然人们通常期望双向通信，但一些“最后一公里”技术为单向通信提供了优化。例如，第4章讲到，在RFC 7228中定义的不同种类的物联网设备可能只是偶尔需要向应用程序报告几个字节的数据。这些类型的设备，特别是通过LPWA技术进行通信的设备，包括发出警报或每日测试报告的火警警报、按下或关闭的电气开关以及发送每周指数的水表或煤气表。第4章进一步讨论了LPWA。对于这些情况，不一定需要实现完整的IP堆栈。然而，它需要整体的端到端架构来解决潜在的缺陷。例如，如果只有单向通信将数据上载到应用程序，则无法将软件或固件下载到设备上。这使得集成新特性、漏洞和安全修复变得更加困难。

■ **最后一公里通信路径的开销：**采用IP意味着对结构分层，且每个包的开销根据IP版本而变化。IPv4至少有20字节的报头，IPv6在IP网络层有40字节。对于IP传输层，UDP有8字节的报头开销，而TCP只有20字节。如果设备转发的数据很少，而且只有几字节，那么读者可能会再次具有比设备数据更多的头部开销，特别是在应用LPWA技术的情况下。因此，读者需要确定是否需要IP应用模式，如果需要，则需要确定如何优化该模式。同样的考虑也适用于在IP上运行的低带宽链路和“最后一公里”链路的平面流量。路由协议和其他详细的网络服务可能不需要优化，也可能需要优化。

■ **数据流模型：**IP应用模式的一个好处是通信是端到端进行的。任何节点都可以轻松地与网络中的任何其他节点交换数据，尽管安全、隐私和其他因素可能会对端到端这一概念进行控制和限制。然而，在许多物联网解决方案中，设备的数据流被限制在一个或两个应用程序中。在这种情况下，自适应模型可以工作，因为只需要在终端设备和一个或两个应用服务器之间转换流量。根据网络拓扑结构和所需的数据流，IP自适应模式和应用模式在“最后一公里”连接中都要发挥作用。

■ 网络多样性：自适应模型的缺点之一是通常依赖于单个物理层和MAC层。例如，ZigBee设备只能部署在ZigBee网络孤岛上。同样的限制也适用于ITU G.9903 G3-PLC节点。因此，在部署时必须考虑哪些应用程序必须在连接这些信息孤岛和世界其他地区的网关上运行。新物理层和MAC层或新应用程序的集成和共存会影响部署和操作的计划方式。这与应用模式无关。

5.2 优化的需要

如前一节所述，物联网主要构建在Internet协议集上。然而，在物联网解决方案中，IP仍然存在挑战。除了应对非IP设备的集成外，我们可能还需要处理物联网在设备和网络级别施加的限制。因此，需要在IP堆栈的各个层进行优化，以处理物联网网络中存在的限制。

下面将详细讨论为什么需要对IP进行优化。在物联网解决方案中，节点和网络本身都可能受到限制。此外，IP正在从版本4过渡到版本6，这可能会进一步限制物联网的空间。

5.2.1 受限节点

如表4-1所示，在物联网解决方案中，不同类型的设备共存。根据物联网中“物”的架构在网络中的功能，它可能提供与IT环境中的普通PC或服务器类似的特性，也可能不提供。

另一个限制是物联网节点上的网络协议栈可能需要通过不可靠的路径进行通信。即使节点上有完整的IP堆栈可用，当拓扑发生变化时，这也会导致诸如吞吐量有限或不可预测以及收敛性低等问题。

最后，功耗是受限节点的关键特性。许多物联网设备都是电池供电的，电池寿命要求从几个月到10年以上不等。这推动了对网络技术的选择，因为诸如以太网、WiFi和蜂窝网络等高速网络还不具备多年的电池续航能力。目前允许应用这些技术的电池供电节点的电池续航

时间少于一年。当然，在不需要电池作为能量来源的节点上，电能消耗不那么重要。

读者还应该注意电池供电节点的功耗需求会影响通信间隔。为了延长电池寿命，我们可以启用低功耗模式，而不是“常开”模式。另一个选项是“常闭”，这意味着只在需要发送数据时才启用通信。

虽然已经有大量证据表明生产型IP协议栈在受限节点上表现良好，但是对这些节点进行分类有助于评估是选用IP应用模式还是自适应模式。物联网受限节点可分为以下几种。

- 资源非常有限的设备，可能不经常通信且通信时只传输几个字节，并且可能具有有限的安全性和管理能力：这就需要IP自适应模式，其中节点通过网关和代理进行通信。

- 具有足够的功率和容量来实现简化的IP堆栈或非IP堆栈的设备：在这种情况下，可以实现优化的IP堆栈并直接与应用程序服务器通信（应用模式）；也可以使用IP或非IP堆栈并通过网关和代理进行通信（自适应模式）。

- 在计算和电源资源方面与普通PC相似，但具有受限的网络容量（如带宽）的设备：这些节点通常实现完整的IP堆栈（应用模式），但网络设计和应用程序行为必须满足带宽限制。

受限节点的定义正在发生演变。计算能力、内存、存储资源和功耗的成本普遍降低。与此同时，网络技术不断改进，提供了更多的带宽和可靠性。在未来，随着技术的改进和成本的降低，这些挑战将逐步解决，为受限节点优化IP的压力将会降低。

5.2.2 受限网络

在Internet的早期，由于技术限制，网络带宽容量受到限制。连接通常依赖于低速调制解调器来传输数据。这些低速连接表明IP可以在低带宽网络上运行。

当今，随着网络的快速发展，高速基础设施随之出现。然而，在“最后一公里”，一些物联网设备无法使用高速连接。原因包括低带宽技术的实施、由于调节传输功率导致的有限的距离和带宽，以及缺乏网络服务或网络服务有限。当理所当然的链路层特性不存在时，网络就受到了约束。一个受限的网络可能有很高的延迟，而且很可能会丢包。

注释：受限网络通常被称为低功耗和有损网络（LLN）。本书中，损耗是指由数据流中断或数据包丢失导致的网络不可靠性。在开发IPv6 RPL协议时，IETF的低功耗和有损网络（RoLL）工作组定义了LLN。IETF工作组是由特定技术领域的个人组成的公开讨论组。他们有一份章程，规定了他们的工作重点和工作内容（本章后面将更详细地讨论RPL）。

受限网络具有独特的特性和要求。与具有高度稳定性和快速链路的传统IP网络不同，受限网络受到低功耗、低带宽链接（无线和有线）的限制。它们的运行速率在几kbit/s到几百kbit/s之间，可以使用星型、网状或组合网络拓扑，以确保能正常运行。

在一个受限网络中，除有限的带宽外，分组传送速率（PDR）在低百分比和高百分比之间振荡也是正常的。有时可能会出现大量不可预测的错误，甚至会失去连接。这些行为可能会出现在无线和窄带电力线通信链路上，其中数据包传送的变化在一天中可能会波动很大。

不稳定的链路层环境在延迟和控制平面反应性方面带来了其他挑战。在一个受限网络中，一个黄金法则是“对故障反应不足”。由于低带宽的限制，网络反应过度会导致网络崩溃，使现有问题更加严重。

控制平面流量也必须保持在最低值；否则，它将消耗数据流量所需的带宽。最后，必须考虑电池供电节点的功耗。任何故障或详细的控制平面协议都可能缩短电池的使用寿命。

综上所述，受限节点和网络对物联网“最后一公里”的连接构成了重大挑战。这促使各种标准组织致力于物联网优化协议。本章后面

将更详细地讨论IP优化。

注释：除优化物联网协议外，IETF还发布了物联网实施指南。这些工作大部分是在IETF轻量级实现指导（LWIG）工作组中进行的。

5.2.3 IP版本

20多年来，IETF一直致力于将互联网从IP版本4过渡到IP版本6，主要驱动力是随着互联网的发展，IPv4的地址空间日益缺乏。IPv6的地址范围要大得多，在可预见的未来不会耗尽。如今，两个版本的IP都在Internet上运行，但是大多数流量仍然基于IPv4。

虽然基于IPv6部署物联网看起来很自然，但大家必须考虑到当前的基础设施及其相关的解决方案、协议和产品的生命周期。IPv4扎根于当前的基础设施中，在大多数情况下需要支持它。因此，物联网必须遵循与互联网本身相似的路径，同时支持IPv4和IPv6两个版本。物联网解决方案需要使用隧道和地址转换等技术来确保IPv4和IPv6之间的交互性。

各种因素决定了IPv4、IPv6或两者都可以用于物联网解决方案。这些因素通常包括仅支持IPv4的传统协议或技术。较新的技术和协议几乎总是同时支持两个IP版本。以下是在物联网解决方案中有必要同时支持IPv4和IPv6的一些主要因素。

■ 应用协议：实现以太网或WiFi接口的物联网设备可以通过IPv4和IPv6进行通信，但应用协议可能会决定IP版本的选择。例如，DNP3/IP（IEEE 1815）、Modbus TCP等SCADA协议，或IEC 60870-5-104标准仅针对IPv4，如第6章所述。因此，目前还没有供应商基于IPv6实现这些协议。对于使用IETF定义的应用程序协议的IoT设备，如HTTP/HTTPS、CoAP、MQTT和XMPP，在两个IP版本都得到支持（有关这些物联网应用层协议的更多信息，请参见第6章）。IP版本的选择仅取决于实施。

■ 蜂窝提供商和技术：带有蜂窝调制解调器的物联网设备依赖于蜂窝技术的产生以及供应商提供的数据服务。对于前三代数据服务（GPRS、Edge和3G），IPv4是基本协议版本。因此，如果IPv6与这些数据服务结合，则必须通过IPv4进行隧道传输。在4G/LTE网络上，数据服务可以使用IPv4或IPv6作为基础协议，具体取决于服务提供商。

■ 串行通信：某些行业中的许多传统设备，如制造业和公用事业，通过串行线路进行通信。数据传输使用专有或基于标准的协议，如DNP3、Modbus或IEC 60870-5-101。在过去，任何距离的串行数据通信都可以通过模拟调制解调器连接来处理。然而，由于服务提供商对模拟线路服务的支持有所下降，因此与这些传统设备通信的解决方案是使用本地连接来实现的。要实现这一功能，需要将传统设备的串行端口连接到通信设备（通常是路由器）上附近的串口。然后，这个本地路由器通过IP将串行通信转发到中央服务器进行处理。串行协议在IP层上的封装是使用原始套接字TCP或UDP等机制实现的。虽然原始套接字会话可以在IPv4和IPv6上运行，但是目前大多数实现只适用于IPv4。

■ IPv6适配层：针对一些物理层和数据链路层的IPv6适配层，最近标准化的物联网协议只支持IPv6。虽然最常见的物理链路层和数据链路层（以太网、WiFi等）规定了两个版本的适配层，但较新的技术，如IEEE 802.15.4（无线个人区域网络）、IEEE 1901.2和ITU G.9903（窄带电力线通信）只指定了IPv6适配层（有关这些物理和数据链路层的更多信息，请参见第4章）。这意味着任何需要IPv6适配层的设备都必须通过只支持IPv6的子网进行通信。IETF针对LLN的路由协议RPL（仅限于IPv6）加强了这一点。本章后面将更详细地讨论RPL路由协议。

注释：转换机制（如使用转换[MAP-T]的地址和端口映射）允许IPv4流量通过IPv6网络转发。这些技术使较老的工业终端设备和应用程序能够继续运行IPv4，即使提供连接的网络是IPv6。通常这些传统设备和应用程序甚至无法通过升级来支持IPv6。有关MAP-T的更多信息，请参见第6章。

5.3 针对物联网来优化IP

虽然互联网协议是物联网成功的关键，但受限节点和受限网络则要求在IP体系结构的各个层和多个协议上进行优化。下面几节将介绍一些市场上已出现的或IETF正在开发的优化方法。图5-1突出显示了优化后的TCP/IP层。

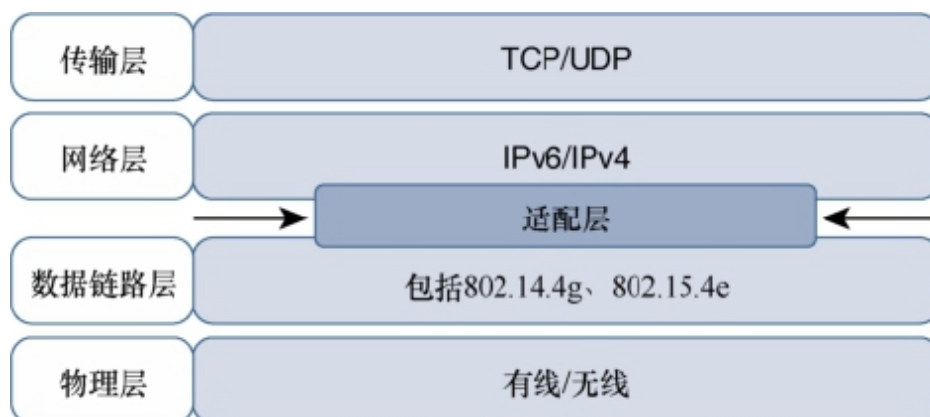


图5-1 使用适配层优化物联网IP

5.3.1 从6LoWPAN到6Lo

在IP体系结构中，必须定义和记录任意给定的第一层（PHY）和第二层（MAC）协议上的IP数据包传输。将IP封装为较低层协议的模型通常称为适配层。

除非该技术是专有的，否则IP适配层通常由IETF工作组定义，并作为征求意见（RFC）发布。RFC是来自IETF的出版物，它正式记录Internet标准、规范、协议、过程和事件。例如，RFC 864描述IPv4包如何封装在以太网帧上，RFC 2464描述如何对IPv6包执行相同的功能。

物联网相关协议遵循类似的过程。主要的区别在于，为物联网设计的适配层可能包括一些优化，以处理受限节点和网络（参见5.2.1节和5.2.2节）。

为受限节点或物联网中的“物”进行优化的适配层的主要示例是6LoWPAN工作组及其继任者6Lo工作组下的适配层。6LoWPAN工作组最初的重点是优化IPv6数据包在IEEE 802.15.4等受限网络上的传输（有关IEEE 802.15.4的更多信息，请参阅第4章）。图5-2显示了一个使用6LoWPAN适配层的物联网协议栈示例，该适配层位于著名的IP协议栈旁，可供参考。



图5-2 利用6LoWPAN和IP协议栈的物联网协议栈比较

6LoWPAN工作组发布了几个RFC，但是RFC 4994是基础性的，因为它定义了帧头，用于头压缩、分片和网络寻址等功能。这些包头可以堆叠在适配层中，以保持这些概念的独立性，同时强制使用结构化方法来表示每个功能。根据实现的不同，可以启用所有或任何这些功能及其相应包头文件的组合。图5-3显示了一些典型的6LoWPAN包头堆栈的示例。



图5-3 6LoWPAN包头堆栈

图5-3显示了与压缩、分片和网络寻址相关的子包头。在后面的小节中，我们将了解关于这些功能的更多信息。

注释：6LoWPAN工作组还发布了RFC 6775。该文档定义了邻居发现和自动配置，建议读者直接参考RFC 6775以了解与6LoWPAN相关的更多信息。

5.3.2 包头压缩

6LoWPAN的IPv6包头压缩最初在RFC 4944中定义，随后由RFC 6282更新。这种功能将IPv6的40字节包头和用户数据报协议（UDP）的8字节包头的大小，在某些情况下缩减至6字节。

注意，6LoWPAN的包头压缩只是为IPv6包头定义的，而不是IPv4。6LoWPAN协议不支持IPv4，事实上，IEEE 802.15.4没有标准的IPv4适配层。

6LoWPAN头文件压缩是无状态的，并且从概念上讲并不太复杂。但是，有很多因素会影响压缩量，例如RFC 4944与RFC 6922的实现、是否包含UDP，以及各种IPv6寻址方案。涉及每个用例以及每个用例的包头字段如何变化超出了本书的范围。但是，本章提供了一个示例，展示了6LoWPAN包头压缩的影响。

在高层级上，6LoWPAN的工作通过利用所有节点参与本地网络而获得的共享信息来完成。此外，它通过假设常用值来省略一些标准的头字段。图5-4中的示例显示了使用6LoWPAN包头压缩所能实现的压缩量。



图5-4 6LoWPAN包头压缩

在图5-4的上半部分，可以看到一个没有启用任何包头压缩的6LoWPAN帧，可以看到完整的40字节IPv6包头和8字节UDP包头。在本例中，6LoWPAN头文件仅为1字节。注意，在IEEE 802.15.4中，未压缩的IPv6和UDP包头在127字节的最大帧大小中只保留了53字节的数据载荷。

图5-4的下半部分显示了一个帧，在该帧中为实现最佳方案而启用了头压缩。6LoWPAN包头增加到2字节来容纳压缩的IPv6包头，UDP减少了一半，从8字节减少到4字节。最重要的是，包头压缩允许载荷增加一倍以上，从53字节增加到108字节，这显然更有效。注意，2字节的包头压缩适用于单元内通信，而单元外部的通信可能不需要压缩包头的某些字段。

注释：虽然没有什么可以阻止在IPv6/6LoWPAN上运行TCP，但是TCP包头压缩并没有定义。主要原因是TCP的拥塞避免算法可能会对LLN的丢包和/或往返延迟差异做出过度反应。

5.3.3 分片

IPv6网络的最大传输单元（MTU）必须至少为1280字节。术语MTU定义了可以传递的最大协议数据单元的大小。对于IEEE 802.15.4，MTU是127字节。我们可以发现这是一个问题，因为IPv6的MTU要大得多，而802.15.4帧中传输的MTU要小得多。为了纠正这种情况，必须在第2层的多个802.15.4帧上对大型IPv6数据包进行分片。

注释：在第4章中，IEEE 802.15.4g标准在使用6LoWPAN适配层时，不受短的127字节MTU限制。本节对分片及其必要性的讨论显然排除了802.15.4版本。

6LoWPAN使用的分片头由3个主要字段组成：数据报大小、数据报标记和数据报偏移量。1字节数据报大小字段指定未分片的载荷的总大小。数据报标记标识有效载荷的片段集。最后，数据报偏移字段描述了特定片段在载荷中的位置。图5-5表示一个6LoWPAN片段头。

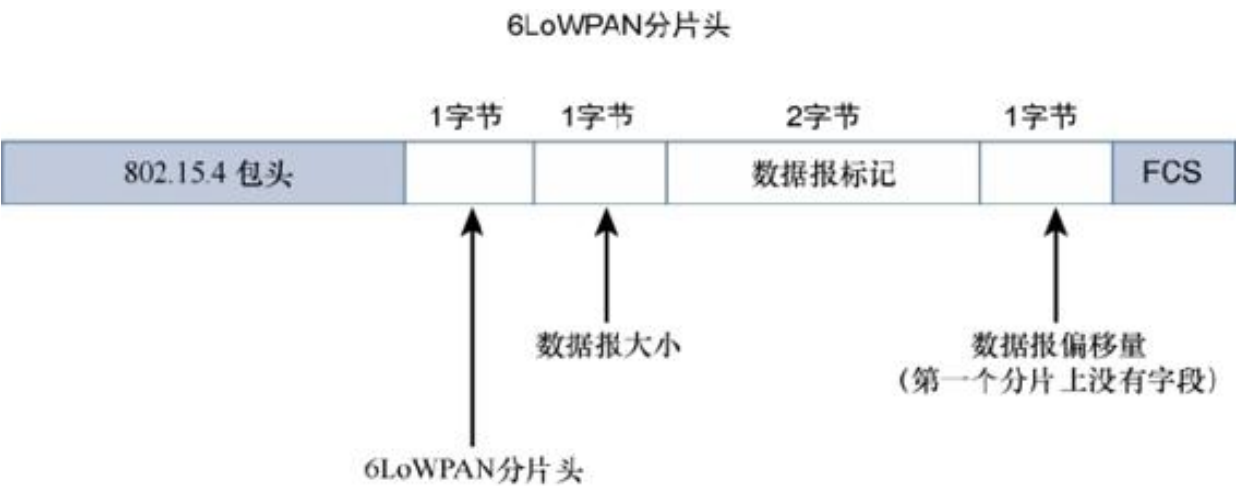


图5-5 6LoWPAN分片头

在图5-5中，6LoWPAN分片头字段本身使用一个唯一的位值来标识它后面的后续字段是分片字段，而不是另一个功能，比如头压缩。同样，在第一个分片中，没有出现数据报偏移字段，因为它将被简单地设置为0。这导致IPv6载荷的第一个分片头只有4字节。分片的其余部分有一个5字节的头字段，因此可以指定适当的偏移量。

5.3.4 网状寻址

6LoWPAN网状寻址（mesh addressing）功能的目的是在多个跳数上转发数据包。为此包头定义了3个字段：跳数限制、源地址和目标地址。与IPv6跳数限制字段类似，网状寻址的跳数限制也提供了帧转发次数的上限。每一跳将该值递减1。一旦该值达到0，它将被删除，不再被转发。

网状寻址的源地址和目标地址字段是IEEE 802.15.4地址，表示一个IP跳数的端点。图5-6详细说明了6LoWPAN网状寻址头字段。



图5-6 6LoWPAN网状寻址头

请注意，网状寻址头用于单个IP子网，是一种称为mesh-under的第2层路由类型。下一节将讨论mesh-under的概念。RFC 4944只规定了这种情况下的功能，因为第2层网状路由规范的定义超出了6LoWPAN工作组的范围，而IETF没有定义第2层路由。除非给定的技术配置文件有要求，否则实现三层IP路由不需要实现网状寻址头。

1. mesh-under与mesh-over路由

对于支持网状拓扑并在物理和数据链路层运行的网络技术，如IEEE 802.15.4、IEEE 802.15.4g和IEEE 1901.2a，存在两个主要选项用于建立可达性和转发数据包。对于第一个选项mesh-under，数据包的路由在6LoWPAN适配层处理。

另一个选项称为mesh-over或route-over，它利用IP路由将数据包发送到目的地。

对于mesh-under路由，IP数据包的路由利用前一节讨论的6LoWPAN网状寻址头在链路层路由和转发数据包。使用术语mesh-under是因为可以使用多个链路层跳数来完成单个IP跳数。节点有一个二层转发表，它们参考该转发表将数据包路由到它们在网络中的最终目的地。边缘网关终接到mesh-under域，边缘网关还必须实现一种机制，以便在已配置的二层协议和在其他三层IP接口上实现的任何IP路由机制之间进行转换。

在mesh-over或route-over的方案中，无论是在网状域内还是在网状域外，IP三层路由用于计算可达性，然后将数据包转发到它们的目的地。每个功能完整的节点充当一个IP路由器，因此每个链路层跳数都是一个IP跳数。当使用不同的链路层技术实现LoWPAN时，mesh-over路由设置是有用的。虽然可以使用传统的IP路由协议，但推荐使用专门的智能对象路由协议，如RPL。本章后面将更详细地讨论RPL。

2. 6Lo工作小组

随着6LoWPAN工作组的工作完成，6Lo工作组试图将重点放在受限节点网络的IPv6连接上来扩展这项已完成的工作。虽然6LoWPAN工作组最初的优化重点是IEEE 802.15.4 LLN，但仍然需要在其他链路层技术上标准化IPv6。

因此，6Lo工作组（现在称为资源受限节点网络上的IPv6）的宗旨是促进受限节点网络上的IPv6连接。该工作组的工作重点如下。

- 对于链路层技术，使用6LoWPAN技术（RFC 4944、RFC 6282、RFC 6775）的IPv6-over-foo适配层规范，包括以下内容。

- 低能耗蓝牙IPv6。

- 通过近场通信传输IPv6数据包。

- 802.11ah上的IPv6。
- 通过DECT超低能耗传输IPv6数据包。
- 在WIA-PA（工业自动化无线网络—过程自动化）上传输IPv6数据包。
- 通过主从/令牌传递传输IPv6（MS/TP）。
- 信息和数据模型，如MIB模块：一个示例是RFC 7388。
- 适用于多个适配层规范的优化：一个示例是RFC 7400。
- 该领域IETF规范所需的信息和维护出版物。

总之，6Lo工作组正在对6LoWPAN适配层进行标准化，该层最初将重点放在IEEE 802.15.4第2层协议上，而其他协议通常具有受限节点。事实上，在6LoWPAN工作组和现在的6Lo工作组的工作基础上，6LoWPAN适配层正在成为物联网网络中连接受限节点的决定性标准。

5.3.5 6TiSCH

多年来，许多专有的无线技术已经被开发和部署在各个行业领域。然而，IEEE 802.15.4物理层和数据链路层规范的发布，以及随后的IEEE 802.15.4e修正案，为无线网络上的标准化、确定性通信开辟了道路。

IEEE 802.15.4e ——TSCH（时隙信道跳变），是IEEE 802.15.4标准媒体访问控制（MAC）部分的一个附加组件，直接继承了其他标准，如WirelessHART和ISA100.11a。

实现IEEE 802.15.4e TSCH的设备按照时分多址（TDMA）调度进行通信。在相邻节点之间调度带宽或时隙单位的分配。这允许对可预测的传输进行编程，并支持确定性的工业应用。相比之下，其他

802.15.4实现并不分配带宽片段。因此，特别是在争用期间，通信可能会延迟或丢失，因为它总是在争用时尽力而为。

为了在IEEE 802.15.4e的TSCH模式上标准化IPv6（称为6TiSCH），IETF成立了6TiSCH工作组。该工作组利用和增强6LoWPAN工作组、RoLL工作组以及CoRE工作组完成的工作，致力于架构、信息模型和6TiSCH配置最小化等方面的工作。RoLL工作组主要研究受限网络的三层路由。RoLL工作组的工作将在5.3.6节进行更详细的讨论。CoRE工作组将在第6章中讨论。

6TiSCH工作组指定的一个重要元素是6top，它是将MAC层和6LoWPAN适配层结合在一起的子层。该子层向上层网络层（如RPL）提供命令；反过来，这些命令支持包括网络层路由决策、配置和控制6TiSCH调度管理在内的功能。

IEEE 802.15.4e标准定义了一个时隙结构，但是它并没有规定如何使用时隙的调度算法。这就留给更高级别的协议来处理，例如6TiSCH。调度非常重要，因为它会影响吞吐量、延迟和功耗。图5-7显示了6top与IEEE 802.15.4e、6LoWPAN HC和IPv6的关系。6LoWPAN HC在本章前面已经介绍过。

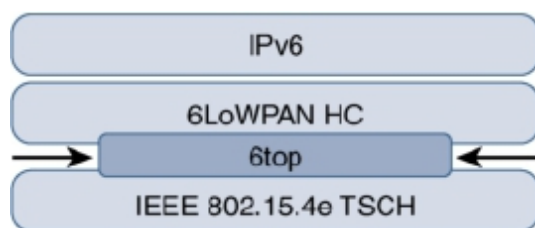


图5-7 6TiSCH的6top子层位置

6TiSCH的调度被分解成单元。单元只是TSCH调度中的一个元素，可以分配给特定节点之间的单向或双向通信。节点仅在调度指示其单元开放通信时才进行传输。6TiSCH架构定义了4种进度管理机制。

■ **静态调度：**受限网络中的所有节点共享一个固定的调度。单元是共享的，节点以时隙aloha的方式争用时隙访问。时隙aloha是通过共享介质进行通信时使用边界发送数据的基本协议。静态调度是

一种简单的调度机制，可以在初始实现时使用，也可以作为网络出现故障时的备用机制。静态调度的缺点是节点可能期望调度中的任何单元中都有一个数据包。因此，能量被白白浪费在监听所有单元上。

■ 邻居间调度：建立一个与观察到的节点间传输数量相关的调度。此调度中的单元可以随着流量需求和带宽需求的变化而添加或删除。

■ 远程监视和调度管理：时隙和其他资源分配由一个管理实体处理，该实体可以处理多个跳数。在某些场景下，调度机制会使用6top甚至CoAP。有关应用层协议CoAP的更多信息，请参见第6章。这种调度机制为节点间的通信分配单元提供了相当大的灵活性和控制性。

■ 逐跳调度：一个节点通过请求路径中每个中间节点上的调度表中的单元分配，预留了一条路径去往多跳以外的目的节点。此时，节点用来触发这种调度机制的协议尚未定义。

除调度管理功能外，6TiSCH架构还定义了3种不同的转发模型。转发是节点对每个数据包执行的操作，它允许将数据包发送到下一跳或上层协议。转发决策以从路由计算中获得的预先存在的状态为基础。6TiSCH转发模式有3种。

■ 跟踪转发（Track Forwarding，TF）：这是最简单、最快的转发模式。该模型中的轨迹是源和目标之间的单向路径。该轨迹是由调度中的一组接收单元与一组设置为发送的接收单元配对构成的。因此，在特定单元或单元组中接收的帧被切换到另一个单元或单元组。无论是哪种网络层协议，都会发生这种转发。

■ 分片转发（FF）：该模型利用6LoWPAN分片构建第二层转发表。6LoWPAN协议中的分片在本章前面介绍过。IPv6数据包可以在6LoWPAN子层进行分片，以处理 IEEE802.15.4载荷大小和IPv6 MTU之间的差异。RPL源路由信息的附加头可能会进一步导致分片的需要。然而，FF定义了一种机制，其中第一个分片基于IPv6包头进行路由。6LoWPAN 子层获取第一个分片的下一跳选择，然后将其应用于该包的

所有后续分片。否则，IPv6数据包将进行逐跳重组，这会增加延迟，对于受限节点来说，可能会消耗大量电能和CPU资源。

■ IPv6转发（6F）：该模型基于其IPv6路由表转发流量。数据包流量应通过传统的QoS（服务质量）和RED（随机早期检测）操作进行优先级排序。QoS是一种基于流优先级的分类方案，RED是一种常见的拥塞避免机制。

对于许多物联网无线网络，不要求必须控制传感器数据的延迟和吞吐量。然而，当需要某种确定性时，6TiSCH提供了一个开放的、基于IPv6的标准解决方案，用于确保无线传感器网络上的可预测通信。然而，6TiSCH在行业中的应用仍在进行中。

5.3.6 RPL

IETF授权RoLL（低功耗和有损网络的路由）工作组来评估所有第3层IP路由协议，并确定为IP智能对象开发路由解决方案的需求。在研究了各种用例和现有协议之后，以及考虑到受限网络的特性和要求，应该开发一种新的路由协议供IP智能对象使用。这种新的距离矢量路由协议被命名为IPv6低功耗和有损网络路由协议（RPL）。RPL规范由RoLL工作组发布为RFC 6550。

注释：除主要的RFC 6550标准外，RPL也在RoLL工作组发布的其他RFC中得到了解决。这些RFC包括RPL用例、RPL特定术语及其定义，以及对协议的其他增强或说明。

在RPL网络中，每个节点充当路由器，成为网状网络的一部分。路由在IP层执行。每个节点检查每个接收到的IPv6数据包，并根据IPv6包头中包含的信息确定下一跳目的地。执行下一跳判断时不需要来自MAC层包头的任何信息。在本章的前面这被称为mesh-over路由。

该协议定义了两种模式来应对计算和内存限制（这是受限节点的共同特征）。

■ 存储模式：所有节点都包含RPL域的完整路由表。每个节点都知道如何直接访问其他节点。

■ 非存储模式：只有RPL域的边界路由器包含完整的路由表。域中的所有其他节点只维护它们的父节点列表，并将其用作通往边界路由器的默认路由列表。这个简化的路由表节省了内存空间和CPU。在非存储模式下通信时，节点总是将其数据包转发给边界路由器，边界路由器了解如何到达最终目的地。

RPL基于有向无环图（DAG）的概念。DAG是一个无环的有向图。这意味着，从图中的任何顶点或点出发，无法沿着一条边或一条线回到同一点。所有的边都排列在指向或终止于一个或多个根节点的路径中。图5-8显示了一个基本的DAG。

一个基本的RPL过程包括构建一个面向目标的有向无环图（DODAG）。DODAG是一个以目标端口为根的DAG。在RPL中，此目标位于称为DODAG根的边界路由器上。图5-9比较了DAG和DODAG。可以看到，DAG有多个根，而DODAG只有一个。

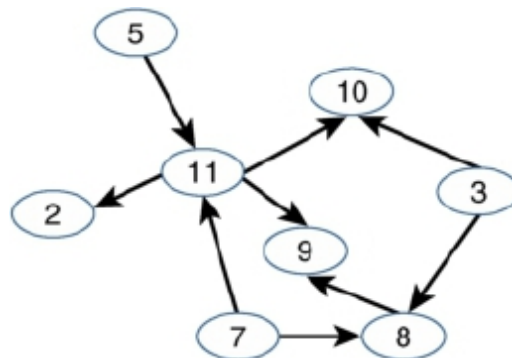


图5-8 有向无环图示例（DAG）

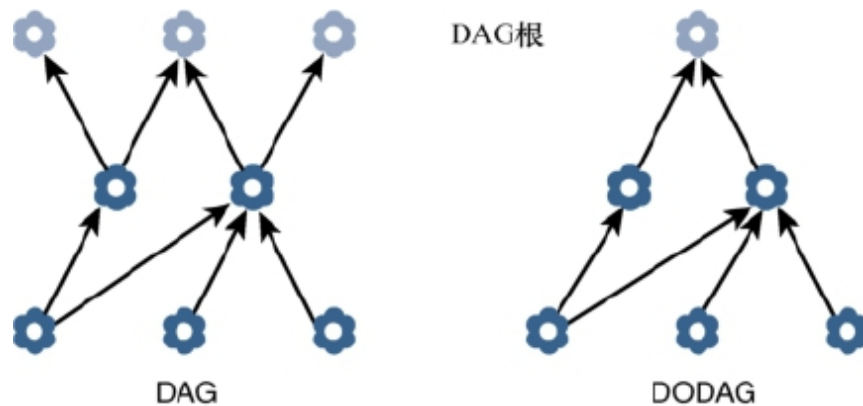


图5-9 DAG与DODAG比较

在DODAG中，每个节点最多维护3个父节点，这些节点提供到达根的路径。通常，其中一个父节点是首选父节点，这意味着它是通向根节点的向上路由的首选下一跳。

由一组跨越所有节点的DODAG父节点集创建的路由图定义了一组完整的向上路由。RPL协议实现应该确保路由是无环的，这是通过禁止所选DODAG父节点的节点来实现的（这些节点距离边界路由器更远）。

RPL中的上行路由是使用DAG信息对象（DIO）消息发现和配置的。节点监听DIO，以处理拓扑中可能影响路由的更改。DIO消息中的信息决定了父节点和到达DODAG根节点的最佳路径。

节点通过使用目的地通告对象（DAO）消息向DODAG根发布其父集，从而建立向下路由。DAO消息允许节点将其存在性和可达性告知其父节点。

在RPL的非存储模式下，发送DAO消息的节点直接将其父集报告给DODAG根（边界路由器），只有根节点存储路由信息。根节点使用这些信息来确定将IPv6数据报传递到网络下游的各个节点所需的源路由。

对于存储模式，每个节点都跟踪DAO消息中公布的路由信息。虽然这对每个节点来说会产生更大的功耗，并占用CPU资源，但好处是数据包可以在网络中的目标之间采用更短的路径。节点可以做出自己的路

由决策；另一方面，在非存储模式下，所有的数据包都必须向上到达根，以获得向下游移动的路由。

RPL消息，如DIO和DAO，运行在IPv6之上。这些消息在边界路由器和其下面的节点之间交换和发布下游和上游路由信息。如图5-10所示，DAO和DIO消息根据确切的类型在DODAG中上下移动。

1. 目标函数（OF）

目标函数（OF）定义如何使用度量来选择路由和建立节点的等级。RFC 6552 和 6719等标准已经发布，用来记录特定于某些用例和节点类型的OF。

例如，基于RFC 6719的最小期望传输数（METX）实现的节点在DIO消息中向其父节点发布METX。每当一个节点建立其等级时，它只需将等级设置为其父节点中当前的最小值。

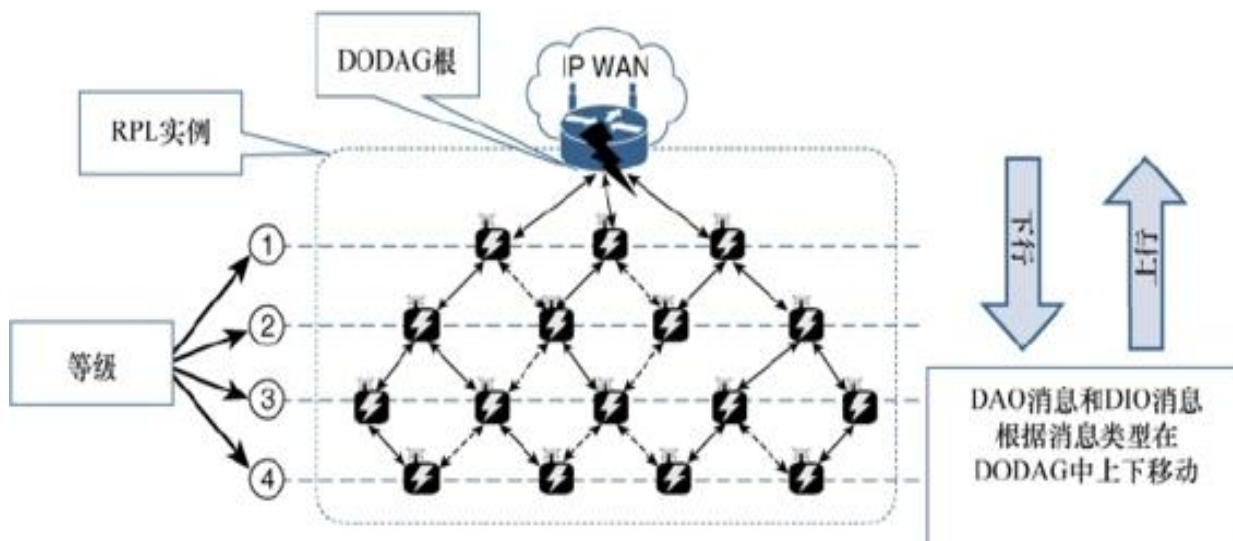


图5-10 RPL概述

2. 等级

等级是节点与根节点距离的粗略近似值，有助于避免路由环路和计数到无穷大的问题。节点只能在接收到带有较大版本号的DIO消息时增加其等级。然而，当节点建立了成本较低的路由时，其等级就会降低。虽然等级与路由度量密切相关，但是等级不同于路由度量，因为它被用作防止路由环路的约束。

3. RPL头

特定的网络层头是为在RPL域中转发的数据报定义的。其中之一是在RFC 6553中进行了标准化，另一个是在RFC 6554中进行了讨论。

RFC 6553定义了一个新的IPv6选项，称为RPL选项。RPL选项位于IPv6逐跳包头中。此包头的目的是利用数据平面包在RPL实例中进行循环检测。如前所述，DODAG只有单路径，而且无环路。

RFC 6554指定用于RPL路由器之间的源路由包头（SRH）。边界路由器或DODAG根目录在指定源路由时插入SRH，以将数据报传送至网状网络的下游节点。

4. 指标

RPL为RFC 6551中的路由定义了大量灵活的新度量和限制。RPL是为了支持供电节点和由电池供电的节点而开发的，它提供了比任何其他路由协议都要完整的一套协议。RFC 6551中定义的一些RPL路由度量和限制包括以下内容。

- 预期传输计数（ETX）：为节点发送一个数据包所需的传输次数分配一个离散值。

- 单跳计数：跟踪路径中遍历的节点数。通常选择具有较低跳数的路径，而不是具有较高跳数的路径。

- 延迟：取决于节能情况。首选具有较低延迟的路径。

■ **链路质量等级：**通过考虑信号衰减和干扰等因素引起的数据包错误率来衡量链路的可靠性。

■ **链路颜色：**通过管理性地设置值来手动影响路由，以使链路在一定程度上是可接受的。

这些值可以针对特定的流量类型进行静态或动态调整。

■ **节点状态和属性：**标识充当流量聚合器的节点以及受高工作负载影响的节点。高工作负载可能表示节点处于高CPU占用率或低内存状态。自然，与工作负载高的节点相比，聚合器节点是首选。

■ **节点能量：**避免使用低功耗节点，这样就不存在电池供电的节点电量耗尽的情况，延长了节点和网络的使用寿命。

■ **吞吐量：**提供节点链路的吞吐量。通常，节省能量的节点使用较低的吞吐量。该度量允许对具有更高吞吐量的路径进行优先级排序。

除RFC 6551中列出的度量标准和限制外，还可以实现其他度量和限制。例如，我们来看一个场景，其中两个约束条件被用作过滤器，用于删除不满足指定条件的链路。

其中一个约束条件是ETX。本章前面已经定义过RFC 6551中描述的ETX。另一个约束条件是相对信号强度指示器（RSSI），它指定接收到的无线电信号的功率。低强度的信号通常可靠性差，易受干扰，从而导致丢包。

在这种情况下，DODAG根和节点构成一个IEEE 802.15.4网络。当一个节点找到一个潜在的父亲节点时，它将邻居节点输入到路由表中。但是，它还没有使用新邻居进行路由。相反，节点必须首先确定其邻居链路质量是否足以转发数据报。

节点通过查看其编程约束来确定到潜在父亲节点的链路质量是否足够好。在本例中，配置的约束是ETX和RSSI。如果两个方向的RSSI都超

过了一个阈值，ETX低于一个阈值，则节点确认到潜在父节点的链路质量足够好。

一旦节点确定到潜在父节点的链接质量足够好，它就将适当的默认路由条目添加到其转发表中。为相邻节点维护RSSI和ETX是在链路层完成的，并存储在链路层邻居表中。

所有链路层单播流量的结果被输入到邻近设备的RSSI和ETX计算中。如果链路质量不够好，则该链接不会被添加到转发表中，因此不用于路由数据包。

为了举例说明，例 5-1 显示了一个简单 RPL 路由树，该路由树位于连接了基于 IEEE 802.15.4g mesh 6LoWPAN的子网的Cisco CGR-1000路由器上。本例中的第一个IPv6地址以1CC5结尾，它标识了RPL树的DODAG根。该DODAG根有到两个节点的分支，由以924D和6C35结尾的两个IPv6地址表示。

例5-1 Cisco CGR-1000上的show wpan <interface> rpl tree

```
pat1# show wpan 3/1 rpl tree
```

```
----- WPAN RPL TREE FIGURE [3] -----  
[2013:DB8:9999:8888:207:8108:B8:1CC5] (2)  
\--- 2013:DB8:9999:8888:89C6:F7C9:D551:924D  
\--- 2013:DB8:9999:8888:95DF:2AD4:C1B1:6C35  
RPL TREE: Num.DataEntries 2, Num.GraphNodes 3
```

路由域中的RPL集成遵循与更传统的IP路由协议相同的规则。路由再分配、过滤、负载平衡和动态再路由可以与其他周知的协议以相同的方式实现。例如，在物联网路由器中，可以看到通过RPL学习的路由被重新分配到更周知的路由协议中，如BGP和EIGRP。

总之，RPL是一种新的路由协议，它使基于IPv6标准的解决方案能够大规模部署，同时以类似于如今的IP基础设施的方式运行。RPL是为

满足受限节点和网络的需求而设计的，这使得它成为物联网传感器网络中基于IPv6的主要网络层路由协议之一。

5.3.7 在受约束的节点上进行身份验证和加密

物联网安全是一个复杂的话题，常常会引发整个行业的讨论和争辩。虽然物联网安全是第8章的重点，但我们在本章中广泛地讨论了受限节点和网络。因此，这里值得一提的是专注于物联网安全性的IETF工作组：ACE和DICE。

1. ACE

与RoLL工作组非常相似，受限环境的身份验证和授权（ACE）工作组任务是评估现有身份验证和授权协议的适用性，并记录它们对某些受限环境用例的适用性。一旦候选解决方案得到验证，ACE工作组将把工作重点放在数据报传输层安全（DTLS）协议的CoAP上（CoAP协议将在第6章中介绍，RFC 6437定义了DTLS安全协议）。ACE工作组将来可能会研究其他安全协议，并特别关注如何将所选择的解决方案适应于HTTP和TLS。

ACE工作组希望为身份验证和授权生成一个标准化的解决方案，以支持对URI标识资源的授权访问（Get、Put、Post、Delete），这些资源托管在受限环境中的资源服务器上。不受限的授权服务器对访问进行调停。这与最初的关注点一致，即客户端设备使用CoAP访问资源服务器上的资源，并受DTLS保护。

2. DICE

新一代的受限节点在受限的接入网上实现一个IP协议栈，期望运行一个优化的IP协议栈。例如，当在传输层实现UDP时，应该在应用层

使用IETF约束应用协议（CoAP）（有关CoAP的更多信息，请参见第6章）。

在由DTLS保护的受限环境中，CoAP可用于控制设备上的资源。受限环境是指存在受限节点和/或受限网络的网络环境。受限网络和受限节点在本章前面讨论过。

受限环境下的DTLS（DICE）工作组致力于在这些环境中实现DTLS传输层安全协议。DICE工作组的第一个任务是为受限节点定义一个优化的DTLS配置文件。此外，DICE工作组正在考虑DTLS记录层对安全多播消息的适用性，并研究如何在受限环境下优化DTLS的握手。

5.4 概要文件和合规性

本章讲到，为智能对象利用Internet协议套件涉及一系列协议和选项，这些协议和选项必须与低层和高层协同工作。因此，配置文件定义、认证和联盟推广可以帮助实施者开发保证设备交互性和/或互换性的解决方案。

本节介绍一些主要的行业组织，它们致力于物联网受限节点和网络配置文件的定义和认证。在物联网领域，我们可以找到来自这些组织的各种文件和推广活动，所以有必要熟悉它们和它们的目标。

5.4.1 智能对象的Internet协议（IPSO）联盟

成立于2008年的智能对象Internet协议（IPSO）联盟经过多年的发展，其目标不断演变。该联盟最初致力于将IP作为智能对象通信的首要解决方案。今天，随着IPSO联盟组织成员之间通过交互性测试来验证智能对象的Internet协议可以协同工作并能正确实施行业标准，该联盟更关注如何使用IP。IPSO联盟没有定义技术，因为这是IETF和其他标准组织的职责，但它记录了基于IP的技术在各种物联网用例中的使用，并参与到行业教育中。正如IPSO联盟在其价值和使命声明中

所宣称的，它希望确保“工程师和产品制造商能够获得构建物联网所需的工具”。

5.4.2 Wi-SUN联盟

Wi-SUN联盟是业界努力定义适用于特定物理层和数据链路层协议的通信配置文件的一个示例。目前，Wi-SUN的主要关注点是IEEE 802.15.4g协议以及该协议对通过UDP传输层运行的应用程序的多服务和安全IPv6通信的支持。

公用事业是Wi-SUN联盟的主要关注领域。从密集的城市社区到农村的广泛地区，Wi-SUN场域网（FAN）能提供极好的覆盖，使智能公用事业网络能够提供弹性、安全和经济高效的连接（FAN在第11章中有更详细的描述）。

5.4.3 线程

为消费者提供智能对象解决方案的公司创建了线程组的概念。线程组定义了一种基于IPv6的无线配置文件，它提供了将250多台设备连接到低功耗无线网状网络的最佳方式。

线程使用的无线技术是IEEE 802.15.4，它与Wi-SUN的IEEE 802.15.4g不同。关于802.15.4和802.15.4g的更多信息以及它们之间的区别，请参见第4章。

5.4.4 IPv6 Ready Logo

最初，IPv6论坛确保了IPv6在全球范围内的推广。一旦IPv6实现变得广泛可用，交互性和认证的需求将导致IPv6 Ready Logo计划的创建。

IPv6 Ready Logo计划已经建立了一致性和交互性测试程序，用来增加用户是实现IPv6时的信心。IPv6核心和特定的IPv6组件（如DHCP、IPSec和客户边缘路由器认证）已经就绪。这些认证得到了整个行业的认可，许多产品已经通过了认证。目前针对物联网的IPv6认证工作正在进行定义。

5.5 小结

在过去的30年中，IP协议套件已经部署在私有和公共网络中，将数十亿的IP设备和用户连接起来。该架构已被证明是高度灵活的，并且在许多方面保护了投资。例如，新的链接类型已经被调整，指定并部署了新的路由和传输协议，支持的应用程序数量超出了预期的数量级。

绝大多数IP协议和技术，包括寻址、地址提供、QoS、传输、可靠性等，都可以作为物联网解决方案重用。在物联网设备节点受限和/或连接到受限网络的情况下，IP可能存在不足。对于一些使用LPWA技术进行“最后一公里”通信的高度受限设备来说，尤其如此。

为了解决这些问题，负责TCP/IP架构的主要标准组织IETF现在正通过工作组来优化物联网和智能对象的IP通信。这些工作组不得不经常开发新的协议，如RPL，或适配层（如6LoWPAN），以处理通常会部署物联网传感器的受限环境。

正如本章所强调的，在物联网中，网络层的基础已经相当稳固。IETF和其他标准机构继续致力于消除网络、协议和用例的缺陷，这些都是推进物联网所必需的。

第6章 物联网应用协议

与第5章讨论的有线和无线接入技术一样，我们选择的物联网应用协议应该取决于它们所应用的用例和垂直行业。此外，物联网应用协议依赖底层本身的特性。例如，适用于一般节点和传统网络的应用程序协议通常不适合受限的节点和网络。

本章将重点介绍如何传输更高层次的物联网协议。具体来说，本章包括以下几节。

■ **传输层：**基于IP的网络要么使用TCP，要么使用UDP。然而，物联网网络的局限性要求我们更仔细地研究这些传统传输机制的使用方式。

■ **物联网应用传输方法：**探讨各种类型的物联网应用数据以及这些数据在网络上的传输方式。

与传统网络相同，在传输物联网应用的数据时，大多数情况下采用TCP或UDP协议。本章对传输方法进行了深入的介绍，这也是本章的主要内容。读者将注意到，与底层物联网协议相同，通常有多种选项和解决方案可用于传输物联网应用程序的数据。这是因为物联网仍在发展和成熟，不仅要考虑新的应用协议和技术的传输，还要考虑传统协议和技术的传输。

6.1 传输层

本节将讨论在物联网网络环境下TCP/IP体系结构支持的传输层协议。对于TCP/IP协议，传输层有两个指定的主要协议。

■ 传输控制协议（TCP）：这种面向连接的协议要求在交换数据之前，在源和目标之间建立一个会话。可以把它看作是一种传统的电话交谈，在这种交谈中，两部电话必须连接起来，并且在双方能够交谈之前建立起通信联系。

■ 用户数据报协议（UDP）：使用这种无连接协议，可以在源和目标之间快速发送数据，但不能保证数据能成功交付。这类似于传统的邮件投递系统，在该系统中，信件被邮寄到目的地，在收到回信之前无法确认这封信已收到。

由于在Internet上主要是人与人之间进行交互，TCP成为传输层使用的主要协议。这在很大程度上是由其固有特性决定的，例如它能够大量数据传输到更小的数据包集合中。此外，它还确保以正确的顺序重新组装数据包、进行流控制和窗口调整，以及重新传输丢失的包。这些好处是伴随着每个包和每个会话的开销成本而产生的，可能会影响数据包传输速率的性能和延迟。

相反，UDP最常用于网络服务中，如域名系统（DNS）、网络时间协议（NTP）、简单网络管理协议（SNMP）和动态主机控制协议（DHCP），或用于传输实时数据流量，包括IP上的语音和视频。在这些情况下，性能和延迟比包重传更重要，因为重发丢失的语音或视频包没有任何价值。当必须保证数据包的接收没有错误时，应用层协议负责提供该功能。

在针对给定的物联网应用层协议选择传输层时，建议评估这种选择对栈的上下层的影响。例如，本章后面讨论的大多数工业应用层协议都是通过TCP实现的，而它们的规范可以支持这两种传输模型。原因在于，这些工业应用层协议通常比较旧，而且是在数据链路层通常不可靠且需要错误保护时部署的。

虽然TCP的使用可能不会对一般的计算平台和高数据速率网络造成压力，但它可能具有挑战性，而且在受限的物联网设备和网络上通常产生过大的开销。当物联网设备每次只需要发送几个字节的数据时尤

其如此。当使用TCP时，每个数据包至少需要增加20字节的TCP开销，而UDP只需要增加8字节。TCP还需要建立和维护一个开放的逻辑通道。

物联网节点也可能受到数据链路层固有特性的限制。例如，第5章中讨论的低功耗和有损网络（LLN）可能无法很好地支持大量TCP会话。

这可以解释为什么新的物联网应用协议（如受限应用协议[CoAP]）几乎总是使用UDP，以及为什么工业应用层协议的实现可能需要优化和采用UDP传输层（如果运行在LLN上）。例如，设备语言报文规范/能源计量配套规范（DLMS/COSEM）应用层协议事实上是欧洲标准，它是公用事业领域中流行的智能电表读取协议。对该协议进行调整或优化取决于底层的物联网传输协议。例如，如果将蜂窝网络上的DLMS/COSEM传输与LLN部署进行比较，应该考虑以下内容。

■ 为蜂窝网络选择TCP，因为这些网络通常更健壮，可以处理开销。对于LLN来说，设备和网络本身通常都受到约束，因此UDP是更好的选择，而且通常会强制使用UDP。

■ 通过在LLN上提供“长期联系”，DLMS/COSEM可以减少与会话建立相关的开销。长期联系意味着会话只建立一次，因为保持会话建立所需的通信开销比在一段时间内打开和关闭多个单独会话所需的通信开销要小得多。相反，对于蜂窝网络，在传输后通过拆解开放的关联能更好地控制成本。

■ 在传输大量DLMS/COSEM数据时，蜂窝链接是优化每个开放关联的首选方法。少量的数据可以通过LLN有效地处理。由于在LLN上的丢包率通常比在蜂窝网络上高，因此在LLN上保持少量数据传输限制了大量字节的重新传输。

多播需求还受到为传输层选择的协议的影响。通过多播，一条消息可以发送到多个物联网设备。在物联网环境中，这对于同时升级多个物联网设备的固件非常有用。另外，请记住多播只使用UDP。

为了保证互操作性，认证和合规性配置文件（如Wi-SUN）需要指定第1层到第4层的堆栈。这使得所选的技术能够与堆栈的不同选项兼容，同时也与IP兼容（第4章介绍了更多关于Wi-SUN的信息）。

总之，TCP和UDP是TCP/IP协议在传输层的两个主要选择。物联网受限设备与网络的性能和可扩展性受到这一选择的影响。

6.2 物联网应用传输方法

由于物联网应用协议类型的多样性，有多种方法可以在网络上传输这些协议。有时我们可能需要处理具有特定需求的传统实用程序和工业物联网协议，有时则可能需要考虑更现代的应用层协议的传输需求。为了更容易做出这些决策，有必要对常见的物联网应用程序协议进行分类，然后重点关注每个类别可用的传输方法。后文将探讨物联网应用协议的类别及其传输方法。

■ 应用层协议不存在：在这种情况下，数据载荷直接传输到较低层的顶部。不使用应用层协议。

■ 监控和数据采集（SCADA）：SCADA是最常见的工业协议之一，但其开发远远早于IP时代，并已经适用于IP网络。

■ 基于Web的通用协议：通用协议，如以太网、WiFi和4G/ LTE，可以在许多消费者和企业级别的物联网设备上找到，这些设备可以在不受限制的网络上通信。

■ 物联网应用层协议：物联网应用层协议被设计为在占用空间较小的受限节点上运行，并且能够很好地适应蜂窝、卫星链路或受限的6LoWPAN网络的网络带宽约束。本章后面介绍的消息队列遥测传输（MQTT）和受限应用协议（CoAP）是物联网应用层协议的两个著名示例。

6.2.1 应用层协议不存在

如第4章所述，IETF RFC 7228设备定义为0类，只发送或接收几个字节的数据。由于各种各样的原因（例如处理能力、功率限制和成本因素），这些设备没有实现完全结构化的网络协议栈（例如IP、TCP或UDP），甚至没有实现应用层协议。0类设备通常是严格受限的简单智能对象。实现一个健壮的协议栈通常没有用，有时在可用资源有限的情况下甚至是不可能的。

例如，考虑通过LPWA LoRaWAN（第4章中讨论过）基础设施发送数据的低成本温度和相对湿度（RH）传感器。温度用2字节表示，RH用另外2字节的数据表示。因此，这个小数据载荷直接在LoRaWAN MAC层上传输，不使用TCP/IP。例6-1显示了温度和相对湿度的原始数据，以及应用程序如何对其进行解码。

例6-1 解码温度和相对湿度传感器的数据

```
Temperature data payload over the network: Tx = 0x090c
Temperature conversion required by the application
 $T = Tx/32 - 50$  to  $T = 0x090c/32 - 50$  to  $T = 2316/32 - 50 = 22.4^{\circ}$ 
RH data payload over the network: RHx = 0x062e
RH conversion required by the application:
 $100RH = RHx/16-24$  to  $100RH = 0x062e/16-24 = 74.9$  to  $RH = 74.9\%$ 
```

虽然许多受限设备（如传感器和执行器），都采用了没有应用层的部署方式，但这种传输方法尚未标准化。从交互性的角度来看，缺乏标准化使得这种传输方法很难实现普遍应用。

假设将例6-1扩展到来自不同制造商的不同种类的温度传感器。这些传感器将以不同的格式报告温度数据。每个传感器传输的数据中始终存在一个温度值，但是解码这些数据的方式取决于供应商。如果将此场景扩展到数百或数千个传感器上，那么允许各种应用程序接收和解释以不同格式传递的温度值的问题就会变得越来越复杂。这个问题的解决方案是使用物联网数据代理，如图6-1所示。物联网数据代理是

一种中间件，它将传感器输出标准化为一种通用格式，然后可以由授权的应用程序检索（第1章介绍过物联网数据代理的概念）。

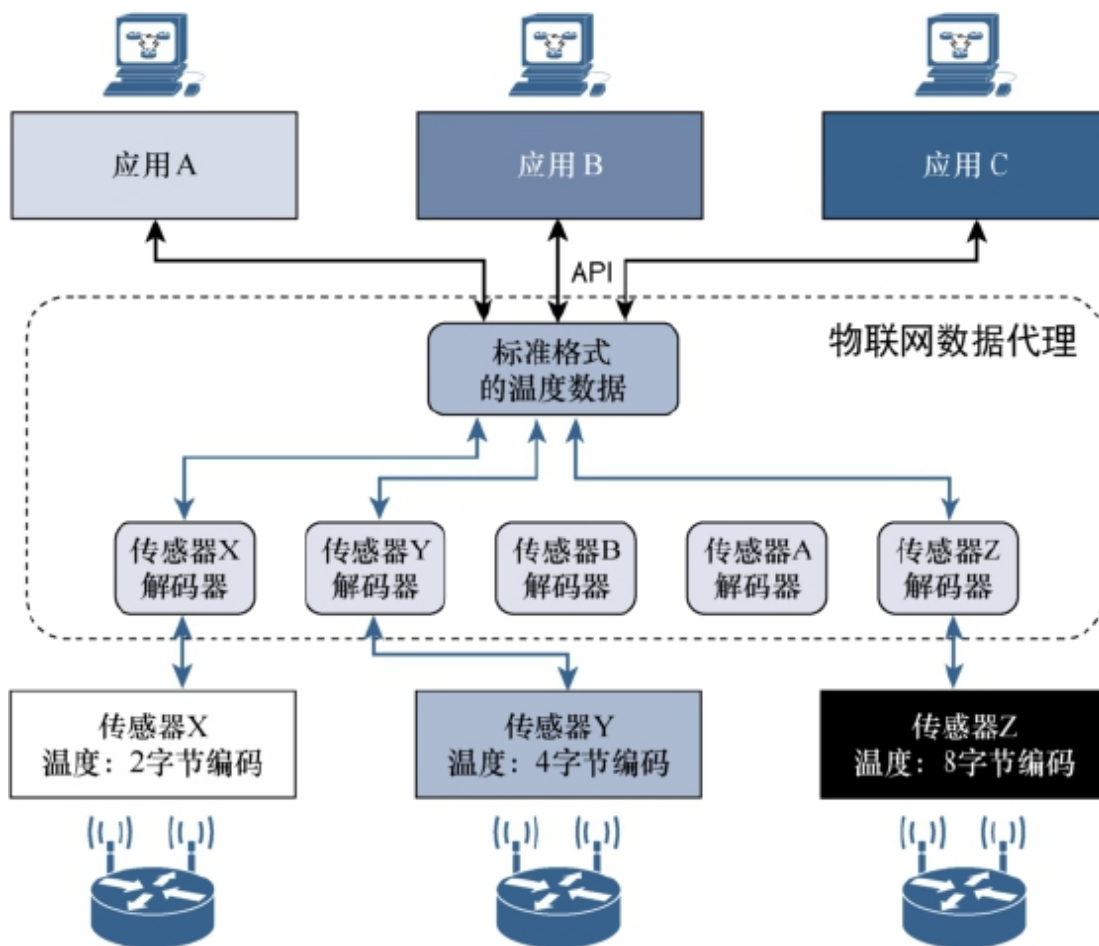


图6-1 物联网数据代理

在图6-1中，传感器X、Y和Z都是温度传感器，但是它们的输出编码不同。物联网数据代理可以理解温度编码的不同格式，因此能够将这些数据解码为通用的标准化格式。图6-1中的应用程序A、B和C可以访问这个温度数据，而不需要处理对多种温度数据格式进行解码的问题。

大家应该注意到，从商业角度来看，物联网数据代理也被用来向第三方分发和销售物联网数据。一家公司可以通过另一家公司的应用程序付费访问其数据代理。这使得物联网数据代理成为可能的收入来源，具体取决于它所提供数据的价值。

总之，虽然在不使用结构化网络堆栈的情况下直接传输数据载荷可以明显优化低数据速率网络上的数据传输，但是缺少数据模型意味着每个应用程序都需要了解如何解释特定数据的格式。对于具有不同数据载荷格式的大型设备网络，情况变得越来越复杂。此外，它使得物联网应用环境在演化、开发、交互性等方面具有挑战性，并且通常需要结构化的数据模型和数据代理应用程序。

6.2.2 SCADA

在网络技术和协议领域，物联网是相对较新的一个概念。再加上IP是计算机网络事实上的标准，连接传感器和执行器的旧协议已经进化并使自身适应IP。

监控和数据采集（SCADA）就是这种演变的一个主要表现。SCADA设计于几十年前，是一个自动化控制系统，最初是在没有串行链路IP的情况下实现的，后来才适应以太网和IPv4。

1. 关于SCAD的背景知识

多年来，相关行业已经开发出符合其特定需求的通信协议。其中许多是在大多数通信网络技术都是基于串行链路的情况下定义和实现的，如RS-232和RS-485。这导致了SCADA网络协议的出现。与上一节描述的协议相比，SCADA网络协议的结构好，可以直接运行在串行物理层和数据链路层上。

在高层次上，SCADA系统从远程设备收集传感器数据和遥测数据，同时还提供控制这些数据的能力。在当今的网络中，SCADA系统允许对如何改进业务流程做出全局的、实时的、数据驱动的决策。

SCADA网络可以应用于不同的行业中，但是我们会发现SCADA主要集中在公用事业和制造业/工业领域。在这些特定的行业中，SCADA通常使用某些协议来实现设备和应用程序之间的通信。例如，Modbus及

其修订版是工业协议，用于通过主/从关系监控和编程远程设备。Modbus还应用于建筑管理、交通和能源领域。DNP3和国际电工委员会（IEC）60870-5-101协议主要用于公用事业行业，DLMS/COSEM和ANSI C12协议主要用于高级仪表读数（AMR）。本章后面将更详细地讨论DNP3和IEC 60870-5-101。

如前所述，这些协议可以追溯到几十年前，并且是基于串行链路。因此，在当前的物联网和传统网络上传输它们，则需要从协议和实现的角度做出一定调整。这些调整和其他调整形成了各种SCADA传输方法，这是后续部分的重点。

2. 调整SCADA以适应IP

20世纪90年代，以太网在工业领域的迅速应用推动了SCADA应用层协议的发展。例如，IEC采用开放系统互连（OSI）层模型来定义其协议框架。其他协议用户组也稍微修改了各自的协议，以便在IP基础设施上运行。向以太网和IP迁移的好处包括能够利用现有设备和标准，同时将SCADA子网无缝集成到企业WAN基础设施中。

为了进一步促进传统工业协议在IP网络上的支持，人们对协议规范进行了更新和发布，并且记录了每个协议的IP使用情况。这包括为协议分配TCP/UDP端口号，如下所示。

- DNP3（由IEEE 1815-2012采用）指定在端口20000上使用TCP或UDP在IP上传输DNP3消息。

- Modbus消息服务使用TCP端口502。

- IEC60870 -5-104是IEC60870 -5-101串行协议的改进版，它使用端口2404在以太网和IPv4上运行。

- DLMS用户协会在DLMS/COSEM绿皮书（第5版或更高版本）或IEC 62056-53和IEC 62056-47标准中指定了一个基于TCP/IP的通信概要文件，允许通过IP和端口4059进行数据交换。

注释：DNP3协议基于IEC 60870-5标准。因此，虽然DNP3不能与IEC 60870-5进行交互，但其运行方式和功能非常相似。两者都与SCADA网络有关，DNP3主要在美国和加拿大应用，IEC 60870-5则应用于欧洲。参见第11章以了解这些SCADA协议如何应用于公用事业网络。

这些传统的串行协议已经适应并发展为利用IP和TCP/UDP作为网络和传输机制。这使得公用事业和其他公司能够继续利用它们在设备和基础设施上的投资，利用现代IP网络支持这些传统协议。我们通过将DNP3作为一个典型的用例来深入研究这些传统的串行协议是如何演变成使用IP的。

与许多其他SCADA协议相同，DNP3基于主/从关系。这里的术语“主机”指的是位于公用事业公司控制中心的功能强大的计算机，而“从设备”是一种远程设备，其计算资源位于变电站等位置。DNP3特别将从设备称为“分站”。

分站监控设备，收集指示设备状态的数据（如断路器是开或关），并测量电压、电流、温度等。然后，当请求该数据时，将该数据传输给主机，或者以异步方式发送事件和警报。主机还发出控制命令，例如启动电机或复位断路器，并记录输入的数据。

IEEE 1815-2012规范描述了如何调整DNP3协议实现，以运行在TCP（推荐）或UDP上。该规范定义了DNP3协议和IP层之间的连接管理，如图6-2所示。除了实现网络连接所需的配置参数和方法外，连接管理还将DNP3层与IP层链接起来。IP层对DNP3层是透明的，因为一个站点的协议栈的每个部分都与另一个站点的相应部分进行逻辑通信。这意味着DNP3端点或设备对正在发生的底层IP传输毫不知情。

在图6-2中，主机端通过执行TCP 主动开启（active open）来进行连接。分站通过执行 TCP被动打开（passive open）来侦听连接请求。双端点定义为一个进程，它既可以侦听连接请求，也可以根据需要在通道上执行主动打开操作。

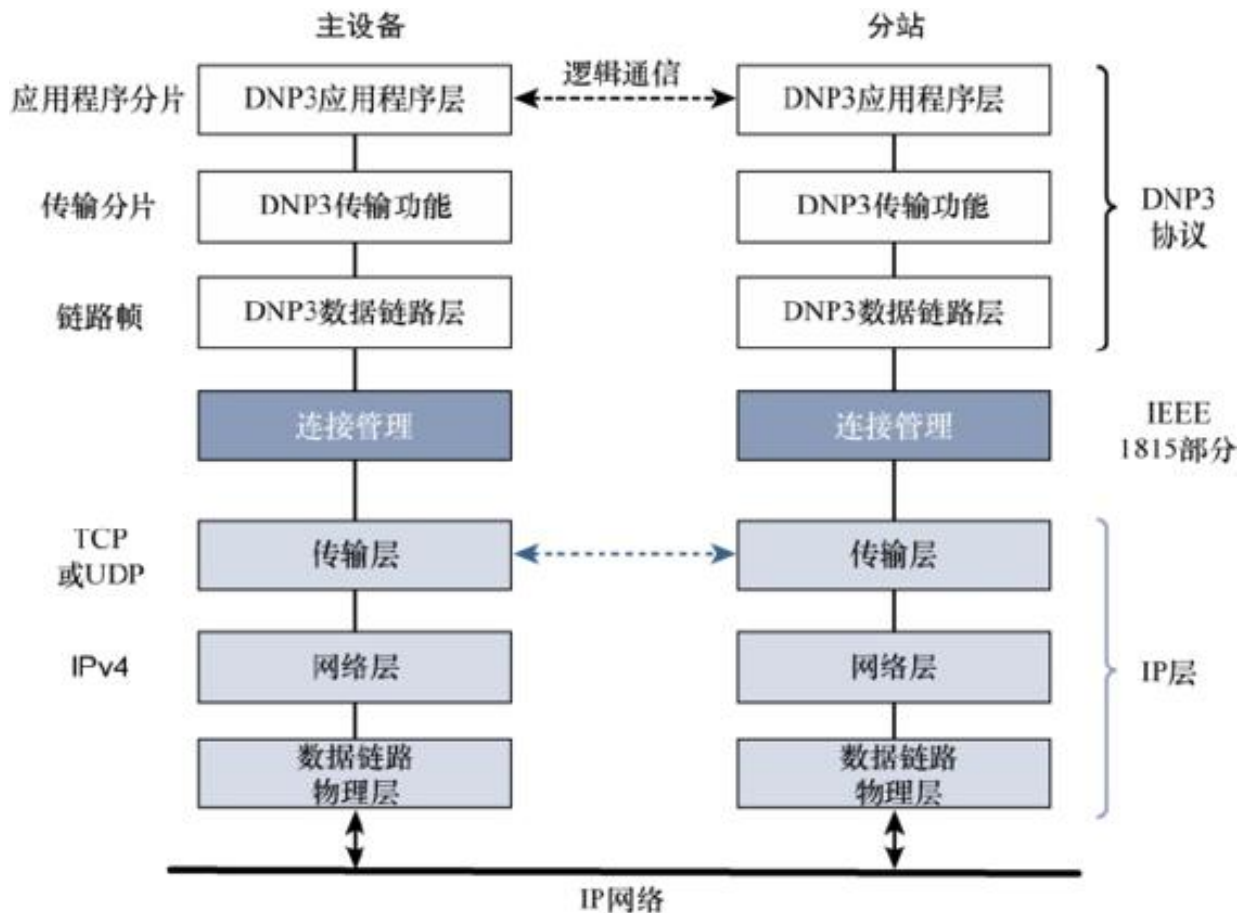


图6-2 用于在IP上传输串行DNP3 SCADA的协议栈

主站可以从一个UDP数据报解析多个DNP3数据链路层帧，而DNP3数据链路层帧不能跨越多个UDP数据报。当TCP保活（keepalive）计时器监视连接状态时，可能会建立到主服务器的单个或多个连接。保活消息是作为DNP3数据链路层状态请求实现的。如果没有收到对保活消息的响应，则认为连接已断开，并采取适当的操作。

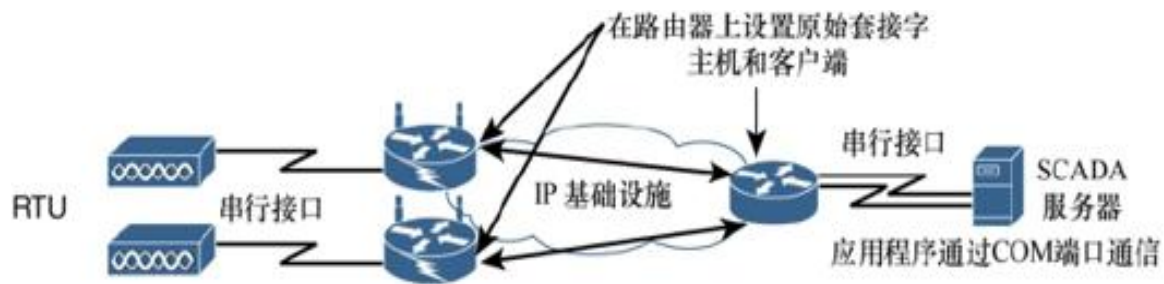
3. 通过IP网络以隧道方式传输传统的SCADA

在现代IP网络中，传统工业协议（如DNP3和其他SCADA协议）的部署要求在集成多代设备或操作时具有灵活性，这些设备或操作与不同版本的应用服务器相关联。这些设备或操作对IP的支持可能不同，因此需要不同的解决方案。理想情况下，首选端到端的IP支持，为此可在DNP 3模式下使用类似IEEE 1815-2012的解决方案。否则，可以通过

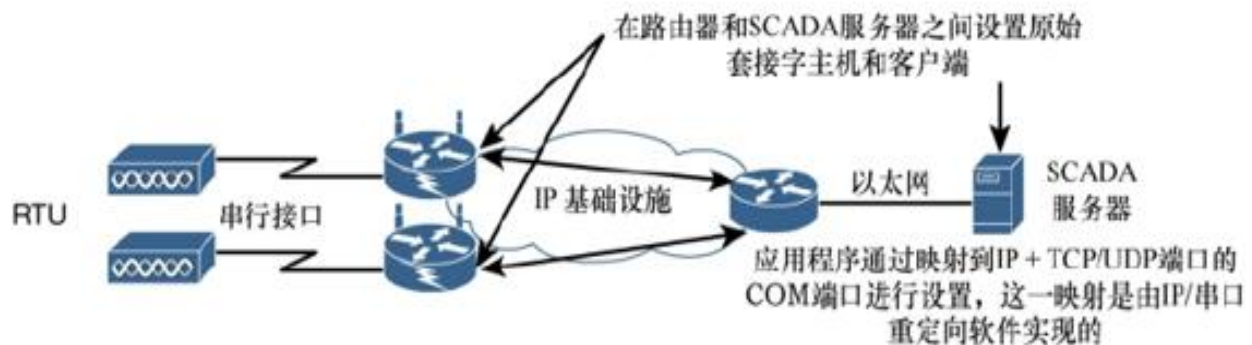
使用TCP或UDP上的原始套接字进行隧道传输，或者安装一个中间设备，在串行协议版本及其IP实现之间执行协议转换，从而在IP上实现原始串行协议的传输。

原始套接字连接只是表示串行数据被直接打包到TCP或UDP传输中。此实例中的套接字是由IP地址和TCP或UDP端口组成的标准应用程序编程接口（API），用于通过IP网络访问网络设备。更现代的工业应用服务器可能支持这种功能，而较老的版本通常需要其他设备或软件来处理使用原始套接字实现从纯串行数据到IP串行数据的转换。图6-3详细描述了传统SCADA服务器尝试与远程串行设备通信的原始套接字场景。

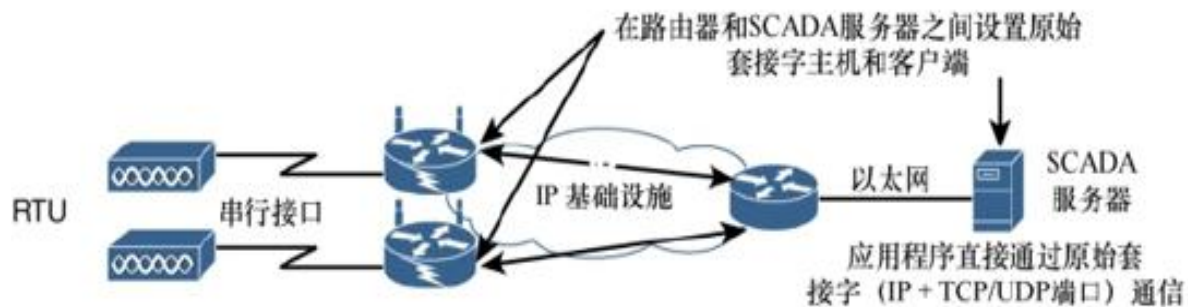
在图6-3中的所有场景中，请注意路由器通过串行接口连接到远程终端单元（RTU），远程终端单元通常与SCADA网络相关联。RTU是一种多用途设备，用于监视和控制各种系统、应用程序和管理自动化设备。从主/从的角度来看，RTU是从设备。在图6-3中的每个场景中，与RTU相对的是一个SCADA服务器（或主服务器），它可以改变连接类型。实际上，这里还可以显示其他传统的工业应用服务器。



场景A: 路由器之间的原始套接字——SCADA服务器上没有更改



场景B: 路由器和SCADA服务器之间的原始套接字——不需要在服务器上更改SCADA应用程序，但是要添加IP/串口重定向软件和以太网接口



场景C: 路由器和SCADA服务器之间的原始套接字——SCADA应用程序了解如何通过原始套接字和以太网接口直接通信

图6-3 传统工业串行协议的原始套接字TCP或UDP场景

在图6-3中的方案A中，SCADA服务器和RTU都与各自的路由器直接串行连接。路由器在链路两端终止串行连接，并使用原始套接字封装在IP网络上传输串行载荷。

方案B在SCADA服务器端有一个小变化。SCADA服务器上安装了一个软件，它将串口COM端口映射到IP端口。这种软件通常称为IP/串口重定向器。IP/串口重定向器实质上终止了SCADA服务器的串行连接，并使用原始套接字连接将其转换为TCP/IP端口。

在图6-3中的方案C中，SCADA服务器支持本地原始套接字功能。在方案A和方案B中，路由器或IP/串口重定向软件必须将SCADA服务器的串行端口映射到IP端口，而在方案C中，SCADA服务器完全支持原始套接字连接。

注释：虽然图6-3突出了使用原始套接字在IP上通过隧道传输较旧的基于串行的SCADA协议，但是该机制也可以用于隧道传输不属于SCADA的其他传统串行通信协议。

4. SCADA协议转换

如前所述，用于跨IP网络传输传统串行数据的原始套接字连接的替代方案是协议转换。通过协议转换，可将传统的串行协议转换为相应的IP版本。例如，图6-4显示了两个串行连接的DNP3 RTU和两个通过IP支持DNP3的主应用程序，它们控制并从RTU中提取数据。在图6-4中，物联网网关执行协议转换功能，支持RTU与服务器之间的通信，尽管一端是串行连接，另一端使用IP连接。

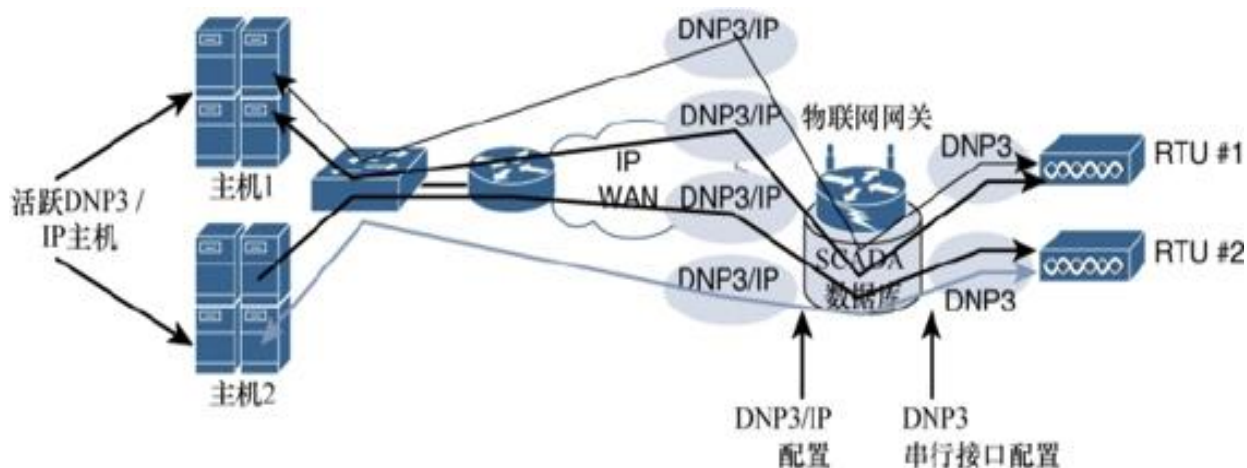


图6-4 DNP3协议转换

通过运行协议转换，图6-4中连接到RTU的物联网网关实现了一种靠近网络边缘的计算功能。添加靠近边缘的计算功能，有助于扩展物联网网络中的分布式智能。这可以通过在物联网网关或路由器上提供计算资源来实现，如下面的协议转换示例所示。或者，这也可以直接在连接多个传感器的节点上执行。在这两种情况下，这被称为雾计算（有关雾计算的更多信息，请见第2章）。

注释：在图6-4中，DNP3显示为正在转换的协议。然而，图中的场景同样适用于IEC 60870-5。例如，可以使用IEC 60870-5-101或T101代替使用DNP3连接物联网网关的RTU。另一方面，IEC 60870-5-104或T104将取代DNP3/IP。

5. 使用MAP-T在LLN上传输SCADA

由于LLN的局限性，工业协议的实现至少应该通过UDP完成。这反过来要求应用服务器和设备都支持并实现UDP。虽然SCADA和其他传统工业协议的长期发展是针对IPv6提供原生的支持，但必须强调的是，目前支持IP的大多数工业设备（甚至可能是全部）只支持IPv4。当部署在纯IPv6的LLN子网上时，需要实现一种转换机制，比如MAP-T（RFC 7599）。这使得部署能够对应用程序和设备透明地利用原生IPv6进行传输。

图6-5描述了一个方案，其中一个传统端点通过运行6LoWPAN的LLN连接到一个支持IP的SCADA服务器。传统端点可以运行各种工业和SCADA协议，包括DNP3/IP、Modbus/TCP或IEC60870-5-104。在这个方案中，传统设备和SCADA服务器只支持IPv4（当今业界的典型情况）。然而，IPv6（带有6LoWPAN和RPL）被用于连接到端点。正如在第5章中讨论的，6LoWPAN是一个为受限网络设计的标准化协议，但它只支持IPv6。在这种情况下，终端设备、端点和SCADA服务器只支持IPv4，但是中间的网络只支持IPv6。

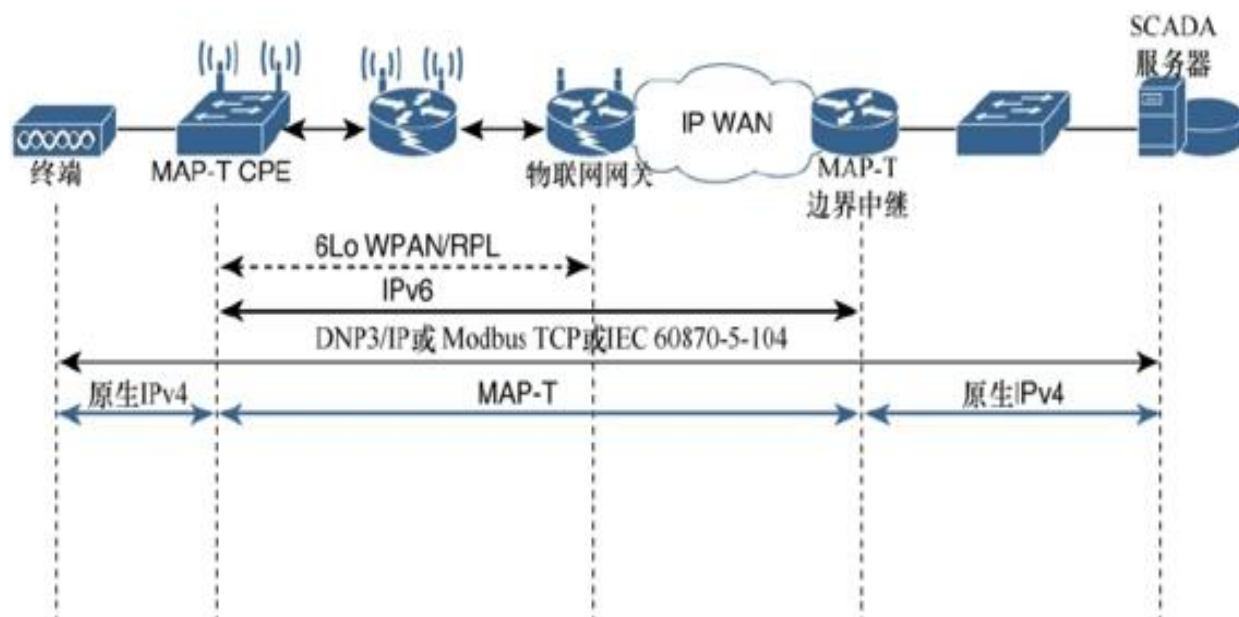


图6-5 带有MAP-T的6LoWPAN网络上的DNP3协议

这个问题的解决方案是使用在第5章中介绍的MAP-T协议。MAP-T在IPv4和IPv6协议之间建立适当的映射。这允许传统的IPv4流量通过IPv6网络转发。换句话说，传统设备和协议可以继续运行IPv4，即使网络需要IPv6。

在图6-5中，左侧的IPv4端点连接到客户端设备（Customer Premise Equipment, CPE）。MAP-T CPE设备具有到RPL网状网络的IPv6连接。在右侧，支持原生IPv4的SCADA服务器连接到MAP-T边界网关。因此，MAP-T CPE设备和MAP-T边界网关负责从IPv4到IPv6的MAP-T转换。

SCADA和其他工业传统协议的实现仍然广泛部署于许多行业中。虽然传统的SCADA已经从旧的串行连接发展到支持IP，但是在许多年内混合部署的情况依然存在。为了解决这一挑战，OT网络需要原始套接字和协议转换等机制来在现代IP网络上传输传统的协议。即使传统设备具有IPv4功能，受限制的网络部分通常需要IPv6，而不是IPv4。在这些情况下，可以使用MAP-T解决方案来实现IPv4数据在IPv6网络上传输。

6.2.3 基于Web的通用协议

多年来，基于Web的协议在消费者和企业应用程序与服务中变得很常见。因此，在开发物联网应用程序、服务和设备时，为了简化数据和设备从原型机到生产环境的集成，尝试利用这些协议是有意义的。

行业对基于Web的通用协议的熟悉程度很高。因此，具有基本Web编程技能的程序员可以从事物联网应用程序的开发，这可能会带来交付和处理物联网实时数据的创新方式。例如，生成事件的物联网设备可以启动视频捕获，同时向协作工具（如Cisco Spark Room）发送通知。此通知使得技术人员和工程师立即开始处理相关信息。除了对基于Web的协议的普遍高度认知外，人们对Web环境的扩展方法也有很好的理解，这在大量开发物联网设备消费者应用程序时至关重要。同样，必须分析受限节点和网络的定义，以选择最合适的协议（第5章讨论了受限节点和网络）。在不受限制的网络上，如以太网、WiFi或3G/4G蜂窝网络，带宽不是一个潜在的问题，基于详细数据模型表示（包括XML或JavaScript对象表示法[JSON]）的数据载荷可以通过HTTP/HTTPS或WebSocket传输。这使得实现人员可以在类似于Web应用程序的情境中开发物联网应用程序。

HTTP/HTTPS客户端/服务器模型是万维网的基础。具有高级功能的嵌入式Web服务器软件现在只需要很少的内存（在某些情况下可以达到几十KB）。这样就可以在一些受限设备上使用嵌入式Web服务软件。当考虑在物联网设备上实现Web服务时，必须仔细权衡是连接客户端还是连接服务器端。仅将数据推送到应用程序的物联网设备（例如，向天气应用程序报告数据的基于以太网或WiFi的气象站，或向健康应用程序发送数据的支持WiFi的体重秤）可能需要在客户端实现Web服务。HTTP客户端只启动连接，不接受传入的连接。

另一方面，物联网的一些设备，比如视频监控摄像机，可能在服务器端实现了Web服务。然而，由于这些设备通常具有有限的资源，因此必须保持较低的传入连接数量。此外，应该考虑在数据建模方面进

行高级开发，将工作负载从设备转移到客户端，包括PC、移动电话、平板电脑和云应用程序上的Web浏览器。

支持协同应用（如语音和视频、即时消息、聊天室和物联网设备）的实时通信工具之间的交互也正在出现。这推动了人与物联网设备之间实现更简单的通信系统的需求。解决这一需求的协议之一是可扩展消息和呈现协议（Extensible Messaging and Presence Protocol, XMPP）。

注释：在物联网中，通常可以看到简单对象访问协议（SOAP）和表述状态转移（REST）都被用作Web服务访问协议。SOAP基于可扩展标记语言（Extensible Markup Language, XML），从编码的角度来看它冗长而复杂，解析速度较慢，但它是通用的，并且具有内置的错误处理功能，可以使问题更容易解决。XML是一种规范，它详细描述了一组编码文档和其他数据结构的规则，以一种人类和计算机都可读的方式进行编码。作为SOAP的一个简单的轻量级替代方案，REST通常为请求实现一个简单的URI或JSON，而不是XML。JSON比XML更便于阅读和理解。而且，REST本身并不像SOAP那样是基于标准的协议，而是一种体系结构风格。

关于SOAP和REST复杂性的详细讨论超出了本书的范围，但是它们在物联网中的Web服务方面占有一席之地。从高层次的角度来看，REST的简单性使其更适合轻量级客户端上的应用程序，比如移动设备和嵌入式设备。另一方面，SOAP对企业 and 业务应用程序有更好的依附性，并且有更强的安全性需求。许多程序员都认为REST是未来的趋势，但同时我们会发现SOAP在某些应用程序中仍然非常普遍。

总之，物联网从现有的基于Web的协议中受益匪浅。这些协议，包括HTTP/HTTPS和XMPP，通过周知的和可扩展的编程技术，简化了Internet中物联网设备的集成。

然而，要完全解决受限设备和网络的问题，则需要优化的物联网协议。下一节将讨论这些协议。

6.2.4 物联网应用层协议

在考虑受限网络和/或大规模部署受限节点时，冗长的基于Web的协议和数据模型协议对于物联网应用程序来说可能过于繁重。为了解决这个问题，物联网行业正在研究新的轻量级协议，这些协议更适用于大量受限节点和网络。最流行的两种协议是CoAP和MQTT。图6-6突出显示了它们在通用物联网协议栈中的位置。

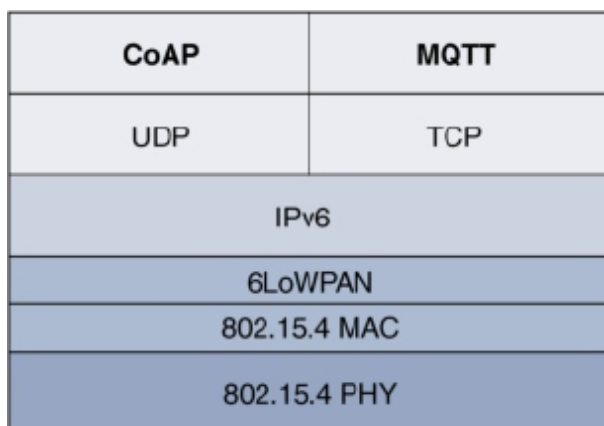


图6-6 用于CoAP和MQTT的高级物联网协议栈示例

在图6-6中，基于IEEE 802.15.4网状网络的CoAP和MQTT自然位于这个物联网堆栈示例的顶部。虽然会有一些例外，但我们几乎总是会发现CoAP部署在UDP上，MQTT运行在TCP上。后面几节将深入研究CoAP和MQTT。

1. CoAP

受限应用协议（CoAP）是IETF受限RESTful环境（CoRE）工作组为面向资源的应用程序开发一个通用框架时产生的，该框架的目标是受限节点和网络。第5章讨论过受限节点和网络。

CoAP框架定义了操作传感器和执行器以进行数据或设备管理的便捷方式。IETF CoRE工作组发布了多种CoAP标准轨道规范，包括以下内容。

■ RFC 6690: Constrained RESTful Environments (CoRE) Link Format

■ RFC 7252: The Constrained Application Protocol (CoAP)

■ RFC 7641 : Observing Resources in the Constrained Application Protocol (CoAP)

■ RFC 7959 : Block-Wise Transfers in the Constrained Application Protocol (CoAP)

■ RFC 8075: Guidelines for Mapping Implementations: HTTP to the Constrained Application Protocol (CoAP)

CoAP消息传递模型主要是为了方便端点之间通过UDP交换消息，包括安全传输协议数据报传输层安全（DTLS）。IETF CoRE工作组正在研究其他传输机制，包括TCP、安全TLS和WebSocket。LWM2M开放移动联盟定义的用于物联网设备管理的短消息服务（SMS）上的CoAP也在考虑中。

RFC 7252提供了使用DTLS保护CoAP的更多细节。它指定如何为CoAP端点配置键和筛选列表，定义了4种安全模式：NoSec、PreSharedKey、RawPublicKey和Certificate。NoSec和RawPublicKey实现是必需的。

从格式化的角度来看，CoAP消息由一个短的固定长度的头字段（4字节）、长度可变但必需的标记字段（0~8字节）、选项字段（如果有必要）和载荷字段组成。图6-7详细说明了CoAP消息格式，它在降低解析复杂性的同时提供了较低的开销。



图6-7 CoAP消息格式

在图6-7中可以看到，CoAP消息格式相对简单且灵活。它允许CoAP提供低开销，这对于受限网络非常重要，同时也便于对受限设备进行解析和处理。表6-1概述了CoAP消息的各个字段。

表6-1 CoAP消息字段

CoAP 消息字段	字段描述
Ver (版本)	标识 CoAP 版本
T (类型)	定义以下 4 种消息类型之一：可确认 (CON)、不可确认 (NON)、确认 (ACK) 或重置 (RST)。CON 和 ACK 在图 6-9 中有更详细的介绍
TKL (标记长度)	指定标记字段的大小 (0~8 字节)
代码	指示请求消息的请求方法和响应消息的响应代码。例如，在图 6-9 中，GET 是请求方法，2.05 是响应代码。有关此字段值的完整列表，请参考 RFC 7252
消息 ID	检测重复消息，用于将 ACK 和 RST 消息类型与 Con 和非消息类型进行匹配
标记	使用 TKL 指定的长度关联请求和响应
选项	指定选项编号、长度和选项值。该字段提供的功能包括指定请求的目标资源和代理功能
载荷	携带 CoAP 应用程序数据。该字段是可选的，但当它存在时，全为 1 (0xff) 的一个字节位于载荷之前。该字节的目的是描绘选项字段的结尾和载荷的开头

CoAP可以在IPv4或IPv6上运行。但是，建议将消息放入单个IP包和UDP载荷中，以避免分片。对于IPv6，默认的MTU大小为1280字节，并且不允许跨节点分片，最大 CoAP消息大小可以达到1152字节，包括载荷的1024字节。在IPv4的情况下，由于IP分片可能存在于整个网络中，因此应该将自己限制为更保守的值，并设置IPv4禁止分片 (DF) 位。

虽然大多数传感器和执行器流量使用小数据包载荷，但是一些用例（例如固件升级）需要具有发送更大载荷的能力。CoAP不依赖于IP

分片，而是定义了一对块（Block）选项（在RFC 7959中），用于在多个请求/响应对中传输来自资源表示形式的多个信息块。

如图6-8所示，跨物联网基础设施的CoAP通信可以采用各种路径。连接可以是位于相同或不同受限网络上的设备之间的连接，也可以是设备与通用Internet或云服务器之间的连接，所有这些连接都在IP上运行。还定义了代理机制，RFC 7252详细介绍了CoAP的基本HTTP映射。由于HTTP和CoAP都是基于IP的协议，所以代理功能实际上可以位于网络中的任何位置，而不必位于受限和非受限网络之间的边界。

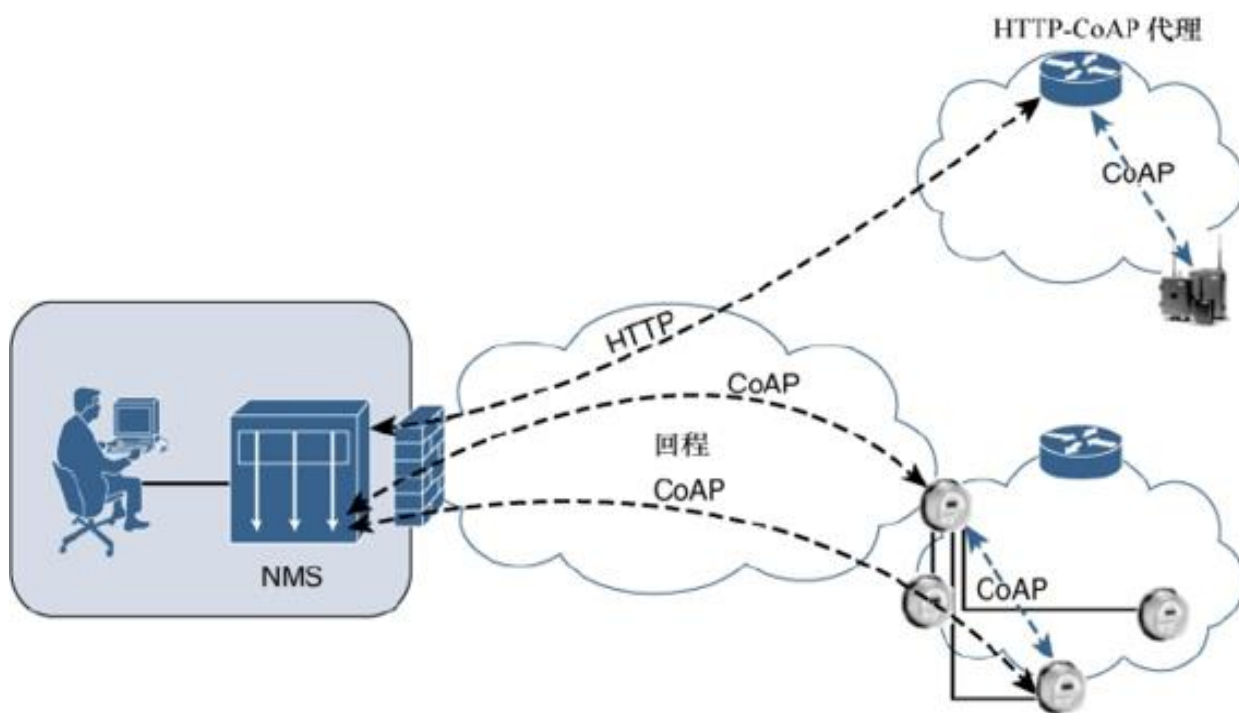


图6-8 物联网基础设施中的CoAP通信

就像HTTP一样，CoAP基于REST体系结构，但是有一个“物”同时充当客户端和服务端。通过异步消息的交换，客户端通过服务器资源上的方法代码请求操作。服务器上的统一资源标识符（Uniform Resource Identifier, URI）标识此资源。服务器使用可能包含资源表示的响应代码进行响应。CoAP请求/响应语义包括GET、POST、PUT和DELETE方法。

例6-2显示了CoAP URI格式。可以发现CoAP URI格式类似于HTTP/HTTPS。coap/coaps URI方案标识资源，包括主机信息和可选的UDP端口，由URI中的主机和端口参数表示。

例6-2 CoAP URI格式

```
coap-URI = "coap: " "/" host [": " port] path-abempty ["?" query]
coaps-URI = "coaps: " "/" host [": " port] path-abempty ["?" query]
```

CoAP定义了4种类型的消息：可确认的消息、不可确认的消息、确认消息和重置消息。这些消息中包含的方法代码和响应代码使消息可以携带请求或响应。CoAP代码、方法和响应代码、选项号和内容格式已由IANA指定为受限的RESTful环境（CoRE）参数。

在UDP上运行时，CoAP在CoAP数据头被标记为“可确认的”时提供可靠的消息传输。此外，CoAP支持带有默认超时的基本的拥塞控制、带有指数回退机制的简单停止和等待重传，以及通过消息ID检测重复的消息。如果一个请求或响应被标记为可确认，则接收方必须使用相同的消息ID明确是接受还是拒绝消息，如图6-9所示。如果接收方无法处理不可确认的消息，则发送重置消息。

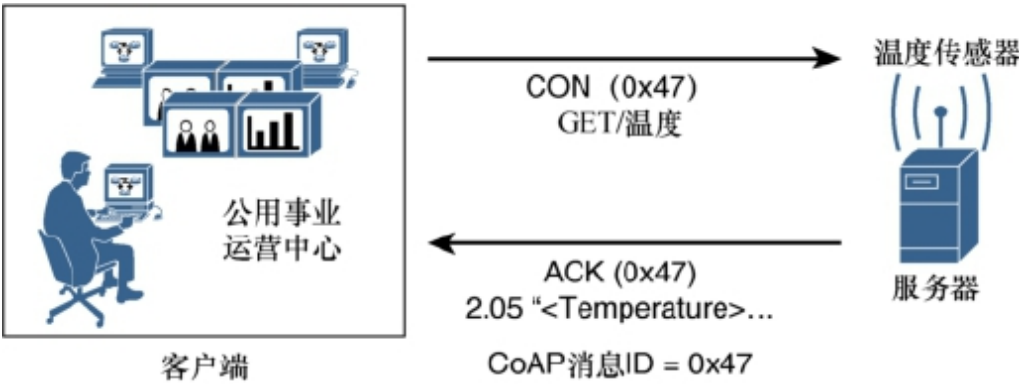


图6-9 CoAP可靠传输示例

图6-9显示了一个公用设施操作中心，它充当CoAP客户端，右侧的CoAP服务器作为温度传感器。客户端和服务端之间的通信使用一个CoAP消息ID 0x47。CoAP消息ID确保可靠性，并用于检测重复消息。

图6-9中的客户端发送一条GET消息以从传感器获取温度。请注意，此GET消息的消息ID为0x47，并且该消息被标记为CON。CoAP消息中的CON（可确认）标记意味着消息将被重新传输，直到接收方发送具有相同消息ID的确认（或ACK）消息为止。

在图6-9中，温度传感器确实以引用正确消息ID 0x47的ACK消息进行应答。此外，此ACK消息将成功响应GET请求本身。这由位于请求数据后面的2.05响应代码来表示。

CoAP支持利用IP多播将数据发送到一组设备。用CoAP实现IP多播时，需要使用all-CoAP-node多播地址。对于IPv4，该地址是224.0.1.187，对于IPv6，该地址是FF0X::FD。这些多播地址由CoAP节点连接，这些节点在监听默认CoAP端口5683的同时向其他端点提供服务。因此，端点可以通过多播服务找到可用的CoAP服务。多播的一个典型用例是为一组物联网设备（如智能电表）部署固件升级。

由于在物联网端点上通常没有实现手动配置，因此需要由CoAP客户端发现提供服务和资源的CoAP服务器。来自CoAP服务器的服务可以通过学习命名空间中的URI或通过all-CoAP-node多播地址来发现。当使用URI模式发现服务时，默认端口5683用于非安全CoAP，而端口5684用于DTLS安全的CoAP。CoAP服务器必须在这些端口上处于监听状态，除非不同的端口号与命名空间中的URI关联。

与访问Web服务器资源相似，CoAP规范在RFC 6690中提供了资源之间关系的描述。该标准将CoRE链路格式定义为具有指定Internet媒体类型的载荷。列出CoAP服务器资源链接的一个默认方式是设置一个周知的相对URI，例如/.well-known/core。

为了提高响应时间和减少带宽消耗，CoAP支持基于响应代码的缓存功能。要使用缓存条目，CoAP端点必须验证当前的请求，而且存储的响应必须与之匹配，包括所有选项（除非标记为NoCacheKey）。这将确认存储的响应是新的或有效的。

CoAP实现有多种。有些是使用开放源码许可证发布的，另一些是供应商解决方案的一部分。

综上所述，CoAP是一种适用于物联网框架的关键应用协议。因为它的标准化是由IETF CoRE工作组领导的，所以它与其他IETF工作组密切协同工作，特别是那些关注受限节点和网络的工作组，如6Lo、6TiSCH、LWIG、RoLL、ACE和COSE。因此，CoAP针对物联网受限节点和网络进行了充分优化，同时利用传统的Web编程技术使其更容易被开发社区所理解。

2. 消息队列遥测传输（MQTT）

在20世纪90年代末，来自IBM和Arcom（2006年被Eurotech收购）的工程师在寻找一个轻量级、经济高效的可靠协议来监控大量来自于一个中央服务器位置的传感器及其数据，这种协议通常由石油和天然气行业使用。他们的研究促使了消息队列遥测传输（MQTT）协议的开发和实现，该协议现在由结构化信息标准促进组织（OASIS）进行标准化。

考虑到石油和天然气行业的恶劣环境，一种非常简单的、只有几个选项的协议被设计出来。这个协议考虑了受限节点、不可靠的广域网回程通信和具有可变延迟的带宽限制等因素。这些是基于TCP/IP体系结构选择客户端/服务器和发布/订阅框架的一些基本原理，如图6-10所示。

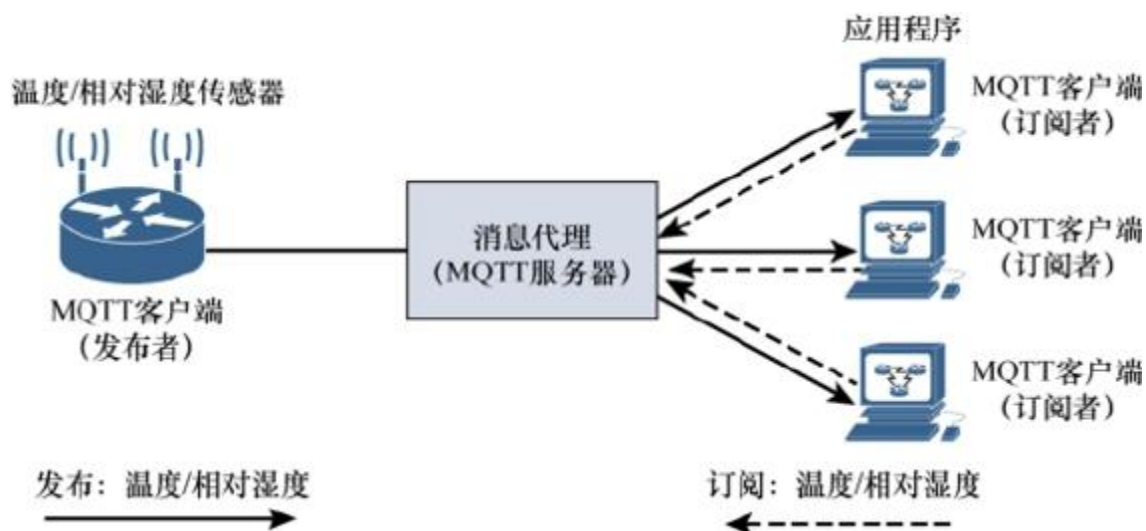


图6-10 MQTT发布/订阅框架

MQTT客户端可以充当发布者，向充当MQTT消息代理的MQTT服务器发送数据（或资源信息）。在图6-10中，左侧的MQTT客户端是一个温度（Temp）和相对湿度（RH）传感器，它发布其Temp/RH数据。MQTT服务器（或消息代理）接受来自发布者的网络连接和应用程序消息，例如Temp/RH数据。它还处理订阅和取消订阅过程，并将应用程序数据推送给充当订阅者的MQTT客户端。

图6-10右侧的应用程序是MQTT客户端，它是左侧发布者或传感器生成的Temp/RH数据的订阅者。这种模式是周知的，订阅者表示希望从发布者那里接收信息。一个很好的协作和社交网络应用程序的例子是Twitter。

使用MQTT，客户端可以订阅发布者信息树中的所有数据（使用通配符）或特定数据。此外，MQTT中存在的消息代理可以将充当发布者和订阅者的客户端之间的数据传输进行解耦。事实上，发布者和订阅者甚至不知道（或不需要知道）彼此。进行这种解耦的一个好处是，MQTT消息代理确保在出现网络故障时可以缓冲和缓存信息。这也意味着发布者和订阅者不必同时在线。

MQTT控制包使用端口1883在TCP传输层运行。TCP确保MQTT客户端和MQTT服务器之间有一个有序的无损的字节流。可以选择在端口8883上使用TLS保护MQTT，还可以使用WebSocket（在RFC 6455中定义）。

MQTT是一种轻量级协议，因为每个控制包由一个2字节的固定包头组成，头字段可选，载荷可选。应该注意到，控制包可以包含高达256 MB的载荷。图6-11所示为MQTT消息格式。



图6-11 MQTT消息格式

与图6-7中的CoAP消息格式相比，可以看到MQTT包含一个更小的包头（2字节），而CoAP有4字节。包头中的第一个MQTT字段是消息类型，它标识消息中MQTT包的类型。MQTT 3.1.1版本中指定了14种不同类型的控制包。它们中的每一个都有一个唯一的值，该值被编码到消息类型字段中。注意，值0和15是保留的。表6-2总结了MQTT消息类型。

表6-2 MQTT消息类型

消息类型	值	流向	描述
CONNECT	1	客户端到服务器	请求连接
CONNACK	2	服务器到客户端	连接确认
PUBLISH	3	客户端到服务器 服务器到客户端	发布消息
PUBACK	4	客户端到服务器 服务器到客户端	连接确认
PUBREC	5	客户端到服务器 服务器到客户端	发布已接收
PUBREL	6	客户端到服务器 服务器到客户端	发布

续表

消息类型	值	流向	描述
PUBCOMP	7	客户端到服务器 服务器到客户端	发布完成
SUBSCRIBE	8	客户端到服务器	订阅请求
SUBACK	9	服务器到客户端	订阅确认
UNSUBSCRIBE	10	客户端到服务器	取消订阅请求
UNSUBACK	11	服务器到客户端	取消订阅确认
PINGREQ	12	客户端到服务器	Ping 请求
PINGRESP	13	服务器到客户端	Ping 响应
DISCONNECT	14	客户端到服务器	客户机断开连接

MQTT包头中的下一个字段是DUP（重复标志）。设置此标志后，允许客户端可以标记之前已经发送但是没有收到确认的数据包。

QoS包头字段允许选择3个不同的QoS级别。本章后面将更详细地讨论这些问题。

下一个字段是保留（Retain）标志。保留（Retain）标志仅存在于PUBLISH消息（见表6-2）中，它通知服务器保留消息数据。这允许新订阅者立即接收最新的已知值，而不必等待发布者的下一次更新。

MQTT消息头中的最后一个强制字段是剩余长度字段。该字段指定其后面的MQTT数据包中的字节数。

每个客户端和服务端之间的MQTT会话由4个阶段组成：会话建立、身份验证、数据交换和会话终止。每个连接到服务器的客户端都有一个唯一的客户端ID，这允许在双方之间标识MQTT会话。当服务器向多个客户端传递应用程序消息时，每个客户端都是独立处理的。

在订阅资源时会生成SUBSCRIBE/SUBACK控制包，而取消订阅则是通过交换UNSUBSCRIBE/UNSUBACK控制包来执行的。平稳的连接终止是通过DISCONNECT控制包完成的，该控制包还为客户端提供了这一功能，即客户端通过重新发送其客户端ID来重新建立连接，并恢复操作。

消息代理使用主题字符串或主题名称为其订阅者筛选消息。订阅资源时，订阅服务器指示用于构造主题名称的一个或多个主题级别。MQTT主题名称中的斜杠（/）用于分隔主题树中的每个级别，并为主题名称提供层次结构。图6-12用adt/lora.adeunis说明了这些概念。adt/lora.adeunis是主题级别，adt/lora/adeunis/0018B2000000023A是主题名称的示例。

客户端在订阅主题名称时具有很强的灵活性。通过使用通配符，可以订阅一个确切的主题，或者同时订阅多个主题。订阅可以包含一个通配符，以允许同时订阅多个主题。

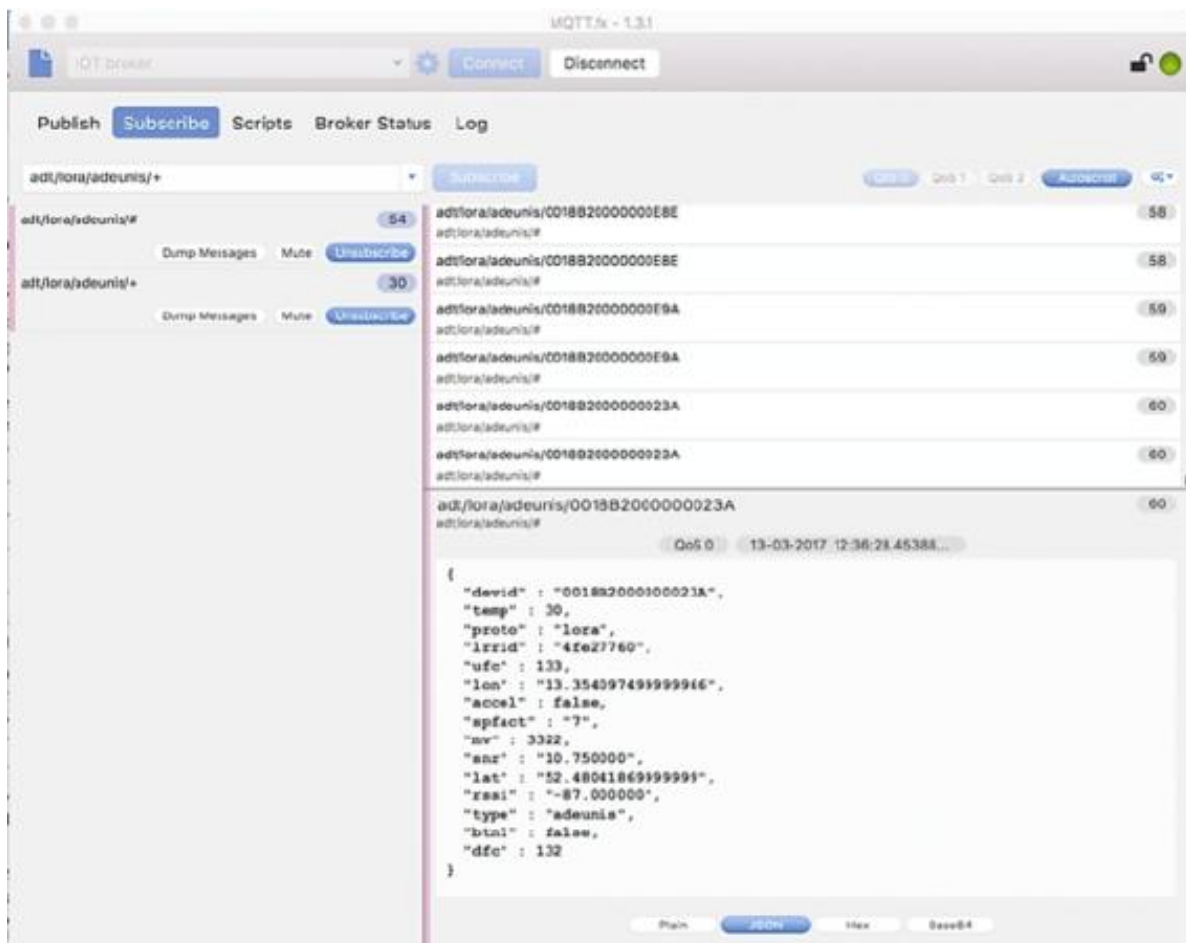


图6-12 MQTT订阅示例

井号（#）是一个通配符，可以匹配主题中的任意级别。多级通配符表示父级和任意数量的子级。例如，订阅adt/lora/adeunis/#可以接收整个子树，其中可以包含以下主题名称：

- adt/lora/adeunis/0018B20000000E9E
- adt/lora/adeunis/0018B20000000E8E
- adt/lora/adeunis/0018B20000000E9A

加号（+）是一个通配符，只匹配一个主题级别。例如，adt/lora/+允许访问adt/lora/adeunis/和adt/lora/abeeway，但不允许访问adt/lora/adeunis/0018B20000000E9E。

当订阅以通配符（#或+）开始时，服务器必须排除以美元符号（\$）开头的主题名称。通常，这些类型的主题名称用于信息代理的内部统计。因此，客户端无法将消息发布到这些主题。例如，订阅+/monitor/Temp不会接收任何发布到\$SYS/monitor/Temp的消息。本主题可作为该温度传感器的控制通道。

PINGREQ/PINGRESP控制包用于验证客户端和服务器之间的连接。与作为IP一部分的ICMP ping类似，它们是一种保活数据包，有助于维护和检查TCP会话。

通过TLS保护MQTT连接被认为是可选的，因为它在受限的节点上需要更多的资源。当不使用TLS时，客户端在连接启动期间发送一个明文用户名和密码。MQTT服务器实现还可以接受匿名客户端连接（用户名/密码为“空白”）。在实现TLS时，客户端必须验证服务器证书以进行正确的身份验证。根据服务器的配置，客户端身份验证还可以通过与服务器交换证书来执行。

MQTT协议提供3个级别的服务质量（QoS）。MQTT的QoS是在与发布者或订阅者交换应用程序消息时实现的，它与大多数人熟悉的IP QoS不同。交付协议是对称的。这意味着客户端和服务器可以各自扮演发送方或接收方的角色。交付协议只涉及将应用程序的消息从单个发送方传递到单个接收方。以下是MQTT QoS的3个级别。

■ QoS 0：这是一种“至多一次”交付的尽力而为数据服务，而且不会对数据进行确认。发布者一次将消息发送到服务器，服务器一次将其发送给订阅者。接收方不发送响应，发送方不执行重试。消息要么到达接收者，要么根本不到达。

■ QoS 1：该QoS级别确保发布者和服务器之间以及服务器和订阅者之间的消息交付至少发生一次。在PUBLISH和PUBACK包中，包标识符包含在可变的包头中。如果消息未被PUBACK包确认，则将再次发送该消息。此级别保证“至少一次”交付。

■ QoS 2: 这是最高的QoS级别，在不能接受消息丢失或重复时使用。与此QoS级别相关的开销会增加，因为每个数据包都包含一个带有包标识符的可选变量头。在确认收到发布消息时，需要两个步骤的确认过程。第一步通过 PUBLISH/PUBREC 包对完成，第二步通过 PUBREL/PUBCOMP 包对完成。此级别提供了称为“恰好一次”交付的“保证服务”，只要消息交付一次，就不考虑重试次数。

如前所述，QoS流程对于发送方和接收方的角色是对称的，但是存在两个独立的事务。一个事务发生在发布客户端和MQTT服务器之间，另一个事务发生在MQTT服务器和订阅客户端之间。图6-13提供了3个不同级别的MQTT QoS流的概述。

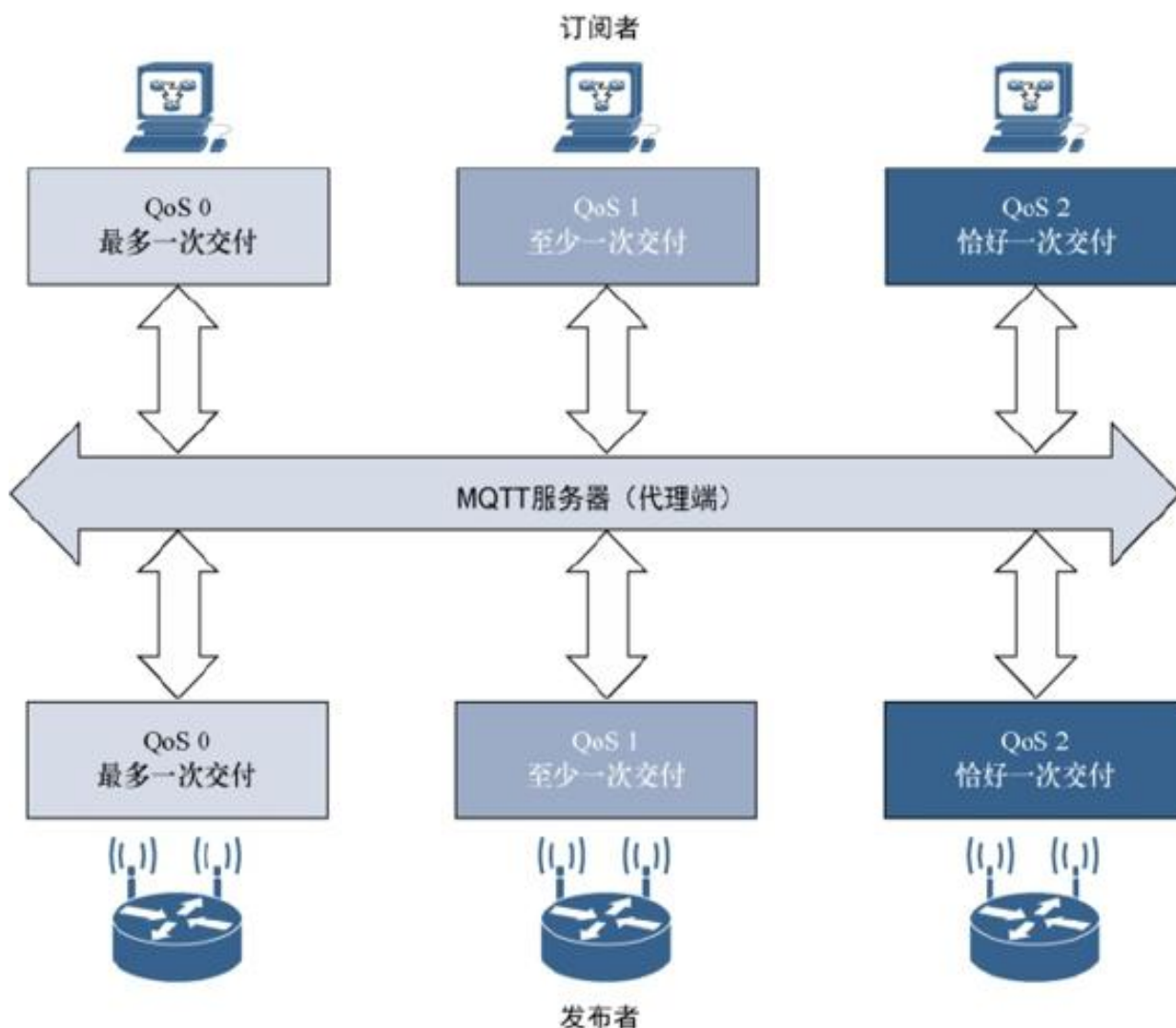


图6-13 MQTT QoS流

注释：MQTT流每一端的客户端都设置QoS级别。发布客户端在与MQTT服务器通信时也需 设置QoS级别。另一方面，客户端订阅者在与MQTT服务器进行订阅时也要设置QoS级别。如图6-13所示，在大多数情况下，客户端到代理端之间的QoS保持不变。但是，您应该注意到，在某些情况下，QoS级别会发生变化，并且端到端的QoS会不相同。

与CoAP一样，现在可以使用多种MQTT实现。它们要么作为开源许可发布，要么集成到供应商的解决方案中，比如Facebook Messenger。

注释：MQTT.fx是一个用于工作和试验MQTT的免费工具（见图6-12）。

本章已经详细讨论了CoAP和MQTT，大家应该可以回答这样的问题：“对于给定的用例，哪种协议更好？”以及“我应该在物联网网络中使用哪一个？”。不幸的是，答案并不总是明确的，MQTT和CoAP都有自己的用武之地。表6-3从物联网的角度概述了MQTT和CoAP之间的差异，以及它们的优缺点。

表6-3 CoAP与MQTT的比较

要素	CoAP	MQTT
主要传输协议	UDP	TCP
典型的消息传递	请求/响应	发布/订阅
LLN 的有效性	非常好	低/尚可(将 UDP 与 MQTT 配对的实现更适合 LLN)
安全性	DTLS	SSL/TLS
沟通模式	一对一	多对多
优点	轻量级、快速、低开销, 适用于受限网络; 使用易于编码的 RESTful 模型; 易于分析和处理受限设备; 支持多播; 异步和同步消息	TCP 和多个 QoS 选项提供了健壮通信; 通过使用代理体系结构实现简单管理和可扩展性
缺点	不像基于 TCP 的 MQTT 那么可靠, 所以应用程序必须确保可靠性	受限设备和网络的开销更高; TCP 连接可以耗尽低功耗设备; 不支持多播

总之, MQTT “多对多”的订阅框架不同于“一对一”的 CoAP 模型, 这使它成为某些部署的更好选择。MQTT 基于 TCP, 它确保有序无损的连接。当与 UDP 和灵活的消息格式配对时(可选的方式), 它具有较低的开销, 支持 TLS 以实现安全性, 并提供 3 种级别的 QoS。这使得 MQTT 成为物联网成功采用和发展的关键应用层协议。

6.3 小结

本章讨论了物联网协议栈。第 4 章介绍了 PHY 层和 MAC 层的物联网选项, 第 5 章详细介绍了网络层的选项。

本章主要讨论物联网中应用协议的传输。本章首先讨论 TCP 和 UDP。根据应用的不同, 这两种协议在物联网中都有自己的用武之地。

本章的其余部分重点介绍传输物联网应用数据的各种方法。第一种方法是不存在应用层协议，其中数据载荷直接在较低层上传输。需要物联网数据代理来扩展这种传输应用数据的方法。

第二种方法是IP适配应用层。该技术利用IP适配层传输来自非IP堆栈的应用程序数据。传统的工业协议（如DNP3）属于这一类，需要原始套接字和协议转换等功能才能在IP网络中成功通信。

接下来讨论的方法是基于Web的通用协议（如HTTP），它可以用于非受限网络，如以太网和WiFi。

最后讨论的在上层处理物联网应用数据的方法是使用物联网应用层协议。该方法处理受限节点和网络，适用于大多数物联网网络。特殊协议（如CoAP和MQTT）处理物联网应用程序的数据需求，对于需要在低带宽网络上进行通信且占用空间较小的智能对象非常有效。

第7章 物联网的数据和分析

在经典的美国科幻电视剧《星际迷航》（Star Trek）中，一个名为“特里布尔”（tribble）的毛茸茸的外星生物被带上了“进取号”（Enterprise）星际飞船。起初，可爱的特里布尔被当作宠物，但其不同寻常的特性开始显现：它能够以惊人的速度复制自己，以至于飞船很快就充满了特里布尔的复制体，他们开始消耗飞船上的所有补给并开始干扰飞船的系统。

物联网产生的数据问题很可能类似于“特里布尔的麻烦”。起初，物联网数据只是一种好奇的产物，如果处理得当，它很有用。然而，随着时间的推移，越来越多的设备加入物联网，这些系统产生的数据使服务器难以承受。这些数据不仅开始消耗宝贵的网络带宽，而且在对这些数据尝试处理、排序和分析时，服务器资源的负担也越来越重。

传统的数据管理系统对所谓的“大数据”的需求毫无准备。正如本书所讨论的，物联网的真正价值不仅在于连接事物，还在于这些事物产生的数据、通过这些关联的事物实现的新服务，以及数据可以揭示的商业洞见。然而，要使数据有用，需要以组织和可控制的方式处理数据。因此，物联网需要一种新的数据分析方法。

本章将通过物联网的角度提供数据领域的概览，内容如下。

■ **物联网数据分析简介：**本节介绍物联网分析的主题，并讨论结构化和非结构化数据之间的区别。本节还讨论分析与物联网数据的关系。

■ **机器学习：**一旦拥有了数据，你将如何使用它，以及如何从中获得商业洞察力？本节将深入探讨用于从物联网数据中获得商业洞察力的机器学习的主要类型。

■ **大数据分析工具和技术：**大数据是物联网领域最常用的术语之一。本节研究当今大数据中最常用的一些技术，包括Hadoop、NoSQL、MapReduce和MPP。

■ **边缘流分析：**物联网要求实时、尽可能接近终端进行数据处理和分析。本节将探讨如何使用流分析进行此类处理和分析。

■ **网络分析：**本节介绍了在物联网系统中使用Flexible NetFlow进行网络流分析的概念。NetFlow可以帮助我们更好地理解整个系统的功能，提高物联网的安全性。

7.1 物联网数据分析简介

在物联网世界中，从传感器创建大量数据是常见的，也是最大的挑战之一——从传输的角度来看如此，从数据管理的角度来看也是如此。物联网可以产生海量数据的一个示例是在商业航空工业中部署在飞机上的传感器。

现代喷气发动机装有数千个传感器，每秒可产生高达10GB的数据。如图7-1所示的现代喷气发动机可能会配备大约5000个传感器。因此，一架双引擎商用飞机每天平均运行8小时，每天将产生超过500TB的数据，而这仅仅是来自引擎的数据！今天的飞机有成千上万的其他传感器连接到机身和其他系统。事实上，现代大型喷气式飞机的一个机翼上就装有1万个传感器。



图7-1 商业飞机的引擎

每架商用飞机每天获取拍字节（PB）数据的难度并不大——这只是针对一架飞机来说的。全世界每天大约有10万次商业航班。仅来自商业航空业务的物联网数据量就是惊人的。

这个示例只是众多体现出物联网愈发严重的大数据问题的示例之一。以尽可能有效的方式分析这些数据属于数据分析的范畴。数据分析必须能够及时地从数据中提供可操作的见解和知识，无论数据的数量或形式如何，否则无法充分实现物联网的优点。

注释：另一个关于物联网产生的数据量以及数据分析需求的示例是公用事业行业。即使是中等规模的智能电表网络，每天也能提供10亿个以上的数据点。有关这一数据挑战的更多细节，请参阅第2章。

在深入研究数据分析之前，有必要定义几个与数据相关的关键概念。首先，并非所有的数据都是相同的；可以用不同的方法对其进行分类和分析。根据数据的分类方式，可以应用各种数据分析工具 and 处理方法。从物联网的角度来看，两个重要的分类依据是数据是结构化的还是非结构化的，以及数据是处于活动状态还是静止状态。

7.1.1 结构化数据与非结构化数据的比较

结构化数据和非结构化数据是重要的分类，因为从数据分析的角度来看，它们通常需要不同的工具集。图7-2提供了结构化数据和非结构化数据的比较。

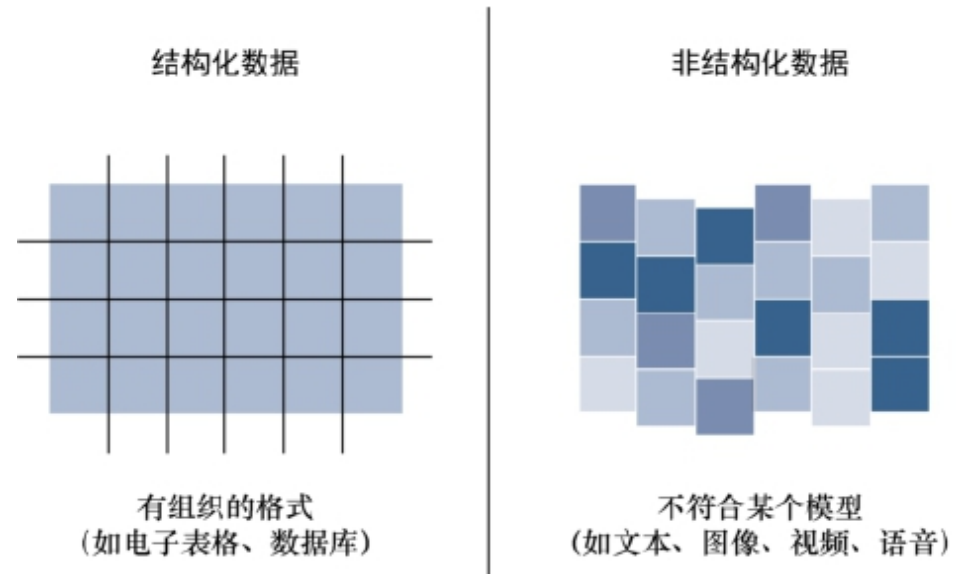


图7-2 结构化数据与非结构化数据的比较

结构化数据意味着数据遵循这样一种模型或模式，即这种模型或模式定义了数据的表示或组织方式，这意味着它非常适合于传统关系数据库管理系统（RDBMS）。在许多情况下，我们会发现结构化数据以简单的表格形式出现，例如电子表格中的数据占据特定的单元格，并且可以明确地定义和引用。

结构化数据可以在大多数计算系统中找到，包括从银行交易和发票到计算机日志文件和路由器配置在内的所有内容。物联网传感器数据通常使用结构化的值，如温度、压力、湿度等，这些值都以已知格式发送。结构化数据易于格式化、存储、查询和处理；由于这些原因，它一直是用于进行业务决策的核心数据类型。

由于结构化数据具有高度组织化的格式，因此可以使用大量的数据分析工具来处理这类数据——从自定义脚本到Microsoft Excel和Tableau等商业软件，大多数人都对结构化数据比较熟悉。

非结构化数据缺乏通过传统编程方法来理解和解码数据的逻辑模式。这种数据类型的示例包括文本、语音、图像和视频。一般来说，任何不完全符合预定义数据模型的数据都被归类为非结构化数据。

据估计，大约80%的业务数据是非结构化的。正因为如此，可以应用于非结构化数据的数据分析方法，如认知计算和机器学习，理所当然地受到了高度关注。使用机器学习应用程序，如自然语言处理（NLP），可以解码语音。使用图像/人脸识别应用程序，可以从静态图像和视频中提取关键信息。本章后文将更深入地讨论使用机器学习技术处理非结构化的物联网数据。

注释：第三种数据分类是半结构化数据，有时包括在结构化和非结构化数据中。大家可能猜到了，半结构化数据是结构化数据和非结构化数据的混合，并且具有与两者相同的特性。虽然不属于关系型数据，但是半结构化数据包含一定的模式和一致性。电子邮件是半结构化数据的一个很好的例子，因为字段定义得很好，但是正文字段和附件中包含的内容是非结构化的。其他示例包括JavaScript对象表示法（JSON）和可扩展标记语言（XML），这是在Web和一些物联网数据交换中经常使用的数据交换格式。

物联网中的智能对象生成结构化和非结构化数据。结构化数据由于其明确定义的组织结构，更容易管理和处理。非结构化数据可能更难处理，通常需要不同寻常的分析工具来处理数据。熟悉这两种数据分类非常重要，因为了解使用的是哪种数据分类可以更加容易地集成适当的数据分析解决方案。

7.1.2 动态数据与静态数据

与大多数网络一样，物联网网络中的数据要么在传输中（“动态数据”），要么被保存或存储（“静态数据”）。动态数据的示例包括传统的客户端/服务器交换，比如Web浏览和文件传输，以及电子邮件。保存到硬盘、存储阵列或USB驱动器中的数据是静态数据。

从物联网的角度看，来自智能对象的数据被认为是移动数据，因为它通过网络路由到最终目的地。这通常是在边缘使用雾计算进行处理。当在边缘处理数据时，数据可能被过滤、删除或转发以便进一步处理，并可能存储在雾节点或数据中心。数据不会停留在边缘（有关边缘和雾计算的更多信息，请参阅第2章）。

当数据到达数据中心时，可以像在边缘一样对其进行实时处理，而数据仍然在移动。与分析存储数据的工具相比，具有这种功能的工具（如Spark、Storm和Flink）相对来说还处于起步阶段。本章后文将提供关于这些实时流分析工具的更多信息，这些工具是Hadoop生态系统的一部分。

物联网网络中的静态数据通常可以在物联网代理或数据中心的某种存储阵列中找到。从数据分析的角度来看，有很多工具可供使用，特别是关系数据库中用于结构化数据的工具。这些工具中最著名的是Hadoop。Hadoop不仅可以处理数据，而且还可以存储数据。本章稍后将对此进行更详细的讨论。

7.1.3 物联网数据分析概述

来自智能对象的物联网数据的真正的重要性只有在数据分析能带来可操作的商业智能和见解时才能实现。数据分析通常根据生成的结果类型进行分解。如图7-3所示，数据分析结果有4种类型。

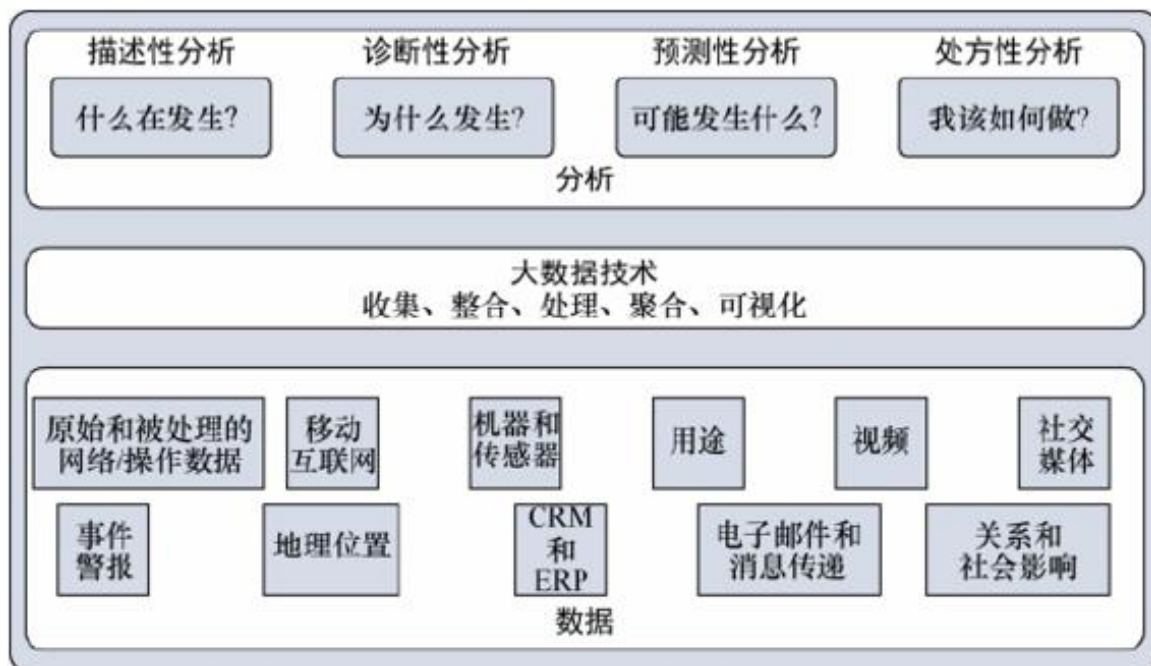


图7-3 数据分析结果的类型

■ **描述性分析**：描述性数据分析告诉我们现在或过去正在发生什么。例如，卡车发动机中的温度计每秒报告一个温度值。从描述性分析的角度来看，可以随时提取这些数据，以了解卡车发动机的当前运行状况。如果温度值过高，则可能出现冷却问题或发动机承受了太多的负荷。

■ **诊断性分析**：当我们对“为什么”感兴趣时，诊断性数据分析可以提供答案。继续以卡车发动机中的温度传感器为例，我们可能想知道为什么卡车发动机会出现故障。诊断性分析可能表明发动机温度过高，发动机过热。对由大量智能对象生成的数据应用诊断性分析，可以清楚地了解问题或事件发生的原因。

■ **预测性分析**：预测性分析的目的是在问题发生之前对其进行预测。例如，通过使用卡车发动机的历史温度值，预测性分析可以对发动机中某些部件的剩余寿命进行估计，从而在故障发生之前主动更换这些组件。或者，如果卡车发动机的温度值随着时间的推移开始缓慢上升，这可能表明需要更换机油或进行其他类型的发动机冷却维护。

■ 处方性分析：处方性分析超越了预测性分析，为即将出现的问题提出了解决方案。对卡车发动机的温度数据进行处方性分析，可能会计算出各种替代方案，从而经济有效地维护卡车。这些计算可能包括更频繁地更换机油和冷却维护所需的成本，以及在发动机上安装新的冷却设备或升级到租用一台功率更大的发动机。处方性分析着眼于各种因素，并提出适当的建议。

预测性分析和处方性分析都是资源密集型的，并且增加了复杂性，但是它们提供的价值远远大于描述性分析和诊断性分析的价值。图7-4所示为4种数据分析类型，以及它们在复杂性和价值增长方面的排名。可以看出，描述性分析是最简单的，同时提供的价值也是最小的。另一方面，处方性分析提供了最多的价值，但实现也是最复杂。物联网领域的大多数数据分析依赖于描述性和诊断性分析，但对大多数企业和组织来说，向预测性和处方性分析的转变是可以理解的。

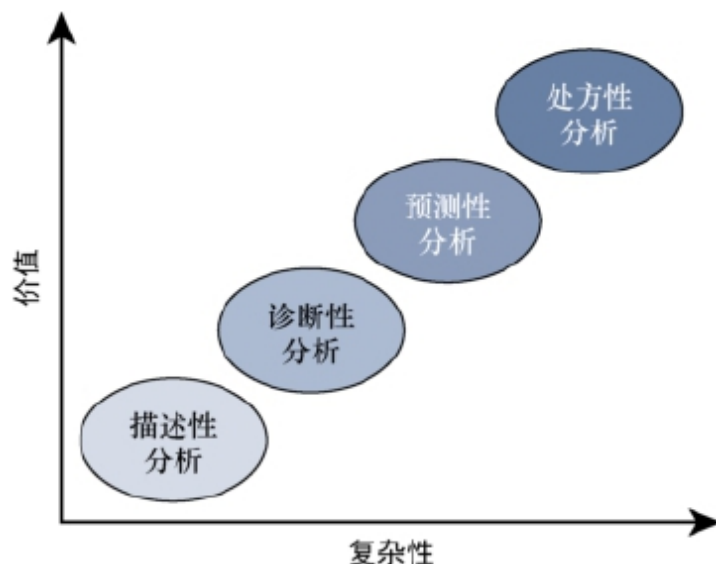


图7-4 价值和复杂性因素在数据分析类型中的应用

7.1.4 物联网数据分析面临的挑战

随着物联网的发展，传统的数据分析解决方案受到了挑战。例如，传统的数据分析通常使用标准的RDBMS和相应的工具，但是物联网的世界要求更高。虽然关系数据库仍然用于某些数据类型和应用程

序，但它们常常与物联网数据的性质相冲突。物联网数据为关系数据库带来了两个挑战。

■ **扩展性问题：**由于大多数物联网网络中存在不断发送数据的大量智能对象，关系数据库可以非常迅速地增长到难以置信的大小。这可能会导致解决性能问题的成本非常高，通常需要更多的硬件以及变更体系结构。

■ **数据的波动性：**对于关系数据库，从一开始就正确设计模式是至关重要的，否则它会减慢或停止数据库的运行。由于缺乏灵活性，必须将模式的更改保持在最低限度。然而，物联网数据是不稳定的，因为数据模型可能会随着时间的推移而改变和演进。通常需要动态模式，以便可以每天甚至每小时对数据模型进行更改。

为了应对扩展性和数据波动性等挑战，人们开始使用另一种类型的数据库NoSQL。结构化查询语言（SQL）是用于与RDBMS通信的计算机语言。顾名思义，NoSQL数据库是不使用SQL的数据库。它不是以关系数据库的传统表格的形式建立的。NoSQL数据库不强制执行严格的模式，它们支持复杂的、不断发展的数据模型。这些数据库本身也具有更高的可扩展性。有关NoSQL的更多信息，请参阅7.3.2节。

除物联网带来的关系数据库挑战外，物联网拥有大量频繁变化的智能对象数据，还带来了数据的实时流媒体特性和网络级别的数据管理方面的挑战。

流数据是作为智能对象传输数据而生成的，具有挑战性，因为它通常具有非常大的容量，只有能够被实时分析和响应，流数据才有价值。流数据的实时分析允许用户检测模式或异常，这些模式或异常可能表明需要某种即时响应的问题或情况。为了能够影响这个问题的结果，用户必须能够在产生数据时进行过滤和分析，尽可能接近边缘。

实时分析流数据的市场正在快速增长。主要的云分析提供商，如谷歌、微软和IBM，都提供流分析服务，并且可以在内部使用各种其他应用程序（本章后面将深入讨论边缘流分析）。

物联网给分析带来的另一个挑战是在网络数据领域，即网络分析。由于物联网网络中有大量的智能对象正在通信和传输数据流，确保这些数据流得到有效的管理、监控和安全是一项挑战。诸如Flexible NetFlow和IPFIX等网络分析工具提供了检测网络中物联网数据流中的不规则模式或其他问题的能力。网络分析（包括Flexible NetFlow和IPFIX）将在本章后面详细讨论。

7.2 机器学习

物联网的核心主题之一是如何理解生成的数据。由于肉眼无法看出这些数据中的规律，因此需要使用专门的工具和算法来找到数据关系，从而获得新的商业洞察力。这就引出了机器学习（ML）这个主题。

机器学习、深度学习、神经网络和卷积网络都是我们听说过的与大数据和物联网相关的词汇。ML确实是物联网的核心。智能对象收集的数据需要进行分析，并在此分析基础上执行智能操作。手工执行这种操作几乎是不可能的（或者说非常缓慢和低效）。机器需要快速处理信息，并在达到阈值时立即做出反应。例如，每当在无人驾驶汽车、人群中的异常模式识别或任何其他自动化智能机器辅助决策系统领域取得新进展时，ML就是使该进展成为可能的工具。但ML并不是新鲜事物，它是在20世纪中叶发明的，实际上在20世纪80年代就过时了。那么，发生了什么使ML成为物联网和数据分析的新工具呢？

7.2.1 机器学习的概述

事实上，机器学习是一系列技术的一部分，这些技术通常被归为人工智能（AI）。这个词曾经让科幻小说爱好者梦想到两足机器人和有意识的机器，或者梦想到一个机器奴役人类的矩阵世界。事实上，人工智能包括允许计算系统使用任何技术来模拟人类智能的所有技术，从非常先进的技术逻辑到基本的if-then-else决策循环。任何使

用规则进行决策的计算机都属于这个领域。一个简单的示例是可以帮助我们找到停车位置的应用程序。每隔一段时间对司机位置的GPS读数会计算出司机开车的速度。由一个基本的阈值系统来确定司机是在开车（例如，“如果速度大于20英里/小时或30公里/小时，则开始计算速度”）。当司机停车并断开与汽车蓝牙系统的连接时，应用程序只会记录下断开连接时的位置。这是车停放的位置。除人工智能（电脑知道司机把车停在哪里）外，规则集非常简单。

在更复杂的情况下，静态规则不能简单地插入到程序中，因为它们需要可以更改或不完全理解的参数。一个典型的例子是在计算机上运行的听写程序。该程序被配置为识别字典中每个单词的音频模式，但它不理解语音的特定内容——重音、音调、速度等。我们需要录制一组确定的句子，以帮助该工具将已知单词与读单词时发出的声音匹配起来。这个过程叫作机器学习。ML关心的是计算机需要接收一组处理后的数据以帮助更高效地执行任务的任何过程。ML是一个广阔的领域，但可以简单地分为两大类：监督学习和无监督学习。

1. 监督学习

在监督学习中，用已知正确答案的输入训练机器。例如，假设我们正在训练一个系统来识别矿井隧道中何时有人。配备有基本摄像头的传感器可以捕捉形状，并将其返回给一个计算系统，该系统负责确定形状是人还是其他物体（比如一辆汽车、一堆矿石、一块石头、一块木头等）。使用监督学习技术，成百上千的图像被输入到机器中，每个图像都进行了标记（在本例中为人类或非人类）。这就是所谓的训练集。算法用于确定图像之间的公共参数和共同点差异。比较通常在整个图像的尺度上进行，或者逐像素进行。图像被调整为具有相同的特征（分辨率、颜色深度、中心图形的位置等），并对每个点进行分析。人类图像在特定位置具有特定类型的形状和像素（对应于脸、腿、嘴等的位置）。将每幅新图像与一组已知的“良好图像”进行比较，并计算一个偏差，以确定新图像与一般人类图像的差异，从而确定显示的是一个人类图形的概率。这个过程叫作分类。

经过训练，机器应该能够识别人类的形状。在实际进行现场部署之前，通常使用未标记的图片对机器进行测试（根据使用的ML系统，这称为验证或测试集），以验证识别级别是否处于可接受的阈值。如果机器没有达到预期的成功水平，就需要更多的训练。

在其他情况下，学习过程并不是将其划分为两个或多个类别，而是寻找一个正确的值。例如，管道中石油的流速是由管道的大小、石油的黏度、压力等几个因素决定的。当使用测量值来训练机器时，机器可以预测出新的、未测量的黏度的流速。这个过程叫作回归；回归预测数值，而分类预测类别。

2. 无监督学习

在某些情况下，监督学习并不是机器帮助人类做出决策的最佳方法。假设我们正在处理来自小型发动机制造工厂的物联网数据。生产的发动机中平均约有0.1%需要进行调整，以防止以后出现缺陷，我们的任务是在它们安装到机器并从工厂发货之前识别它们。由于有数百个部件，因此可能很难检测出潜在的缺陷，而且几乎不可能训练机器来识别可能不可见的问题。但是，我们可以测试每个发动机并记录多个参数，如声音、压力、关键部件的温度等。一旦数据被记录下来，我们就可以用图像表示这些元素之间的关系（例如，温度是压力、声音与转速随时间变化的函数）。然后，我们可以将这些数据输入计算机，并使用数学函数来查找组。例如，我们可以决定根据发动机在给定温度下发出的声音对其进行分组。操作这种分组的标准函数K-means集群可以找到一组发动机的平均值（例如，温度的平均值、声音的平均值）。使用这种方法对发动机进行分组，可以快速发现属于同一类别的几种发动机（如链锯式小型发动机、割草机式中型发动机）。所有相同类型的发动机产生的声音和温度与同一组的其他成员相同。

在发动机分组中偶尔会有一台发动机显示出异常的特性（略微超出预期的温度或声音范围）。这是我们用于手动评估的发动机。与这一确定过程相关的计算过程称为无监督学习。这种类型的学习是无监督的，因为事先没有“好”或“坏”的答案。这是一个群体行为的变

化，计算机可以学习到一些不同的东西。当然，发动机的这个例子非常简单。在大多数情况下，参数是多维的。换句话说，要计算成百上千个参数，并在多个参数中累积较小的偏差用于识别异常。图7-5显示了这种分组和偏差识别逻辑的一个示例，绘制了3个参数（组件1、组件2和组件3），并发现了4个不同的组（集群）。我们可以看到一些点远离各自的组。我们应该对显示这种“集群外”特性的单个设备单独进行更仔细的检查。

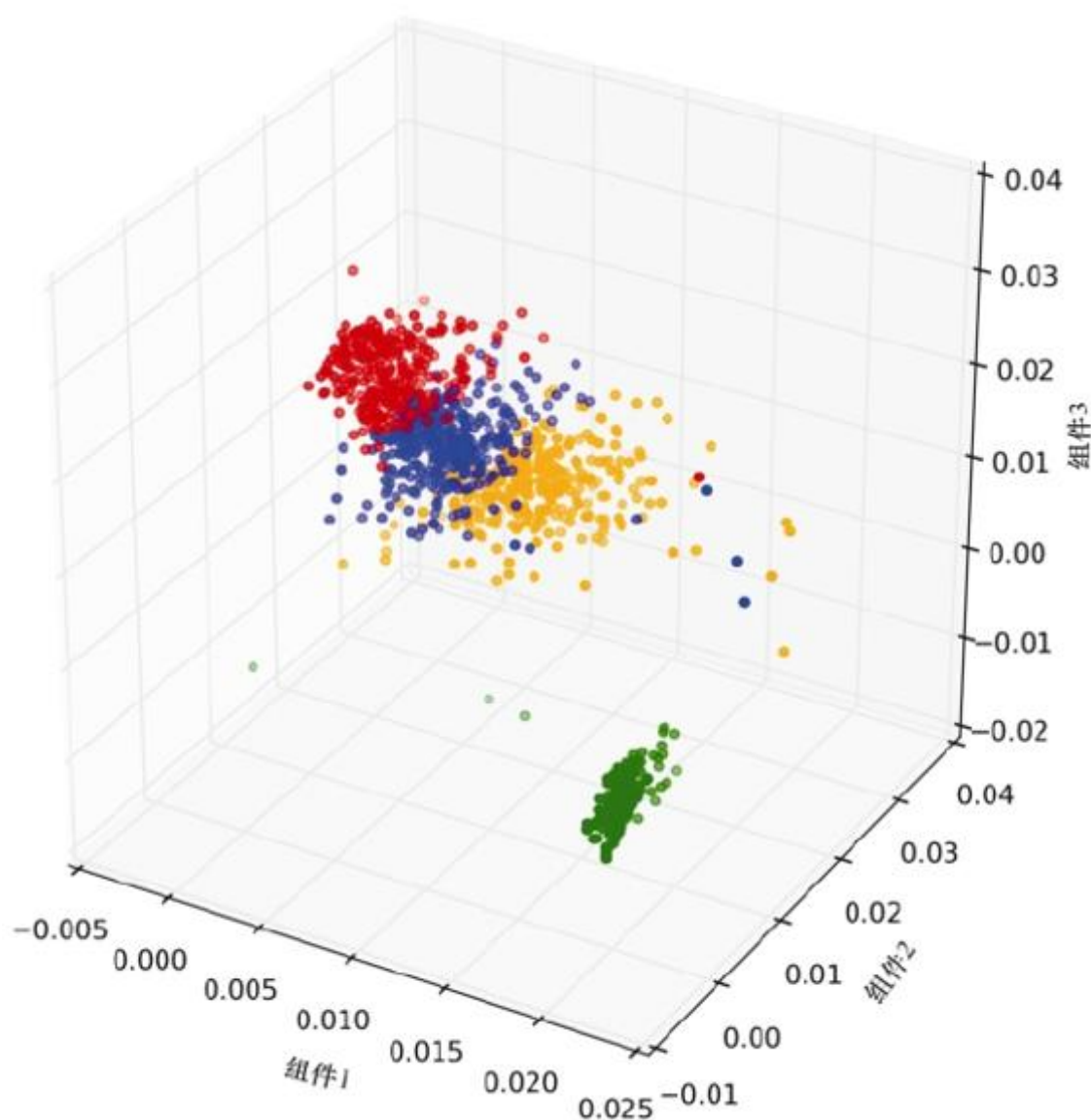


图7-5 聚类 and 偏差检测实例

3. 神经网络

处理多个维度需要大量的计算能力。也很难确定要输入哪些参数，以及哪些组合变量会引发警告。同样，监督学习只有在训练集很大的情况下才有效；训练集越大，预测的准确性越高。这一要求在一定程度上使ML在20世纪80年代和90年代逐渐消失。训练机器的过程通常被认为过于昂贵和复杂。

自21世纪初以来，廉价的计算能力以及对超大数据集的访问（通过互联网共享）使ML重新焕发了活力。与此同时，所使用的算法的效率也取得了巨大进步。以采矿作业中的人体形状识别为例。区分人与车很容易。计算机可以识别出人类有不同的形状（如腿或手臂），而车辆没有。区分人类和其他哺乳动物要困难得多（尽管非人类的哺乳动物在矿井中并不常见）。同样的道理也适用于区分小货车和货车。当我们看到它们时可以轻松分辨出来，但是训练一台机器来区分它们需要的不仅仅是基本的形状识别。

这就是神经网络发挥作用的地方。神经网络是模拟人类大脑工作方式的ML方法。当看到一个人时，大脑的多个区域被激活，用来识别颜色、动作、面部表情等。大脑将这些因素结合起来，得出“看到的形状是人类”的结论。神经网络模仿同样的逻辑。信息经过不同的算法（称为单元）处理，每个算法负责处理信息的一个方面。一个单元计算的结果值可以直接使用，也可以输入到另一个单元进行进一步的处理。在这种情况下，神经网络有几个层次。例如，处理人类图像识别的神经网络可能在第一层有两个单元来确定图像是否有直线和锐角，因为车辆通常有直线和锐角，而人体没有。如果图像成功通过第一层（因为没有或只有一小部分的锐角和直线），第二层可能会寻找不同的特征（是否存在面孔、手臂等），然后第三层可能会将图像与各种动物的图像进行比较，并得出结论“该形状是人（或不是人）”。神经网络之所以效率最高，是因为每个单元处理一个简单的测试，计算速度相当快。该模型如图7-6所示。

神经网络如何识别照片中的狗

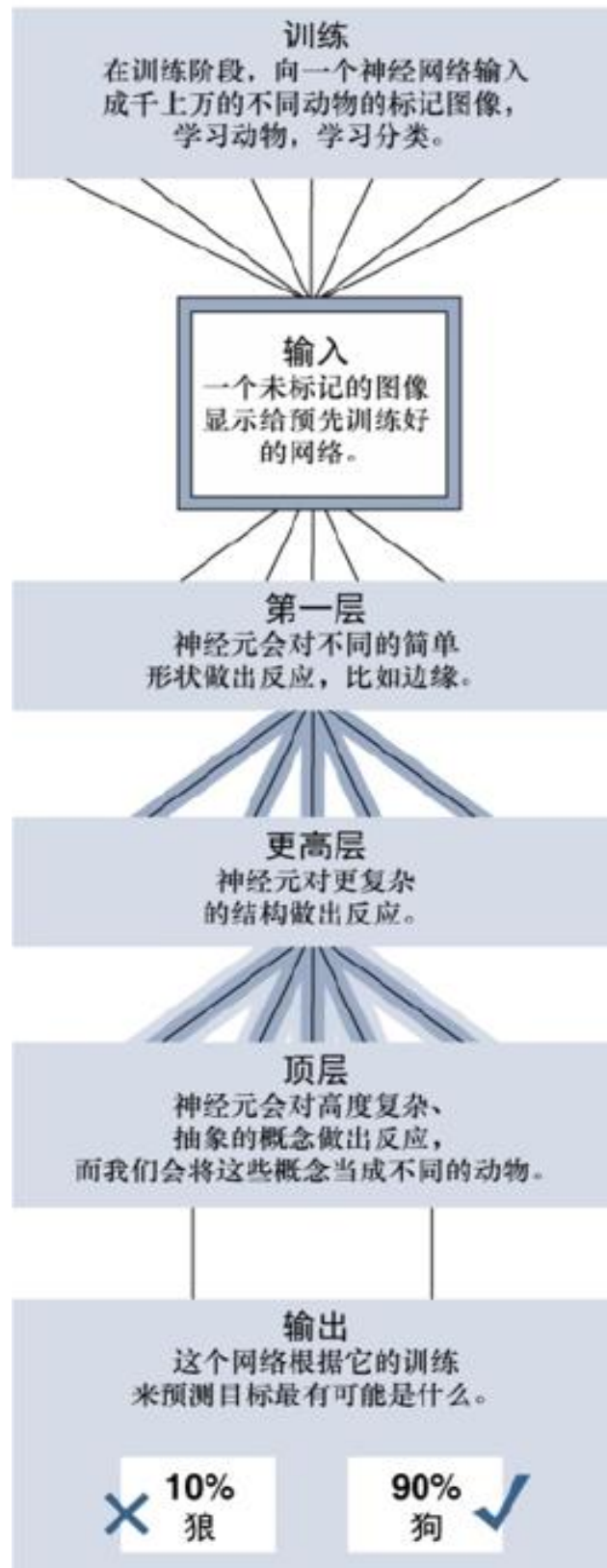


图7-6 神经网络的例子

相比之下，旧的监督ML技术会在训练阶段将人体图像与潜在的数十万幅图像进行逐像素比较，实现困难且成本较高（需要大量训练），操作起来也比较慢。神经网络一直是许多研究工作的主题，其中多项研究和优化工作已经检查了单元和层的数量、每层处理的数据类型，以及用于处理数据的算法类型和组合，以使处理特定应用程序的效率更高。图像处理可以通过某些类型的算法进行优化，而这些算法对于人群运动分类可能不是最优的。在这种情况下，可能会发现另一种算法，它将彻底改变这些运动的处理和分析方式。

从某种意义上说，神经网络依赖于这样一种思想，即信息被分成几个关键部分，每个组成部分都被赋予一个权重。权重的比较共同决定了这个信息的分类（没有直线+脸+微笑=人类）。

当一个层的结果被输入另一层时，这个过程被称为深度学习（“深度”是因为学习过程不止有一个层）。深度学习的一个优点是，拥有更多的层可以实现更丰富的中间处理和数据表示。在每一层，数据都可以被格式化，以便下一层更好地利用。这个过程提高了整体结果的效率。

7.2.2 机器学习与从大数据中获取智能

理解机器学习的原理后，它在物联网中的应用就显而易见了。难点在于为每个用例确定正确的算法和正确的学习模型。这种分析超出了本章的范围，但是将ML的操作分成两个大的子组是有用的。

■ **本地学习：**在这个组中，数据在本地收集和处理，要么在传感器本身（边缘节点）中，要么在网关（雾节点）中。

■ **远程学习：**在这个组中，数据被收集并发送到一个中央计算单元（通常位于特定位置或云中的数据中心），在那里进行处理。

注释：与这两个子组相关联的术语是遗传学习。这个术语是指当地单位从其他地方获得的学习成果。例如，一台处理计算机可以从多个传感器和网关收集数据，对这些数据执行ML，并将产生的行为更改请求或结论发送回网关和传感器。这种新获得的知识优化了本地操作，并且是遗传学习（而不是简单的本地学习）。

无论处理数据的位置（以及处理数据的规模）如何，ML在物联网中的常见应用围绕以下4个主要领域展开。

■ **监控：**智能对象监控其运行的环境。处理数据是为了更好地理解运行条件，这些条件可以指外部因素，如空气温度、湿度或矿井中是否存在二氧化碳，也可以指内部操作因素，如泵的压力、管道中石油的粘度等。ML 可以用于监测，以检测早期故障情况（例如，K-means偏差显示超出范围的行为）或更好地评估环境（例如机器人根据识别的形状自动分类材料或在仓库或供应链中挑选货物）。

■ **行为控制：**监控通常与行为控制一起工作。当给定的一组参数达到预先定义的目标阈值（即有监督的）时或通过偏离平均值（即无监督的）动态学习时，监视功能将生成警报。这种警报可以传递给人，但更高效、更先进的系统会触发纠正措施，比如增加矿井隧道中的新鲜空气流量，转动机械臂或降低管道中的油压。

■ **操作优化：**行为控制通常旨在根据阈值采取纠正措施。然而，分析数据时也会导致改进整个过程的变化。例如，智慧城市的水净化厂可以根据使用的化学物质（来自A公司或B公司）、温度，以及与什么搅拌机制（搅拌速度和深度）相关联，实施一个系统来监控净化过程的效率。神经网络可以在一层或多层中将多个这样的单元组合在一起，来估计在目标空气温度下最佳的化学混合物和搅拌混合物。这种智能可以帮助工厂减少化学物质的消耗，同时仍然在相同的净化效率水平上运行。作为学习的结果，行为控制导致了不同的机器动作。我们的目标不仅是对这些行为进行试验，而且是要提高这些行为的效率和效果。

■ **自我修复、自我优化：**深度学习快速发展的一个方面是闭环。基于ML的监视触发了机器行为的变化（变化由人工监视）和操作优

化。反过来，ML引擎可以被编程来动态监视和组合新参数（随机或半随机），并在结果显示可能的增益时自动推断和实现新的优化。系统实现了自学习和自优化。它还可以检测新的K-means偏差，预先检测出新的潜在缺陷，从而使系统能够自我修复。系统的修复需要外部因素（通常是人类操作者）的介入，但诊断是自动化的。在许多情况下，系统还可以自动订购被检测到接近故障的设备，或自动采取纠正措施以避免故障（例如，降低操作速度、修改机器的运动以避免薄弱环节的损坏）。

对于所有这些操作，物联网ML的一个具体方面是规模。安装在街道灯杆上的气象传感器可以提供当地污染程度的信息。在整个城市范围内，当局可以监测移动的污染云，以及雾、湿度、压力和地形对全局和当地的影响。所有这些信息都可以与交通数据相结合，从而在全局范围内规范交通灯模式，减少工业污染源的排放，或者在受影响较大的轴线上增加公共交通工具的密度。同时，在局部，灯杆上的LED可以增加或降低亮度，改变其颜色以适应当地环境。这种变化可以由局部条件处理（局部学习）或遗传学习来驱动。

将特定和专业系统上的雾计算与来自多个来源的数据的云计算相结合，并衍生出全局或本地纠正措施的能力，是ML在物联网领域如此强大的原因。随着开放系统和智能对象的爆炸式增长，关联和交叉优化的应用非常广泛。

7.2.3 预测分析

物联网的机器学习和大数据处理非常好地回答了第1章提出的问题“什么是物联网”，该模型的高级阶段是网络自诊断和自优化。在物联网世界中，这种行为如前所述。当来自多个系统的数据组合在一起并进行分析时，可以对系统的状态进行预测。例如，第13章介绍了安装在机车上的传感器。多个智能物体测量车厢之间的拉力、每个车轮的重量和其他多个参数，为驾驶员提供一种巡航控制优化形式。与此同时，摄像头会观察前方的轨道状态，音频传感器会分析轨道上每个车轮的声音，并对多个发动机参数进行测量和分析。所有这些数据

都可以返回到云中的数据处理中心，该中心可以重新创建每台机车的虚拟副本。对每台机车的状态进行建模以及把这些信息与整个城市、省、州或国家其他相同类型的机车轨道上的预期出行和状态（和被检测到的故障）进行整合，使得分析平台能够对可能影响每列火车和每辆机车的问题做出非常准确的预测。这种预测分析允许预先维护，能够提高操作的安全性和效率。

同样，与大数据相结合的传感器可以预测矿山作业车辆、制造机器或任何可监控系统以及其他类似系统的缺陷或问题。

7.3 大数据分析工具和技术

虽然Hadoop确实是当今许多大数据实现的核心，对于初次接触数据管理的人来说，将大数据和Hadoop互换使用是一个常见的错误。但它并不是唯一的问题。大数据分析可以由许多不同的软件组成，它们一起收集、存储、操作和分析所有不同的数据类型。通过定义大数据的概念有助于更好地理解形势。一般情况下，行业将大数据归类为“三个V”。

■ **Velocity（速度）**：指收集和分析数据的速度。Hadoop分布式文件系统旨在快速地获取和处理数据。智能对象能够以非常快的速度生成机器和传感器数据，并且要求数据库或文件系统具有同样快速的接收功能。

■ **Variety（多样性）**：指不同类型的数据。通常我们会看到数据被归类为结构化、半结构化或非结构化数据。不同的数据库技术可能只能接受其中一种类型。Hadoop能够收集和存储所有这3种类型。当将来自物联网设备的结构化机器数据与来自其他来源（如社交媒体或多媒体）的非结构化的数据相结合时，这可能是有益的。

■ **Volume（容量）**：指数据的规模。通常，数据规模是使用极低的吉字节、拍字节，甚至是另一个极端的艾字节来衡量的。一般而言，大数据实现的规模超出了单个节点上本地连接的存储磁盘的可用

容量。对于一些大型部署，经常可以看到由数十个、数百个甚至数千个节点组成的服务器集群。

大数据的特征可以通过数据的来源和类型来定义。首先是机器数据，由物联网设备生成，通常是非结构化数据。其次是事务性数据，这些数据来自于从这些系统上的事务中产生数据的源，并且具有高容量和结构化的特点。再次是社交数据源，通常是高容量和结构化的。最后是企业数据，即体积较小、结构非常复杂的数据。因此，大数据由所有这些独立来源的数据组成。

在检查数据源时，还需要考虑从每个数据源摄取的数据量，这决定了数据存储层的设计。我们还应该考虑从摄取系统获取数据的机制（即推或拉）。数据源的类型（数据库、文件、Web服务、流）也需要考虑，因为它也决定了数据的结构。

数据摄取层是连接数据源和存储的层。它是对数据进行预处理、验证、提取和临时存储以供进一步处理的层。对于数据摄取，有几种模式需要考虑。首先是多源摄取，它将多个数据源连接到摄取系统。在此模式中，摄取节点接收来自多个源的数据流，并在将数据传递给中间节点和最终存储节点之前进行处理。此模式通常在批处理系统中实现，并且在实时系统中实现（由于数据的可用性存在延迟，因此不太常见）。

在有助于定义物联网的行业中，数据收集和分析并不是新概念。长期以来工业垂直行业一直依赖于从各种过程中获取、收集和记录数据的能力，以记录趋势并跟踪性能和质量。

例如，许多工业自动化和控制系统将数据输入到两种不同的数据库类型：关系数据库和历史数据库。关系数据库，如Oracle和Microsoft SQL，适合于事务或流程数据。它们的优点是能够分析一段时间内到达的数据之间的复杂数据关系。历史数据库对系统和过程中的时间序列数据进行了优化。它们的核心是数据的存储和检索速度，将每个数据点记录在一个序列中，并记录与记录系统相关的信息。这些数据可能包括传感器读数、材料数量、温度读数或流量数据。

关系数据库和历史数据是成熟的技术，已经伴随我们多年，但是数据管理市场中的新技术为传感器和机器数据开辟了新的可能性。这些数据库技术大致可以分为几个类别，在物联网环境中使用时，每种技术都有各自的优势和潜在的缺陷。其中3个最流行的类别是大规模并行处理系统、NoSQL和Hadoop。

7.3.1 大规模并行处理数据库

几十年来，企业一直使用关系数据库来存储结构化、行和列风格的数据类型。关系数据库通常被分为一个大的数据存储类别，称为数据仓库。尽管它们是大多数数据架构的核心，但它们通常用于长期归档和数据查询（这通常需要几分钟或几小时）。这方面的一个示例是查询过去一年生产的所有具有特定规格的产品。根据数据库中的项数和问题的复杂性，响应可能会很慢。

大规模并行处理（MPP）数据库建立在关系数据仓库概念的基础上，但其设计目的是处理速度更快、更高效，并支持更少的查询时间。为了实现这一点，MPP数据库利用了扩展架构中设计的多个节点（计算机），这样数据和处理都分布在多个系统中。

MPP有时被称为分析数据库，因为它们被设计为允许快速查询处理，并且通常具有内置的分析功能。顾名思义，这些数据库类型跨多个处理器和节点并行处理大量数据集。MPP体系结构（见图 7-7）通常包含一个主节点，负责协调集群中的所有数据存储和处理。它以“无共享”的方式运行，每个节点都包含本地处理、内存和存储，并独立运行。数据存储和节点之间以结构化的类似于SQL的格式进行优化，允许数据分析师使用常见的SQL工具和应用程序处理数据，对复杂SQL查询进行分布和优化，从而显著提高响应速度。由于存储在MPP上的数据必须仍然符合这种关系结构，因此它可能不是物联网实现中使用的唯一数据库类型。由于数据的来源和类型可能有所不同，因此需要比关系数据库更灵活的数据库。

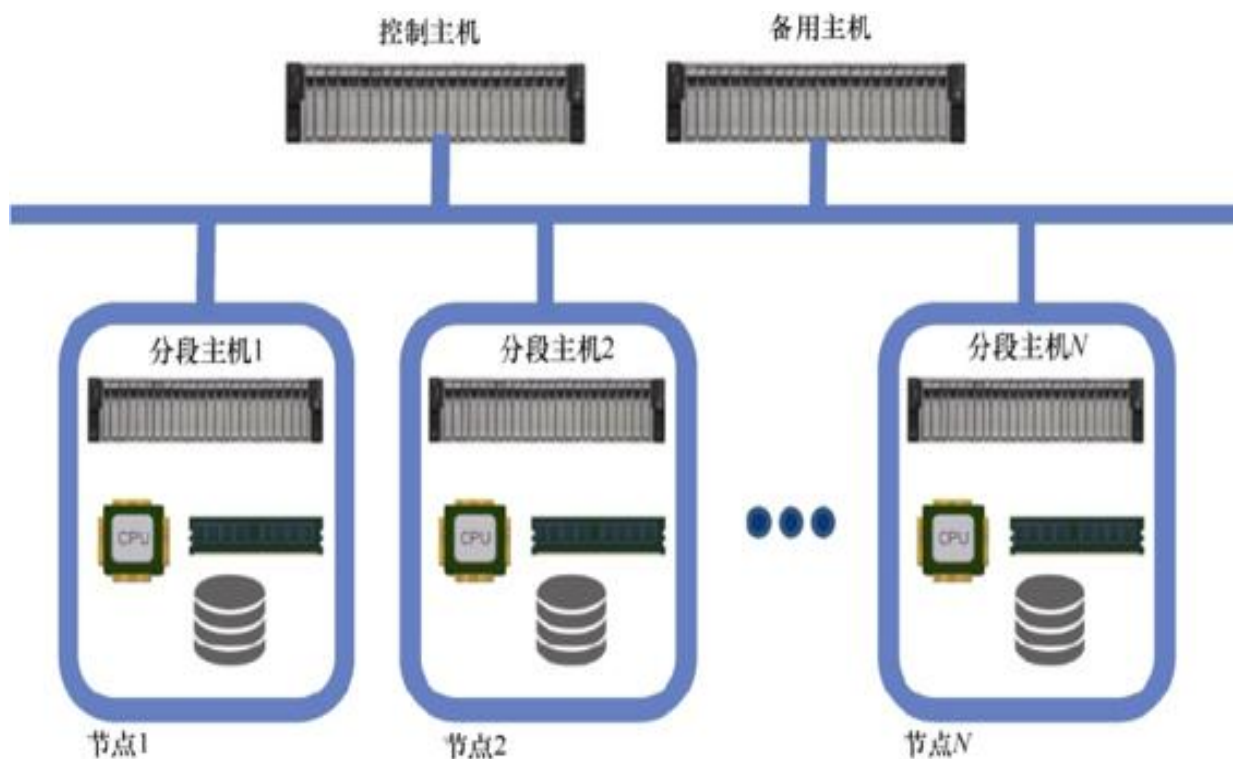


图7-7 MPP无共享架构

7.3.2 NoSQL数据库

除了支持由数据仓库和MPP处理的结构化数据外，NoSQL（“不仅是SQL”）是一类支持半结构化和非结构化数据的数据库。NoSQL不是一种特定的数据库技术；相反，它是一个涵盖了以下几种不同类型数据库的术语。

- **文档存储：**这种类型的数据库存储半结构化数据，如XML或JSON。文档存储通常具有查询引擎和索引功能，允许进行许多优化查询。

- **键值存储：**这种类型的数据库存储关联数组，其中一个键与一个关联值配对。这些数据库易于构建和扩展。

- **宽列存储：**这种类型的数据库存储类似于键值存储，但是值的格式可能因行而异，即使在同一个表中也是如此。

■ 图形存储：这种类型的数据库是根据元素之间的关系组织的。图形存储通常用于社交媒体或自然语言处理，其中数据之间存在非常大的联系。

NoSQL是为了支持现代Web应用程序的高速、紧急的数据需求而开发的，通常不需要多次重复使用。最初的目的是快速获取网络级应用程序生成的快速变化的服务器日志和点击流数据，这些数据不能整齐地放入关系数据库所需的行和列。与其他数据存储类似，如MPP和Hadoop（稍后讨论），NoSQL是横向扩展的，允许数据库跨越多个主机，甚至可以在地理上进行分布。

将NoSQL数据库扩展到其他节点类似于在其他分布式数据系统中进行扩展，其中附加的主机由主节点或进程管理。这个扩展可以由一些NoSQL实现自动执行，也可以手动配置。这种灵活性使NoSQL成为保存与智能对象相关的机器和传感器数据的良好选择。

在符合NoSQL类别的数据库类型中，键值存储和文档存储往往最适合所谓的“物联网数据”。键值存储是当今许多RDBMS（如MS SQL、Oracle和DB2）的基础技术。然而，与传统的RDBMS不同，NoSQL上的键值存储不限于单片机系统。NoSQL键值存储能够以较高的速率同时处理索引和持续性。这使得它成为时间序列数据集的良好选择，这些数据集在给定的时间间隔内记录一个值，例如传感器的温度或压力读数。

通过允许快速更改数据库模式，NoSQL文档数据库比键值存储数据库更灵活。不完全适合行和列的半结构化或非结构化数据可以与有组织的时间序列数据共享同一数据库。非结构化数据可以有多种形式；两个例子是用于QA的生产线上的成品照片和设备的维护报告。

许多NoSQL数据库提供了额外的功能，比如能够在数据库本身中查询和分析数据，从而避免了将数据转移到其他地方处理。它们还提供了通过API查询数据库的各种方法，因此很容易与其他数据管理应用程序集成。

7.3.3 Hadoop

Hadoop作为数据存储库和处理引擎，它可能是最受欢迎的选择。Hadoop最初是谷歌和Yahoo!的项目成果，其最初的目的是为数百万个网站建立索引，并为开源搜索引擎快速返回搜索结果。最初，该项目有两个关键要素。

■ Hadoop分布式文件系统（HDFS）：跨多个节点存储数据的系统。

■ 分布式计算系统：一个分布式处理引擎将一个大的任务分解成可以并行运行的小任务。这两个元素在当前的Hadoop发行版中仍然存在，并为本章后面讨论的其他项目提供了基础。

与前面讨论的MPP和NoSQL系统非常相似，Hadoop依赖于一个扩展架构，该架构利用本地处理、内存和存储来分发任务，并为数据提供一个可扩展的存储系统。MapReduce和HDFS都利用这种分布式架构来存储和处理大量数据，因此能够利用集群中所有节点的资源。对于HDFS，此功能由集群中的专用节点处理，包括NameNodes和DataNodes（见图7-8）。

■ NameNode：这是在HDFS上添加、移动、删除和读取数据的关键部分。它们协调数据的存储位置，并维护每个数据块的存储位置和复制位置的映射。与HDFS的所有交互都通过主（活动的）NameNode进行协调，如果主NameNode发生故障，一个备用NameNode将通知这一变更。NameNode从客户端获取写请求，并以可配置的块大小在可用节点上分发这些文件，通常为64 MB或128 MB的块。NameNode还负责指示数据节点应该在哪里进行复制。

■ DataNode：DataNode是按NameNode的方向存储数据的服务器。通常在Hadoop集群中有许多数据节点来存储数据。数据块分布在多个节点上，为了实现冗余，通常需要在节点之间复制三次、四次或更多次。将数据写入其中一个数据节点之后，DataNode根据复制策略选择两个（或更多）附加节点，以确保整个集群中的数据冗余。磁盘冗余技术，如独立磁盘冗余阵列（RAID），通常不用于HDFS，因为NameNode和DataNode与这种复制技术协调块级别的冗余。

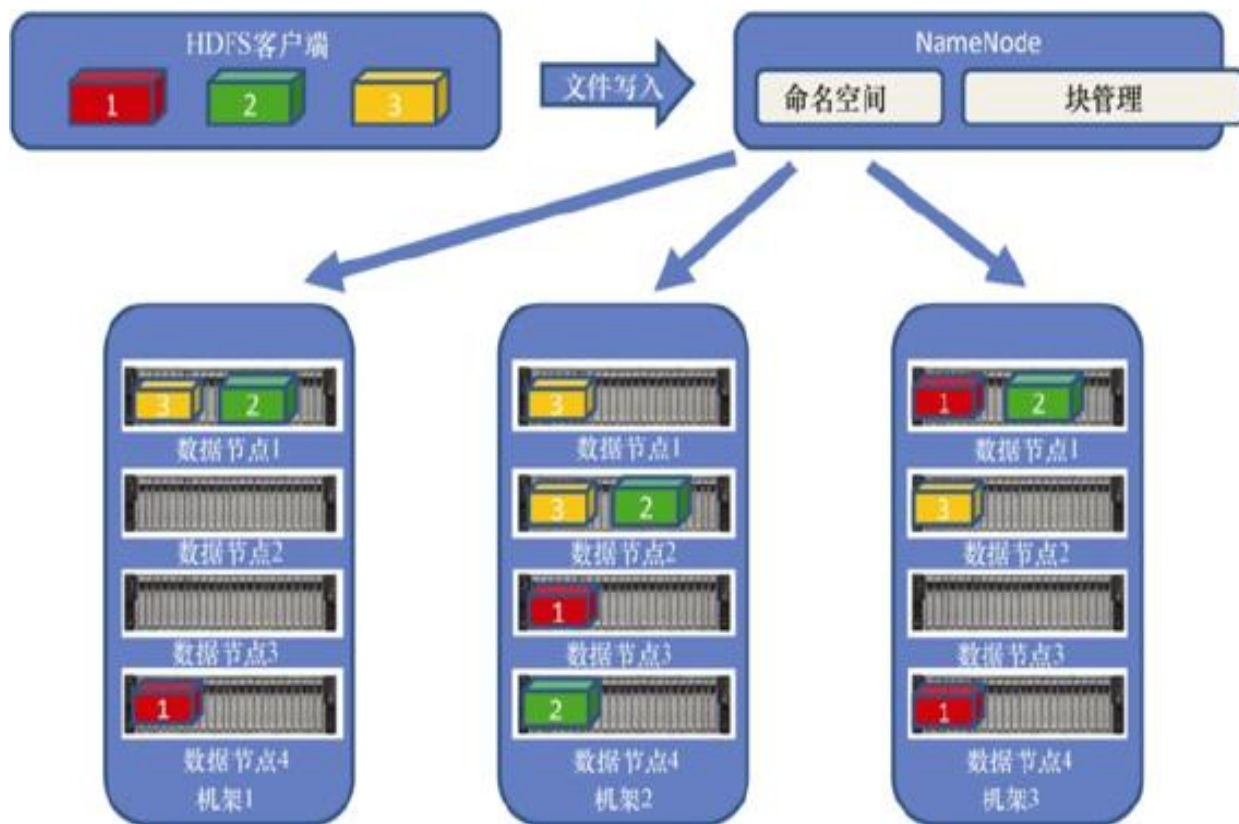


图7-9 将文件写入HDFS的流程

YARN

Hadoop 2.0 版本引入了 YARN（Yet Another Resource Negotiator，另一个资源协商器）来增强MapReduce的功能。在最初的版本中，MapReduce负责整个集群的批数据处理、作业跟踪和资源管理。YARN用于接管资源协商和作业/任务跟踪，允许MapReduce只负责数据处理。

通过开发专用的集群资源调度器，Hadoop除了使用MapReduce进行批处理外，还能够向其核心功能集中添加额外的数据处理模块，包括交互式SQL和实时处理。

7.3.4 Hadoop生态系统

如前所述，Hadoop在物联网数据的收集、存储和处理方面扮演着越来越重要的角色，因为它具有高度可扩展性，并且能够处理大量数据。许多组织已经采用Hadoop集群来存储和处理数据，并寻找免费的软件包来为其分布式Hadoop集群添加额外的功能。自从2011年Hadoop首次发布以来，已经开发了许多项目来增加Hadoop的功能，这些项目统称为Hadoop生态系统。

Hadoop最初作为一个分布式存储和处理系统时可能很薄弱，但后来发展成为一个健壮的项目集合。这些项目组合在一起，创建了一个非常完整的数据管理和分析框架。Hadoop现在由100多个软件项目组成，能够支持数据生命周期中的几乎所有过程，包括收集、存储、处理、分析和可视化。每个单独的项目都是整个数据管理解决方案的独特部分。下面几节将介绍其中的几个包，并讨论如何使用它们来收集或处理数据。

1. Apache Kafka

处理实时事件（如通常由智能对象生成的事件）的一部分是将它们放入处理引擎中。从传感器或日志文件收集数据并准备对其进行处理和分析的过程通常由消息传递系统完成。消息传递系统的设计目的是接收数据或消息，从数据生成的地方接收数据并将数据传递到流处理引擎，如Spark Streaming或Storm。Apache Kafka是一个分布式、可扩展且快速的发布-订阅消息传递系统。它由主题或消息代理组成，其中生产者编写数据，消费者从这些主题中读取数据。图7-10显示了来自智能对象（生产者）的数据流通过Kafka中的主题去往实时处理引擎。由于Kafka的分布式特性，它可以在集群配置中运行，可以同时处理许多生产者和消费者，并在节点之间交换信息，允许主题分布在多个节点上。Kafka的目标是提供一种连接数据源的简单方法，并允许用户以他们喜欢的方式连接到数据源。后文描述了其中的几个包，并讨论了如何使用它们来收集或处理数据。

Apache Spark

Apache Spark是一个内存中的分布式数据分析平台，旨在加速Hadoop生态系统中的进程。Spark的“内存”特性使它能够非常快速地执行作业。在MapReduce操作的每个阶段，数据被读写回磁盘，这意味着通过每次磁盘操作都会引入延迟。但是，使用Spark，这些数据的处理被转移到高速内存中，这显著降低了延迟，加快了批处理作业的速度，并允许近乎实时地处理事件。

实时处理由Apache Spark项目中的一个名为Spark流的组件完成。Spark流是Spark Core的一个扩展，负责从消息传递系统（如Kafka）获取实时流数据，并将其分成更小的微批。这些微批次被称为离散流。Spark处理引擎能够对这些较小的数据块进行操作，从而能够快速了解数据并进行后续操作。由于这种“即时反馈”的功能，Spark正成为许多物联网部署的重要组成部分。控制人员安全的系统、制造业的时间敏感过程和交通管理的基础设施控制都受益于这些实时流媒体功能。

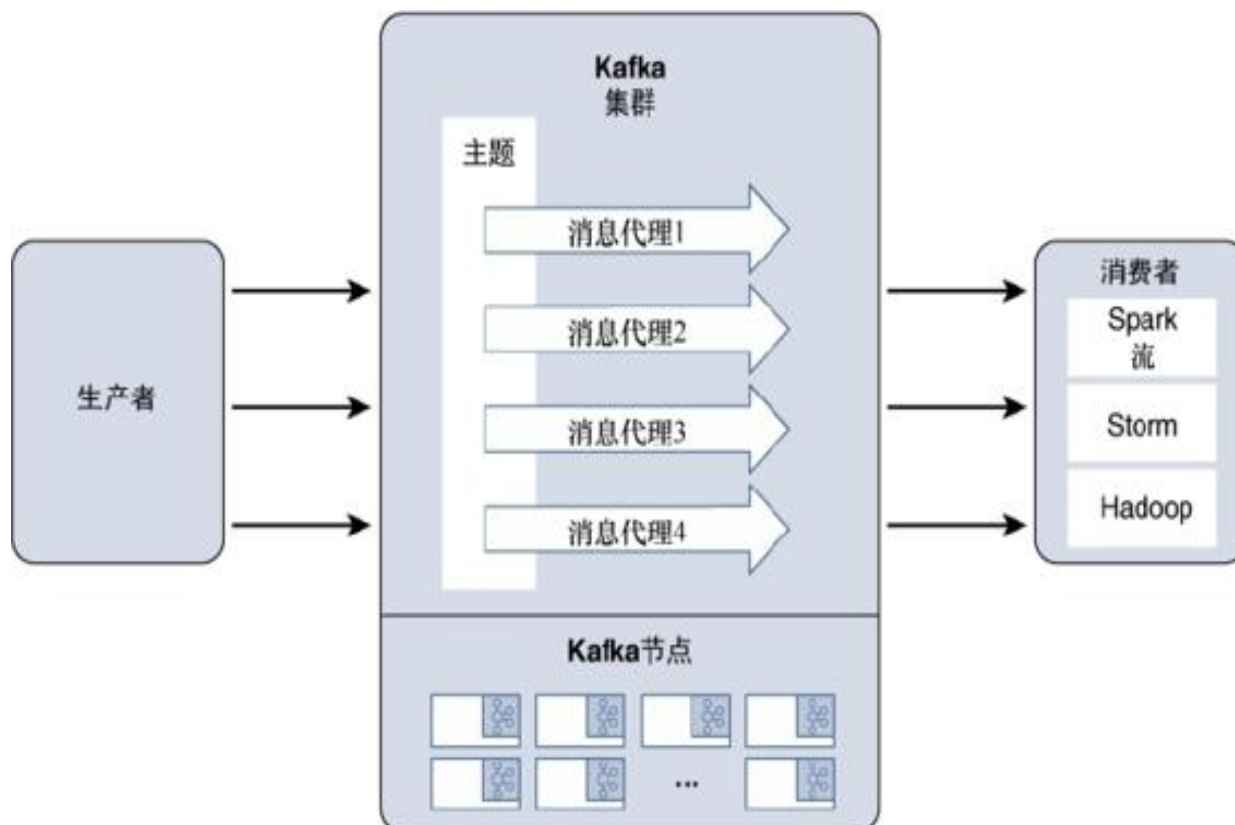


图7-10 Apache Kafka数据流

Apache Storm和Apache Flink

当使用Hadoop生态系统时，用户通常会发现不同的项目非常相似，并且通常与其他项目有很大的重叠。数据流功能就是这样。例如，Apache Spark通常用于分布式流分析和批处理。Apache Storm和Apache Flink是其他为分布式流处理设计的Hadoop生态系统项目，通常用于物联网用例。Storm可以从Kafka中获取数据并以一种近乎实时的方式进行处理，Apache Flink也可以。这个领域正在迅速发展，随着项目的发展，它们的流行程度也在发生变化。

2. Lambda架构

最终，支持许多物联网用例的数据基础设施的关键元素涉及使用多种技术收集、处理和存储数据。同时，在查询动态数据（流）和静态数据（批处理）时需要结合Hadoop生态系统项目。目前正在利用的一个架构就是Lambda架构。Lambda是一个数据管理系统，它由两层组成，一层用于接收数据（批处理和流处理），另一层用于提供组合后的数据（服务）。这些层允许前面讨论的包（如Spark和MapReduce）独立地对数据进行操作，专注于为其设计和优化的关键属性。数据从消息代理（通常是 Kafka）获取，并由每一层并行处理，结果数据被传递到数据存储，在那里可以运行额外的处理或查询。图 7-11 显示了通过Lambda架构的并行数据流。

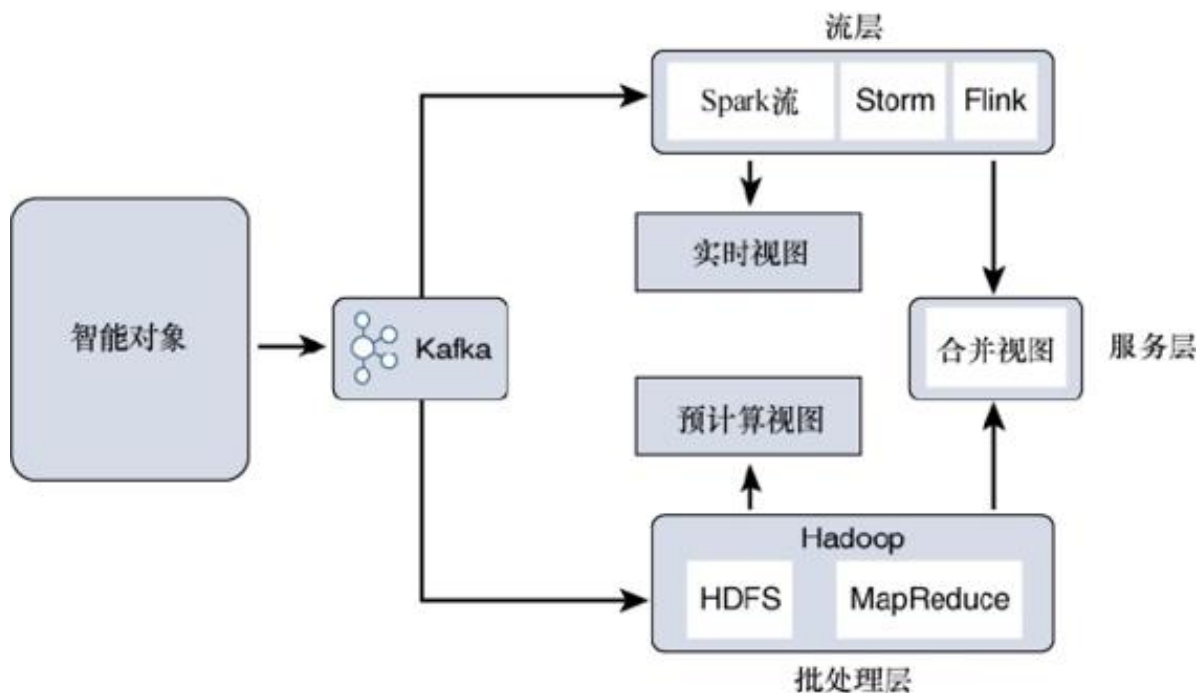


图7-11 Lambda架构

Lambda架构并不局限于Hadoop生态系统中的包，由于其广度和灵活性，生态系统中的许多数据包很好地满足了每一层的需求。

■ **流层：**该层负责事件的近实时处理。Spark流、Storm或Flink等技术被用来快速接收、处理和分析这一层的数据。对于需要快速响应的事件，可以触发警报和自动操作，如果不立即处理，则可能导致灾难性的后果。

■ **批处理层：**批处理层由批处理引擎和数据存储组成。如果将Hadoop生态系统的其他部分用于其他层，则MapReduce和HDFS可以轻松满足需求。其他数据库技术，如MPP、NoSQL或数据仓库，也可以提供该层所需的数据。

■ **服务层：**服务层是一个数据存储和中介，它根据预期的结果或数据视图来决定查询哪个摄取层。如果请求聚合或历史视图，则它可能调用批处理层。如果需要实时分析，它可能会调用流层。服务层通常被数据消费者用来同时访问两个层。

Lambda架构可以提供一個健壯的系統來收集和處理大量的數據，並具有以不同速率分析數據的靈活性。這種架構的一個限制是它在網絡中的位置。由於其中許多組件的處理和存儲需求，這些部署中的絕大多數位於數據中心或雲中。如果處理系統距離生成數據的設備只有幾毫秒或幾秒鐘的時間，這可能會限制分析的效率，從而無法快速響應。在這種情況下，可能需要分布式邊緣處理架構來增強中央數據中心基礎結構。

7.4 邊緣流分析

過去幾年IT發展的一個主要領域是向雲服務進行過渡。幾乎每個大型技術公司現在都在銷售來自雲端的軟件和服務，其中包括數據分析系統，無論它們是作為公共雲運營商提供的服務，還是構建在大型私有數據中心雲中。然而，在一個集中式的雲中分析大量時間敏感的物聯網數據的效果通常並不理想。

在物聯網領域，大量數據是動態生成的，通常需要立即進行分析和響應。在邊緣生成的數據量不僅巨大，這意味著需要對雲或數據中心的帶寬需求進行設計以匹配，而且數據可能對時間非常敏感，需要及時關注，而且不可能等待在雲中進行深入分析。

數據分析被廣泛應用的一個行業是賽車界。例如，在一级方程式賽車比賽中，每輛賽車都有150~200個傳感器，這些傳感器合在一起每秒能產生1000個以上的數據點，每場比賽會產生數百GB的原始數據。傳感器數據從車輛傳輸出來，然後通過軌道側的無線傳感器接收。在比賽中，天氣狀況可能會發生變化，輪胎狀況會發生變化，事故或其他比賽事件使得幾乎總是需要一種適應性強且靈活的比賽策略。隨着比賽的發展，何時進站、使用什麼輪胎、何時通過、何時減速都需要在幾秒鐘內做出決策。研究組發現，通過對行駛數據的分析可以獲得巨大的洞察力，從而獲得更好的比賽結果——這些數據可能來自許多不同的來源，包括賽道傳感器、汽車遙測技術和天氣報告。

大多数车队使用复杂的数据分析系统来调整比赛策略，但在很多情况下，这些设备都位于车队的数据中心，远离赛道。对于一个将分析软件放在英国数据中心的团队来说，澳大利亚（最遥远的比赛场地）的延迟是几百毫秒。在世界上遥远的地方，不仅收集和分析这些数据所需的时间较长，效率低下，而且可能意味着成功的比赛策略（能够适应不断变化的环境）与因缺乏灵活性而无法向车手发送有意义的指令，这两者之间存在巨大差别。简而言之，它可能决定了一场比赛的输赢。

7.4.1 大数据和边缘分析的比较

大数据通常指的是收集并存储在云中的非结构化数据。数据的收集是随着时间的推移进行的，以便可以通过批处理工具（如RDBMS、Hadoop或其他工具）对其进行分析，从而获得业务见解，并从数据中获取价值。Hadoop和MapReduce等工具非常适合处理需要对大量复杂的非结构化数据进行深度分析的问题。然而，由于它们与物联网终端之间的距离较远，以及将所有数据带回云端所需的带宽较大，它们通常不太适合对生成的数据进行实时分析。

在将数据分析应用到前面讨论的赛车示例时，大数据分析基于数据中心或云的性能来分析车队和玩家的所有统计数据。虽然大数据可以实时应用分析（如前所述），但它主要关注的是对大量数据进行批量作业分析。流式分析包括分析正在进行的比赛，并试图根据实时的实际表现来确定谁将赢得比赛，这种分析通常是在尽可能接近边缘的情况下进行的。流式分析允许用户持续实时监控和评估数据，以便随着比赛的进展调整或微调策略。

在物联网中，通过在边缘进行流式分析（在传感器本身或非常接近传感器的位置，例如集成到网关的雾节点），可以实时处理数据，而无须等待云中批处理的结果。这是否意味着流式分析将取代云中的大数据分析？不一定。它们都有各自的作用，都有助于改进业务洞察力和流程。

从某种意义上说，如果原始数据是在数据中心生成的，那么进行本地分析是有意义的。但是，如果大部分数据是由分布在广阔区域内的传感器在偏远地区生成的呢？为了在创建数据时使其真正有效，需要对数据进行分析，并对尽可能接近边缘进行响应。一旦在边缘进行了分析和简化，生成的数据就可以发送到云上，并随着时间的推移获得更深入的分析结果。同样重要的是，边缘不是只在一个地方。边缘是高度分布式的，这意味着边缘的分析需要高度协调和结构化。这也意味着在一个通信系统中，边缘/雾节点能够在必要时相互通信，并向云中的大数据系统报告结果。

从业务的角度来看，流分析涉及在数据仍然有价值时（在它变得陈旧之前）对其进行处理。例如，道路传感器结合GPS定位应用程序可能会告诉司机由于交通原因而避开某条高速公路。这些数据只在一小段时间内有价值。从历史数据看，在某一段高速公路上发生了多少交通事故或交通堵塞，或者根据过去的交通数据预测交通堵塞，可能会很有趣。然而，对于接收该信息的交通司机来说，如果不立即对数据采取行动，这些数据就没有什么价值。

从安全的角度来看，在边缘对分析和预处理的数据进行即时访问，可使得组织意识到网络中的异常，以便在这些异常扩散到网络的其他部分之前能够快速控制它们。

综上所述，边缘流式分析的关键价值包括以下几个方面。

■ 在边缘缩减数据：物联网设备生成的数据总量一般与设备数量成比例。这些设备的规模可能会非常大，它们产生的数据量也会非常大。若将所有这些数据传递到云端，则效率低下，而且在带宽和网络基础设施方面的开销也非常大。

■ 在边缘进行分析和响应：一些数据只在边缘有用（例如工厂控制反馈系统）。在这种情况下，最好对数据进行分析，并根据生成数据的位置采取相应的行动。

■ 时间敏感性：当需要对数据进行及时响应时，将数据传递到云端以供将来处理会导致延迟不可接受。边缘分析允许对不断变化的条件做出即时响应。

7.4.2 边缘分析的核心功能

要在边缘执行分析，需要将数据视为实时流。大数据分析专注于静态的大量数据，而边缘分析则持续处理动态的数据流。边缘的流式分析可以分为3个简单的阶段。

■ 原始的输入数据：这是从传感器进行分析处理单元的原始数据。

■ 分析处理单元（APU）：APU过滤并组合数据流（或根据需要分离数据流），根据时间窗口组织数据流，并执行各种分析功能。此时，APU中运行的微服务可能会对结果产生影响。

■ 输出流：输出的数据被组织成有洞察力的流，用于影响智能对象的行为，并传递到云端进行存储和进一步处理。与云的通信通常通过标准的发布/订阅消息传递协议（如MQTT）进行。

图7-12展示了边缘APU中数据处理的各个阶段。

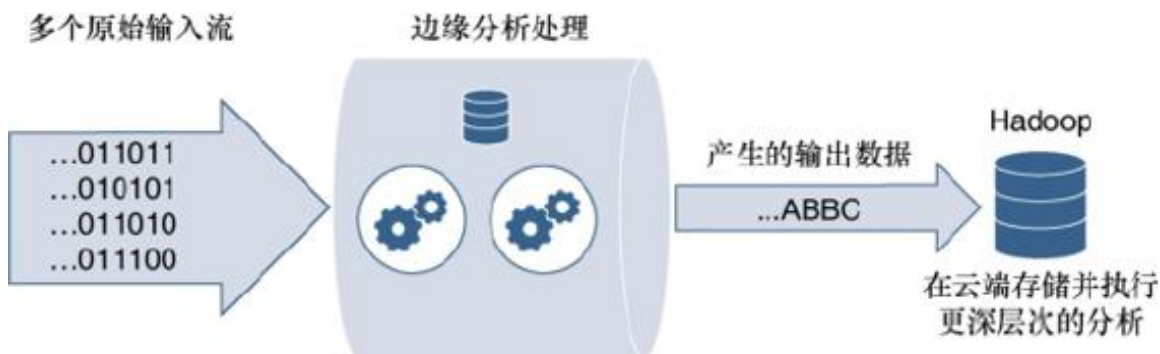


图7-12 边缘分析处理单元

为了进行实时分析，APU需要执行以下功能。

■ 过滤：物联网终端产生的流数据可能非常大，而且大部分都是无关的。例如，传感器可以简单地定期轮询以确认它仍然可以访问。这些信息实际上并不相关，可以忽略不计。过滤功能可以识别重要的信息。

■ 转换：在数据仓库领域，提取、转换和加载（ETL）操作用于将数据结构转换为可用于其他目的的形式。与数据仓库ETL的操作类似，在流式分析中，一旦数据被过滤，就需要对其进行格式化以便处理。

■ 计时：作为实时流数据流，需要建立一个计时环境。这可能与传感器每分钟的平均温度读数相关。例如，图7-13显示了一个APU，它接收来自多个报告温度波动的传感器数据。在这种情况下，APU根据过去两分钟的平均值来报告传感器每分钟的平均温度（例如，在实时监测食品杂货店的食物时，需要监测露天制冷装置的温度波动平均值，以确保食物的安全）。注意，左侧是已清理的流数据。该数据以流的形式呈现给分析引擎（请注意图右下角的排列），该引擎建立时间窗口并计算过去两分钟内的平均温度，每分钟报告一次结果（在图的右侧）。

定义流和窗口

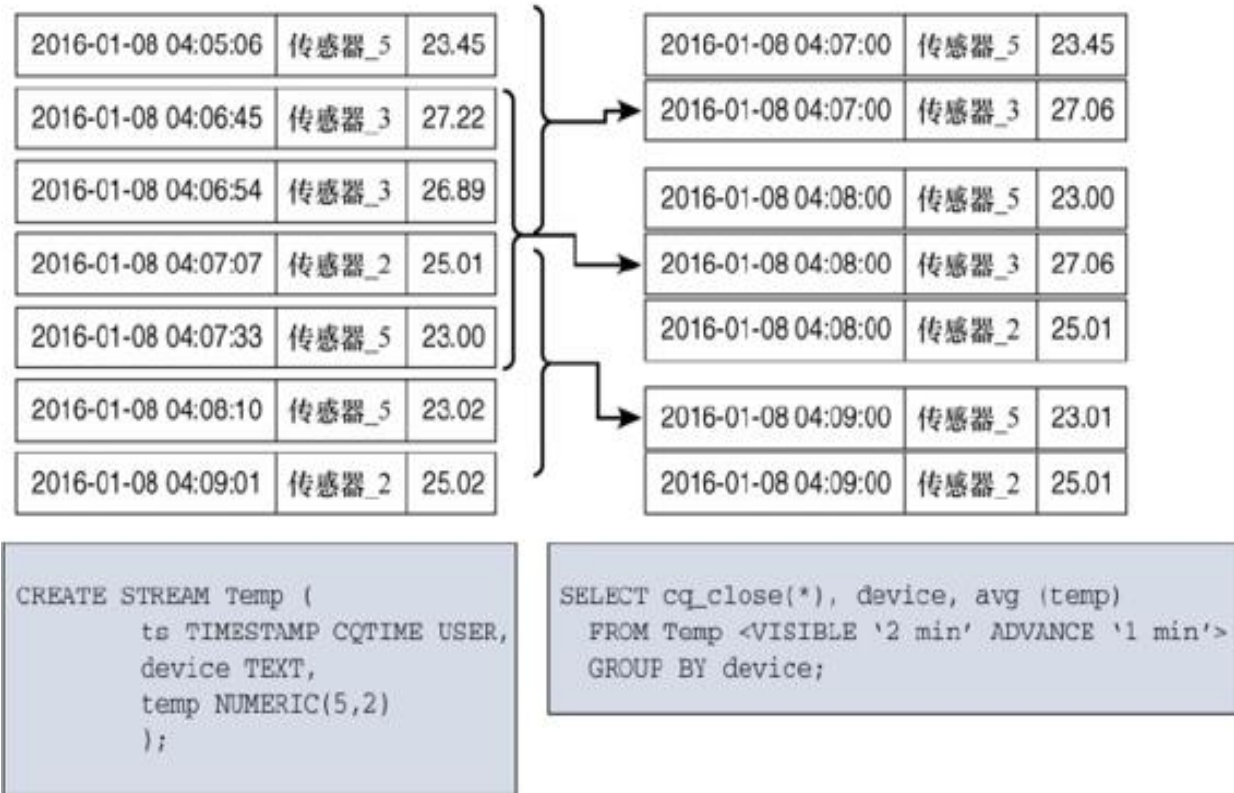


图7-13 示例：建立时间窗口，分析来自传感器的平均温度

■ **关联：**当来自不同类型的传感器的多个数据流组合在一起时，流数据分析变得非常有用。例如，在医院，测量病人的几个生命体征，包括体温、血压、心率和呼吸频率。这些不同类型的数据来自不同的仪器，但当这些数据被组合和分析时，它提供了患者在任何给定时间的健康状况的描述。然而，关联不仅仅是结合实时数据流。另一个关键方面是将实时测量数据与已有的或历史数据相结合和关联。例如，历史数据可能包括患者的以往病史，如血液检测结果。通过结合历史数据，可以为实时流数据提供强大的情景，并对患者的当前状况有更多了解（见图7-14）。

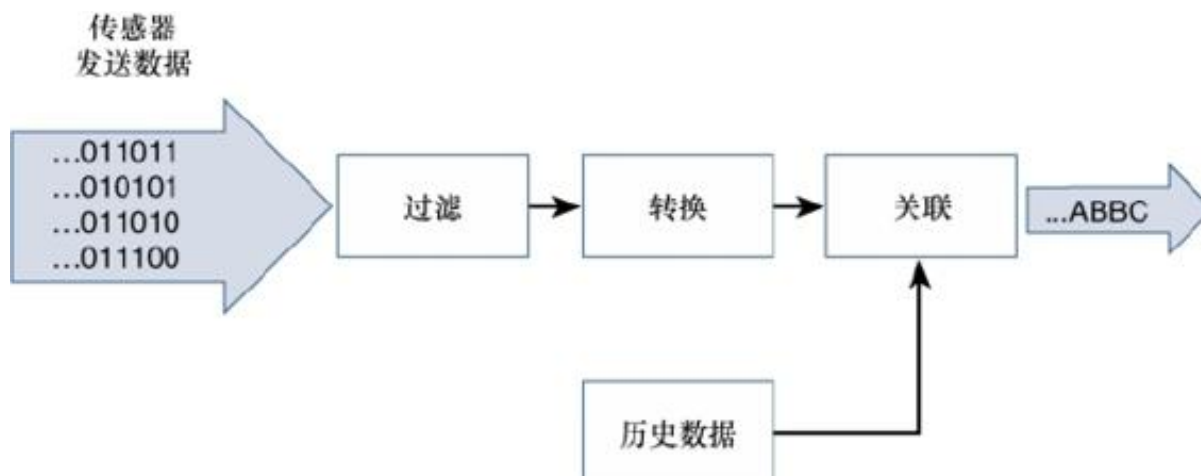


图7-14 将数据流与历史数据关联起来

■ **匹配模式：**一旦数据流被正确地清理、转换，并与其他实时流以及历史数据集关联，即可使用模式匹配操作来对数据进行更深入的了解。例如，假设APU已经收集了患者在一段时间内的生命体征，并且已经了解了所监视的每个变量的预期模式。如果出现意外事件，如心率或呼吸的突然变化，模式匹配算子会认为这是不正常的，并采取某些行动，例如向护理人员发出警报。根据应用程序定义的标准，模式可以是简单的关系，也可以是复杂的关系。机器学习可以用来识别这些模式。

■ **改进商业智能：**归根结底，边缘分析的价值在于改进以前不可用的商业智能。例如，对医院中的患者进行边缘分析，可以使工作人员更快地响应患者不断变化的需求，还可以减少发送到云中的非结构化（而且并不总是有用）的数据量。随着时间的推移，业务逻辑的变化可以改进基本的运营，为医院带来更高的护理水平和更高的效率。

7.4.3 分布式分析系统

根据应用程序和网络架构的不同，分析可以在整个物联网系统的任何位置进行。流分析可以直接在边缘、雾中或云数据中心执行。尽管没有硬性规定应该在哪里进行分析，但是有一些指导原则。我们已经讨论了在边缘处减少数据的价值，以及分析信息以便在信息过时之

前对其进行响应的价值。从边缘后退一步，用更多的数据获得更广阔的视野也是有价值的。当你站在森林中间盯着一棵树看时，你很难看到森林。换句话说，当我们从边缘退一步，观察更广泛的数据集时，有时可以获得更好的见解，并对数据做出更理想的反应。

这就是雾计算的价值所在（雾计算在第2章进行了介绍）。雾分析可以向我们展示一个设备之外的东西，让我们能看到边缘节点的整合，以及从更广的集合内关联数据。图 7-15显示了一家石油钻井公司测量石油钻机上的压力和温度的示例。虽然直接在边缘进行分析可能有一些价值，但是在该例子中，传感器通过MQTT消息代理与雾分析节点通信，从而允许更广泛的数据集（MQTT在第6章中进行了详细讲解）。雾节点位于同一石油钻井平台，从多个边缘设备执行流式分析，通过扩展的数据集，它可以获得更好的洞察力。它可能无法像直接在边缘设备上执行分析那样快速地响应事件，但它仍然接近于在事件发生时进行实时响应。一旦雾节点完成了数据处理，它将结果传递给云（同样通过MQTT的消息代理），以便通过大数据分析工具进行更深入的历史分析。

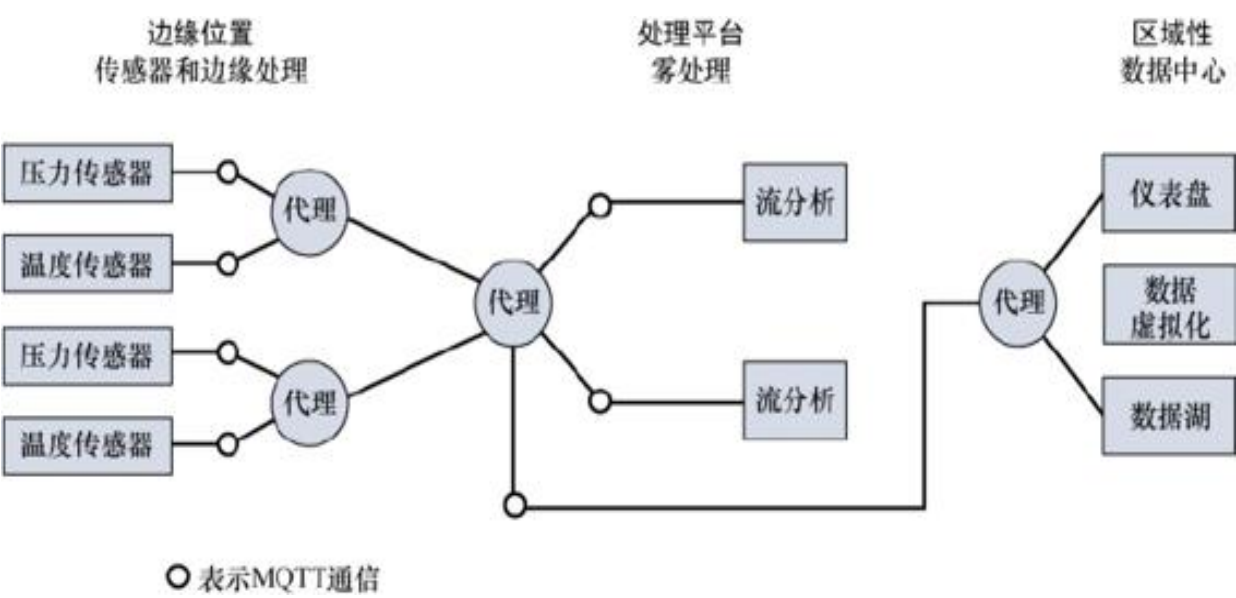


图7-15 物联网系统的分布式分析

7.5 网络分析

另一种在物联网系统管理中极其重要的分析形式是基于网络的分析。与前面讨论的数据分析系统不同，它们关注的是在端点生成的数据中发现模式，而网络分析关注的是从网络流量的角度发现通信流中的模式。网络分析能够分析由协议构成的通信模式的细节，并在整个网络中将其关联起来。我们能够通过该模式了解网络中的正常行为，并快速识别由于次优路径、入侵恶意软件或过度拥塞而导致的网络问题的异常情况。流量模式分析是物联网网络工程师排除故障最强大的工具之一。

如第6章所述，物联网端点与一般的计算平台不同，它被设计为直接与极少数特定的应用服务器通信，如物联网消息或数据代理，或特定的应用服务器和网络管理系统。因此，可以说物联网解决方案和用例紧密结合了设备和应用。图7-16显示了在智能电网的聚合路由器上执行的场域网（FAN）流量分析。

这种行为代表了在执行网络分析时可以利用的一个关键方面，网络分析为可扩展的物联网部署提供了处理容量规划的能力，并提供了安全监控，以检测集中式或分布式架构（如雾计算）的异常流量和模式（如协议的异常流量峰值）。

假设物联网设备将其流量发送到特定的服务器，或者直接发送到应用程序，或者将数据负载封装在给定协议中的物联网代理。这涉及一对源地址和目标地址，以及与应用层相关的TCP或UDP端口号，这些信息可以用于网络分析。

物联网采用IP架构框架的驱动力之一，是利用互联网服务提供商（ISP）以及私营企业网络广泛了解和部署的工具和流程。为了监控网络基础设施，事实上的行业标准和协议允许对IP流量流进行普遍的特征描述，包括识别网络基础设施中的源地址和/或目标地址、定时数据和数据量，以及应用程序类型。可以在网络的不同位置收集流统计信息。例如，可以使用集中式路由器或交换机来聚合子网，也可以使用高度分布式的节点来连接基础设施的“最后一公里”，从而收集流信息。在以已知格式收集数据后，可以将其发送到外部网络分析工具，

该工具向网络管理人员提供独特的服务，如安全性和性能监视以及容量规划。

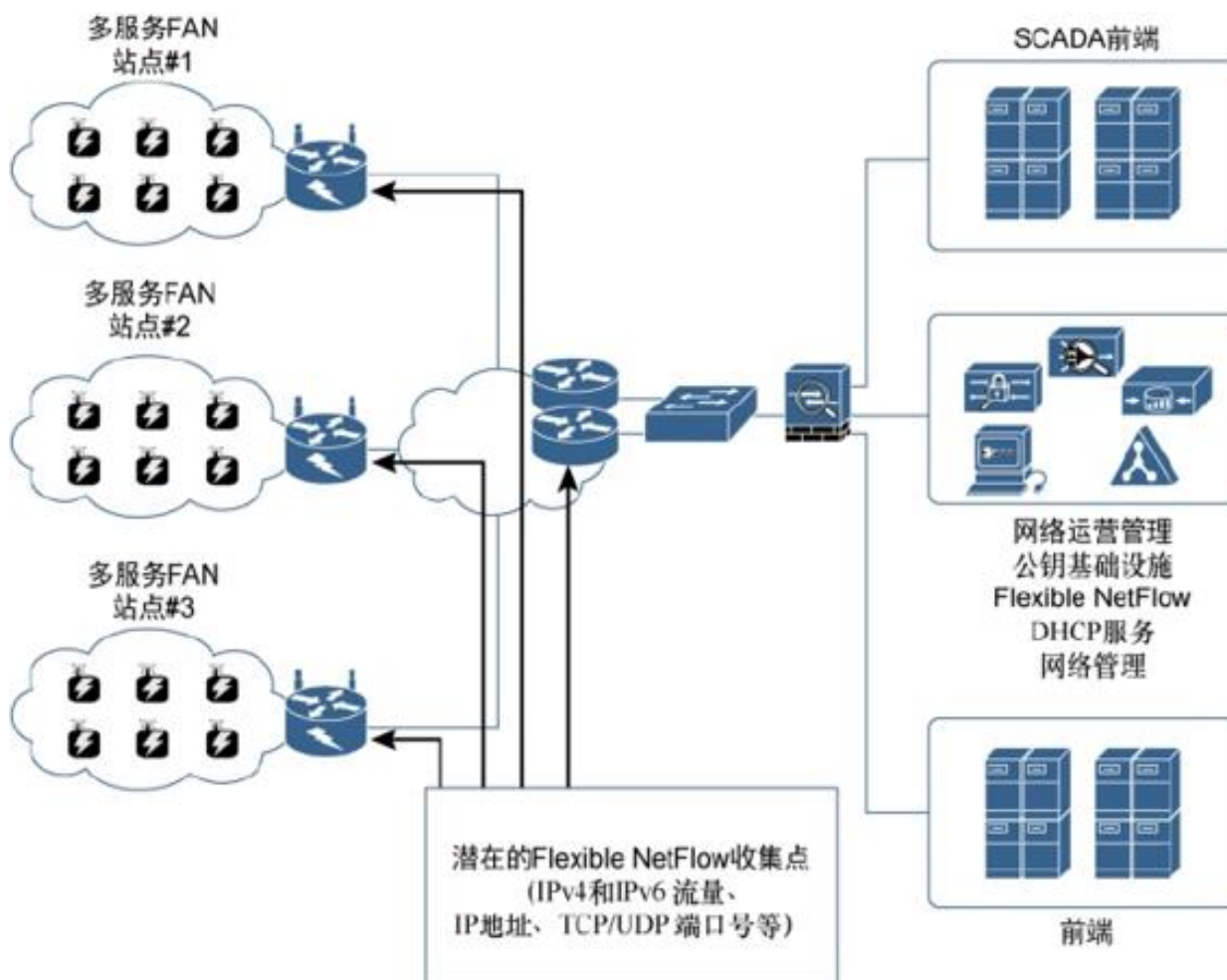


图7-16 智能电网FAN分析与NetFlow实例

在物联网基础设施部署的背景下，对于第4章、第5章和第6章中讨论的技术，流分析的好处如下（其他网络管理服务除外）。

■ 网络流量监测和分析：来自网络层的流量采集提供了全局和分布式的近实时监视功能。IPv4和IPv6网络范围内的流量和模式分析有助于管理员主动检测问题，并在问题发生时快速排除故障和解决问题。

■ 应用流量监测和分析：监测和分析可用于获得物联网接入服务基于时间的详细视图，如应用层协议，包括MQTT、CoAP和DNP3，以及

在网络上使用的相关应用程序。

■ **容量规划：**流量分析可用于跟踪和预测物联网流量增长，并在部署新位置或服务时，通过分析长期捕获的数据，帮助制定升级计划。该分析为跟踪和预测物联网网络的持续增长提供了机会。

■ **安全分析：**由于大多数物联网设备通常产生的流量较小，并且总是将数据发送到同一服务器，因此网络流量行为的任何变化都可能意味着网络安全事件，如拒绝服务（DoS）攻击。通过确保没有任何流量发送到物联网领域之外，可以加强安全性。例如，使用LoRaWAN网关，应该不会看到在LoRaWAN网络服务器和网络管理系统之外发送或接收流量。这样的流量可能预示着某种攻击。

■ **计费：**在场域网中，路由器或网关通常是物理隔离的，需要利用公共蜂窝服务和VPN进行回程。部署中可能有数千个网关通过蜂窝网络连接“最后一公里”的物联网基础设施。因此，流监控可以用于分析和优化计费，与其他专用应用程序（如Cisco Jasper）形成互补，后者的应用范围比监控数据流更广。

■ **数据仓库和数据挖掘：**流数据（或衍生信息）可以存储起来，供日后检索和分析，以支持对多服务物联网基础设施和应用程序的主动分析。

7.5.1 Flexible NetFlow架构

Flexible NetFlow（FNF）和IETF IPFIX（RFC 5101、RFC 5102）是广泛用于网络的协议示例。本节将介绍FNF的基本原理以及如何将其用于物联网部署。

FNF是Cisco系统开发的一种流技术，广泛部署于世界各地。FNF的主要优势如下。

■ 流数据具有灵活性、可扩展性和聚集性。

- 能够监控大范围的数据包信息并产生关于网络行为的新信息。
- 增强的网络异常和安全检测。
- 用户可配置流量信息，用于执行自定义的流量识别，并能够关注和监控特定的网络行为。
- 多种审计技术融合为一种审计机制。

1. FNF组件

FNF的主要组成部分如图7-17所示。

流的第一个数据包将使用关键字段创建流条目，此流的其余数据包将仅更新统计信息（字节、计数器、时间戳）

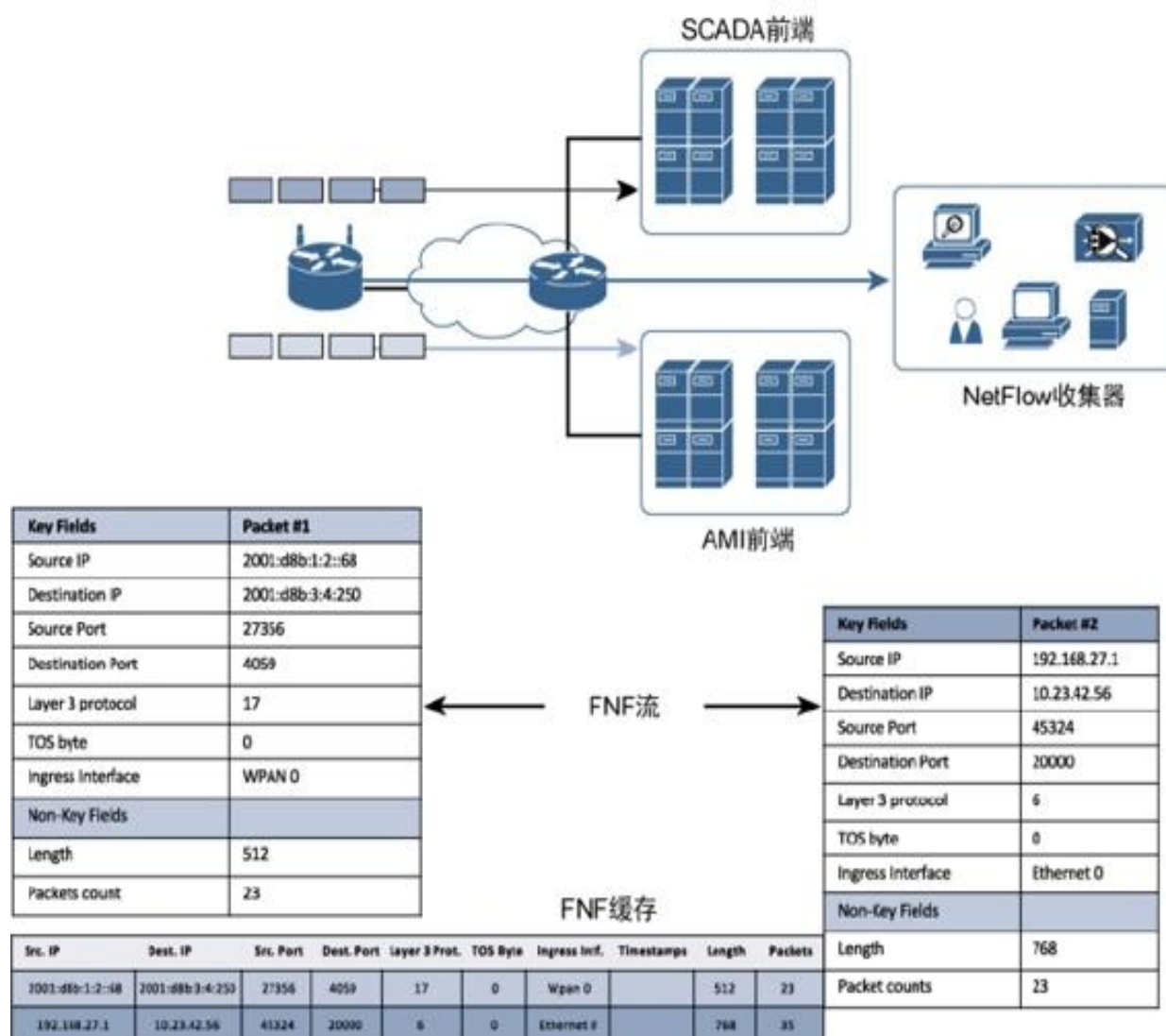


图7-17 Flexible NetFlow概述

■ FNF流监控器（NetFlow缓存）：FNF流监控器描述NetFlow缓存或缓存中存储的信息。流监控器包含缓存中具有关键字段（用于创建流、每个流记录的唯一性的匹配声明）和非关键字段（作为流的属性或特征收集）的流记录定义。另外，流监视器的一部分是流导出器，它包含关于NetFlow信息导出的信息，包括NetFlow收集器的目标地址。流监控器包括各种缓存特性，包括用于导出的计时器、缓存的大小，以及包采样率（如果需要）。

注释：在路由器或交换机中转发的每个数据包，都要对其检查一组IP包属性。这些属性是流的IP包标识或关键字段，并确定包信息是否唯一或与其他包类似。如果包密钥字段是唯一的，则在流记录中创建一个新条目。流的第一个包使用关键字段创建流条目。此流的其余包仅更新统计信息（字节、计数器、时间戳）。流描述的这种方法是可扩展的，因为大量的网络信息被压缩到称为NetFlow缓存的NetFlow信息数据库中。可以将附加信息（非关键字段）添加到流记录并导出。非关键字段不用于创建或描述流，而是被导出并添加到流中。如果一个字段是非关键字段，通常只有流的第一个数据包用于该字段中的值。例如流时间戳、下一跳IP地址、子网掩码和TCP标志。

■ FNF流记录：流记录是一组关键和非关键NetFlow字段值，用于描述NetFlow缓存中的流。为了便于使用，可以预定义流记录，也可以由用户自定义流记录。典型的预定义记录并聚合流数据，并允许用户使用针对NetFlow的常见应用程序。用户定义的记录允许在流记录中选择特定的关键或非关键字段。用户定义字段是Flexible NetFlow的关键，它允许NetFlow描述和导出各种信息。不同的网络管理应用程序将根据它们所监视的内容（例如，安全检测、流量分析、容量规划）支持特定的用户定义和预定义的流记录。

■ FNF导出器：访问NetFlow数据有两种主要方法：在命令行界面（CLI）上使用show命令，以及使用应用程序报告工具。与SNMP查询不同，NetFlow导出器定期将信息推送到NetFlow报告收集器。Flexible NetFlow导出器允许用户定义可以将导出的流发送到何处、导出流的传输类型和导出流的属性。可以为每个流监视器配置多个导出器。

■ 流导出计时器：计时器指示应该将流导出到集合和报告服务器的频率。

■ NetFlow导出格式：仅指示流报告格式的类型。

■ 用于收集和报告的NetFlow服务器：这是流导出的终点。通常通过一个分析工具来完成，该工具用于寻找流量模式中的异常情况。

图7-18展示了来自智能电网FAN的FNF记录的分析报告。在本例中，FNF收集器能够查看各种应用程序的流量模式以及FAN上的管理流

量。

2. 多服务物联网网络中的Flexible NetFlow

在多服务物联网网络环境中，建议在路由器上配置FNF，以聚合来自“最后一公里”的路由器的连接。这提供了在云核心网络和物联网“最后一公里”网络（虽然不是物联网设备之间）之间流动的所有服务的全局视图。FNF还可以在“最后一公里”网关或雾节点上配置，以提供更细粒度的可见性。但是，必须注意通过报告消耗了多少北向数据。

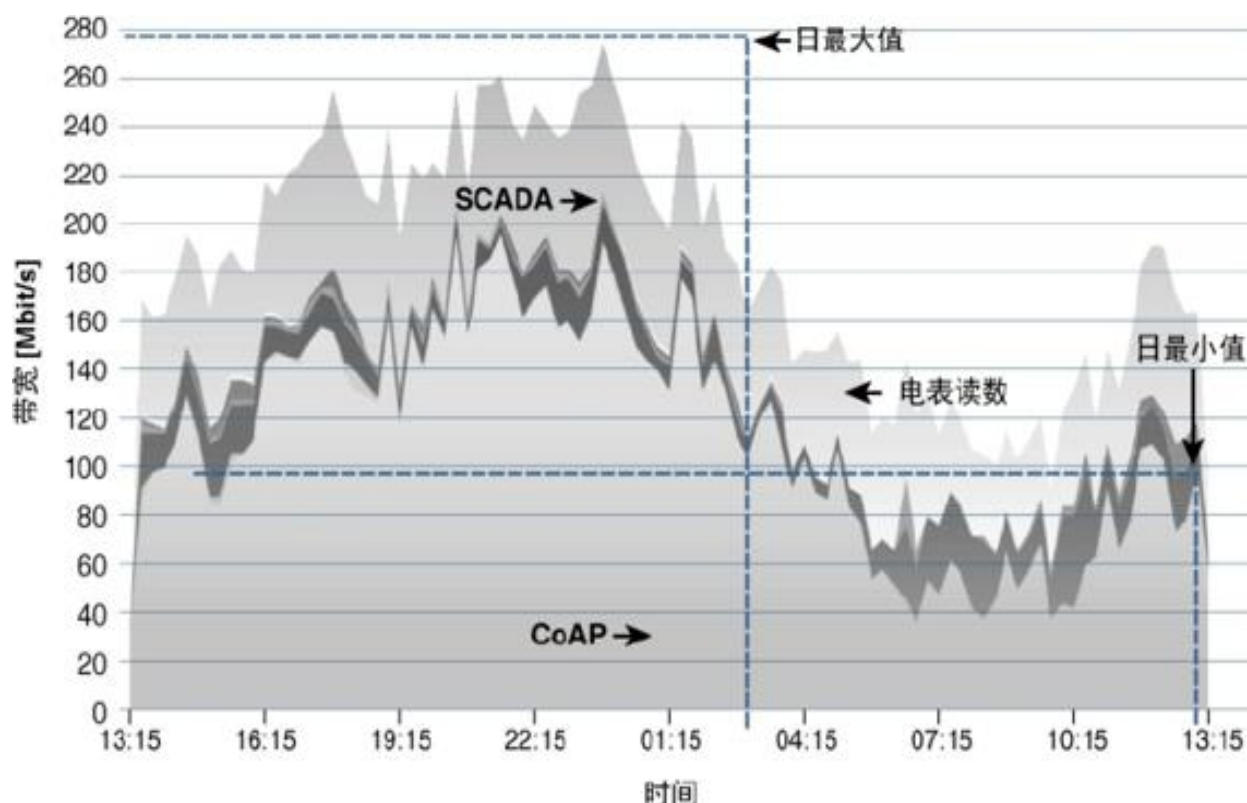


图7-18 智能电网FAN的FNF流量报告

然而，并非所有物联网系统都能够在网关进行流量分析。例如，LoRaWAN网关只是将MAC层的传感器流量转发给集中式的LoRaWAN网络服务器，这意味着目前无法进行流量分析（基于第3层）。在使用通过物

联网代理发送数据的MQTT服务器时，也会遇到类似的问题。在物联网网络中部署流分析工具的其他挑战如下。

- 雾计算和边缘计算的分布式特性可能意味着在可能不支持流分析的地方处理流量，因此损失了可见性。

- IPv4和IPv6的本地接口有时需要检查VPN隧道内部，这可能会影响路由器的性能。

- 额外的网络管理流量由FNF报告设备生成。因此，需要审查增加带宽的额外成本，特别是回程网络使用蜂窝或卫星通信的情况下。

总之，现有的网络分析协议和工具可以为物联网环境提供巨大的价值，帮助实现物联网环境的自动化和安全。

7.6 小结

物联网系统正在产生大量数据，远远超过以往任何时候。这种从各种形式的连接和网络工具中不断生成数据的新范式为获得新的见解和提高效率创造了前所未有的机会。物联网的商业价值不仅在于连接设备的能力，还在于理解这些设备创建的数据。因此出现了一种新的数据管理形式：物联网数据分析。

传统的数据管理是由关系数据库执行的，关系数据库负责处理表中结构良好的数据，这些表和数据结构之间的关系很容易理解，并且可以通过SQL轻松访问。然而，物联网设备生成的大部分数据是非结构化的。随着时间的推移，物联网数据被收集起来，成为大数据，需要特殊处理才能揭示数据湖中的模式。

为了解锁数据的价值，需要执行机器学习的特殊算法来处理数据并找到模式。不同类型的机器学习可以用于特定的目的，包括有监督网络、无监督网络和神经网络。

物联网数据的处理发生在云或数据中心，由NoSQL、Hadoop和MPP等大数据分析系统执行。这些系统是专门为处理物联网系统产生的各种海量和高速数据而设计的。

随着时间的推移，流媒体边缘分析系统已经被开发出来，不仅可以过滤和减少物联网设备产生的数据，还可以对尽可能靠近网络边缘的物联网设备进行近实时响应。

最后，本章讨论了另一种形式的分析——网络分析。网络分析并不关注数据的内容，而是用于发现网络通信行为中的模式，帮助识别和预防安全漏洞，规划网络演进，以及更好地理解各种网络元素的行为。

总之，网络分析有多种形式。它们中的每一个都在物联网世界中扮演着关键角色，有助于定义连接事物的真正价值。

第8章 物联网安全

人们常说，如果第三次世界大战爆发，这场战争将在网络空间进行。随着物联网将越来越多的系统聚集在网络连接的“保护伞”下，安全性变得前所未有的重要。从为我们提供电力的电网系统到控制城市交通的红绿灯，再到保持飞机有序高效飞行的系统，网络、设备以及使用它们的应用程序的安全性是现代通信系统的基础和必要条件。在这样一个世界中提供安全并非易事。安全是极少数（如果不是唯一的话）必须与外部力量持续对抗以达到预期结果的技术学科之一。更复杂的是，这些外部力量能够利用传统技术和非技术方法（例如物理安全、操作流程等）来实现它们的目标。由于潜在的攻击载体如此之多，信息和网络安全是一个具有挑战性但又引人入胜的主题，它对技术供应商、企业和服务提供商都至关重要。

几十年来，信息技术（IT）环境一直面临着活跃的攻击和信息安全威胁，这些事件和经验教训是众所周知和有据可辨的。相比之下，运营技术（OT）环境是传统且封闭的，与其他网络的连接非常有限。因此，OT系统遭受网络攻击的历史要短得多，记录在案的事件也少得多。因此，学习机会和记载事件的主体及其相应的缓解措施并不像在IT世界中那样丰富。OT世界的安全性还涉及比IT世界更广泛的范围。例如，在OT中，security这个词几乎等同于safety。事实上，构成工业物联网安全基础的许多工业安全标准也纳入了设备和人员安全建议。

正是由于这些原因，本章将重点放在保护OT环境的核心原则上。IT安全是一个广阔的领域，有许多图书专门介绍它的各个方面。在一章中不可能详尽地讨论这个主题，所以我们重点关注OT安全以及IT安全的基本要素。此外，第3部分的行业特定章节讨论了安全性在特定行业纵向领域的应用。

本章提供了OT安全的历史观点、它是如何发展的，以及它面临的一些共同挑战，并且详细说明了保护IT和OT环境之间的一些关键区别。最后，本章探讨了创建更安全的工业环境的一些实际步骤，包括将现代IT网络安全引入传统工业环境的最佳实践。本章包括以下内容。

■ OT安全简史：本节概述OT环境是如何演变的，以及这种演变对保证运营网络安全的影响。

■ OT安全面临的常见挑战：本节概述了操作环境中的各种安全挑战，包括传统系统、不安全协议和资产。

■ IT和OT安全实践及系统的差异：本节提供了企业IT环境和OT环境中的安全实践之间的比较。

■ 正式的风险分析结构（OCTAVE和FAIR）：本节提供了一个整体的视角，以确保运营环境和风险评估框架的安全，这个风险评估框架包括组成控制系统的人员、流程和供应商生态系统组件。

■ 安全在运营环境中的阶段性应用：本节描述了将现代网络安全引入现有工业网络的阶段性方法。

[8.1 OT安全简史](#)

为了更好地了解工业环境的现状，区分假设和现实是很重要的。在信息技术领域，很少有话题比网络安全更能引起恐惧、不确定或怀疑。因此，本章仅限于列举官方来源的事件和数据，而不是公共媒体报道或未经证实的第三方陈述。

与大多数其他行业相比，工业环境中的网络安全事件可能会导致对人类生命构成威胁，以及破坏设备、基础设施和环境等物理后果。虽然工业环境中确实存在传统的IT相关安全威胁，但OT安全事件的物理表现和影响才是吸引媒体关注和引起广泛公众关注的原因。

据报道，网络安全攻击造成物理破坏的一个事例是Stuxnet恶意软件。另一个事例是德国一家冶炼厂发生的一起损坏熔炉的事件。在这两起事件中，多个步骤都导致了不希望出现的结果。许多现行的安全政策和缓解程序没有得到重视；如果实施得当，它们本可以阻止或可能完全停止攻击。例如，人们认为Stuxnet在最终被识别和发现之前，已经被部署在USB记忆棒上长达两年。

除物理损坏外，由于网络安全事故，OT环境还发生了运营中断。例如，在2000年，澳大利亚昆士兰州马鲁希郡的污水控制系统被远程控制，并向周围水域排放了80万升污水。2015年，乌克兰配电运营商基辅电力公司（Kyiv Oblenergo）的控制系统被攻击者远程控制，停电持续数小时，导致几天内数千名用户的服务质量下降。在这两种情况下，已知的缓解技术都可以用于更早地检测攻击，或者有能力阻止这些攻击劫持生产系统和影响服务。

从历史上看，攻击者都是技术熟练的个人，对技术和所攻击的系统有深刻的了解。然而，随着技术的进步，人们发明了使攻击更容易实施的工具。使问题进一步复杂化的是，这些工具变得更加广泛和容易获得。令这个问题更加复杂的是，许多在物联网环境中使用的传统协议已有几十年的历史，而且在最初开发时没有考虑到安全性。这意味着技术能力有限或没有技术能力的攻击者现在都有可能发动网络攻击，这大大增加了攻击的频率，并对终端构成了全面威胁。然而，一个普遍的误解是，攻击者总是占有优势，而终端操作人员缺乏有效的防御能力。运营商的一个重要优势是，它们对环境更加熟悉，对流程有更好的了解，因此可以利用多种技术和能力来抵御网络攻击。这一点至关重要，因为网络将继续面临不断演变和变化的攻击方法，而这些攻击方法将越来越难以防范和应对。

通信网络，包括本地的和地理上分散的，已经在工业环境中使用了几十年。例如，公用事业中变电站的远程监测与制造业中半自治系统之间的通信就是这种OT网络的长期实例。这些OT专用通信系统通常是独立的，并且与同一公司的传统IT企业网络物理隔离。虽然它遵循“通过隐藏实现安全”的传统逻辑，但这种网络划分形式导致了IT和OT网络的独立演化，两者之间的互连被严格隔离和监控。

工业网络 and 传统IT商业网络之间的隔离被称为“空气间隙”，这表明两者之间没有联系。虽然在某些行业有明显的这种极端孤立的例子，但它实际上并不是当今大多数物联网网络的准确描述。从广义上讲，OT和IT网络环境之间存在不同数量的互连，两者之间的许多相互依赖关系影响着互连的水平。

除了由不同的工业环境强加的策略、法规和治理外，还有一定数量的最终用户偏好和特定于部署的设计，它们决定了IT和OT环境之间的隔离程度。当一些组织继续保持严格的隔离时，另一些组织开始允许某些元素的互连。在工业环境中一个常见的例子是使用以太网和IP传输控制系统。尽管IT和OT网络在世界大部分地区仍然是分开运行和管理的，但当前的趋势是以IT中心技术为基础（如TCP/IP、以太网和公共API）来整合网络。

与传统工业环境中的非标准和专有通信方法相比，OT领域中不断增长的IT技术的发展带来的好处是可访问性提高和熟练的操作人员越来越多。与这些众所周知的IT标准相关联的问题是，安全漏洞更加广为人知，对这些系统的滥用往往更容易发生，并且规模要大得多。这种可访问性和规模使安全性成为一个主要问题，特别是运营领域中的许多系统和设备从未被设想在一个共享的、基于开放标准的基础设施上运行，而且它们的设计和开发并不具备高水平的内置安全功能。

工业环境中的项目通常是资本密集型的，预期寿命可以用几十年来衡量。与基于IT的企业不同，OT部署的解决方案通常没有理由进行更改，因为它们的设计是为了满足特定的（通常是一次性的）功能，并且没有需要升级的要求或动机。OT中的一个重点和优先级是系统正常运行时间和高可用性，因此通常只进行更改来修复错误或引入新的系统功能，以此支持该目标。因此，部署的OT系统通常具有较慢的开发和升级周期，并且可能很快与传统IT网络环境不同步。其结果是OT技术和负责这些操作系统的人员的知识都比他们的IT同行更新得更慢。

目前部署的大多数工业控制系统及其组件和有限的相关安全元素都是在很少遵守公开和开放标准的情况下设计的。这些系统的专有性

质意味着来自外部世界的威胁不太可能发生，也很少得到解决。然而，OT系统漏洞被暴露和被报告的趋势越来越明显。图8-1显示了自2010年以来工业控制系统（ICS）漏洞披露的历史。虽然报告的数量在过去几年中一直在增加，但很可能还有许多其他漏洞没有被报告或发现。



图8-1 2010年以来工业控制系统漏洞披露历史

由于大多数OT环境的变化速度较慢，升级周期较长，因此工业通信和计算技术的安全性投资远远落后于传统IT企业环境的安全性投资。

8.2 OT安全面临的常见挑战

物联网面临的安全挑战绝不是新的，也不局限于特定的工业环境。下面将讨论物联网面临的一些常见挑战。

8.2.1 网络架构的侵蚀

保护工业环境的两个主要挑战是初始设计和持续维护。最初的设计挑战源于这样一个概念，即网络是安全的，因为它与企业物理上是隔离的，与外部世界的连接很少甚至没有，并且假定攻击者缺乏足够的知识来执行安全攻击。在许多情况下，最初的网络设计是完善的，甚至遵循定义良好的行业最佳实践和标准，例如第2章中介绍的控制层次结构的普渡模型。网络安全面临的挑战和最大的威胁是标准和最佳实践被误解或维护不善。事实上，从安全设计的角度来看，了解通信路径是不安全的比不知道实际的通信路径要好。更常见的情况是，随着时间的推移，原本可靠的设计可能会被临时更新和对硬件及机器的个别更改所破坏，而不考虑到更广泛的网络影响。这种增长导致了对扩展网络的错误估计，并以独立的方式引入了无线通信，而没有考虑到对原始安全设计的影响。在许多情况下，随着时间的推移，这些不受控制或控制不良的OT网络演化会导致网络和系统安全性较为薄弱或不充分。

不同行业内部和不同行业间的安全网络设计中存在着广泛的差异。例如，电力公司在利用现代技术进行业务活动方面有着悠久的历史。在北美，有来自监管部门的监管要求，如北美电力可靠性公司（NERC）的关键基础设施保护（CIP）（详见第11章），要求采取合理规范的操作来实现安全的网络连接和控制。相比之下，在其他行业，往往没有立法要求或合规政策，这导致了安全能力的广泛差异。

在许多行业中，控制系统由包、控制模块或组件组成，这些组件是独立的，可以作为网络的半自治部分进行集成。这些包可能没有完全或紧密地集成到整个控制系统、网络管理工具或安全应用程序中，从而导致潜在的风险。

8.2.2 普遍的遗留系统

由于工业环境中设备的静态特性和较长的生命周期，许多操作系统可能被视为遗留系统。例如，在电力设施环境中，旧机械设备的机架仍然与现代智能电子设备（IED）一起运行的情况并不罕见。在许多情况下，遗留组件并不局限于孤立的网络段，而是已经整合到IT操作环境中。从安全的角度来看，这是潜在的危险，因为许多设备可能有历史上未修补和更新的漏洞或弱点，或者甚至可能由于设备的老化而无法使用补丁。

除了端点之外，通信基础设施和共享的集中式计算资源通常不是按照现代标准构建的。事实上，它们的通信方法和协议可能是世代相传的，并且必须与通信路径中最古老的操作实体进行互操作。这包括交换机、路由器、防火墙、无线接入点、服务器、远程访问系统、补丁管理和网络管理工具。所有这些都可能有可利用的漏洞，必须加以保护。

8.2.3 不安全的操作协议

许多工业控制协议，特别是那些基于串行的协议，在设计时没有强大的安全性要求。此外，它们的操作常常在假定的安全网络中进行。除了任何固有的弱点或漏洞外，它们的操作环境可能没有考虑到安全访问控制。

工业协议，如监视控制和数据采集（SCADA）（见第6章），特别是较老的变体协议，存在共同的安全问题。这方面的3个例子是通信端点之间通常缺乏身份验证、无法保护静态或动态数据，以及控制粒度不足，无法正确指定接收方或避免默认的广播方法。在独立系统中，这些可能不是那么重要，但是在区域之间或较长的网段上，例如广域网（尤其是公共广域网），它们可能是重要的考虑因素。

这些协议的结构和操作通常是公开的。虽然它们可能是由私有公司发起的，但是为了互操作性，通常会将它们发布给第三方来实现。因此，破坏协议本身并引入不轨之徒是一件相对简单的事情，这些不

轨之徒可能利用协议来破坏控制系统，用于侦察或攻击目的，从而在正常的系统操作中导致不良影响。

下面讨论一些常见的工业协议及其各自的安全问题。注意，许多协议都有串行、IP或基于以太网的版本，不同版本的安全性挑战和漏洞也不同。

1. Modbus

Modbus在许多行业中都很常见，例如公用事业和制造环境，并且有多种变体（例如串口、TCP/IP）。它是由第一个可编程逻辑控制器（PLC）供应商Modicon创建的，自20世纪70年代以来一直在使用。它是工业部署中使用最广泛的协议之一，其开发由Modbus组织管理。有关Modbus的更多细节，请参阅第6章。

存在于Modbus中的安全挑战并不罕见。通信端点的身份验证不是默认操作，因为它允许不合适的源向接收者发送不正确的命令。例如，要使消息到达目的地，只需要正确的Modbus地址和函数调用（代码）即可。

一些较老的基于串行的Modbus版本通过广播进行通信。某些版本不具备限制广播功能的能力。接收方有可能对没有明确针对它的命令执行操作。此外，攻击可能会影响无意接收的设备，从而减少了解网络拓扑结构细节的需要。

初始化应用程序也不执行Modbus消息内容的验证。相反，Modbus依赖于网络堆栈来执行这个函数。这可能会导致协议在系统中滥用。

2. DNP3（分布式网络协议）

DNP3存在于多个部署场景和行业中。它在公用事业中很常见，在离散和连续过程系统中也存在。与许多其他ICS/SCADA协议一样，它的

目的是在控制器和简单的IED之间进行串行通信（有关DNP3的详细信息请参阅第6章）。

DNP3有一个明确的安全版本，但是DNP3仍然有许多不安全的实现。DNP3非常强调信息的可靠传递，这种强调虽然通常是非常可取的，但从安全的角度来看也有特定的弱点。在DNP3的情况下，参与者允许未经请求的响应，这可能引发不希望的响应。这里缺少的安全元素是在系统状态中建立信任的能力，从而信任所提供信息的准确性。这类似于以太网中免费ARP消息所带来的安全缺陷，而现代以太网交换机中的动态ARP检查（DAI）已经解决了这一问题。

3. ICCP（控制中心间的通信协议）

ICCP是北美公用事业中常用的控制协议，经常用于公用事业之间的通信。考虑到它必须跨越不同网络之间的边界，它拥有的额外的暴露水平和风险等级，可能会使公用事业公司受到网络攻击。

与其他控制协议不同，ICCP从一开始就被设计为用于跨广域网工作。尽管发挥了这一作用，但ICCP的最初版本在安全领域仍存在一些重大缺陷。一个关键的漏洞是系统通信不需要身份验证。其次，它没有将跨协议的加密作为默认条件启用，因此可将连接暴露给中间人（MITM）攻击和重放攻击。

4. OPC（过程控制OLE）

OPC基于Microsoft的互操作方法论——对象链接和嵌入（OLE）。这是一个在IT领域和个人计算机中使用的IT标准在工业网络中用作控制协议的示例。

在工业控制网络中，OPC被限制为在控制空间的高层运行，依赖于Windows平台。对OPC的关注始于它所运行的操作系统。Windows操作系统中的许多设备都是旧的，没有完全修补，并且由于大量众所周知的

漏洞而处于危险之中。对OPC的依赖可能会加强这种依赖。虽然OPC的新版本增强了安全功能，但它们也开辟了新的通信模式，这种模式具有积极和消极的安全潜力。

与OPC特别相关的是对远程过程调用（RPC）协议的依赖，它产生了两类漏洞。第一个要求我们能够清楚地了解与RPC相关的一些漏洞，第二个要我们确定这些漏洞给特定网络带来的风险级别。

5. 国际电工委员会（IEC）协议

IEC 61850标准的创建是为了适应不受供应商约束的电力系统工程，这将反过来允许供应商和标准化的通信协议之间的互用性。最初定义了 3 种消息类型：MMS（制造消息规范）、GOOSE（面向对象的通用子站事件）和SV（采样值）。Web服务是后来添加的第四个协议。这里提供了一个简短的总结，更多关于IEC协议的信息，请参阅第11章。

■ MMS（61850-8.1）：MMS是一种客户端/服务器协议，它利用TCP/IP并在第3层运行。它提供了与其他SCADA协议（如IEC 60870和Modbus）相同的功能。

■ GOOSE（61850-8.1）：GOOSE是一个通过以太网多播运行的第二层协议。它允许智能电子装置在发电机房之间和变电站之间水平交换数据，特别是在联锁、测量和跳闸信号之间。

■ SV（61850-9-2）：SV是通过以太网组播运行的第二层协议。它携带电压和电流样本，通常在过程总线上运行，但它也可以在站点总线上流动。

GOOSE和SV都是通过发布/订阅模型运行的，没有可靠的机制来确保数据被接收。

IEC 61850有几个已知的安全缺陷，熟练的攻击者可以利用这些缺陷破坏控制系统。身份验证嵌入在MMS中，但它是基于明文密码的，并且身份验证在GOOSE或SV中不可用。固件通常没有签名，这意味着无法

验证其真实性或完整性。GOOSE和SV具有有限的消息完整性，这使得模拟发布者相对容易。

当该标准首次发布时，这些协议中的安全能力很低，但IEC 62351通过引入众所周知的基于IT的安全措施（如证书交换）解决了这一问题。

IEC 60870广泛应用于欧洲的SCADA远程控制系统，特别是电力公用事业行业，以及地理分布广泛的控制系统。该标准的第5部分概述了端点之间用于交换远程控制消息的通信配置文件。60870-5-101为串行实现配置文件，60870-5-104为IP实现配置文件，60870-5-103用于保护设备。同样，在IEC 60870-5的早期迭代中，缺乏安全性。IEC 62351正在解决这一问题，60870-5-7安全扩展工作适用于60870-101和60870-104。

8.2.4 其他协议

很多时候，关于工业系统安全性的讨论都集中在工业控制协议上，就好像它们是所有要观察或考虑的内容。这种假设是狭隘的，在很多层面上都存在问题。实际上，强烈建议安全从业人员在执行任何类型的控制或安全措施之前，要识别通过网络的流量的所有方面。特别要对任何网络（包括ARP、UDP、TCP、IP和SNMP）的最基本协议、传输机制和基本元素进行适当的审计、处理和理解。

一些特殊环境还可能具有其他后台控制协议。例如，许多物联网网络一直延伸到各个传感器，因此使用了诸如受限应用协议（CoAP）（参见第6章）和数据报传输层安全（DTLS）等协议，这些必须从安全的角度单独考虑。

8.2.5 设备不安全

除了使用的通信协议和遗留系统的安装基础之外，控制和通信元素本身也有漏洞记录。正如本章前面提到的（见图8-1），在2010年之前，安全界很少关注工业计算，因此OT系统没有经历与IT系统相同的火线测试。图8-2通过简单地将Black Hat安全会议上提出的工业安全主题的数量与工业控制系统报告的漏洞数量叠加，以图形化的方式显示了这一点。Black Hat关于OT安全主题的演示与发现的漏洞数量之间的相关性是显而易见的，其中包括相关的发现速度在变慢。

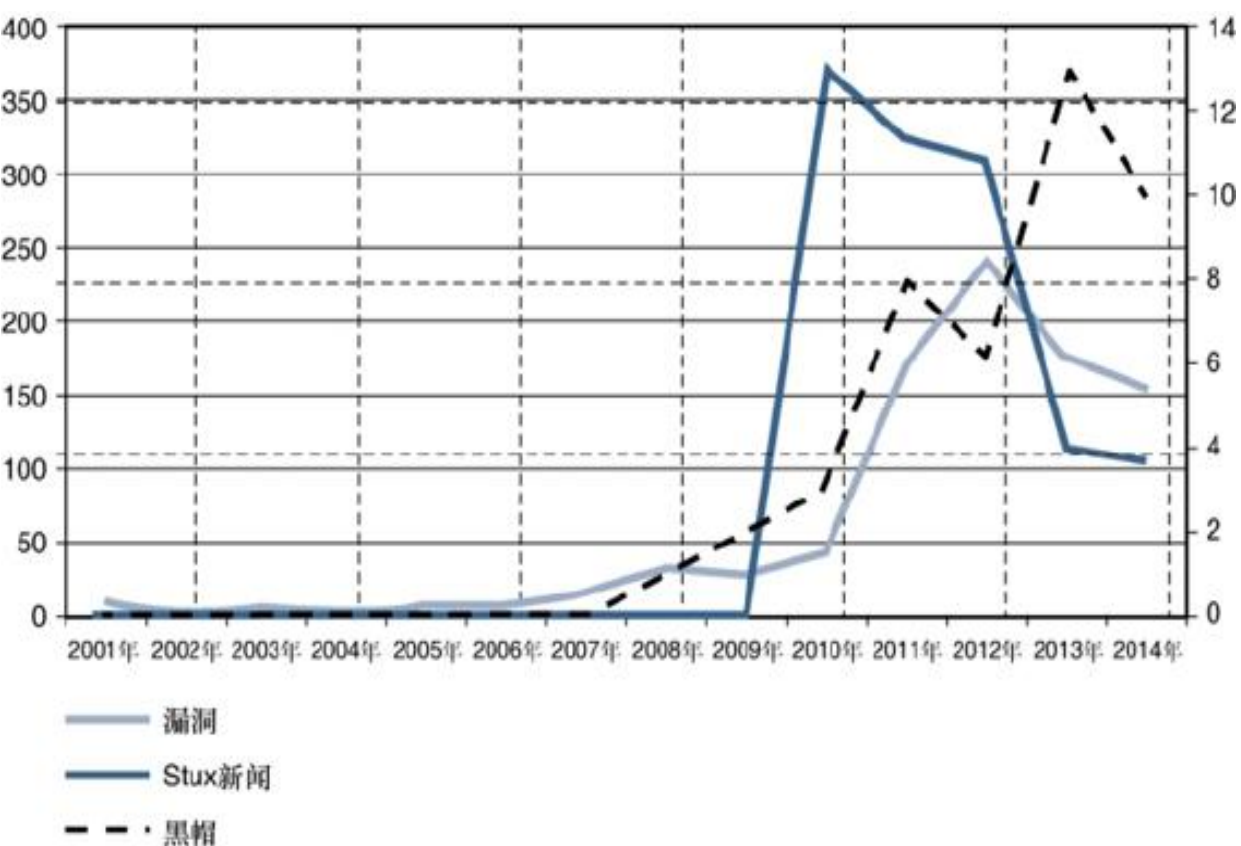


图8-2 工业Black Hat演示与发现的工业漏洞的相关性

要了解设备不安全的本质，重要的是回顾所发现的漏洞和受影响的设备类型的历史记录。回顾2000-2010年的时间段，可以看到，大部分的发现都是发生在运行网络的较高级别，包括受信任的控制系统，这些控制系统可以运行工厂、传输系统、石油管道或任何正在使用的关键功能。

不难理解为什么这些系统是脆弱的。首先，许多系统使用的软件包可以很容易地下载和使用。其次，它们运行在通用硬件和标准操作系统上，例如Microsoft Windows。最后，Windows和这些应用程序中使用的组件是传统的IT安全研究人员所熟知的。当长期存在的工具或技术足以突破目标的防御时，就不需要开发新的工具或技术了。例如，最著名的工业计算机攻击Stuxnet最初之所以成功，是因为它能够利用Windows中一个此前未知的漏洞。

ICS供应商社区在安全功能和实践以及与第三方安全研究人员的合作方面也落后于IT同行。尽管如此，这种情况已经开始得到业界的重视，并且通过最近一系列措施得到改善，这些措施旨在正式解决工业环境中的安全漏洞和系统测试问题。虽然有一些正式的标准，如ISO/IEC 15408（通用标准）、ISO/IEC 19790和其他一些标准，但是仍然没有几个正式的安全测试实体。除了正式测试之外，几乎没有法规会强制执行针对设备安全测试的通用标准。

就在不久前，安全研究领域还被视为一种威胁，而不是一种揭露潜在危险的有价值且通常免费的服务。虽然情况有所改善，但OT方面的努力仍然远远落后于基于IT的创新，比如bug赏金奖励计划和高级漏洞准备计划，以及类似于Microsoft主动保护计划（MAPPP）的事情。更进一步说，在工业领域，甚至没有类似的法律用来保护个人隐私数据。尽管许多国家和地区要求在个人和财务数据可能被泄露时予以通知，但在电力公用事业行业之外，很少有法律要求报告可能会危及生命的事件。

8.2.6 对外部供应商的依赖

虽然现代IT环境可能将业务操作外包或将某些处理或存储功能委托给云，要求IT硬件资产的原始设备制造商来操作设备的情况并不常见。然而，这种程度的供应商依赖在一些工业领域并不少见。

直接和按需访问工厂或现场的关键系统有时直接被写入合同，或需要有效的产品保证。这在许多行业都有明显的好处，因为它允许供

应商远程管理和监控设备，并在出现问题时主动提醒客户。虽然可以编写合同来描述设备监测和管理要求，并明确说明需要什么类型的访问以及在什么条件下访问，但它们通常无法解决安全漏洞的共同责任问题或确保通信安全的过程。

这种对供应商的依赖和控制并不局限于远程访问，还需要对获得计算机和网络访问权限的非雇员进行现场管理，且同样需要遵守控制条件和共享责任声明。

8.2.7 安全知识

在工业运营领域，技术投资主要集中在互联互通和计算方面。与IT行业相比，它在安全方面的投资要少得多。根据研究公司Infonetics的数据，2015年工业防火墙市场的规模仅为整个防火墙市场的4%左右。

与OT安全专家相关的另一个挑战是工业劳动力的年龄相对较高。根据美国劳动局（US Bureau of Labor）的一项研究，2000-2012年，北美制造业工人与其他非农业工人的平均年龄差距扩大了一倍，而且这一趋势没有逆转的迹象。与此同时，新的连接技术开始在OT工业环境中引入，这些环境需要最新的技术，比如TCP/IP、以太网和无线技术，这些技术正在迅速取代基于串行的传统技术。通信网络的迅速扩张和对工业控制敏感的劳动力的需求造成了安全意识方面同样严重的差距。

OT安全知识方面的这一差距正在积极得到解决。工业安全环境教育稳步增长，特别是在电力公用事业领域，如NERC CIP（CIP 004）和IEC 62351（01）等法规要求持续培训。

由于工业空间安全的重要性，所有可能的攻击面都被认为是不安全的。不幸的是，考虑到破坏这些系统可能对公众造成的巨大影响，尽管在这些领域投入了大量的安全投资，但人们对于以IT为中心的技术和外部连接的关联，仍然存在一种健康的偏执。由于OT和IT环境之

间的历史文化与哲学差异，将工业网络提升到最新和最安全的水平是一个缓慢的过程。

8.3 IT和OT安全实践及系统的差异

了解企业IT环境和以行业为重点的OT部署之间的差异非常重要，因为它们直接影响应用于它们的安全性实践。本章前面简要讨论了其中的一些领域，下面将更明确地讨论这些领域。

8.3.1 控制层次结构的普渡模型

无论在何处出现安全威胁，都必须坚定地、毫不含糊地加以处理。IT信息通常用于做出业务决策，例如流程优化中的决策，而OT信息通常用于做出物理决策，例如关闭阀门、增加压力等。因此，业务领域还必须将物理安全 and 环境因素作为其安全策略的一部分，而这通常与IT领域无关。从组织上看，IT和OT团队与工具在历史上是分开的，但是这种情况已经开始改变，并且它们已经开始聚合，从而引入更传统的以IT为中心的解决方案来支持运营活动。例如，防火墙和入侵防御系统（IPS）等系统已经开始在物联网网络中使用。

由于传统意义上分离的OT和IT域之间的边界变得模糊，因此必须调整它们的策略并更加紧密地合作以确保端到端的安全性。工业OT环境中的设备类型通常比IT环境中的设备类型更适合于任务和特定于工业协议的操作。此外，它们的运模式也有所不同。

工业环境由操作域和企业域组成。为了了解控制系统的安全性和网络需求，需要使用逻辑框架来描述控制系统的基本组成和功能。第2章介绍的控制层次普渡模型是全球工业环境中使用最广泛的框架，用于制造业、石油和天然气以及许多其他行业。IT按照功能层次和区域对设备进行划分，并已被纳入ISA99/IEC 62443安全标准，如图8-3所

示。有关控制层次结构的普渡模型如何应用于制造业和油气行业的更多细节，请参见第9章和第10章。



图8-3 基于普渡模型的控制层次结构逻辑框架

此模型标识操作级别并定义每个级别。企业和运营领域被划分为不同的区域，并通过工业非军事区（DMZ）严格隔离。

■ 企业区域

■ 第5级：企业网络。企业级别的应用程序，如企业资源规划（ERP）、客户关系管理（CRM）、文档管理，以及来自外部世界的Internet访问和VPN入口等服务，都属于该级别。

■ 第4级：业务规划和物流网络。IT服务属于此级别，可能包括调度系统、物流应用程序、优化和规划系统，以及本地IT服务，如电话、电子邮件、打印和安全监控。

■ 工业非军事区

■ **DMZ**：DMZ提供了一个缓冲区，在该缓冲区中，可以在运营区域和企业区域之间共享服务和数据。它还允许对有组织的控制进行简单分段。默认情况下，不应该有任何流量通过DMZ；所有内容都应起始于或终止于该区域。

■ 运营区域

■ **第3级：运营和控制**。该级别包括管理工作流以生成所需的最终产品，以及监控和控制整个运营系统所涉及的功能。这可能包括生产调度、可靠性保证、系统范围的控制优化、安全管理、网络管理，以及可能需要的其他IT服务，如DHCP、DNS和计时。

■ **第2级：监控**。该级别包括区域控制室、控制器状态、控制系统网络/应用程序管理，以及其他与控制相关的应用程序，如人机交互（HMI）和历史记录。

■ **第1级：基本控制**。在这个级别上，控制器和IED、专用HMI和其他应用程序可以相互通信以运行部分或全部控制功能。

■ **第0级：过程**。这是传感器和执行器等设备以及驱动器、电机和机器人等机器与控制器或IED通信的地方。

■ 安全区域

■ **安全关键性**。这个级别包括用于管理控制系统安全功能的设备、传感器和其他设备。

与普渡模型一样，在架构级别设计工业网络的一个关键优势是，它允许在每个级别和级别之间正确应用安全性。例如，IT网络通常位于第4级和第5级，并且使用IT网络通用的安全原则。低层级是工业系统和物联网网络所在的位置。如图8-3所示，DMZ位于IT层和OT层之间。显然，为了保护较低的工业层，应该使用防火墙、代理服务器和IPS等安全技术来确保只使用来自预期端口上可信来源的授权连接。在DMZ甚至在较低级别之间，应该使用能够理解控制协议的工业防火墙来确保OT网络的持续运行。

尽管模型的每个级别都可能存在安全漏洞，但很明显，由于设备和系统的连接性和复杂性，较高级别的攻击面更广，因此被入侵的可能性更大。这并不意味着从安全的角度看，较低的级别不重要；相反，这意味着它们的攻击面更小，如果正确地实施缓解技术，对整个系统的影响可能更小。图8-4对2011年发布的与工业安全相关的漏洞进行了回顾，我们发现在框架的较高级别检测到的漏洞更多。

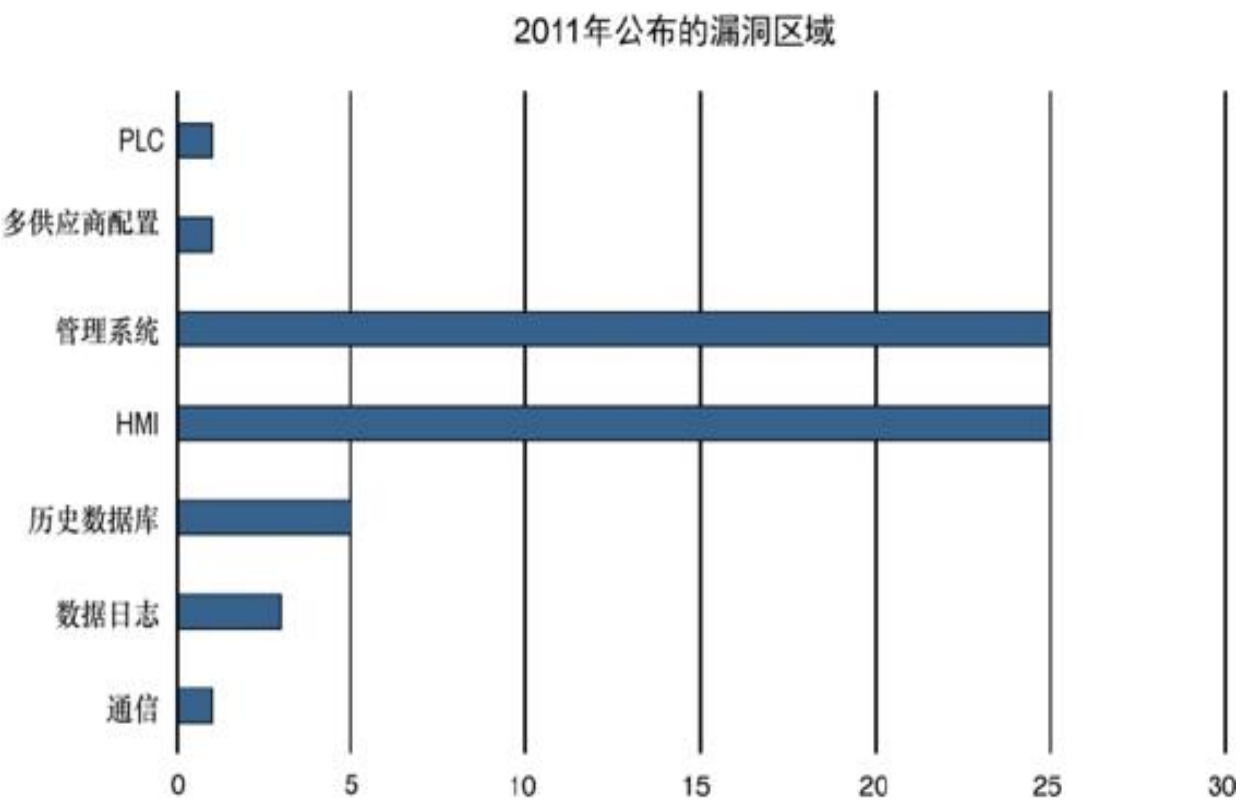


图8-4 2011年发布的漏洞区域工业安全报告

8.3.2 OT网络特性影响安全

虽然IT网络和OT网络开始融合，但在如何操作和处理流量方面，它们仍然保持着许多不同的特征。这些差异会影响在安全策略上下文中如何处理它们。例如，比较一下IT和OT网络之间流量的性质。

■ IT网络：在IT环境中，有许多不同的数据流。从典型的IT端点发出的通信数据流的传输距离相对较远。它们经常通过交换机层遍历

网络，最终到达一组本地或远程服务器，它们可以直接连接到这些服务器。以电子邮件、文件传输或打印服务形式出现的数据很可能都将被发送到中央数据中心，在那里它将在更多的本地服务（如打印机）中响应或触发操作。在电子邮件或Web浏览的情况下，端点发起的操作将脱离企业网络的限制，并可能在全球传播。

■ OT网络：相比之下，在OT环境（级别0~3）中，通常有两种类型的运营流量。第一个是本地流量，它可能包含在一个特定的数据包或区域中，以提供本地监控和闭环控制。这是用于实时（或接近实时）进程的流量，不需要离开进程控制级别。第二种类型的流量用于监控区域或整个系统。SCADA流量就是一个很好的例子，其中关于远程设备的信息或来自某一功能的汇总信息在系统层面共享，以便操作人员能够了解整个系统或部分系统如何运行。然后，操作人员可以根据这些信息实现适当的控制命令。

当IT端点通信时，通常是与许多连接进行简短而频繁的对话。通信的本质是开放的，几乎任何人都可以与其他人交谈，比如通过电子邮件或浏览。尽管存在明显的访问控制，但这些控制大多位于应用程序级别，而不是网络级别。

在OT环境中，端点通信通常是点对点的，比如SCADA主机到SCADA从站，或者利用发布/订阅类型模型的多播或个播。通信可以是TCP或UDP，也可以两者都不是（如PROFINET的情况，在第9章讨论）。

在OT领域，网络时间通常反映企业使用NTP/SNTP对主时间源进行设备计时的情况，许多用例需要非常精确的时钟源和非常精确的时间同步/分布，以及可测量的、连续的延迟/抖动。一些工业应用需要通过IEEE 1588、PTP（精确时间协议）定时，这样来自源和目标的信息可以在微秒间隔内精确测量和比较，而通信设备的延迟不超过50纳秒。发送和接收信息时的抖动也必须最小化，以确保正确的操作。相比之下，在企业领域，语音通常被认为是最高优先级的应用程序，一般单向延迟为150毫秒或更多。在许多石油和天然气行业、制造业和电力公共行业的操作环境中，延迟必须小于10微秒。导致延迟的安全攻击，如拒绝服务攻击，可以通过破坏定时机制引发系统故障。

IT网络通常更加成熟，使用最新的技术。这些成熟的现代网络实践对于满足IT环境所需的高度灵活性至关重要。虚拟网络、虚拟工作空间和虚拟服务器非常常见。在任何一个时刻，很可能有各种类型的设备活跃地参与到任何给定的网络中。因此，灵活的互用性至关重要。为了实现互用性，通常只有很少的专有通信行为，并且重点通常放在开放标准上。向IPv6的迁移仍在继续，高阶网络服务（如服务质量[QoS]）也很正常。端点不仅在它们的通信过程中是杂乱的，而且它们需要操作来自大量不同供应商的大量应用程序。这些计算系统的开放性意味着有大量的协议正在穿越OT网络。

工业网络通常仍然依赖串行通信技术，或者混合使用串行和以太网。这意味着不仅许多设备缺乏IP功能，而且甚至不可能像监控IP或以太网那样监控和保护串行通信。在某些环境中，网络是非常静态的，这意味着可以建立一个流量模式的基线，并监控其变化。在静态环境中，可以更容易地管理和保护设备、协议和流量的可见性。然而，移动设备和临时连接在持续增长，尤其是在交通和智慧城市等行业，以及其他众多行业中移动车队也在增长。这些动态和可变的网络很难进行基线化、监控和保护。

8.3.3 安全优先级：完整性、可用性和机密性

安全优先级由每个环境中资产的性质决定。在IT领域，最关键的元素和攻击目标是信息。在OT领域中，关键资产是流程参与者：工人和设备。基于这些差异，安全优先级也存在差异。

在IT商业世界，有法律、法规和商业义务来保护数据，特别是那些可能受雇于或不受雇于组织的个人的数据。这种对隐私的强调着重于数据的保密性、完整性和可用性，而这些数据不一定在系统或物理资产上。与计算设备可以保存或提供访问的信息相比，丢失计算设备的影响被认为是最小的。相比之下，在OT世界，由于安全漏洞导致设备丢失意味着生产停止，公司无法进行基本的运营。存储在这些设备上的信息丢失并不是特别重要，但在操作环境中肯定存在机密数据集，这些数据集可能会产生经济影响，例如配方和工艺。

在操作空间中，过程参与者的安全和连续性被认为是最关键的问题。因此，我们的目标是设备的持续正常运行时间和操作人员的安全。其结果是强调可用性、完整性和机密性。损失的影响甚至可能会导致生命期缩短。

8.3.4 安全焦点

安全焦点通常由组织所经历的安全影响历史所驱动。在IT环境中，最痛苦的经历通常是提取或破坏关键数据的入侵活动。其结果是对资本财货和人力进行了大量投资，以减少这些外部威胁，并尽量减少潜在的内部的不轨之徒。

在OT领域，由于外部因素造成的损失历史并不长，尽管对人类造成伤害的可能性明显要高得多。其结果是，所经历的安全事件更多地来自人为错误，而不是外部攻击。工业安全方面的兴趣和投资主要集中在标准访问控制层。在一定程度上，OT的分歧在于将应用层控制扩展到高级控制器层和接收操作层之间。本章后文将介绍与此方法相关的价值和风险的更多信息。

8.4 正式的风险分析结构（OCTAVE和FAIR）

在工业环境中，有许多标准、指南和最佳实践可用来帮助理解风险以及如何减轻风险。IEC 62443是全球工业垂直领域最常用的标准。它由若干部分组成，包括用于风险评估的62443-3-2和用于从网络和通信角度保护工业环境的基本要求的62443-3-3。此外，ISO 27001广泛应用于组织人员、流程和信息安全管理。美国国家标准与技术研究院（NIST）还为关键基础设施提供了一系列文件，如NIST网络安全框架（CSF）。在公用事业领域，北美电力可靠性公司（NERC）的关键基础设施保护（CIP）为北美公用事业公司制定了有法律约束力的指导方针，IEC 62351是电力行业的网络安全标准。

任何工业环境的关键在于需要从整体上解决安全问题，而不仅仅是关注技术。它必须包括人员和过程，并且应该包括构成控制系统的所有供应商生态系统组件。

在本节中，我们将简要回顾这两种风险评估框架。

■ 来自卡内基·梅隆大学软件工程研究所的OCTAVE（操作性关键威胁、资产和脆弱性评估）。

■ 来自开放组（The Open Group）的FAIR（信息风险因素分析）。

这两个框架致力于建立一个更安全的环境，但是使用两种不同的方法和优先级。对环境的了解是防范安全风险的关键，并在推动优先事项方面发挥关键作用。

8.4.1 OCTAVE

OCTAVE 经历了多次迭代。本节重点介绍的版本是 OCTAVE Allegro，其目标是实现一个轻量级且负担较轻的过程。Allegro 假定一个健壮的安全团队没有处于待命状态，或者没有准备好立即启动全面的安全审查。鉴于许多业务技术领域同样缺乏以安全为重点的人力资源，这种方法及其所作的假设是非常恰当的。图8-5展示了OCTAVE Allegro的步骤和阶段。

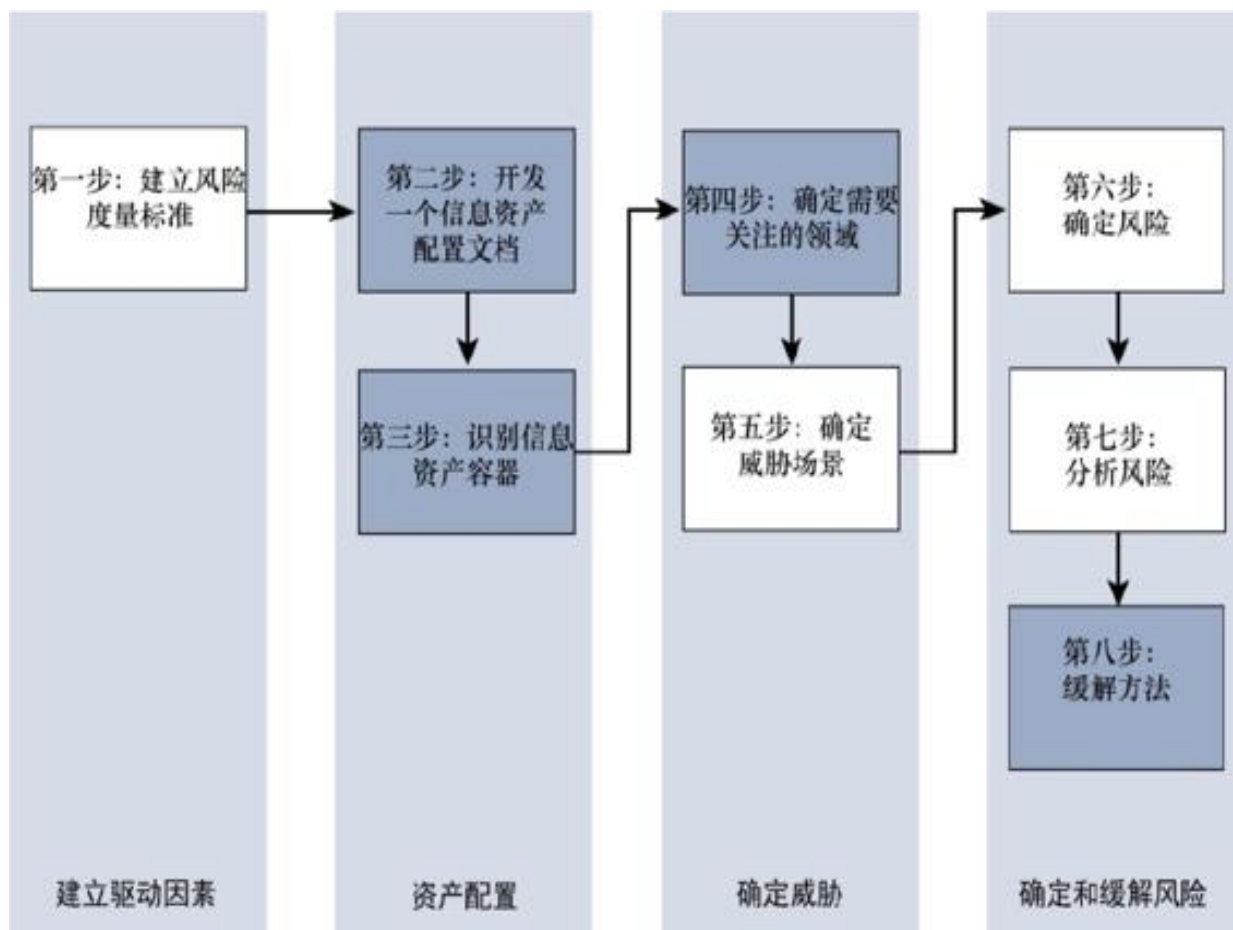


图8-5 OCTAVE Allegro的步骤和阶段

OCTAVE Allegro法的第一步是建立风险度量标准。OCTAVE提供了一种相当简单的方法来实现这一点，强调影响、价值和度量。拥有风险度量标准的意义在于，在后期的任何阶段都可以对参考模型进行优先级排序。虽然OCTAVE有更多细节可供参考，但建议使用FAIR模型进行风险评估。

第二步是开发一个信息资产配置文档。这个文档包含资产、资产的优先级、与每个资产相关的属性，包括所有者、保管人、人员、明确的安全需求和技术资产。强调过程的重要性是很重要的。当然，信息保护的这一需求并没有消失，但操作安全和连续性更为关键。

在这个资产配置文件中，流程是完成资产定义的多个子阶段。其中一些仅仅是调查和报告活动，例如确定与IT相关的资产和属性，例如其所有者、保管人、与IT交互的人工参与者，以及IT技术资产的组

成。但总有一些基于判断的属性，比如优先级排序。系统不是简单地分配一个任意的排名，而是需要一个确定优先级的理由。通过了解资产属性，特别是技术组件，可以应用适当的威胁缓解方法。通过应用风险评估，安全投资水平可以与单个资产匹配。

第三步是识别信息资产容器。粗略地说，这是传输的范围和信息可能驻留的位置，指的是计算元素及其通信网络。然而，它也可以指物理表现，如硬拷贝文件，甚至是了解信息的人。注意，这里的可操作目标是信息，其中包括派生信息的数据。

在OCTAVE中，重点是容器级别，而不是资产级别。其价值在于减少容器内用于信息操作的潜在抑制。在OT领域，重点是减少容器化操作空间中的潜在抑制。如果信息的某个属性是其特有的，那么整个容器将使用该属性进行操作，因为信息是定义元素。在某些情况下，这可能不是真的，即使在IT环境中也是如此。离散的原子级数据只有在其他数据的上下文中才可能成为可操作的信息。同样，在不了解其他元素的情况下获取的操作数据也可能没有特别的价值。

第四步是确定需要关注的领域。此时，我们将从数据流、接触和属性焦点转移到通过将与安全相关的属性映射到更侧重于业务的用例来做出判断的方式。在这个阶段，分析人员查看风险概况并深入研究前面提到的风险分析。它不再仅仅是事实，还有一个创造性的因素可以纳入评估。组织内外的历史都可以做出贡献。参考类似的操作用例和安全故障事件是合理的关联。

密切相关的是第五步，其中确定了威胁场景。威胁被广泛地（恰当地）确定为潜在的不良事件。这个定义意味着来自恶意和意外原因的结果都是可实施的威胁。就业务重点而言，这种考虑很有价值。正是在这一点上，产生了明确的参与者、动机和结果。这些场景在威胁树中进行描述，以跟踪不期望结果的路径，而这些结果又可以与风险度量关联。

第六步确定风险。在OCTAVE范围内，风险是一个未知结果的可能性。这将扩展到关注组织如何受到影响。对于更集中的分析，可以将

其本地化，但是对组织的潜在影响可能会超出操作范围。

第七步是分析风险，努力对风险的影响进行定性评估。在这里，第一步中定义的风险度量标准被明确地引入到过程中。

最后，在第八步应用缓解方法。这个阶段需要产生3个结果或决定。一种可能是接受风险，但是不执行任何操作，只是记录下情况、可能的结果和接受风险的原因。第二种是通过必要的措施来降低风险。通过回顾威胁场景到资产配置文件，应该可以发现并实施一对补偿控制来减轻这些威胁/风险对。最后可能采取的行动是推迟决策，这意味着风险既不被接受，也不被降低。这可能意味着进一步的研究或活动，但这不是过程所需要的。

OCTAVE是一个以信息为中心的平衡过程。然而，它在规则和很大程度上不受约束的广度方面所提供的功能被其缺乏安全特性的缺点所抵消。有一种假设是，除这些步骤外，似乎还有识别具体缓解措施的方法，这些措施可以映射到分析过程中暴露的威胁和风险。

8.4.2 FAIR

FAIR（信息风险因素分析）是来自The Open Group的风险定义的技术标准。虽然信息安全是重点，就像OCTAVE一样，但FAIR在运营技术中有明确的应用。与OCTAVE一样，它也允许非恶意的参与者作为潜在的危害因素，但是它更加强调了这一点。对于许多业务组来说，这是对现有应急计划的一个可喜的承认。与OCTAVE不同的是，它非常强调命名，风险分类法定义是一个非常具体的目标。

FAIR强调明确的定义和风险及相关属性是可度量的。可度量的、可量化的度量是重点关注的一个关键领域，它应该能够很好地适应拥有丰富数据的运营领域。

在其基础上，FAIR将风险定义为可能的损失频率和可能的损失规模。有了这个定义，就出现了一个清晰的子元素层次结构，风险分类

法一方面关注频率，另一方面则关注数量。

损失事件频率是威胁代理作用于资产并导致组织损失的结果。这种情况在给定频率下发生，称为威胁事件频率（TEF），其中指定的时间窗口成为一个概率。有多个子属性定义事件的频率，所有这些都可以通过某种形式的度量来理解。威胁事件频率应用于一个漏洞。这里的漏洞不一定是某种计算资产的弱点，而是更广泛地定义为目标资产由于所应用的操作而失败的概率。这里还有更多的子属性。

风险分类的另一方面是可能损失量（PLM），它开始对影响进行量化，并再次强调可度量的指标。FAIR规范强调了一些成本估算是多么短暂，而当信息安全成为讨论的目标时，这种情况可能确实存在。幸运的是，OT运营商非常重视运营效率和分析，这使得理解和量化成本变得非常容易。

FAIR定义了6种形式的损失，其中4种是外部损失，2种是内部损失。对运营团队来说，特别重要的是生产力和重置损失。反应损失也得到了合理衡量，罚款和判决尽管容易衡量，但很难预测。最后，竞争优势和声誉是最难衡量的。

注释：关于OCTAVE Allegro和FAIR的讨论是一个正式的风险分析过程的基础。虽然还有其他的机制，但它们都表示可以应用于OT环境的机制。

8.5 安全在运营环境中的阶段性应用

安全从业人员的目标是安全保护他们负责的环境。对于运营技术人员来说，这个过程是不同的，因为要保护的优先级和资产与IT环境有很大的区别。本章详细讨论了这些差异，但是IT安全从业人员使用的许多流程仍然有效，并且可以在OT环境中使用。有一个关键概念需要掌握，那就是物联网环境的安全是一个持续的过程，在这个过程中可以采取一些步骤，但没有真正的终点。

下面几节将介绍一种分阶段的方法，将现代网络安全应用到基本上已经存在的传统工业网络中。

8.5.1 网络基础设施和资产的安全

考虑到典型的物联网或工业系统中的网络、计算或操作元素可能已经存在多年，而且物理布局在很大程度上定义了运营过程，这种引入现代网络安全的分阶段方法从非常温和、非侵入性的步骤开始。

我们需要分析和保护基本的网络设计。大多数自动化过程系统甚至分级能源分配系统在网络设计和操作设计之间具有高度的相关性。ISA99和IEC 62443的基本原则是将功能划分为区域（单元），并通过导管的概念保护和控制跨越这些区域边界的通信。对此，建议由安全专业人员发现其网络 and 所有通信通道的状态。

图8-6所示为过程控制层次结构中的层间安全模型和层间通道。



图8-6 在过程控制层次结构模型中级别和区域之间的安全性

对于较旧的网络设备，正常的网络发现过程可能存在很大的问题。事实上，为了追求更高的安全性、保密性和操作状态而进行的发

现过程可能会导致这三者的退化。在这种情况下，网络发现过程可能需要手动检查物理连接，从最高可访问的聚合点开始，一直到最后的访问层。此发现活动必须包括对无线接入点的搜索。为了降低风险，任何在线网络映射都应该尽可能被动地进行。

值得注意的是，这种规定的过程在一个较小的封闭环境中更有可能成功，比如在工厂地板上。在地理上分布的环境中，可能无法跟踪网络，在这种情况下，远程连接可能不是物理的，或者可能由外部通信提供商承载。对于运营网络的这些部分，需要与其他实体建立明确的合作关系。

这个网络跟踪过程的一个附加活动是记录物理连接的连接状态。这不仅仅查看在哪些端口有哪些光纤或电缆，而且是观察每个网络设备上其他物理连接（如USB、SD卡、警报通道、串行或其他连接）的使用或运行状态。对于使用更新的网络设备和协议的更现代的环境，还可以使用NetFlow和IPFIX等工具来发现网络通信路径。

当网络映射到达聚合点时，继续映射到已连接的资产级别是值得的。

通常，在IT环境中，发现的第一阶段主要关注与网络相关的资产。资产仍然是关键的，但是从效率和关键性的角度来看，通常建议找到进入区域（单元）的数据路径，而不是区域内设备之间的串行连接。需要持续关注的一件事是始终存在的危险、不安全且常常没有文档记录的便利端口，任何物理端口未被物理锁定或没有实施保护策略都是一个失控的威胁载体。

一旦网络被物理映射，下一步是通过网络基础设施中的交换机和路由器ARP表和DHCP请求执行连接性分析。无论是好是坏，这将有助于进一步阐明已经发生的连接。防火墙和网络基础设施数据有助于了解哪些设备正在与其他设备通信，以及通信路径是什么。

在这个阶段，应该对网络有充分的理解，并为安全连接做好准备。

现代网络设备提供了丰富的访问控制和安全通信功能。从单元/区域级别开始，重要的是要确保每个区域有一个清晰的入口/出口聚集点。如果很好地确定了通信模式，就可以应用访问控制策略来管理谁以及什么内容可以进入这个过程的物理部分。如果不希望明确控制流量，那么就从只用警报的操作开始。随着时间的推移，我们应该有足够的信心来应用控制。

在上游级别，考虑流量控制，如拒绝服务（DoS）保护、流量标准化活动和服务质量（QoS）控制（例如标记流量、黑洞流量，或限制速率的清除器级别的流量）。这里的目标是确保这些聚合的流量段能够毫无障碍地承载高优先级的流量。

网络基础设施还应该提供通过安全管道保护区域之间通信的能力（见图8-6）。主要的方法是以虚拟专用网（VPN）的形式进行加密通信。VPN可以有多种形式，例如站点到站点，它适用于变电站和控制中心之间，或者可能适用于单元到单元的通信。远程访问控制可以在更特殊的情况下建立，并利用基于浏览器的VPN和基于安全套接字层（SSL）的VPN的便利性。如果延迟问题不是特别严重，可以使用媒体访问控制安全性（MACSec）逐跳加密来允许潜在的控制和关键节点的可见性。

下一个发现阶段应该与网络上资产的软件和配置保持一致。此时，网络管理员的权限和角色可能不足以访问所需的信息。当然，网络基础设施及其状态在网络管理员的监控范围内，但是单个资产可能不在其中。在这一点上，组织合作是成功的必要条件。对于一个经验丰富的IT网络从业人员来说，这种情况并不少见。特别是在大型企业中，通信、传输和连接它们的资产之间存在责任和控制分离，这是非常普通的。在运营层面，也需要与负责管理OT资产的人员进行类似的合作。

有合理的信息来源描述OT资产的配置状态。与流程相关联的控制系统保存历史数据，这些数据描述了连接的内容和那些资产正在做什么。对历史数据的回顾应该提供关于存在哪些资产以及对它们执行哪些操作的概念，并且应该识别固件更新和运行状况等内容。要分析的

大量数据可能具有挑战性，但如果数据组织正确，它将对理解资产操作有价值。

完成初始资产清单后，我们可以根据网络和资产启动风险分析，并确定安全需求的初始范围。

8.5.2 部署专用的安全设备

下一个阶段是使用集中的安全功能扩展安全足迹。目标是为网络内的流量提供可视化、安全性和保密性。可视化提供了对应用程序和通信行为的理解。通过可视化，我们可以设置反映区域间和管道安全性所需行为的策略操作。

虽然网络元素可以提供具有连接历史或某种流数据的简化视图，但是当查看网络上的数据包时，我们会真正理解其中的原理。这种程度的可视化通常是通过深度包检查（DPI）技术实现的，比如入侵检测/预防系统（IDS/IPS）。这些技术可以用来检测多种感兴趣的流量，从简单地识别应用程序在做什么、通信是否被混淆、漏洞利用是否针对具体漏洞，到被动地识别网络上的资产。

以识别资产为目标，IDS/IPS可以检测网络上存在什么类型的资产。被动操作系统识别程序可以捕获暴露在网络上通信的基本操作系统和其他应用程序的模式。捕获的MAC地址中的组织唯一标识符（OUI）可能来自ARP表探查，这是另一种可视方式。结合前面提到的物理和历史数据，这是一种有价值的工具，可以在无须危险地侵入关键系统的情况下扩展资产。

特定于应用程序的协议也可以被IDS/IPS系统检测到。对于更类似于IT的应用程序，用户代理是有价值的，但是传统上，端口号和其他协议区分符的组合有助于识别用户代理。有些应用程序的行为只能在某些软件版本中找到。了解这些差异有助于确定在特定资产上运行的软件版本。

在应用程序和工业协议中有明确定义的命令，通常还有相关的参数值。同样，可以配置IDS/IPS来识别这些命令和值，以了解正在执行的操作以及正在更改的相关设置。

所有这些操作都可以在非介入式部署场景中完成。现代的DPI实现可以在带外工作。查看数据包副本不会影响流量性能或延迟。它很容易成为深入了解网络上发生的活动的最安全的方法。

可视化和对网络连接的理解揭示了发起访问控制活动所需的信息。访问控制通常是通过访问控制列表（ACL）实现的，几乎所有现代网络设备都可以使用访问控制列表。但是，为了提高可扩展性，最好使用专用的防火墙。提供强大的分割和区域访问控制是第一步。然而，访问控制不仅限于典型的地址和协议标识符。现代防火墙能够识别与访问网络的用户相关的属性，从而允许对“who”元素进行控制。此外，访问控制可以与应用程序和应用程序行为保持一致。有了正确的工具集，现代的OT人员可以确保只有特定用户类中的操作符才能对特定资产启动任何外部命令。

安全性是一个特别的优点，因为可以通过IDS/IPS在单元/区域边缘管理应用程序控件。用于观察的技术也可以人为地确定传递给目标资产的值。例如，在一个由机器人进行操作的制造场景中，可能有一个区域是机器人潜在操作范围内的工人经常光顾的。这个范围对于单元的物理布局是唯一的，参数的变化可能会对工厂工人造成物理伤害。使用IDS/IPS，系统可以检测到参数值超出安全范围，并采取一致的行动以确保工人的安全。

安全性和保密性在语言学上是紧密相关的，但是对于安全从业人员来说，安全性通常与威胁联系在一起。威胁识别和保护是基于DPI的IPS的关键属性。

成熟的IPS有数千个威胁标识符，它们处理已知可远程利用漏洞的所有资产类型。在某些情况下，威胁标识符的性质是通用的，可以作为一种通用技术，而不必与漏洞类型的特定应用程序实例相关联。

专用安全设备的放置优先级根据安全从业人员对风险的感知而不同。如果可视化是不完整的，并且考虑到在创建主动防御之前需要进一步的知识，则应该将安全设备放置在感知到这个差距的地方。需要注意的是，获得可视化或处理风险的过程是动态的。网络会改变，随着知识的积累，新的优先级（以可见的威胁或缩小差距的形式）会产生新的重点。由于这种动态性，专用安全设备的位置也可以更改。换句话说，在一个位置启动设备后，在后续也可以移动它来解决安全漏洞。

我们必须做出决定，这不可避免。在这里，我们讨论了不同位置的相对优点。部署在操作单元可能是最细粒度的部署场景。我们所说的细粒度指的是网络的最底层部分，它使基于网络的访问达到最低级别的操作资产。正如前面所讨论的，带外或在线部署的性质取决于组织对在线操作的通畅程度和实际实施控制的愿望。在任何一种情况下，工业安全设备都应该直接连接到交换机，该交换机表示进入单元的接入点。该位置为安全控制、可视化和威胁提供了最高级别的控制。如果网络设计已经正确地分割为单个区域入口点，那么这就是一个最佳部署位置。出于安全考虑，可以施加应用程序控制，以确保应用程序更改不允许危险设置。当威胁经过设备时，可以减轻威胁，并且可以使进出单元的流程可见。

如果安全设备除了执行深包检查外，还可以终止VPN，则会启用一个特别有价值的功能。安全的通信（可能来自组织外部的供应商代表）可以在进入设备时终止，然后进行检查。终止的时间成本将与在交换机上所做的工作类似，然后检查访问网络的远程用户正在进行的操作是否可行。当然，任何潜在的威胁流量也可以停止。

如果需要区域/单元容纳关键的基础设施并且进行远程操作，则建议对网络和安全基础设施进行一致的高可用性配置。

出于纯可视化的目的，最好将镜像或镜像端口挂载在交换机上。控制功能必须在线才能真正对不期望的流量采取行动。在大多数情况下，首选位置位于汇聚层和区域交换机之间的区域/单元接入交换机的上游。在区域资产和区域接入交换机之间也可以使用安全设备。

对于更广泛、更详细的控制级别，将专用安全设备放置在汇聚交换机上游是首选方法。如果网络中有多个区域通过汇聚交换机，其中大部分是冗余功能，但它们之间没有通信，则这可能是一个更有效的部署点。

在某一时刻，最低区域层之上的功能层将连接到网络，在这些功能及其区域/单元的OT之间应该有一个设备。在下一层，可能有HMI或其他较低级别的操作工具。出于安全考虑，该层与单元之间的控制点非常重要。

在网络的较高级别上有大量功能更强大的资产，比如标准的网络设备（例如，目录服务器、网络监控工具、远程访问和代理服务器、打印服务器、安全控制设备）。更侧重于操作的功能包括工程工作站和操作控制应用程序等设备。根据运行过程的多样性和网络拓扑，这些运营结构可以在相同级别的其专属子区域（子网）内复制。根据控制访问的需要，可能有理由在子区域之间使用专用的安全设备，但在大多数情况下，这是一个需要上面和下面放置控件的区域。

以下是更需要工业意识和硬件加固的地方。由于有一定数量的工业通信流通过这一层，建议使用专用的安全工具。

在这个最高级别之上，建议使用一个具有以IT为中心的威胁控制功能的专用安全设备。如果这里承载的应用程序在本质上与IT环境中的应用程序（例如，基于Windows或Linux的应用程序）相似，则需要公共网络基础设施、基于Web的访问等来实现适当的可见性、控制和保护。对所有入口点（上面和下面）应用这样的控制是很重要的。不应该假设以IT为中心的威胁只能来自DMZ之上的IT/企业层。攻击者不会局限于这种想法。

有证据表明报废的操作系统和软件组件存在于操作环境中。此类系统最常见和最不幸的一个特性是，可能无法进一步修补安全漏洞。为了在正式的支持日期结束之后保护这些系统，我们引入了虚拟补丁层的概念。其思想是，可以通过这些系统通信的网络路径来应用漏洞

保护。虽然这并不能代替及时修补，但它可能是一种适合组织的风险接受策略的缓解方法。

操作空间的逻辑边界是DMZ（非军事区），这是两个不同的计算领域之间的安全边界。该领域的设备旨在以一种安全的方式在企业IT领域和工业OT领域之间架起沟通的桥梁。安全性应该同时应用于这一层之上和之下。

在我们结束运营安全的第二阶段之前，必须再次强调，无论在什么位置，安全都是一个持续的过程。应用的策略和获得的知识不应停滞不前。情况将不可避免地发生变化，因此安全部署（甚至是网络本身）必须发生改变以适应变化。无论将安全执行设备和它们采用的策略部署在何处，必须随时准备对它们进行更改。

8.5.3 高阶策略收敛和网络监控

到目前为止，我们关注的都是非常基本的概念，这些概念很常见，并且很容易由网络工程小组实现。找到有相应经验的网络专业人员甚至培训没有经验的人并不困难。

另一种为网络工业空间增加价值的安全实践是融合，即跨运营边界采用和集成安全措施。这意味着协调组织的IT和OT双方的安全性。IT和OT空间的收敛正在合并，或者至少在以前截然不同的IT和OT边界之间有积极的协调。从安全的角度来看，这个遵循了这样一个观点，即大多数进入运营空间的新网络和计算技术都是在IT空间中发现和建立的。与这些新技术相关的实践和工具很可能在IT领域更加成熟。

企业范围内的高级实践与访问控制、威胁检测和许多其他可能有益于OT安全性的安全机制相关。如前所述，关键是调整方法以适应目标环境。

有些领域更可能需要某种跨IT和OT环境的协调。其中两个领域是远程访问和威胁检测。对于远程访问，大多数大型工业组织通过IT网

络回程传输通信。有些通信（如电子邮件和Web浏览）是很明显的通信类型，可能会涉及共享IT基础设施。通常，需要对OT资产进行某种远程访问的供应商或顾问也会遍历网络的IT端。有鉴于此，OT安全从业者跨越面向Internet的安全层，通过核心网络，协调从远程启动器到工业界的切换点，再到更深层次物联网资产在内的访问控制策略，将具有重要的价值。使用通用的访问控制和操作配置在更大程度上简化和保护网络设备，而不是由不同的组织创建特定的方法。使用位置信息、参与设备的安全姿态、用户标识和访问目标属性都是现代访问策略工具可以使用的标准功能。这种复杂性在工业环境中是一种相对较新的实践，因此，如果这些功能可用，OT安全从业人员将从与IT从业人员的协调中获益。

网络安全监控（NSM）是一个发现网络入侵者的过程。它通过收集和分析指标和警告来确定事件的优先级并进行调查，前提是事实上存在不希望出现的事件。

NSM的实践并不新鲜，但即使在相当成熟的大型组织中，它的实施也不够频繁或彻底。造成这种不充分利用的原因有很多，但缺乏教育和组织耐心是常见的原因。为了简化这种方法，有大量现成可用的数据，如果检查这些数据，就会暴露入侵者的活动。

需要注意的是，NSM本质上是一个通过审查已经发生的证据和行为来发现的过程。这并不意味着这是一个纯粹的事后分析行为。如果我们认识到入侵活动与安全性非常类似，是一个持续的过程，那么我们将看到攻击者必须经历一系列类似的阶段。部署的工具将减慢这个过程，并创造检测和阻止攻击者的机会，但是很少有单个事件表示整个攻击。NSM是最有可能发现攻击过程的范围并进而定义其补救范围的学科。

8.6 小结

随着各个行业为了追求运营效率、提高安全性和竞争能力而进行现代化，它们必须确保在现代化的进程中足够安全。现代化进程通常在旧的和高度脆弱的OT资产和过程中启动更大的连通性。安全性是必须在整个变更和操作的整个生命周期中应用的进程。为了实现安全性，组织必须能够定义风险，并对如何最好地解决风险做出明智的选择。

幸运的是，将威胁带来的风险降到最低的许多方法都是现成可用的。使用正确的设备和策略可以确保网络连接的安全性。通过专用的工业安全设备和做法，可以识别和控制来自不安全实践、攻击和远程访问需求的威胁。随着时间的推移，存在着通过趋同和合作来扩大降低风险的机会。学习IT环境中更广泛和成熟的安全实践和工具，以及协调防御层以保护关键工业资产，是运营环境的关键安全促进因素。

第9章 制造业

每个行业的商业需求时刻都在发生变化，制造业也不例外。对制造商来说，控制成本和提高效率一直都很重要，但随着行业模式的变化和竞争的加剧，现在的主要焦点正转向创新和改进的商业模式。在数十年的生产系统和供应链成本挤压之后，制造商认识到，进一步的成本控制可能只会阻碍客户服务，并为竞争打开大门。

在数字化和物联网的推动下，这些经济变化正引发制造业的大规模颠覆。本章将探讨这些颠覆性的力量，并探讨用于数字化工厂和连接机器的创新架构。本章包括以下内容。

■ **互联制造业简介：**从研究导致数字化颠覆的技术开始，讨论了互联工厂的策略以及对制造商的业务利益。

■ **互联工厂的体系结构：**借助以太网和IP，工业自动化和控制系统（IACS）网络技术正在融合。本节将探讨一个互联工厂框架，重点介绍由Cisco和Rockwell公司联合开发的Converged Plantwide Ethernet（CPwE）体系结构。

■ **工业自动化控制协议：**本节将讨论制造业中使用的各种网络和控制协议，包括以太网/IP、PROFINET和Modbus/TCP。

■ **互联工厂的安全：**本节将探讨互联工厂中的关键安全考虑事项，以及如何使用正确的设计方法来解决这些问题。

■ **互联工厂的边缘计算：**互联机器产生的数据量是巨大的。本节研究如何在互联工厂中实现边缘计算，以改进数据管理和可见性。

9.1 互联制造业简介

在最近一项对400多名制造企业领导者的SCM World调查中，约80%的参与者表示，他们最大的挑战是满足客户交付日期和对未预见事件的响应。图9-1显示了本次调查的结果。

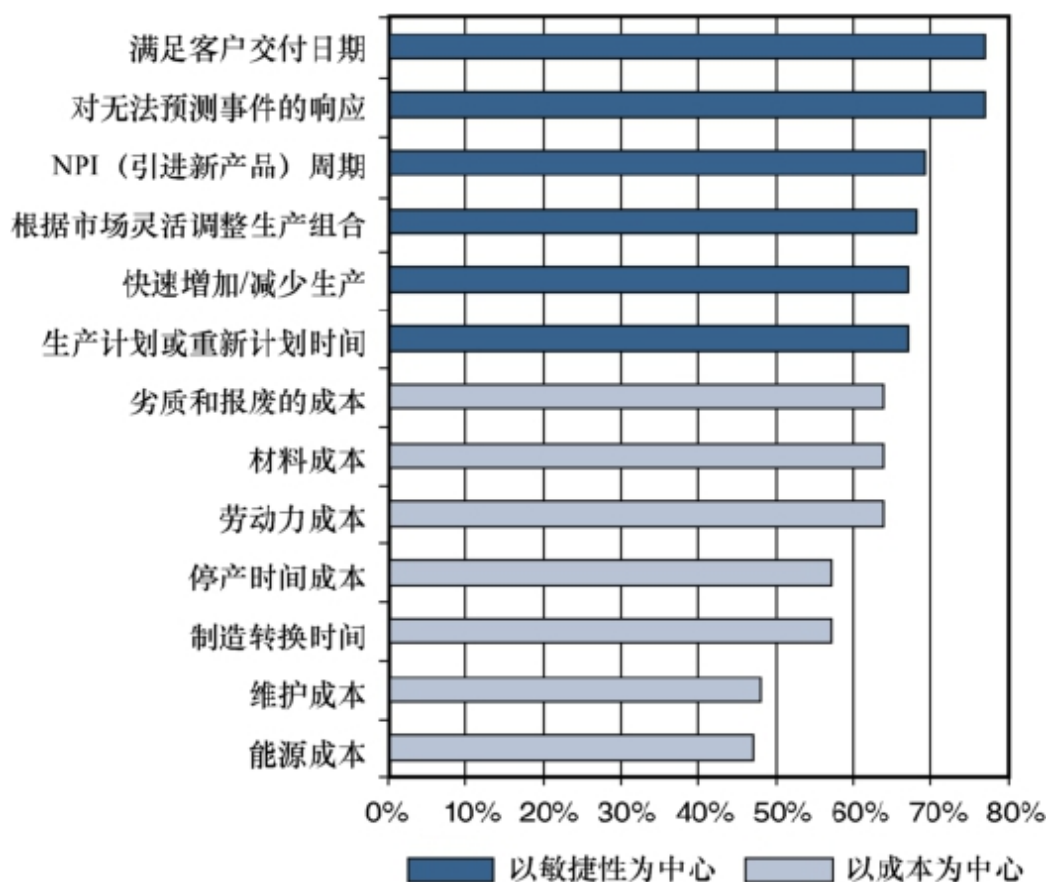


图9-1 将关注点从成本转移到敏捷性

在充满活力的经济环境中，制造商认识到有必要迅速扭转项目的颓势，需要能够根据市场需求迅速扩大、调配和调整生产能力。然而，在经济波动和长周期的资产投资的影响下，制造商往往使用着老化的生产设施，这阻碍和降低了它们的灵活性。例如，据估计，美国自动化基础设施的平均使用年限是自1938年以来最长的。美国近75%的工厂的运行时间已经超过了20年。世界各地的工厂都面临着类似的挑战：它们老化的资产不仅减缓了创新，而且计划外停工还造成了数十亿美元的损失。

将以前未连接的机器连接到智能数据系统，进而使用机器生成的数据以更高效的方式更好地利用现有投资，被视为工厂现代化的唾手

可得的成果。摆在制造商面前的机会是巨大的。据估计，全世界有6000万台机器，其中90%没有联网，绝大多数机器的使用年限都在15年以上。把这些机器连接起来，并更好地利用它们产生的数据，这变得越来越紧迫。

数字化颠覆制造业的核心是与物联网相关的技术。

■ **数据驱动的制造业：**大数据正在改变制造业的面貌。制造商希望访问从机器生成的所有数据，以实时监控质量控制，提高整体设备效率（OEE），并减少计划外停机。OEE是一个用于衡量制造业生产率的著名指标。制造商还在探索使用这些数据的方法，以便在市场波动或其他需求发生时支持快速的工具更新。

■ **OT和IT收敛：**在工厂的物联网环境中，运营技术由可编程逻辑控制器（PLC）、计算机和其他技术组成，这些技术通常与IT中使用的技术类似，但由IT外部的业务运营商运营和拥有。IP网络使机器和工厂之间的集成更加紧密，而工厂网络和企业网络之间的界线正变得越来越模糊。制造商正在超越传统的束缚，寻找将其业务整合到单一网络基础设施下的方法（有关OT和IT聚合的更多信息，请参见第1章）。

■ **以更低的成本改进技术：**新技术为规模化、自动化和基于平台的机器连接、监控和优化创造了条件。在这种不断发展的技术状态下，机器操作可以看作是一个完全连接的网络系统的一部分，而不是一个独立的系统。计算、交换、路由和安全性的融合有可能降低连接机器的成本。

■ **机械制造OEM专注于新的优先事项：**原始设备制造商（OEM）正面临着新的基于云的供应商的破坏，这些供应商打算提供“机器即服务”（MaaS），通过从云端进行零接触部署，机器可以快速部署到工厂车间，从而提供对这些机器的远程连接和监控。这产生了一个新的焦点，即提供更好的客户体验，并强调售后产品和服务。制造商正在寻求接近100%的正常运行时间和零接触部署。它们还在探索通过远程连接和监控来控制支持成本的方法。

9.1.1 互联制造的物联网战略

制造商如何应对互联工厂的挑战？为了实现敏捷性和大规模定制，需要对由于数十年的成本控制而老化的工厂进行技术上的重大改进。数字转型需要依赖于关键的信息技术进步，其中许多已经被证明和广泛应用于其他行业。

也许制造业最重要的趋势是软件的普及。软件和硬件之间的界线正在日益消失。许多以前在我们日常生活中需要硬件实现的事情现在可以用软件来实现。记得电话答录机吗？它是带有微型盒式磁带的小型录音盒，现在作为软件存在于智能手机或服务提供商托管的云端服务器中。同样的情况也发生在工业环境中，越来越多的物理控制现在作为软件存在于人机界面（HMI）中。在一些工厂中，仅存的物理控制是紧急停止按钮。软件相对于硬件的优势在于，新功能和软件补丁管理起来更简单，成本更低。

我们现在进入了这样一个世界：机器制造商只需向机器发送一个软件更新，就可以远程排除和修复导致意外停机的机器。此外，利用人工智能（AI），机器现在能够自我诊断问题。在中断发生前几天，问题就会暴露出来，在计划的维护窗口期间，机器通过软件更新进行自我修复。通用电气（General Electric）首席执行官Jeff Immelt表示，如果你昨晚睡觉时还是一家工业企业，那么今天醒来时将是一家软件和分析公司。

软件分析在提高敏捷性和效率方面也发挥着重要作用。制造商需要全面了解关键绩效指标（KPI），这些指标统一了车间、企业和整个供应链的活动。这种实时数据收集和分析是领导制造商物联网计划的主要重点。

最近一项针对制造业高管的研究是，要求他们对阻止实现物联网和数字制造目标的障碍进行排名。前三个障碍与缺乏对机器、车间和供应链的数据和数据访问的可见性有关。图9-2显示了该调查的完整结果。

有人描述了未来的制造业，工厂将不再需要任何人，而且会“熄灯”。在这些工厂中，机器人和人工智能系统将完全实现生产功能的自动化。所有机器将能够自我诊断和自我修复。无处不在的分析将能够提供对生产过程和整个供应链所有方面的实时可见性。所有这些都将通过软件和基于以太网的互联工厂基础设施来实现。我们可能还需要几年时间才能实现这一愿景，但是技术基础已经存在，并且现在已经开始部署到离散的制造环境中。

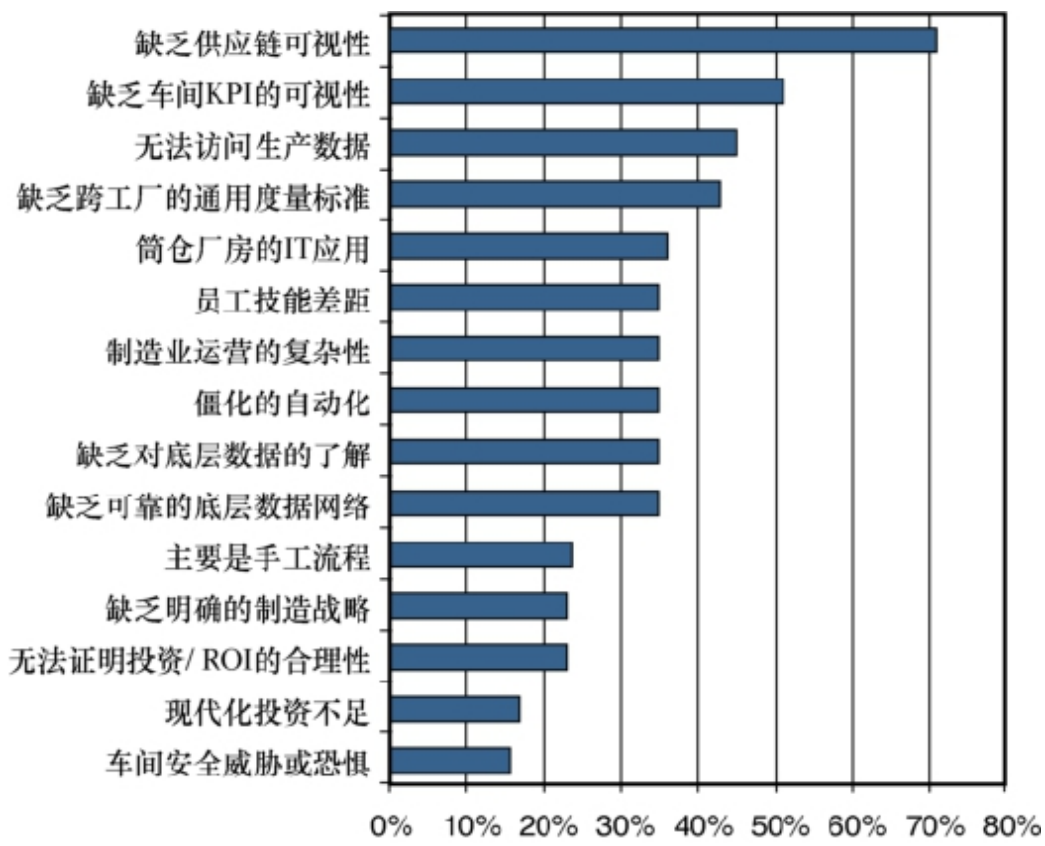


图9-2 与信息可见性相关的主要障碍

注释：制造业通常分为两类：离散制造和过程制造。离散制造是指生产不同的产品，如计算机、钓竿和手工工具。过程制造是指大批量生产的产品，如食品、水泥和化学品。

9.1.2 通过物联网推动业务改进

令制造商鼓舞的消息是，尽管技术和商业模式正在发生巨大变化，IT和OT生产网络的融合不可避免，但是将业务流程改进和质量工作作为重点的相同衡量标准如今仍然适用于物联网和数字制造计划。

注释：“六西格玛”方法是制造业追求质量的一个例子。“六西格玛”是一组数据驱动的制造技术，用于减少缺陷。该名称取自将任何流程的平均值与最接近的规范限值之间的偏差限制在6个以内的目标，目标是在99.99966%的时间内实现无缺陷产品。这种方法最初是由摩托罗拉的工程师比尔·史密斯提出的，后来成为通用电气首席执行官杰克·韦尔奇关注的焦点。如今“六西格玛”是一套用于持续质量改进的工具和方法。

随着与工厂和整个企业内资产的连接性的改善、可见性的提高，制造商期望在关键的制造指标上有显著改进。改进包括减少计划外停机时间、提升质量和改进OEE。

有这样一个案例：一家领先的机器人制造商为一家领先的汽车制造商实现了实时数据分析和预测维护应用程序，完全避免了数千个机器人的计划外停机。这为制造商在短短几周内减免了大约4000万美元的停机损失。这些事例使人们对制造业数字化转型的可能性抱有更高的期望。

9.2 互联工厂的体系结构

过去，传统的工厂网络是临时部署的。它们被隔离在企业IT网络之外。此外，工厂中的网络安全通常仅限于工业DMZ，这使得机器基本上不受保护。工厂很少部署包含身份策略和安全远程访问工具的网络级安全系统，这些工具允许将工厂级数据安全地扩展到云端。这种情况正在发生改变。企业开始将其工业自动化和控制系统（IACS）与IT应用程序和分析工具结合起来，以提供控制和分析功能，从而产生运营和业务效益。

CPwE是一个架构框架，它为IACS设备和设备提供网络服务，并促进安全集成到企业网络中。在详细讨论CPwE框架之前，定义几个关键

术语并回顾IACS参考模型非常重要，CPwE充分利用了IACS参考模型。

9.2.1 工业自动化与控制系统参考（IACS）模型

几十年来，制造商依赖于许多不同类型的技术来实现工厂内的通信。这些协议通常依赖于特定于供应商的专有通信协议，而这些协议反过来又需要专门构建并且特定应用于供应商的专用网络。

如今，以太网和IP已经成为IACS通信系统的标准。IACS参考模型使用一个逻辑框架来描述制造系统的网络和安全功能。根据20世纪90年代由普渡大学计算机集成制造联盟（Purdue University Consortium for Computer Integrated Manufacturing）开发的普渡控制层次模型（Purdue Model for Control Hierarchy），制造业将设备划分为不同层次的功能。第8章讨论了控制层次结构的普渡模型。国际自动化协会（ISA99）制造和控制系统安全委员会（现为IEC-26443）已经确定了基于这个层次结构的制造逻辑框架，如图9-3所示。

企业区域	企业网络	第5级
	现场业务规划及物流网络	第4级
非军事区	非军事区——共享访问	
制造区域	现场生产运营和控制	第3级
单元/区域	区域控制	第2级
	基本控制	第1级
	过程	第0级

图9-3 基于普渡模型的ISA99 / IEC-62443 IACS逻辑框架

IACS逻辑框架标识了制造工厂的功能区和级别，并定义了每个级别的操作（注意这里使用的命名是级别，而不是层，以避免与协议栈模型混淆，比如OSI模型）。这些区域的定义如下。

■ **安全区：**安全区中的系统通常与IACS网络进行硬连线，并保持独立。该区域的安全系统的功能是在紧急情况下提供IACS关机功能（停止按钮）。可以将此视为硬连线故障保险，用于在发生危险事件时保护人员和设备。

■ **制造区域：**制造区域由单元/区域（第0~2级）和现场级制造（第3级）活动组成。制造区域很重要，因为所有对监视和控制工厂IACS操作至关重要的IACS应用程序、设备和控制器都在这里。为了支持工厂安全运营和IACS应用程序的运行，在制造区域和企业区域（第4级和第5级）之间有一个安全的分隔。

■ **单元/区域：**单元/区域是工厂内的机器区域。在一个工厂中通常有多个单元/区域。例如，在电子工厂中，可能有一个单元/区域是组装过程区域。单元/区域可能只由一个控制器和相关设备组成，也可能由大型装配线上的多个控制器组成。事实上，一个工厂可能有许多单元/区域。对于CPwE体系结构而言，单元/区域是一组IACS设备和控制器，它们参与制造过程的功能方面的实时控制。为了控制功能流程，IACS设备需要与其他IACS设备进行实时通信，这意味着连接它们的网络需要快速可靠。这个区域基本上有3个活动级别。

■ **第0级：过程。**第0级是制造物联网中的“物”级，由参与制造流程的传感器和执行器组成。这些物联网设备执行IACS功能，如移动制造机器人、喷涂、驱动电机和焊接。这些设备与第1级中的基本控制设备通信。

■ **第1级：基本控制。**第1级是控制制造过程的控制器所在的位置。这些控制器与第0级物联网设备交互。在离散制造中，控制器通常是PLC，在过程制造中称为分布式控制系统（DCS）。

■ 第2级：区域控制。第2级包括单元/区域内需要运行时监控和操作的功能。例如HMI、警报和控制工作站。

图9-4说明了0~2级设备的类型和相应的接口。

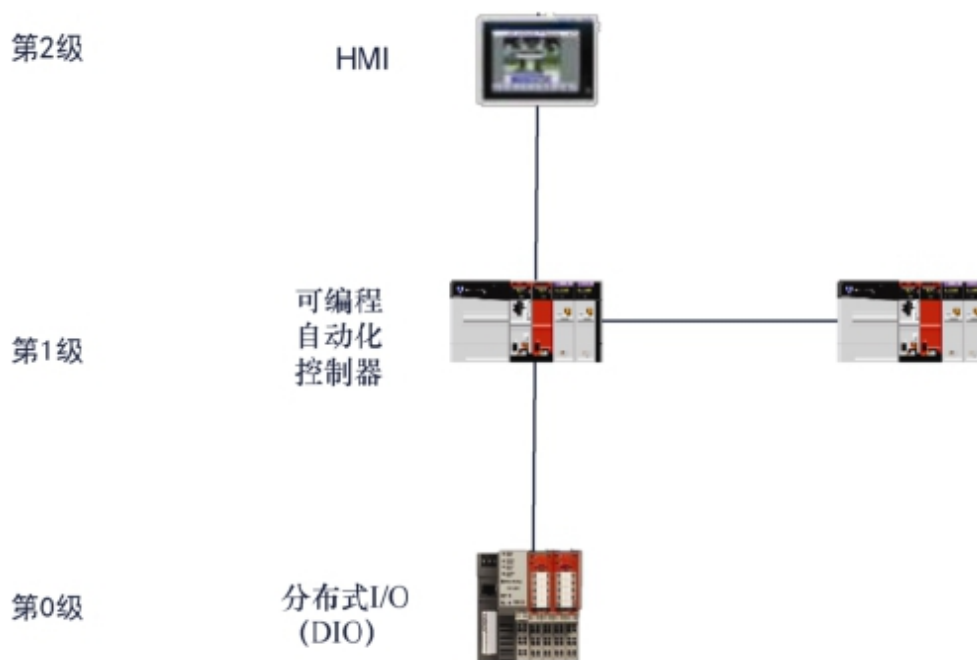


图9-4 IACS控制器信息流

■ 第3级：现场级。第3级应用程序和功能包括SCADA系统、文件服务器、控制室工作站、调度系统和报告系统。注意，该级别不是单元/区域的子集，而是更大的制造区域的一部分。

■ 非军事区（DMZ）：DMZ是工厂运营网络与传统网络之间的CPwE划分。DMZ安全对工厂运营至关重要，因为它保护较低级别的机器免受可能发生在传统企业网络中的恶意活动的攻击。

■ 企业区域：企业区域中的第4级和第5级与传统的IT/企业网络功能相关，包括文件服务、Internet连接和电子邮件系统。

9.2.2 CPwE参考模型

随着制造业对工业应用以太网的接受，利用以太网和TCP/IP的通信协议应运而生。为了应对这一趋势，Cisco和Rockwell公司开始共同开发Converged Plantwide Ethernet (CPwE) 参考模型，该模型主要关注以太网/IP的传输（本章稍后讨论）。

CPwE解决方案旨在使IACS应用程序能够与企业IT系统聚合。图9-5展示了整个CPwE网络体系结构。在这个框架中，单元/区域包含从第0级到第2级的IACS设备。该框架中的设备，如HMI和控制器，属于一个单元/区域网络。HMI就是人机之间的接口。在CPwE体系结构中，IACS设备与以太网/IP通信，并使用以太网实时控制整个单元/区域的流量。CPwE以太网有多种拓扑结构，包括冗余星型、总线/星型和环型。本章稍后将更详细地讨论CPwE拓扑及其使用的冗余技术。

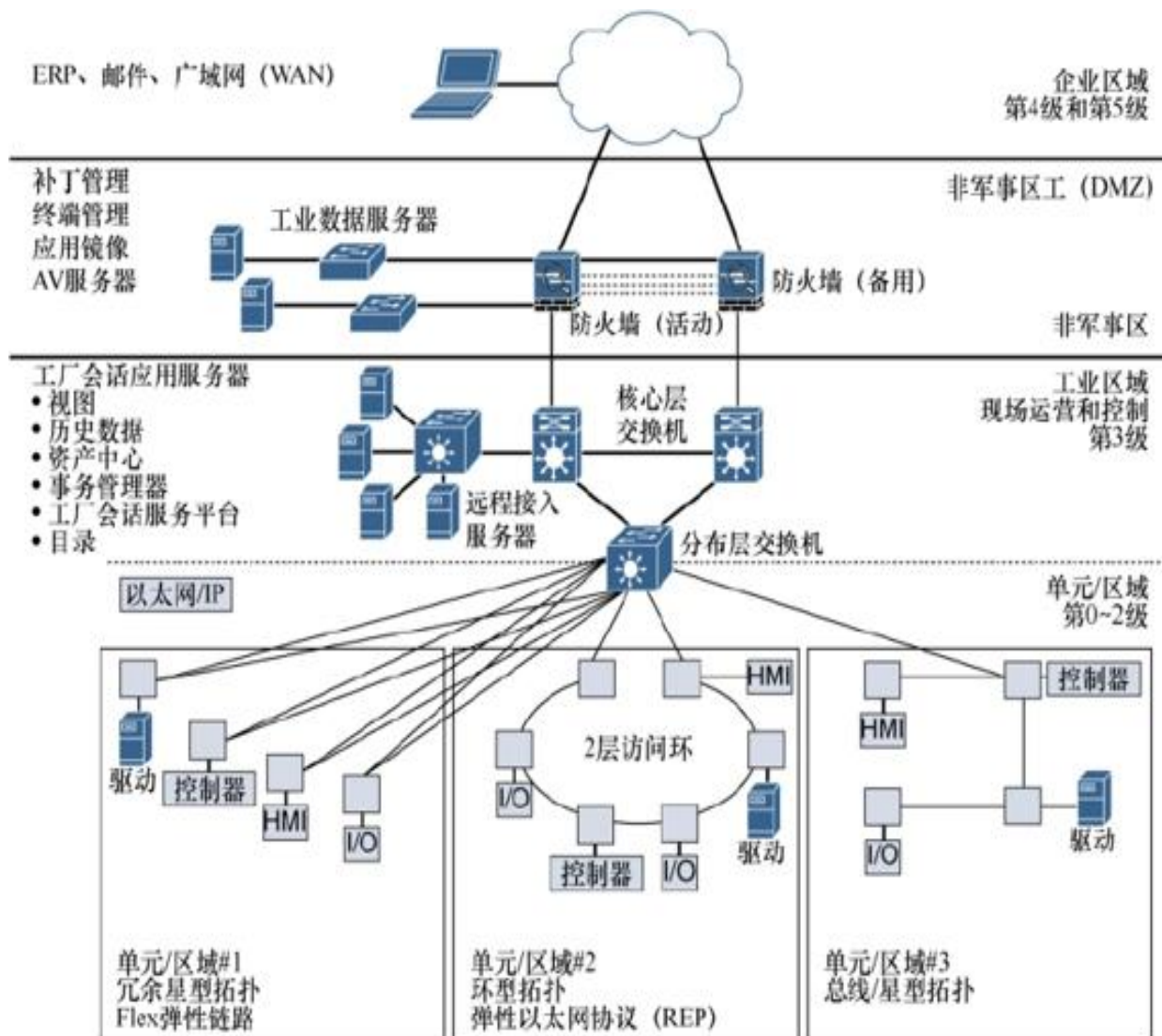


图9-5 CPwE体系结构的高级视图：使用3种不同的单元/区域以太网拓扑

单元/区域内的以太网基础设施设备主要是工业级接入交换机，它们坚固耐用，无风扇，能够抵抗静电，并支持较大的温度范围。在图9-5中，单元/区域与工业区域之间的分配交换机形成一个分界点。因为这些分配交换机与单元/区域中的接入交换机连接到同一以太网段，所以它们也被认为是单元/区域基础设施设备，通常需要加固设备。分布层交换机也是第2级和第3级之间的分界点。

工业区域类似于IACS参考模型的3级，也非常类似于传统的园区网。大多数工厂只有一个工业区域。与大多数园区网一样，工业区域集成了用于工厂IT运营和员工服务的接入交换机，并包含核心网络功

能。工业区域根据需要通过路由分布层交换机提供到多个单元/区域的网络连接。工业区域还支持需要3级应用程序支持的IACS设备的IP路由功能。

非军事区（DMZ）位于工业和企业区域之间，用于安全地管理相邻区域网络之间的流量。这也是工厂防火墙通常用来控制进出工厂网络的流量的地方。

9.2.3 CPwE弹性网络设计

由于IACS网络中敏感的控制器和应用的要求，在单元/区域内，IACS设备之间的网络弹性是一个强制性要求。弹性IACS网络需要支持以下功能。

■ 可用性：在支持IACS应用程序正常运行时间和业务连续性方面，LAN拓扑的设计至关重要。IACS应用程序对局域网的设计有严格的要求，包括网络可用性、性能和设备之间的距离。对于正常运行时间至关重要的关键操作，应该选择IACS以太网拓扑结构中的完全冗余物理路径。

■ 可预测的性能：满足可预测的、可靠的、实时的IACS应用程序流量需求是成功部署CPwE的必要条件。

■ 网络能快速地重新汇聚：当设备或链路发生故障时，网络的恢复时间必须最小化，以免其他IACS设备受到故障的影响。典型的IACS应用程序中断容错限制大约在100 ms以内，并且具有最小的抖动。

■ 支持工业协议：CPwE IACS设备和网络设备需要支持工业应用协议需求。

以下是需要网络弹性的通信模式的示例。

■ 控制器到人机界面。

- 控制器到控制器。
- 控制器到输入/输出端口（I/O；机器传感器和控制器模块）。
- 控制器到变频驱动器（VFD；控制电机的可调节机电驱动器）。
- 控制器到电机控制中心（MCC；在工厂中用来通过一个中央控制器控制大量的电动机）。

如图9-5所示，可以在单元/区域中使用几种不同的以太网拓扑，但是在所有情况下，区域内以太网段的高可用性都是必需的。根据所实现的以太网拓扑，可以使用不同的高可用性技术来实现应用程序的连续性。例如，在一个简单的冗余星型拓扑中，诸如Flex链路或交叉堆叠以太通道等网络弹性技术非常流行。Flex链路有两个上行链路，其中一个活动的，另一个是备用的。如果活动链路由于某种原因失败，则由备份链路接管。

在EtherChannel中，两个上行链路同时使用，两个链路之间的流量是负载均衡的。如果其中一个发生故障，另一个仍处于活动状态，但可用上行带宽只有一半。

我们来看如何使用CPwE模型来改进世界上一家最大的摩托车制造商的制造系统的例子。该公司每个班次都要生产数百辆摩托车，但由于在支持不同车辆的配置时比较复杂，它面临着重大的制造挑战，公司的主要目标是提高制造过程的敏捷性，CPwE能够解决这个问题，方法是通过以太网将机器数据引入中央仪表板。这种方法允许公司对整个工厂的数据进行整理，从而使工厂能够更好地响应情况，并最终极大地减少机器停机时间。

将新机器快速联网并将它们连接到以太网网络的能力带来了更大的灵活性，并显著减少了新模型和新产品的引入，从而缩短了产品的整体上市时间。

1. 弹性以太网协议（REP）

在CPwE参考体系结构中，在单元/区域使用弹性以太网协议（REP）来实现对环型拓扑的高速保护。

与在IEEE 802.1D中标准化的生成树协议（STP）及其支持高速聚合的后续版本相似，REP控制连接到以太网段的一组端口，以确保不存在桥接环路，并且以太网段能够响应拓扑变化。当在光纤基础设施上使用时，REP能够在网段中的链路断开或发生其他拓扑变化（如交换机故障）时实现小于50 ms的聚合时间。REP的另一个关键优势是它不局限于单个以太网段上的少量设备。传统的STP每段只能有7台设备，这个数字很快就会成为工厂的限制因素。相反，REP对于每个段的节点数没有固定的上限，因此支持大的环型拓扑。

对于每个REP段，一台交换机被指定为控制整个环的主节点。主节点需要以下3条关键信息：

- REP控制VLAN的标识，允许REP控制消息在整个网段中进行通信；

- REP段边缘的位置；

- 在正常情况下，将环断开的首选位置，也称为备用端口（如果没有配置任何端口，REP将自动选择备用端口，使决策变得不确定）。

REP段是在以太网段配置了段ID的端口链。当环段中的所有端口都处于活跃状态时，一个端口被确定为备用端口，这意味着它处于阻塞状态，从而防止环成为一个2层桥接环路。如果REP段中的任何其他端口发生故障，则向备用端口发送信号，将状态更改为转发状态，修复损坏的以太网环段，并允许通信继续。

REP使用信号丢失（LOS）检测机制来了解该段上的相邻故障。当交换机端口检测到REP段故障（如光纤中断或物理交换机故障）时，指示链路故障的通知消息被发送到所有其他REP交换机。除了通知备用端

口更改为转发状态外，这些通知消息还指示必须刷新所有交换机的内容可寻址内存（CAM）中的 MAC 地址。这样就形成了一个新的桥接路径。图 9-6和图9-7说明了REP故障通知和修复机制。

注释：尽管目前市场上有许多专用的以太网环保护交换（ERPS）技术（包括REP），但高速 ERPS的标准化工作仍在进行中。这项工作是由G. 8032下的ITU-T领导的。G. 8032与REP有很多相似之处，包括低于50 ms的环保护时间和对多层阶梯拓扑结构的支持。虽然业界现在开始将G. 8032作为高速ERPS的标准，但G. 8032仍然难以满足有限的商业需求。

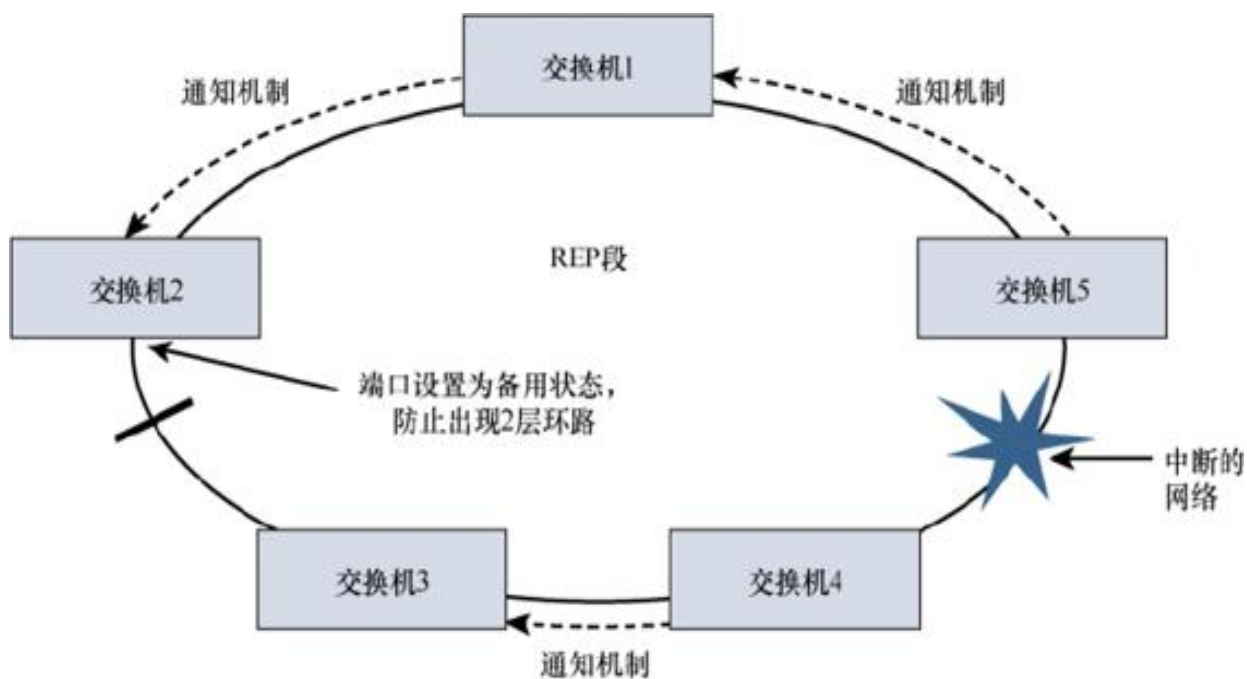


图9-6 当拓扑发生变化时的REP通知



图9-7 REP环段的重新聚合

由于工厂网络的融合推动了制造组织、系统和网络的重大变化，REP在提高应用程序可用性方面发挥了重要作用。在网络中断的情况下，REP网络支持持续的IACS功能并降低停机成本，同时保持生产力和持续运营。部署在REP环境中的应用程序支持多种制造规程，包括批量制造、离散制造、流程制造和混合制造。

2. 聚合网络中弹性的业务价值

设计具有网络弹性的工厂对制造商的业务具有显著的积极影响。越来越多的设备被连接到设备层上。这些设备使用与Internet相同的网络技术进行连接。诸如传感器之类的设备嵌入到收集数据的制造设备中，现在被用作更好地理解复杂过程的工具。如今，当在单元/区域网络设备上的工作需要大量的计划和中断时，弹性网络设计允许单个设备退出服务而不影响单元/区域网络的其余部分。因此，网络更能容忍单点宕机，允许网络升级和维护的灵活性。

基于REP的体系结构增强了生产网络的弹性，以及支持将人员、流程和数据连接到实时应用程序的系统的能力，甚至在网络中断期间也

是如此。在制造业，以太网正在推动新一代联网智能机器的使用，以提高工厂的网络可见度。

9.2.4 CPwE无线

虽然CPwE通常部署在有线以太网访问交换机上，但Plantwide架构越来越多地使用WiFi（IEEE 802.11）来实现关键的IACS应用。这些应用程序与有线以太网应用程序有类似的网络需求，因为它们要求可靠的数据传输和服务质量（QoS）处理，并且关键应用程序的延迟和抖动最小。

CPwE无线网络可用于管理机器、手持设备和自动引导车辆（AGV）。无线带来了灵活性，可以根据需要快速更换生产线或移动资产，而无须进行物理布线。此外，基于位置的标签和传感器如今被用来为在工厂内移动的资产和货物提供可见性。

1. CPwE无线网络架构

WiFi网络在使用共享的无线电频率、易受干扰和覆盖缺陷方面与传统的有线局域网有很大的不同。部署WiFi网络需要周密的规划和设计，以及定期监控，以满足对带宽、QoS处理、吞吐量、可靠性和安全性的期望。最重要的是，工业无线局域网（WLAN）的设计和实现必须满足IACS应用程序的性能要求。

WiFi是一种无线技术，在这种技术中，工作站需要竞争，争取向空中传送帧的机会。这意味着延迟的变化取决于几个因素，包括与AP关联的站点数量、它们发送的流量（包括AP的繁忙程度）和干扰。这可能会给某些对延迟敏感的IACS应用程序带来严重的问题。在控制系统需要可预测延迟的情况下，使用时间敏感网络（TSN）的替代无线技术（如WirelessHART或ISA100.11a）比WiFi更好（这些技术在第4章中讨论过）。这些技术的缺点是它们支持的带宽比WiFi小得多。

如果工厂层选择WiFi，WLAN系统需要根据IACS在工厂内使用WiFi网络的情况进行定制。WLAN应该将IACS集成到更广泛的制造环境中，并且应该考虑广泛的客户端设备类型和应用程序，以及IACS应用程序所需的严格延迟。

图9-8展示了一个使用集中式无线局域网控制器（WLC）来管理分布在整个工厂的AP的架构。通过使用WLC，创建了一个集中式管理模式，从而为无线网络引入了安全和自修复机制。

注释：虽然本章的重点是基于集中式控制器的WLAN，但是CPwE设计和实现指南提供了互联工厂中自主AP部署模型的详细信息。尽管基于控制器的WiFi部署越来越流行，但我们可能会发现许多工厂仍在使用不使用控制器的自主AP。

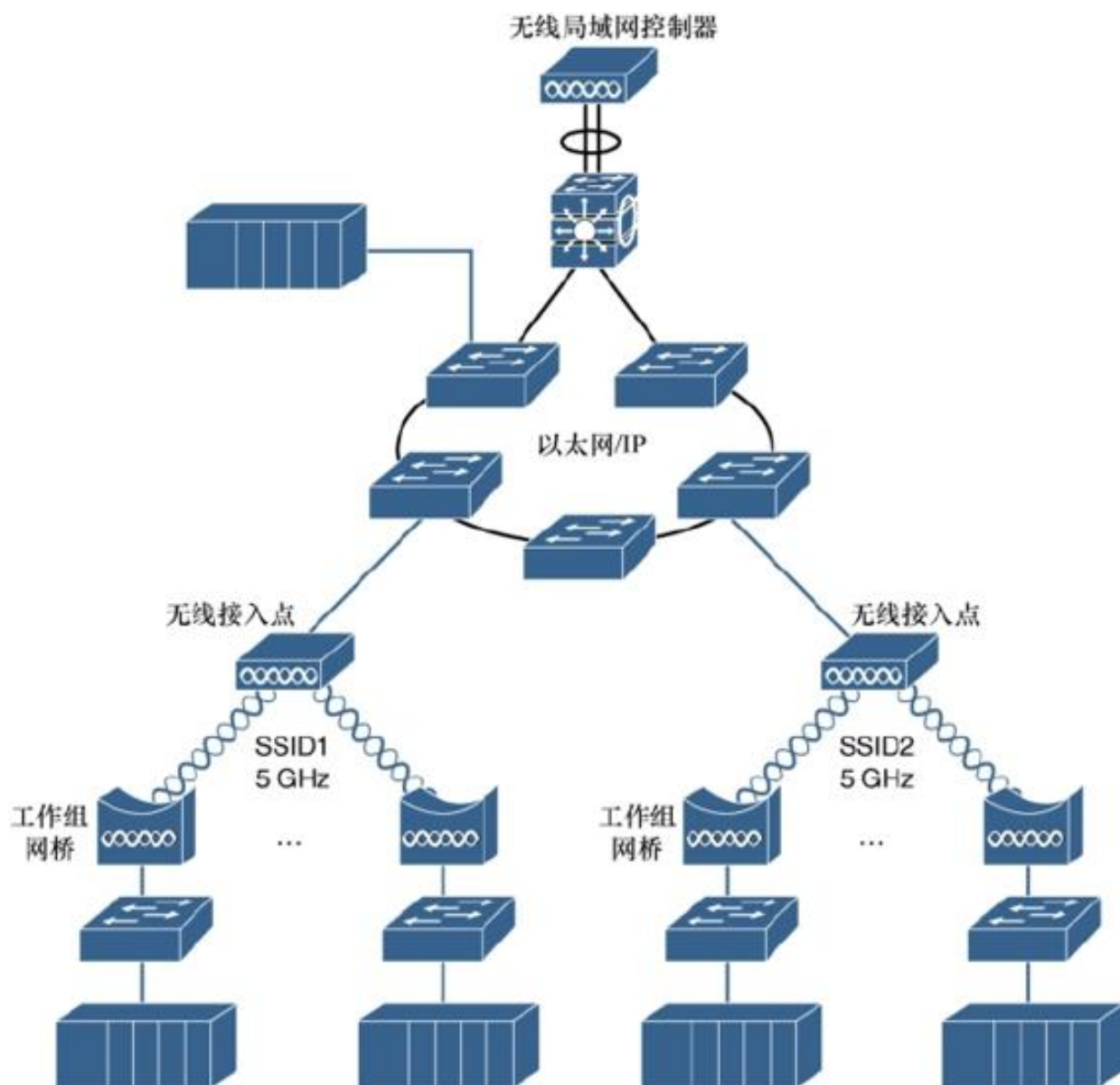


图9-8 一个工厂无线局域网架构

下面是几个在制造环境中使用WiFi的用例。

■ **固定位置设备：**WLAN中的固定位置设备具有永久的工作位置，也称为静态设备。固定位置的无线连接是一种替代有线连接的选择，在难以到达的偏远地区，通常存在安装成本过高或无法安装的情况。使用领域包括过程控制、机器状态监测、固定环境监测和能源工业。在制造环境中，一个常见的用例是需要通过无线链路集成到生产线中的独立原始设备制造商（OEM）机器或设备单元。

■ **移动设备：**移动设备在运行时保持不动，然后在停机状态下移动到新的位置。移动位置后，通常需要建立新的无线连接。例如，设备单元、储存罐、反应器和便携式制造设备。

■ **可操作的重定位设备：**一些移动设备在操作过程中会改变位置，但仍保持在相同的无线覆盖区域。例如旋转平台和唱机转盘、自动存储和检索系统（ASRS）、装配系统、高架起重机以及类似的机器，它们使用无线技术来代替有线解决方案，如感应导轨和滑环。这些应用程序在无线覆盖范围内可能需要无线客户端在位置和方向方面相对于AP发生快速改变。

基于集中式控制器设计原则来部署工厂WiFi网络可以帮助克服许多常见的挑战，包括共享的无线电频率、干扰和覆盖缺陷。无线局域网控制器还允许轻松部署关键技术特性，如QoS、WiFi安全功能和定位服务。

2. 实时位置系统（RTLS）

当工厂的WiFi网络完全到位，并提供了全面的无线覆盖时，它也可以用作RTLS。RTLS解决了工厂中的一个常见问题：管理工厂材料的位置和状态。

基于WiFi的位置跟踪系统通常包括有源电池供电的WiFi射频识别（RFID）标签，这些标签附着在机器、设备单元、车辆或其他设备上，这些设备在工厂内具有一定的移动性。

注意：市场上有各种基于WiFi的位置跟踪系统，这些技术的准确性差异很大。例如，基于RSSI/距离的定位技术需要来自多个接入点的数据来计算设备的位置。RSSI表示接收信号强度指示器，它只是测量传入的无线电波的功率。相比之下，基于WiFi的角度测量（也称为到达角）技术使用单个AP上的一组天线来测量到达角，通常可以产生比RSSI/距离测量方法更准确的位置估计。许多RFID标签使用一个小电池，并以可配置的间隔（从几秒到每小时）发送消息，从而改变了时间维度的准确性。更大的设备可能包括更大的电池，从而允许信号每

秒钟或更频繁地发送。因此，RTLS通常被称为nRTLS（近实时定位系统）。

通过使用RTLS和图形位置可视化工具，装配工人、轮班主管和工厂经理可以通过平板电脑和智能手机查看工厂材料和资产的位置。通过实时跟踪生产情况，车间经理还可以跟踪每条生产线的产量，并确定生产是否达到了每日目标。

RTLS在实践中的一个很好的例子来自世界领先的飞机制造商之一。这家制造商决定在其飞机上的所有安全设备上安装RFID标签。当飞机进行维修时，一项工作是检查每一件设备，并确认原因。没有RFID标签，对每架飞机执行这项工作平均需要花费6.5小时。有了RFID标签，检查每架飞机的时间减少到20分钟。在工厂里，使用RFID标签来定位飞机部件，使得公司可以通过使用移动优化软件更快地组装飞机，该软件可以将部件移动到需要的地方，并移除可能会减少对其他部件进行访问的对象。该公司估计每年每个工厂的利润为1亿美元。

使用RTLS还允许工厂经理监视员工在生产过程中完成各自阶段的速度。RTLS在制造业中的商业价值在于，它帮助工厂经理更好地了解如何提高效率和降低与库存相关的成本。通过跟踪库存和材料的位置，RTLS还可以通过提供准确的交付时间表来帮助改善客户服务。

9.3 工业自动化控制协议

工业自动化应用系统使用一组独特的协议来实现控制、移动、同步和安全。这些工业协议的开发早在以太网和IP出现之前就已经开始了，但近年来，人们一直在努力调整这些自动化协议，以利用现代传输机制的优势。

可用的自动化控制协议的列表很长，但是市场应用最多的3种协议将在以下几节中讨论：以太网/IP、PROFINET和Modbus/TCP。

9.3.1 以太网/IP和通用工业协议（CIP）

以太网/IP是Rockwell公司开发的工业自动化系统的开放标准，现在由开放设备网供应商协会（ODVA）管理。注意，在以太网/IP中，IP代表的是Industrial Protocol，而不是Internet Protocol。工业协议专门用于处理工业自动化应用程序，例如用于控制、安全、移动和配置的应用程序。

以太网/IP使通用工业协议（CIP）适应标准的以太网和TCP/IP技术。CIP是一种通信协议，用于自动化系统和控制系统中的I/O控制、设备配置和数据收集。CIP包括以下通信类型的功能。

■ 隐式消息传递：这种类型的消息传递包括实时I/O数据、功能安全数据、运动控制数据，通常还有UDP多播。

■ 显式消息传递：这种类型的消息传递涉及配置、诊断和数据收集，并基于TCP单播传递消息。

图9-9展示了一个基于以太网/IP的制造网络。如前一节所述，REP用作工业以太网交换机（IES）之间的弹性机制，以传递CIP类别1（实时以太网）和类别3（TCP）消息。

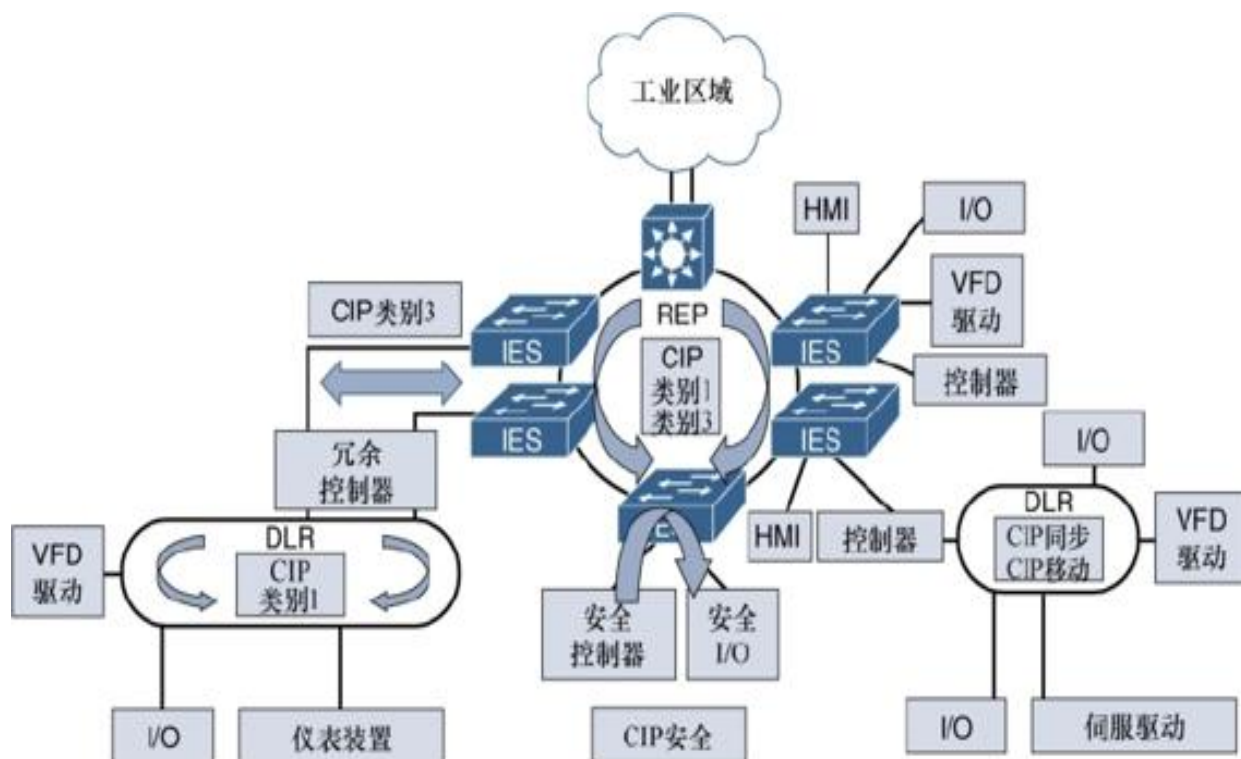


图9-9 基于以太网/IP的工厂网络

以太网/IP还指定了一种称为设备级环（DLR）的冗余协议，当系统需要连续运行时使用该协议，并且能够在环路断开的情况下实现高速重新聚合。DLR被优化部署在这样一个地方，而设备具有集成双端口交换机并且不需要单独的工业以太网交换机的地方。

注释：前面讨论的用于工业应用程序的CPwE参考体系结构主要基于以太网/IP和CIP。

9.3.2 PROFINET

PROFINET（Process Field Net）是一种广泛应用于在控制器与设备之间交换数据的工业技术。PROFINET的主要优点之一是它可以通过高速以太网链路以确定的方式交换消息。与Modbus TCP不同，Modbus TCP使用TCP在设备之间通信（因此要求设备建立和维护TCP套接字连接），或使用以太网/IP进行通信（用到了UDP），而PROFINET能够直

接向应用层发送和接收数据，而不必等待在TCP/IP栈中进行处理（有可能引起可变的延迟）。

注释：**PROFINET**与以太网/IP有何不同？以太网/IP和**PROFINET**是工业自动化的不同标准，是工业以太网现场总线市场的两大领导者。简而言之，以太网/IP由**ODVA**支持，由**Rockwell**公司开发，**Rockwell**公司是制造业的领导者，尤其是在北美。**PROFINET**由**PROFINET**国际（**PI**）支持，是欧洲和中东的市场领导者，它得到了西门子和其他供应商的支持。

从网络的角度来看，关键的区别在于这两个标准如何处理确定性网络和实时通信。以太网/IP利用**UDP/IP**进行实时通信（类似于通过IP应用程序进行语音通信），而**PROFINET**使用独特的**EtherType**绕过**UDP/IP**层，允许直接进行应用程序通信。

PROFINET与标准的**IEEE 802.3**以太网完全兼容，这意味着普通的以太网设备可以与同一网段上的**PROFINET** I/O设备和控制器共存。然而，**PROFINET**与标准以太网也有一些显著的区别。例如，**PROFINET**是一种确定性协议，这意味着在特定的时间发送和接收帧。当控制器需要向设备发送一条消息来停止或更改操作时，这在离散制造中尤其重要。

PROFINET应用程序对时间敏感。网络服务、应用程序和设备都依赖于在严格的延迟允许范围内交付命令和控制流量，这意味着任何由网络引起的延迟都是一个关键的设计考虑因素。为了解决这个问题，**PROFINET**网络被设计成以最小的延迟支持实时**PROFINET**通信，同时支持生产车间的网络弹性。**PROFINET**架构由以下部分组成。

- 工业自动化设备：包括机器人、传感器、执行器和驱动器。
- HMI：HMI提供工业自动化设备的可视化状态报告和控制。
- 控制器：包括PLC和分布式I/O设备。

设计良好的**PROFINET**体系结构具有以下操作优势。

■ 通过使用基于IEC 62439-2标准的具有网络聚合能力的弹性网络体系结构来降低生产停机的风险。IEC 62439-2在9.3.4节中有更详细的介绍。

■ 通过得以验证的参考体系结构增加工厂的正常运行时间，重点关注应用程序的可用性。

■ 通过更好地管理网络资源丰富了来自计算机和应用程序的关键信息访问。

■ 使用符合行业标准的通用系统描述（GSD）文件和兼容PROFINET设备的管理应用程序增强了单窗格管理合规性。GSD文件包含设备的功能和特征，这些功能和特征支持在PROFINET网络中有效地集成、配置和管理设备。

9.3.3 PROFINET架构

连接工厂的PROFINET架构在许多方面与前面讨论的CPwE体系结构相似，包括支持为工业自动化环境中的设备、设备和应用程序提供网络弹性服务。

与CPwE类似，PROFINET利用普渡模型实现控制层次结构。单元/区域（第0～2级）是大多数实时PROFINET流量在工业自动化系统设备之间传输的范围。上层制造区域充当一个或多个单元/区域的聚合点。

PROFINET架构采用严格的流量隔离方法来保护工业自动化应用程序免受外部和内部中断的影响。即使控制网络的中断只持续几毫秒，也会对生产设施的运作产生重大影响。

在图9-10所示的PROFINET架构中，网络弹性是主要的考虑因素。

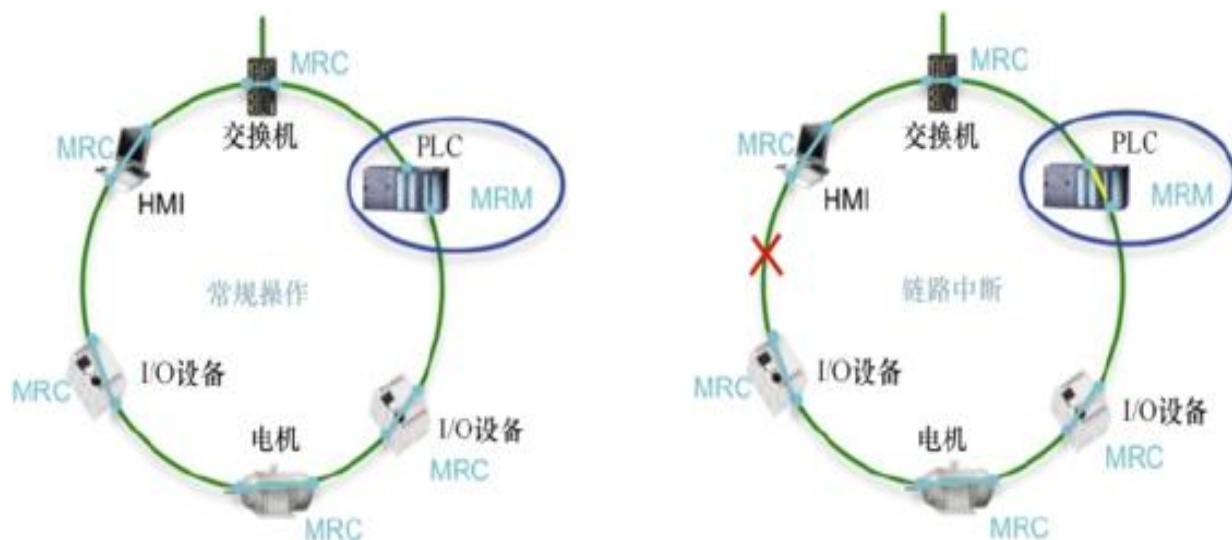


图9-10 PROFINET MRP操作

与CPwE一样，单元/区域是执行大多数工业自动化活动的主要区域。重要的是将该区域视为制造环境的独立实体，其中可用性和性能是最重要的考虑因素。

9.3.4 媒体冗余协议（MRP）

确定性和网络性能是保证单元/区域内PROFINET稳定性的关键要求。工业自动化中的确定性确保以太网帧根据需要被发送和接收。虽然PROFINET设备负责调度和传输以太网帧，但网络对系统确定性的主要影响基于以下性能特征。

- 延迟：消息从起始节点传输到目标节点所需的平均时间。

- 抖动：延迟的变化量。

- 数据包丢失：数据包在从一台设备传输到另一台设备时丢失的数据包的数量，通常用百分比表示。

工业自动化网络需要具有低水平的延迟和抖动，并且需要支持实时应用程序的可靠数据传输。在工业自动化实现中，应用程序的时间需求经常变化，这取决于底层流程、系统或设备。

工业自动化网络必须满足以下实时应用要求。

■ 机器和流程周期时间：这包括工业自动化应用程序从一个操作转移到下一个操作的频率。

■ 请求包间隔（RPI）或I/O更新时间：这是输入和输出发送与接收的频率。

■ 丢包容错：这是应用程序发生错误或故障，在进入安全状态之前连续丢失的数据包间隔数。

为了满足这些严格的要求并防止应用层链路或交换机故障，PROFINET支持一种称为媒体冗余协议（MRP）的环恢复协议。MRP是IEC 62439-2标准中定义的行业协议。MRP允许工业以太网交换机的环路克服单网段故障，且恢复时间与REP类似。MRP适用于工业以太网应用，得到了PROFINET的原生支持。

符合PROFINET的工业以太网交换机支持MRP环中的两个角色。在环型拓扑中，只有一个交换机或工业自动化设备可以充当媒体冗余管理器（MRM），而所有其他设备都可以充当媒体冗余客户端（MRC）。MRM的目的是保持环型拓扑无环路，并在故障发生时提供冗余。MRM通过从一个环路端口发送控制包或测试帧，并在另一个环路端口接收它们来实现这一点。在正常操作期间，控制包被接收，MRM保持一个端口被阻塞以防止环路。如果MRM没有接收到其控制包，这意味着环路是不完整的，并且发生了网络故障。MRM将网络故障通知给MRC。它解除其端口的阻塞，并开始转发以提供连接，直到网络故障得到解决（见图9-10）。

表9-1列出了弹性协议及其与拓扑类型和聚合需求的互操作性。

表9-1 以太网环弹性协议比较

协议	拓扑结构	节点数	典型的聚合时间	评述
802.1D STP	任意结构	最多 7 跳	50s	由于再聚合速度慢，不适合工业自动化，影响实时应用
快速生成树 (802.1w)	任意结构	最多 20 跳	-2~3s	不太适合环型拓扑
MRP	环型结构	50	30~500ms	PROFINET 的一部分
ITU G8032	环型结构	建议 16 跳 (最多 250 跳)	50ms	ITU 标准，类似于 REP
DLR (设备级环路)	环型结构	50	3ms	可预测的再聚合
REP	环型结构	无限制	50~250ms	Cisco 私有协议，但广泛应用于制造业、公用事业和其他工业领域

9.3.5 Modbus/TCP

Modbus 最初在 20 世纪 70 年代由 Modicon (现在的 Schneider) 引入。它是一种串行通信协议，广泛应用于制造业、公用事业和许多其他行业。在制造领域，Modbus 最常用来管理主/从配置中的 PLC。与其他自动化控制标准非常相似，Modbus 已经适应了现代通信标准，包括以太网和 TCP/IP。

Modbus 之所以受欢迎，是因为该协议是一个公开发布的标准，并且在全世界都得到了广泛的认可。Modbus 主/从配置非常适合 TCP 面向连接的特性，但是这种通信模式往往会引入额外的延迟，而且通常不如以太网/IP 或 PROFINET 灵活。Modbus/TCP 在第 6 章中有更详细的讨论。

[9.4 互联工厂的安全](#)

制造业已经成为网络犯罪的首要目标之一。通常，解决方案是通过将工厂网络与IT企业网络断开连接来对其进行隔离。然而，与高层功能断开连接的网络在其功能和业务改进方面受到限制，而这些改进可以通过物联网实现。此外，许多威胁来自底层的计算机和工作站，这些计算机和工作站可以被承包商或雇员不受限制地直接访问。例如，考虑在第2章和第8章中提到的Stuxnet蠕虫病毒，人们认为它是通过内部网络上的物理USB设备引入的。

9.4.1 工业安全的整体方法

没有任何一种产品、技术或方法能够完全保护工业应用程序免受网络攻击。保护IACS资产需要一种深入防御的安全方法，以应对内部和外部威胁。该方法在每个IACS级别实现多层防御（物理、程序和电子）。

一个全面的IACS安全框架应该作为工业控制系统网络的自然延伸。然而，对于几乎没有安全保障的现有IACS部署，可以逐步应用相同的深度防御模型来逐步改进IACS的安全状况。

在大多数情况下，整体工厂安全需要不同的参与方协同工作，包括控制系统工程师、IT网络工程师和IT安全架构师。这些不同的参与方的职责包括以下内容。

- 控制系统工程师：
- IACS设备安全加固（即物理和电子设备）；
- 加强基础设施设备（例如端口安全性）；
- 网络分段；
- IACS应用程序身份验证、授权和审计（例如AAA）。
- 控制系统工程师与IT网络工程师协作：

- 在IACS应用程序中部署基于区域的策略防火墙；
- 操作系统安全加固；
- 网络设备安全加固（例如，访问控制、弹性）；
- 无线局域网接入控制策略。
- IT安全架构师与控制系统工程师协作：
- 身份服务（有线及无线）；
- 目录服务；
- 远程访问服务器；
- 工厂中的防火墙；
- 工业非军事区（IDMZ）设计的最佳实践。

图9-11展示了互联工厂的整体安全架构，并强调了需要实现这些安全功能的位置。

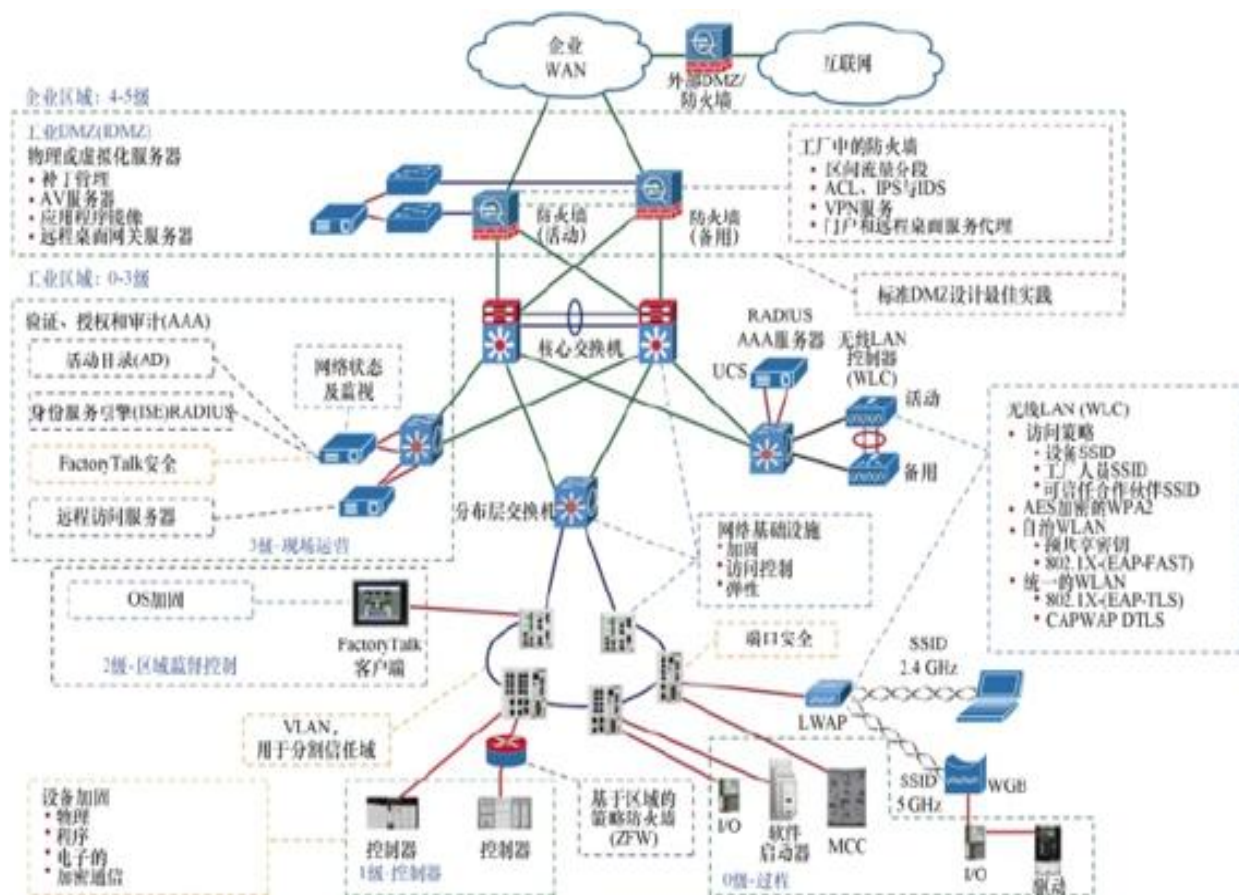


图9-11 工业网络安全框架

虽然工业网络安全是一个庞大的主题，但本书只对其进行简要的讨论。下面几节主要介绍工厂安全性的3个方面：

- 工厂中的网络地址转换；
- 工业DMZ；
- 工厂中的安全身份识别服务。

1. 工厂中的网络地址转换

无论是终端用户、OEM还是系统集成商，都可能需要重用IACS应用程序中的IP地址。网络地址转换（NAT）支持IP地址的重用，而不会在IACS应用程序体系结构中引入重复的IP地址错误。

技术和业务方面促使人们决定使用NAT。

■ **业务驱动：** 机器制造商中的原始设备制造商通常生产具有相同IP地址的类似机器，并且依赖于NAT来快速部署和复制设备单元和机器，包括IP寻址。这有助于降低开发和调试成本。

■ **技术驱动：** 当全厂网络基础设施中的IP地址空间有限，且并非所有设备都需要在设备单元或机器级网络之外进行通信时，就会使用NAT。

Plantwide架构要求每个设备有唯一的IP地址。NAT是一种网络技术，它使控制系统工程师能够构建重用IP地址的IACS应用程序，同时允许这些IACS应用程序集成到更大的Plantwide架构中。

NAT可以被配置为将特定的IP地址从IACS应用程序内部转换到外部工厂的网络中。这样做还可以有效地隐藏IACS应用程序的内部IP寻址方案。NAT转换有两种形式：一对一（1 : 1）和一对多（1 : n）。

需要注意的是，NAT设计需要是可扩展的，因为工厂网络中可能存在多个单元/区域。

如图9-12所示，一个常见的用例是通过线路控制器协调OEM机器的控制功能。在本例中，有多台机器，每台机器都有自己的机器控制器。但是请注意，外部有一个用于两台机器的线路控制器。两个IACS设备都部署了相同的IP地址，并且需要NAT与线路控制器进行通信。

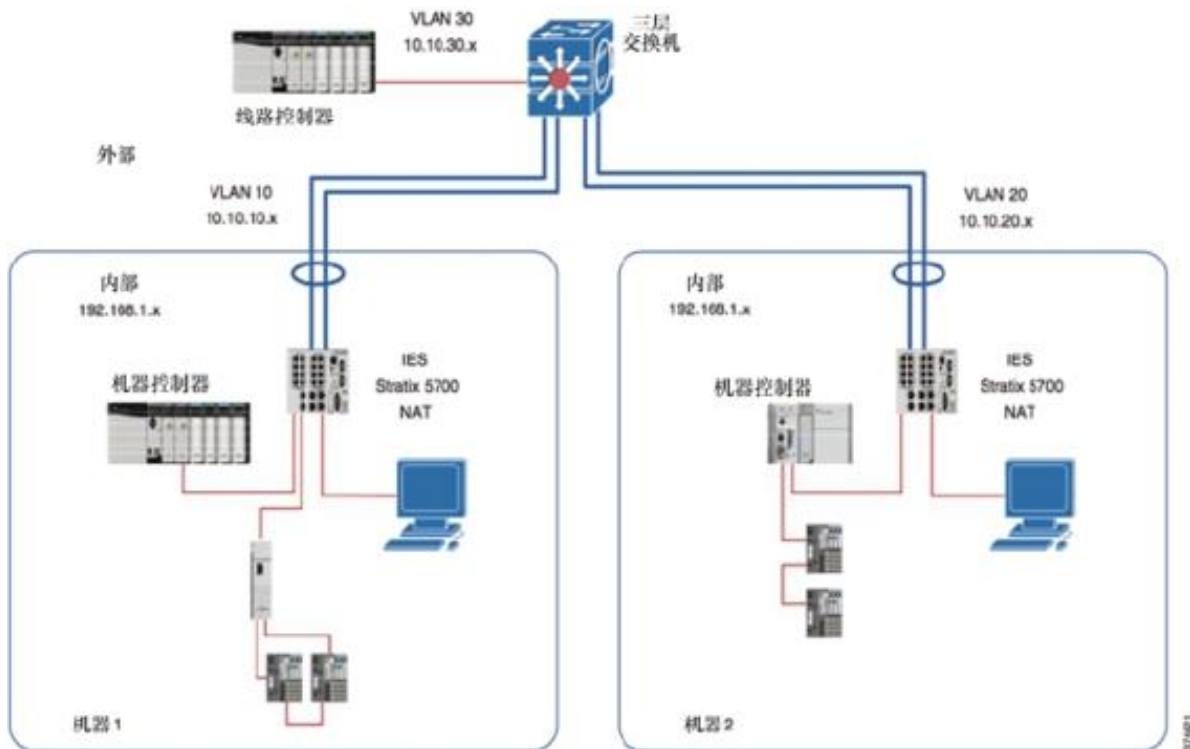


图9-12 使用相同的IP地址部署多台机器（需要用到NAT）

机器1部署VLAN 10，机器2部署VLAN 20，线路控制器部署VLAN 30。机器1的NAT交换机将机器控制器的内部IP地址（192.168.1.x）转换为VLAN 10上的外部IP地址（10.10.10.x）。NAT交换机也将默认网关（第三层交换机）的外部IP地址转换为内部IP地址。相应地，机器2的NAT交换机将机器控制器的内部IP地址（192.168.1.x）转换为VLAN 20上的外部IP地址（10.10.20.x）。同样地，机器2的NAT交换机也将默认网关的外部IP地址转换为内部IP地址。

在第三层交换机和NAT交换机之间，每台机器都有一个唯一的VLAN，每个控制器都有一个唯一的外部IP地址。位于外部的第3层交换机将每个机器控制器的外部IP地址路由到VLAN 30上的线控制器（垂直联锁）或另一台机器的VLAN（水平联锁）。

这个可扩展的用例支持将多个带有重复IP寻址方案的设备单元或机器集成到同一线路控制器VLAN中。对于这个用例，每个设备单元或机器都需要一个支持NAT的工业以太网交换机。还需要一个第3层分布层交换机来支持VLAN之间的路由。

2. 工业DMZ

IACS网络通常在一家制造企业运行。尽管IACS系统中存在一些攻击载体，但是来自企业区域的渗透仍然是安全体系结构的重点。为了应对这种威胁，许多组织和标准机构建议通过部署工业隔离区（IDMZ）将业务系统网络从工厂网络中分离出来。

IDMZ是一个缓冲区，它在可信网络（工业区）和不可信网络（企业区）之间执行数据安全策略。DMZ概念在传统的IT网络中很常见，但在IACS应用中仍处于早期阶段。

IDMZ 作为一个独立的网络存在，位于工业区（在图 9-3 的普渡模型中被标识为制造区域）和企业区之间，通常称为 3.5 级。IDMZ 环境由许多基础设施设备组成，包括防火墙、VPN服务器、IACS应用程序镜像和反向代理服务器，以及网络交换机、路由器和虚拟化服务。

对于安全的IACS数据共享，IDMZ包含在区域间充当代理的资产。跨IDMZ存在多种代理IACS数据的方法：

- 反向代理服务器；

- 应用程序镜像，类似于代理服务器，本质上是在受保护的数据中心之外运行的实际应用程序的副本；

- 远程桌面服务（如Microsoft RDP）。关键的IDMZ设计原则包括以下几点。

- 来自IDMZ两端的所有IACS网络流量都终止于IDMZ中；没有任何IACS流量直接通过IDMZ，工业和企业区域之间没有直接路径。

- 工业管制流量不进入IDMZ，仍在工业区域内。

- 主要服务并不是永久存储在IDMZ中。

- 所有数据都是暂时的，这意味着IDMZ不会永久地存储数据。

- IDMZ中使用功能分区来分段访问IACS数据和网络服务（例如，合作伙伴对资源的访问）。

- 设计合理的IDMZ还支持在被攻陷的情况下断开电源的能力，同时仍然允许工业区在不中断的情况下运行。

3. 工厂中的安全身份识别服务

随着工业网络接入方式的扩展，网络接入安全管理和未知风险控制的复杂性不断增加。随着承包商（如OEM和系统集成商）对厂内访问的需求不断增长，Plantwide网络面临持续的安全威胁。

此外，IACS网络需要针对不受信任（和潜在的危害）的计算机（如承包商或合作伙伴供应商使用的计算机）进行保护。随着制造工厂中承包商设备的扩散和Plantwide操作资源的限制，未能识别和消除的安全威胁给Plantwide操作带来了重大风险。

网络身份服务通过识别正在访问网络的计算机、操作系统和用户的类型来提供一个额外的网络访问和控制层。基于身份并应用相应的策略，身份服务能够将安全策略推送到计算机正在访问的网络基础设施。由于身份服务通常与目录服务（如LDAP或Microsoft Active Directory）绑定，因此通常的做法是使用集中管理的身份服务模型，IT部门维护在工业区域运行的身份系统的管理。

需要注意的是，安全架构可能需要同时支持工厂人员和承包商的有线与无线访问方法。这是通过部署能够在所有网络接入点上建立信任边界的集中式身份服务系统来实现的。

这种方法提供了以下好处：

- 通过综合集中策略访问制造区域和企业区域网络；
- 设备安装流水线化；

- 策略驱动规则和访问控制策略；
- 为承包商和访客提供了客户门户服务。

通过合并集中式身份系统，策略可以实时跨网络应用，这样用户就可以从有线和无线连接体验到对其服务的一致访问。此外，未知设备被定向到管理员定义的安全目的地，在Plantwide操作中没有访问本地资源的权限，而可信设备被授予访问工业区基本平台的权限。

身份服务工具还支持集中式客户门户服务，以及工厂人员、供应商、合作伙伴和客户的自助注册策略。

9.5 互联工厂的边缘计算

车间里的机器能够产生大量的数据。许多工厂应对这一挑战的方法之一是部署PC来收集这些数据。从工厂车间的PC收集数据带来了维护和安全方面的挑战，因为每台PC都需要打补丁和升级操作系统。硬件故障也很常见，因为这些设备在工厂条件下通常不能加固。显然，这种方法使工厂操作很难有效地聚合、处理和响应数据。在对工厂数据分析来获得可见性和潜在商业利益时，这种方法会带来障碍。

网络边缘计算能力的新趋势正在帮助解决这些难题。随着嵌入机器和接近机器边缘的计算设备的出现，这些设备具有交换、路由和安全功能，并具有单一的加固形式，制造商开始意识到连接机器和边缘计算服务的价值。

9.5.1 互联机器和边缘计算

将机器连接到工厂级应用程序需要可扩展、安全且易于实现的通信模型和数据模式。几个开放的制造通信协议已经被开发出来，这些协议提供设备和软件之间的互操作性，允许监控生产车间并从中获取数据。这些协议通常基于XML或HTTP。

对于不同的机器类型存在不同的数据标准，因此我们期望在工厂低层的数据协议中存在一些异构性。例如，MTConnect通常用于计算机数控（CNC）机器，OPC UA广泛用于工业自动化，PackML用于包装机械。

边缘计算平台的新发展将交换、NAT、路由和安全特性整合到一个加固的边缘设备中。这种边缘服务方法降低了保护机器数据收集的成本，并通过在将数据传输到数据中心或云进行进一步分析之前，分析工厂低层的数据来优化可用的网络资源和带宽。

边缘设备通常包括一个基本的开源高效操作系统，比如Linux，它运行一个流分析应用程序，以及相应机器类型所需的标准数据代理。

标准协议的硬件适配器安装在机器上，用于为每台机器定义I/O标记，并将每个标记的状态更改广播到边缘设备上的代理。驻留在边缘设备上的代理被配置为侦听特定的适配器并缓冲预定义的标记。可以配置边缘流分析来解析数据，并确定哪些内容对进一步的考虑和分析有用。然后通过HTTP或XML将经过优化的数据发送到运行大数据分析和处理引擎（如Hadoop）的本地或基于云的数据中心。

OEE分析工具可用于数据可视化。在某些情况下，OEM机器制造商生产定制的分析软件，这些软件可以在本地或通过云交付。图9-13所示为机器硬件适配器用于将数据传递给边缘节点/边缘设备上的代理进行分析，然后只将经过优化的数据发送到云端进行进一步分析。

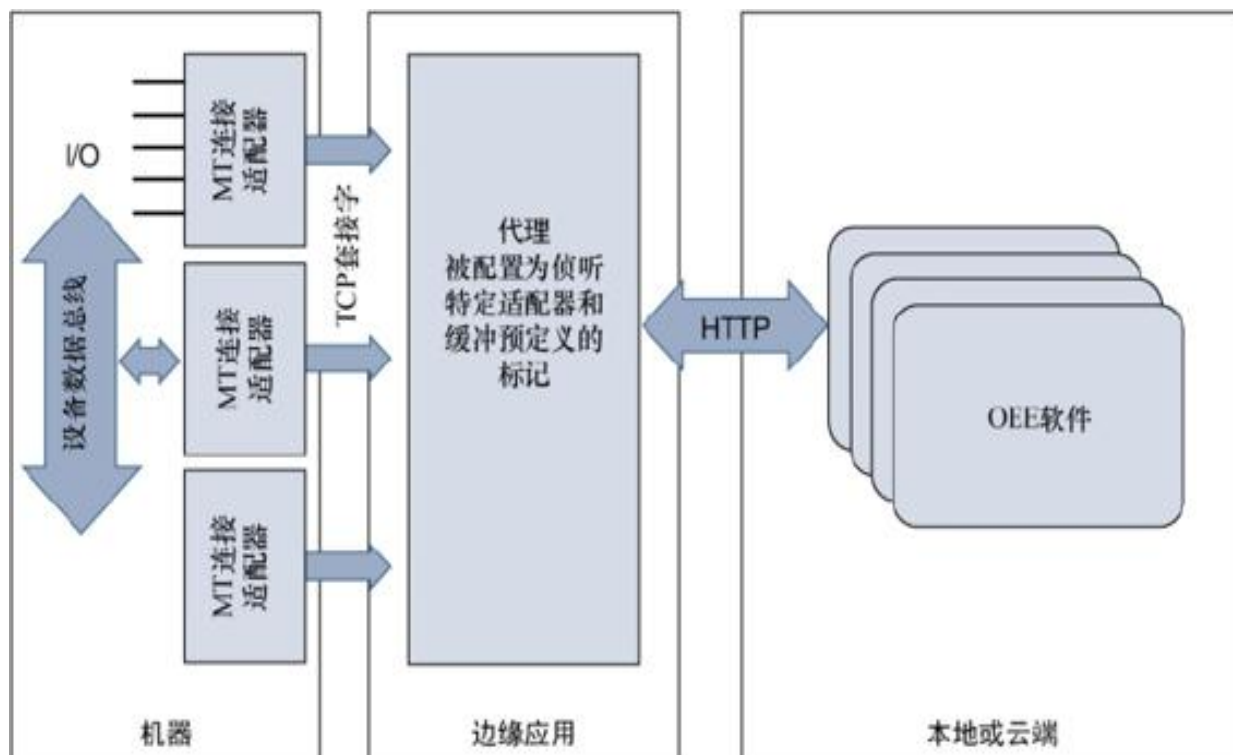


图9-13 基于MTConnect的连接机器模型

由于数据可以来自不同的资源，因此最好在具有身份管理功能的企业门户环境中管理应用程序。随着机器制造商在交付用于预防性维护的OEE分析方面趋于成熟，预计它们将越来越多地使用RESTful API交付Web服务，这些API可以在连接的机器的Web门户中供终端用户制造商使用。现代门户应用程序允许从具有安全标识和单点登录（SSO）功能的不同来源使用这些服务。

对于具有异构底层数据的大型制造商来说，为每种机器类型确定数据标准并与机器制造商合作构建解决方案的任务可能会令人生畏。同时，当使用工业以太网边缘交换机启用弹性、安全且聚合连接的工厂基础设施时，可以在合理的时间范围内实现边缘计算和存储的优势。图9-14展示了如何将边缘计算部署到一个坚固的工业交换机上，该交换机直接连接到制造区域的机器上。

世界领先的工业机器人公司之一就是一个很好的连接工厂边缘计算的例子。这家机器人公司使用边缘计算和大数据分析来识别维护程序，以防止故障发生。通过公司的零停机时间（ZDT）解决方案，在工

厂网络中，机器人通过运行ZDT代理的边缘计算设备进行连接。与优化维护相关的数据被安全传输到托管云环境中，分析软件在云环境中捕获超出范围的异常并预测所需的维护。确定维护周期后，云应用程序将向服务人员发送警报，提醒他们提供服务。然后，所需的部件被及时运送至工厂供下一个定期维护窗口使用。一家大型汽车制造商通过ZDT应用程序连接了数千个机器人，这节省了价值数百万美元的意外停机时间。

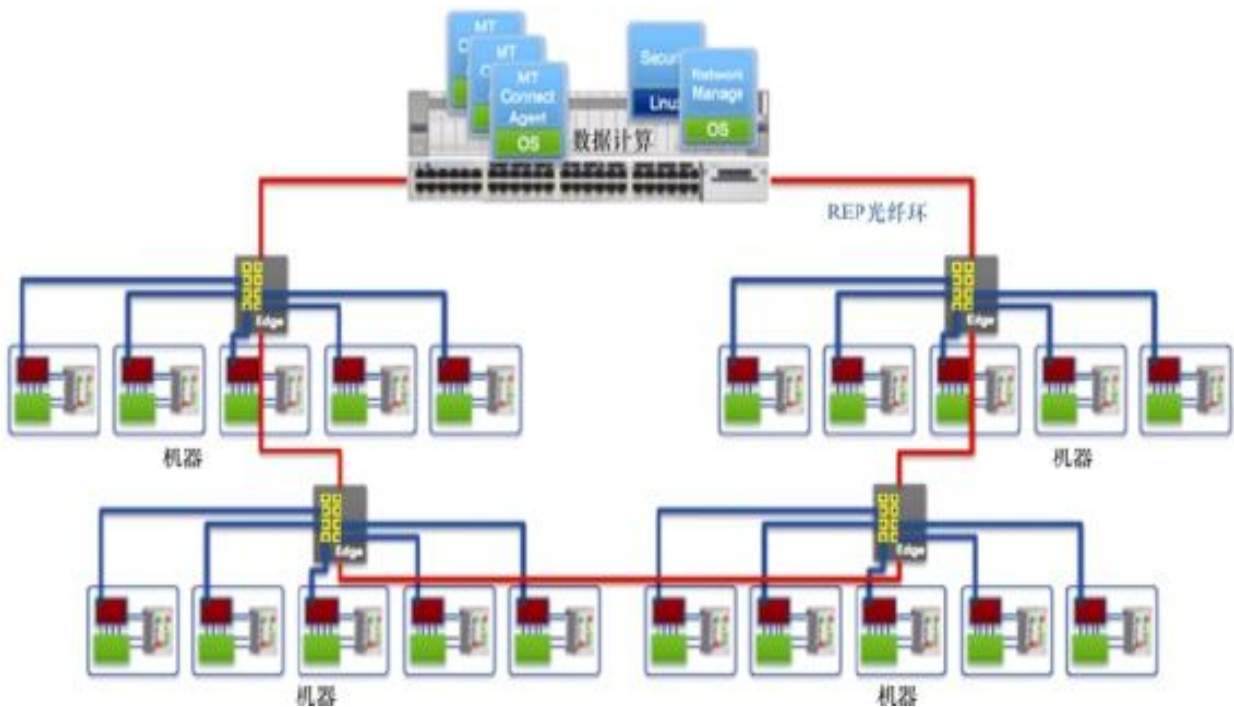


图9-14 部署在单元/区域接入交换机上的边缘计算示例

9.6 小结

制造业正在迅速向数字化转型。制造商正在将完全不同的独立系统迁移到聚合网络和控制协议上。ISA99制造和控制委员会提出了一种被称为IACS模型的体系结构模型，该模型以普渡控制层次模型（ISA99/IEC-62443）为基础建立，其中一系列区域和级别确定了协议集、安全边界和制造工厂的运营模型。由Cisco和Rockwell支持的

Converged Plantwide Ethernet (CPwE) 建立在这个模型上，并为 IACS 的有线和无线网络设计定义了一套指导方针。

聚合工厂架构的基础是单元/区域以太网弹性协议，如 REP、DLR 和 MRP，这些协议允许快速聚合以太网环路。为了支持自动化控制的要求，已经为利用标准通信协议的制造开发了特定的控制协议。3 种最流行的控制协议是以太网/IP、PROFINET 和 Modbus/TCP。

当机器和其他设备连接到工厂内的单元/区域时，它们的安全性至关重要。为了解决这个问题，经常使用私有地址，因此需要在单元/区域内使用 NAT 服务。此外，强烈建议通过身份服务工具对设备/用户进行集中访问控制配置，以确保不受信任的计算机和设备不会在工业区内的网络上使用。

最后，制造商开始从单元/区域内的边缘计算中获益。现在正在部署特定于制造行业的边缘应用程序，这些应用程序在机器上处理机器数据，只将相关数据发送到云或数据中心。

第10章 石油和天然气业

石油和天然气是现代社会最重要的资源之一。现代生活的几乎每一个方面，从运输系统到塑料供应，都依赖于这些商品的供应。如今，石油和天然气公司的主要关注点是如何降低成本、提高效率，并从现有投资中获得更多收益。该行业最重要的关键绩效指标包括控制生产成本和改善危险环境的整体健康与安全。

在这个行业中，越来越多的网络攻击正在危及安全并造成损失。发生这种情况的背景是，深刻的技术变革正在打破传统的工作方式，并推动生产力的快速变化。前所未有的数据增长、先进的分析技术、不断提高的自动化程度和连接性，从根本上改变了原有的工作方式和地点。

与其他行业一样，石油和天然气公司正在将物联网应用于广泛的领域，例如：

- 监控工业设备的状态或行为，以提供可视化和可控性；
- 优化流程和资源利用；
- 改进业务决策。

本章探讨了油气领域的物联网，以及数字化如何成为该行业的一股颠覆性力量。它关注正在用于对这个行业进行数字化的用例和创新架构。本章包括以下内容。

■ 石油和天然气行业简介：本节首先定义油气行业，然后描述该行业的价值链和关键市场参与者。本节着眼于油气行业对价格波动的脆弱性、最重要的行业趋势和相关影响，以及它们为物联网带来的机遇。

■ 作为数字化驱动的行业关键挑战：本节阐述了石油和天然气行业面临的挑战（其中一些受到全球经济形势的影响），以及新技术如何颠覆旧的运行方式。

■ 提高运营效率：本节研究油气物联网系统中关键的运营效率考虑因素、用例和技术。

■ 油气物联网架构：本节探讨油气行业的关键安全考虑因素、用例和技术，以及如何使用正确的设计方法解决这些问题。

10.1 石油和天然气行业简介

为了了解任何行业并成为其业务转型过程中的相关参与者，必须了解该行业的一些背景（包括其产品、流程、主要参与者和当前趋势）。以下各节介绍石油和天然气行业的这些基本先决条件。

10.1.1 石油和天然气的定义

石油和天然气是来源于有机物（主要是小型浮游生物和藻类）的碳氢化合物。在能源价值链中，石油和天然气是主要能源。石油工业中使用的第一级分类涉及常规和非常规的概念，即用于开采的方法，也指用于生产石油和天然气的岩石类型。

常规石油和天然气是在一些可以钻井的油气藏中发现的，这样石油和天然气就可以自然流动，或者被泵抽取到地表。常规石油和天然气也存在于砂岩中，可用传统方法开采。油气资源通常来自另一个地层，但进入砂岩后被不透水盖层包围。常规石油资源是通过钻透帽岩以让石油向上流动的传统方法来开采的，如图10-1所示。

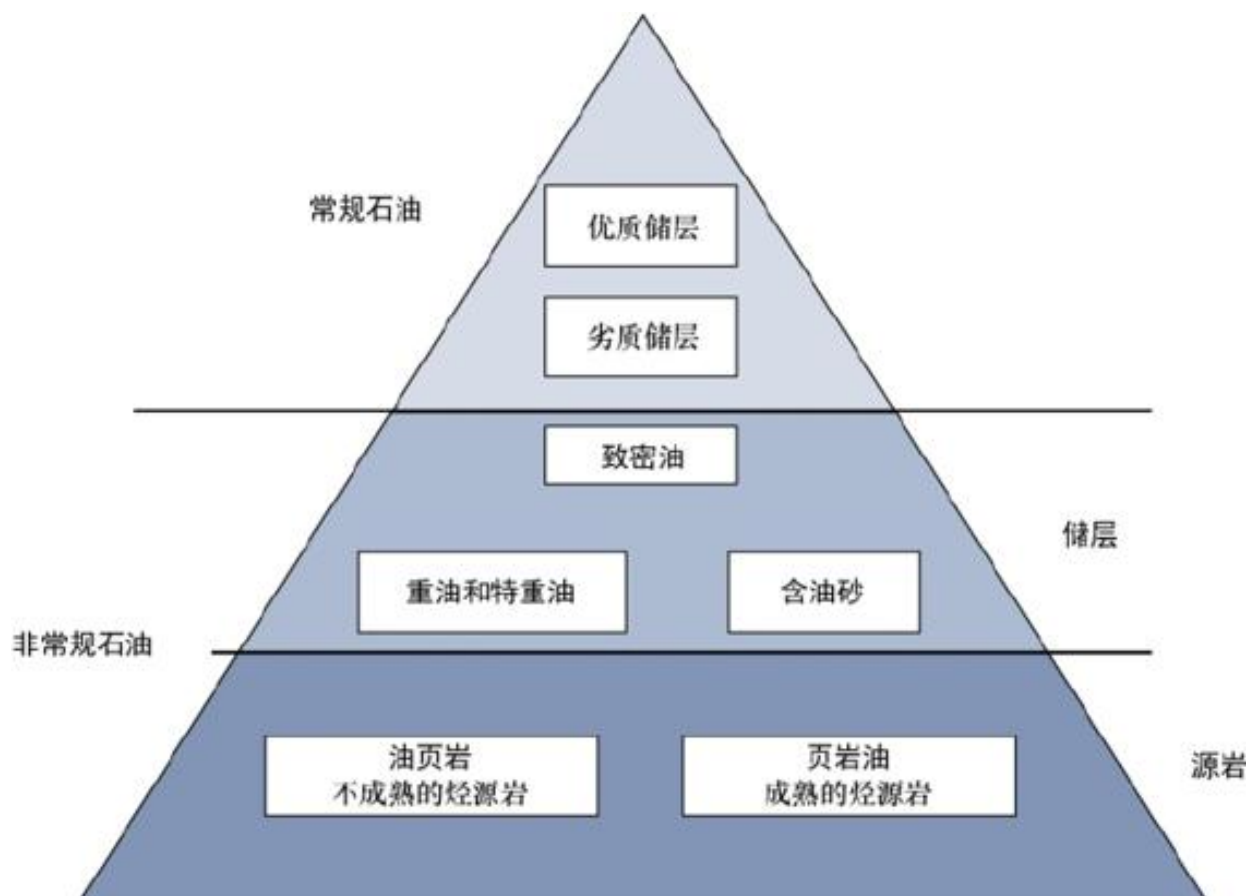


图10-1 常规与非常规油气对比

非常规的石油和天然气不会自然地流经岩石，因此开采起来要困难得多。由于低渗透率和低孔隙度，通常需要大量的井田和地面基础设施。它们的生产或开采采用特殊技术，如水力压裂法。水力压裂法是将高压液体注入地下岩石，迫使现有裂缝裂开，从而开采石油或天然气的过程。

石油有各种成分和类型，如岩石油、矿物油和原油，石油分类的一些示例如下（见图10-1）。

■ **致密油：**致密油是储层中含有的液态烃，其孔隙率极低，渗透率也同样低。

■ **重油和特重油：**这些资源被称为重油，是因为它们的密度和黏度都很高，这使得它们不可能使用传统的方法开采。

■ 油砂：这些沉积物是由沙子和焦油混合而成。

■ 油页岩：油页岩是尚未转化为碳氢化合物的烃源岩，需要加热才能回收。

■ 页岩油：在页岩油中，烃源岩位于地表以下足够远的地方，其中所含的有机物质已经转化为液态碳氢化合物。然而，由于其极低的孔隙度和不透水性，这些液态碳氢化合物仍然困在烃源岩中。开采这些被困住的液态烃需要使用水平钻井和水力压裂技术来人为地增加岩石的渗透性。

为了使石油和天然气以“经济”的数量积累，必须具备以下4个要素。

■ 需要烃源岩来生成碳氢化合物。

■ 需要一个合适的储层来储存碳氢化合物。

■ 需要一个密封的捕集器来容纳碳氢化合物。

■ 这三个元素必须出现在一个动态系统中，在这个系统中它们可以相互作用。

图10-2说明了这4个元素。

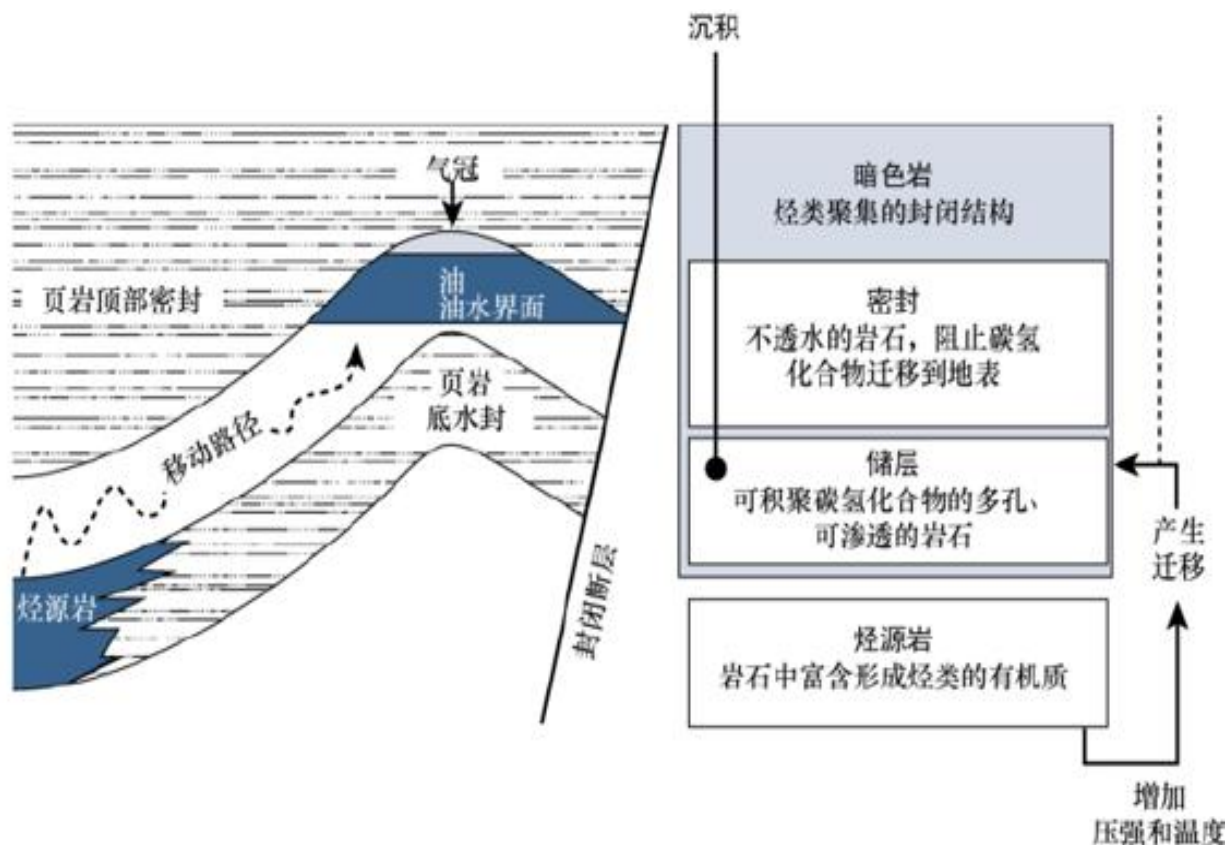


图10-2 从有机质到石油和天然气

与石油不同，天然气的密度和黏度很低，在常温常压条件下无法输送。从井中提取的天然气原料包括甲烷，以及许多其他较重的碳氢化合物的小馏分和各种其他成分，如：

- 乙烷；
- 丙烷；
- 丁烷；
- 烯烃；
- 酸性气体；
- 氮；

- 氮；
- 水；
- 微量污染物。

根据这些成分的组成，天然气有以下几种特性。

- 湿气：甲烷含量低于85%的原料气。
 - 干气：每1000标准立方米含少于15公升凝析油的原料或处理过的天然气。
 - 酸性气体：每标准立方米含5.7毫克以上硫化氢（ H_2S ）的原始气体。
 - 酸性气体：酸性气体含量高的气体，如硫化氢。
 - 凝析油：碳氢化合物和其他化学成分的混合物。
- 原料气被加工成以下各种产品。
- 天然气：通常是90%的甲烷和10%的其他轻烯烃。
 - 液化天然气（NGL）：为石油化工工业提供原料的经过处理的净化产品。
 - 液化石油气：在常温下压缩成液体的丙烷或丁烷或这些气体的混合物。
 - 液化天然气（LNG）：指在零下162℃下被冷藏和液化，用于储存和运输的天然气。
 - 压缩天然气（CNG）：在大气压力下压缩到体积的1%以下的天然气。

10.1.2 石油和天然气价值链

在已经知道了什么是最重要的原材料后，本节将探讨石油和天然气从初级能源到最终产品的转化价值链。油气价值链主要分为3个环节，如图10-3所示。

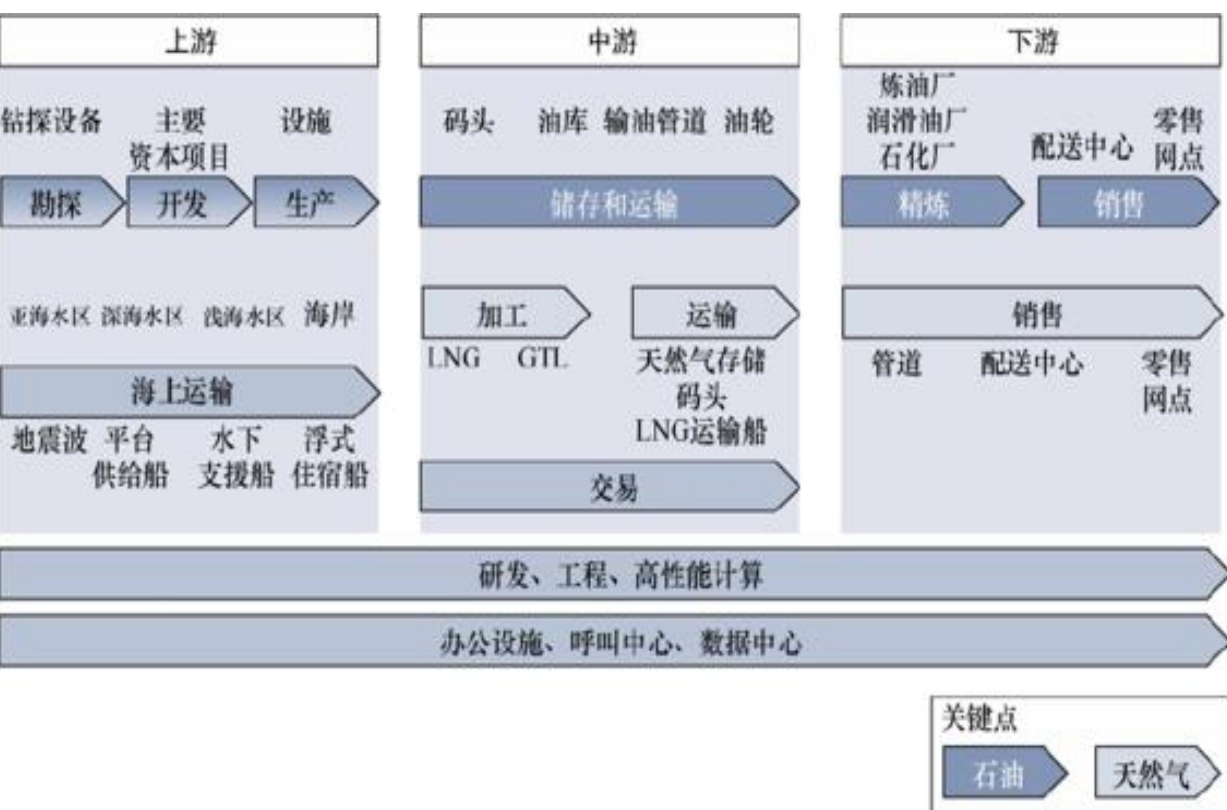


图10-3 油气价值链

■ 上游：该板块主要从事勘探、资本项目开发、原油和天然气生产等相关业务。对于海上钻井平台，运输也被考虑在内。勘探包括在油田开发之前进行的勘探和钻探活动。

■ 中游：这部分业务主要涉及工艺（天然气）、运输（管道、油轮/驳船、卡车和铁路）以及油气存储。在这里，油和冷凝物被加工成特定规格的产品，如汽油或柴油。这部分是影响石油和天然气之间运输和储存成本存在根本差异的地方。管道装置包括驱动压缩机和泵、阀门站、清管器接收和发送设施。为了控制和操作管道，还需要SCADA

系统和管道管理系统（SCADA在第6章中介绍过）。因此，输送天然气和石油是一个复杂而昂贵的过程。

■ 下游：该板块主要关注与精炼、营销、分销和商业化相关的业务。值得注意的是，在这一环节，现代炼油厂的成功取决于规模经济和将各种原油加工成最大数量的高价值燃料和原料的能力。

10.1.3 石油和天然气工业的当前趋势

影响油气行业最重要的因素之一是价格波动。这种波动的核心是供需失衡。本节将讨论导致这种不平衡的主要趋势，以及对行业的影响。

低碳气候政策正在创造一个资源丰富的世界。在全球补贴和气候政策的帮助下，可再生能源技术是全球能源供应低碳支柱的关键组成部分，正在迅速普及。在世界上许多地区，这一趋势已经减少了对包括石油、天然气和煤炭在内的传统初级能源的需求。

2014年1月，欧盟委员会提出了2030年欧盟气候与能源政策框架目标。其核心目标是在1990年的基础上减少40%的温室气体排放量，到2050年至少减少80%的排放量。要实现这些目标，可再生能源必须发挥重要作用。

图10-4显示了1990-2040年欧盟对初级能源的保护需求（百万吨石油当量，Mtoe）。吨石油当量是一个能源单位，定义为燃烧1吨原油所释放的能量。请注意，对清洁初级能源的需求预计将增长，而对污染更严重的能源（煤、石油等）的需求预计将下降。

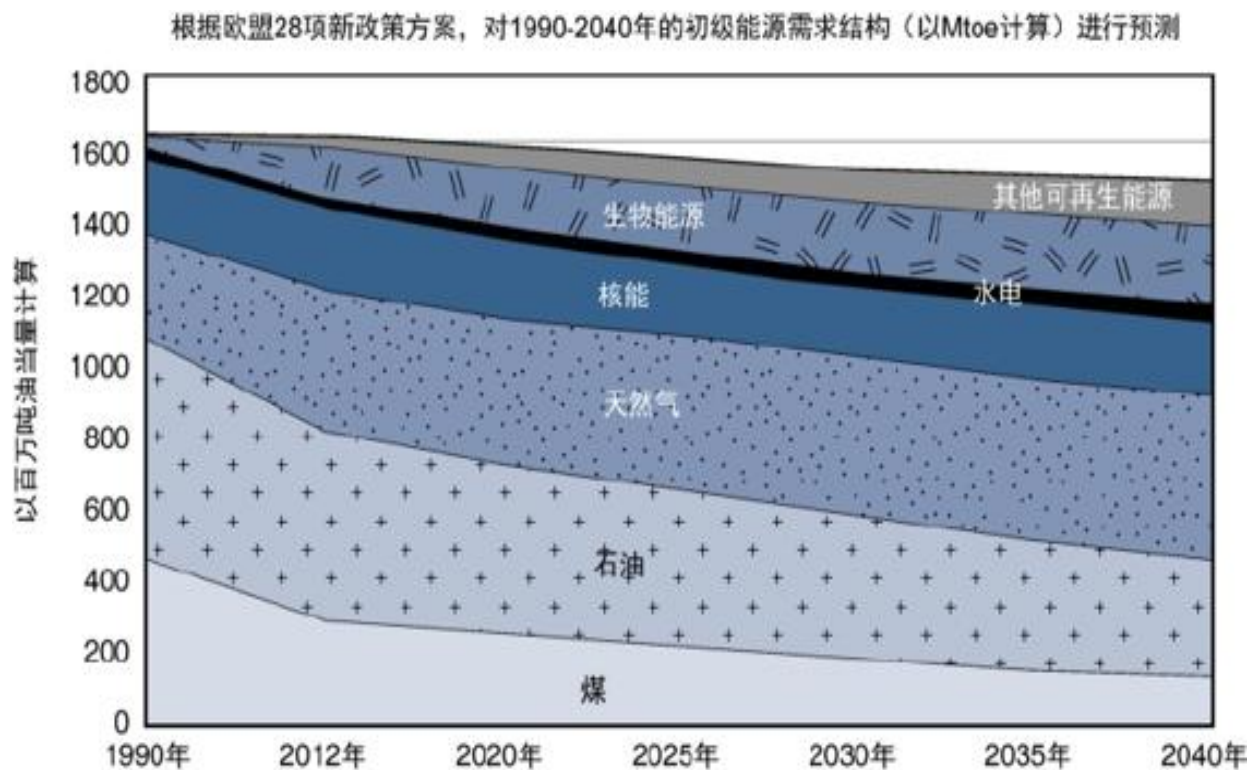


图10-4 国际能源机构世界能源展望（IEA WEO）2014年新政策方案

图10-5显示了从生产到最终消费的一次能源损失（本例中为煤源）的百分比。在本例中，为灯泡供电所需要的能量在经过生产和传输过程后导致了几乎98%的能量损失。这种模式显然是低效的，而且通过技术进行改进的时机已经成熟。

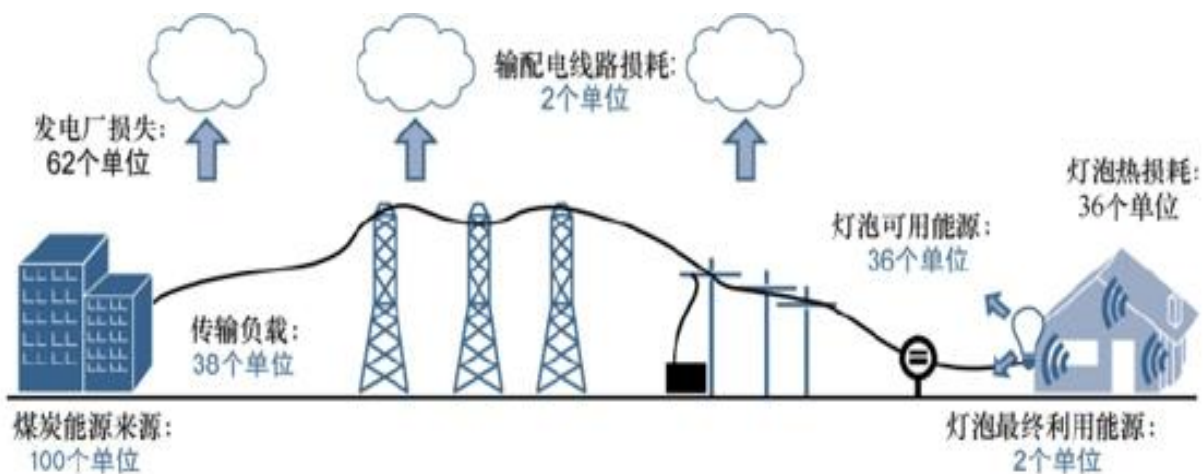


图10-5 从发电到消费的能源效率

能源市场是出了名的动荡，原因往往是能源供应和需求之间的不平衡。许多产油国一直在以创纪录的水平开采石油，导致全球能源价格走低。这种情况导致了对成本、效率和速度的高度关注，石油和天然气公司努力从现有投资中获得更多收益，并抵制新的投资。

另一个趋势是页岩气的产量，尤其是水力压裂技术的突破，使得页岩气在近年来产量显著增加。生产成本相对较低和小规模的生产者较容易进入到行业中，这意味着在面对最微小的市场动态变化时，可以很容易地提高或降低产量，这进一步导致了不稳定。

与技术使用有关的其他趋势已经出现，并正在影响整个工业。例如，技术增强提供的连通性意味着该领域的网络攻击数量增加。严重的网络攻击可能会造成重大的经济损失并影响运营。随着物联网技术的采用，可用的数据量也显著增加。结合数据分析的力量，这有助于提高石油和天然气勘探活动的准确性和效率。数据可用性的改善也意味着公司高管能够比过去更快地做出更明智的决定。

10.2 作为数字化驱动的行业关键挑战

油气行业正面临诸多挑战，其中主要是受到全球经济形势的影响。此外，新技术正在颠覆旧原有的运营模式，带来新的效率和新的期望。挑战可以带来机遇。物联网和数字化，即利用信息技术创新，为运营、工作流程和方法构建新的解决方案和技术的过程，正在为效率和新的商业模式的（闻所未闻的）改善开辟新的道路。

本节按类别介绍了一系列挑战，并建立了与基础数字化要求的映射。在 Top 10 Technology Trends Impacting the Oil and Gas Industry in 2014 报告中，Gartner 确定了以下主要的数字化趋势：

- 高级分析和建模（业务资产规划和优化）；
- 大数据（业务资产规划和优化）；

- IT/OT会聚（数字油田）；
- 智能机器（数字油田）；
- 扩展基础设施（数字油田）；
- 移动性（直观的工作流程）；
- 上游建模套件（直观的工作流程）；
- 协作（直观的工作流程）；
- 云（石油和天然气业务系统）；
- 资产绩效管理（石油和天然气业务系统）。

在表 10-1 中，请注意这些数字化趋势是如何映射到特定的物联网功能的。油气行业面临的主要挑战可以分为3类：

- 降低运营效率和成本；
- 安全性；
- 更快更好地做出决策。

表10-1 油气行业面临的挑战和要求

挑战	数字化需求
低投资背景下的运营效率	
■ 人员有效协作	■ 可用且可靠的实时通信 ■ 与设备无关的集成协作 ■ 实时获取相关信息 ■ 经济高效地接触专家 ■ 通过数字劳动力提高生产力
■ 过程优化	■ 过程自动化 ■ 减少停机时间并提高流程完整性
■ 资产管理与维护	■ 加强对资产的实时监控与控制 ■ 预测性维护
复杂攻击环境中的安全性	
■ 安全操作	■ 补丁管理 ■ 合规性监测 ■ 安全的远程访问
■ 网络可靠性	■ 可用性 ■ 可扩展性 ■ 数据管理 ■ 带宽 ■ QoS ■ 网络安全

续表

挑战	数字化需求
复杂攻击环境中的安全性	
■ 资产安全与保障	■ 物理安全及保障 ■ 过压保护 ■ 停机管理
■ 人员安全和保障	■ 人员监控和工人跟踪 ■ 物理安全及保障
■ 业务连续性	■ 操作仪表板及补救 ■ 过程自动化
■ 网络安全风险与漏洞	■ 入侵预防和检测 ■ 主动事件监控
数据风暴环境下的改进决策	
■ 更快更好的决策	■ 数据分析 ■ 分散计算和数据存储
■ 知识管理和技能短缺	■ 人员培训 ■ 知识管理

这些类别可以划分为子类别，并映射到相应的数字化需求中，如表10-1所示。

表10-1中列出的挑战迫使该行业采用新技术，这些技术在安全、停机时间、效率、环境保护和资产完整性方面带来了改进。图10-6说明了油气行业的价值观念。



图10-6 用例和数字化能力

物联网和石油天然气行业

石油和天然气工业是最早开始利用技术力量的工业部门之一。其活动、流程和对数据的依赖性使数据分析被广泛应用于从勘探技术到工业预防性维护等领域。一般来说，油气田对于人类来说属于危险区，因此健康、安全和环境是至关重要的。在这种情况下，拥有机器对机器通信的数字智能能力可以帮助实现无人工操作，从而使环境更安全。因此物联网对这个行业来说是必要的。

物联网和数字化正在给油气行业带来显著的改善，包括以下方面。

■ **实现可行的数据采集：**具有成本效益且无处不在的通信技术，如工业WiFi、LTE和LoRa，使行业能够首次或实时地从某些资产获取数据，而且使全新的决策能力成为可能。

■ 推动整个价值链的上游、中游和下游的成本节约：成本节约可以通过利用IT和OT的数字融合来消除业务中的壁垒，并重新设计运营模式，从而降低成本、提高生产效率和改进现有资产的利用率。

■ 提高灵活性和降低风险：分析可用于将物联网基础设施生成的实时数据转化为可预测和可操作的意见，从而促进更快更好地决策、提高工人安全性和改善网络安全。

■ 提高生产力，弥合即将到来的人才缺口：利用物联网和协作系统将稀缺的专业知识扩展到偏远地区，在正确的时间为正确的团队提供实时信息，并提供一个有效的机制来吸引和培养下一代的工人，从而提高生产力。

■ 实现盈利增长：增长可以通过物联网来转换业务流程得以实现。通过卓越的运营和更好地利用现有资产（从而延长其寿命）来提高生产力，石油和天然气公司可以提高其利润。

因为油气行业的利润率非常低，所以明确的商业成果至关重要。因此，运营公司需要一个令人信服的商业案例来进行技术投资。帮助延长流动资产寿命或增加其正常运行时间和效率的技术得到了最大程度的优先考虑。有远见的石油和天然气公司认为，当今动荡的市场环境为它们提供了利用新技术获得竞争优势的机会。

对于油气公司来说，物联网价值的最大推动力主要依赖于资产监控和数据管理能力，以便从业务领域收集准确、及时的信息。价值还来自实时执行自动分析、诊断和优化的能力。这意味着需要集成来自多个数据源的数据，自动化收集数据，并快速分析数据，以便确定可执行的措施。

产生物联网价值的第二个领域来自先进的传感器、机器到机器的连接以及大数据分析，这些都有助于公司预测设备故障和维护需求，从而最大限度地减少停机时间。

对任何油气公司来说，数字化转型都不是一个容易的过程，一些障碍应该是可以预见的，比如整合新旧技术的复杂性。例如，大多数

新技术都利用了IP，但是许多遗留技术无法这样做。其他挑战包括以下方面：

- 需要自动形成分析结果，并快速确定和执行结果操作；
- 管道、炼油厂、油井等设备产生的数据量越来越大；
- 安全漏洞扩大；
- 独立的网络和部门。

图10-7提供了一些功能视图，这些功能可以帮助减轻这些障碍，并展示了随着时间的推移，每种功能的业务价值都在增加。物联网是它们的核心。

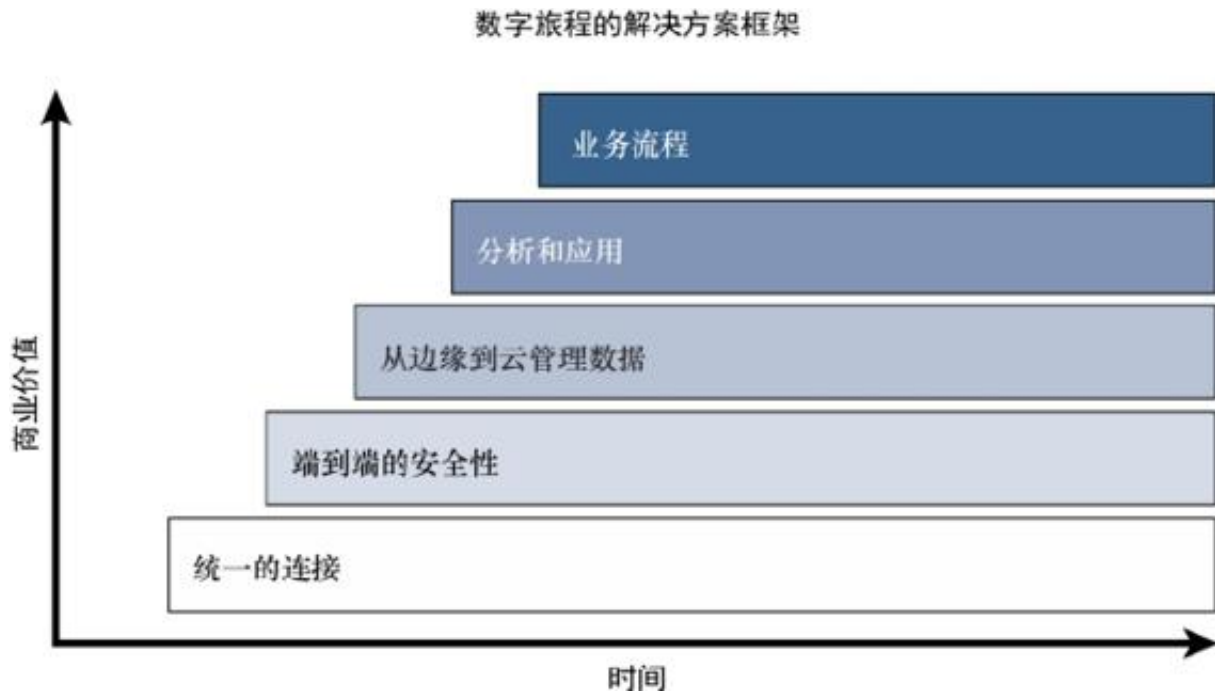


图10-7 物联网和价值驱动因素

10.3 提高运营效率

物联网正在帮助解决油气行业的一些主要挑战，包括：

- 在降低成本背景下的提升运营效率；
- 在工业网络攻击增加的背景下保证安全；
- 更快更好地做出决策。

如前所述，油气产业价值链主要分为上游、中游和下游3个部分。这3个部分在业务流程方面面临类似的挑战。物联网可以在各种不同的用例中帮助解决这些问题。

10.3.1 石油和天然气网络控制层次的普渡模型

在深入研究石油和天然气工业的具体物联网用例之前，需要重新回顾在第2章和第8章讨论过并在第9章应用于制造业的普渡控制层次结构模型。

在过程控制网络（PCN）中，自动化设备连接到一个网络（通常是硬件和软件的组合），该网络负责对关键基础设施（如炼油厂、石油和天然气管道、核电站等）进行指挥和控制。

PCN自动化设备（及其相关组件）构成一个控制系统，称为工业控制网络（ICN）。ICN监视在生产环境中执行各种功能的物理过程，包括控制、保护、安全和态势感知。

控制系统的用例包括监视控制和数据采集（SCADA）、分布式控制系统（DCS）。它们执行的一些功能包括管道操作，如沿着管道远程控制阀门（根据需要关闭或打开阀门），以及用于监控沿着管道移动设备的泵的操作。

随着时间的推移，ICN已经从独立的实体发展为更多的互联网络，它们也带来了IT网络所采用的技术元素。此外，OT人员已经认识到访问IT系统的必要性。IT和OT的这种融合是采用物联网架构的大多数行业面临的共同挑战，它要求OT和IT都具有允许系统间相互访问和信息交换的通信接口。

在如此复杂的系统中，这些组件之间的交互需要一个框架来定义组件之间的通信流，这取决于它们在流程中执行的功能。当今许多行业使用的著名框架是用于控制层次结构的普渡模型。该模型在第2章中简单介绍过，在第9章中具体应用于制造业。本章我们将探讨控制层级的普渡模型如何适用于油气行业的物联网。

控制层次的普渡模型有3个主要组成部分：设施、人员、控制和信息系统。控制和信息系统组件中包含了一些级别，这些级别用来定义和进一步分离企业或组织的OT（控制系统）和IT（信息系统）中的各个区域（见图10-8）。这些级别是在本章中与石油和天然气用例相关的具体引用。

企业区域	企业网络	第5级
	现场业务规划和物流网络	第4级
非军事区	非军事区——共享访问	
运营支持	现场运营和支持	第3级
过程控制/ SCADA区域	监管控制	第2级
	油气设备的基本控制	第1级
	过程控制和仪表总线网络	第0级

图10-8 普渡控制层次模型应用于油气加工

第0～2级表示批量、连续和离散控制；第3级是制造操作和控制；第4级及以上是业务规划和物流。控制层次的普渡模型也用于确定定义网络安全的ISA99/IEC-62443标准中的层次和对象。更详细地查看这些级别，我们可以发现它们为设备提供的功能以一种从底层到顶层描述信息流的方式进行了分层。模型的层次可以分为3个独立的组。

■ 操作级别（0～3级）：0级可以找到物联网中的“物”，比如传感器、电机、执行器和仪表。第1级是炼油厂可编程逻辑控制器

（PLC），以及用于管道SCADA管理的远程终端单元（RTU）和控制处理器。这些设备负责编程或从处于生产/流程级别的第0级设备中提取读数。第2级是工程工作站或数据历史的存储位置；它们负责记录、收集和填充保存进程数据历史的数据库。第3级是人机交互设备运行的地方；服务器运行的软件提供一个图形用户界面来表示进程及其操作、传感器读数和指定的阈值，以帮助监视进程、显示警报等。

■ 业务级别（第4级和第5级）：这些是传统IT系统所在的级别，包括文件和打印服务器、企业电子邮件应用程序、HR系统等，以及企业Internet连接或企业网络的VPN访问。

■ 非军事区（DMZ）：DMZ也称为3.5级，是分隔OT和IT域的区域。通常驻留在DMZ中的系统和应用程序是远程访问解决方案、防病毒和补丁管理服务器、报告仪表板应用程序等。

10.3.2 物联网的石油和天然气使用案例

提高运营效率是许多行业高管的头等大事，尤其是考虑到从加工到最终产品分销至最终消费者的碳氢化合物勘探和开采的成本。

为了降低成本和提高效率，物联网架构需要针对关键油气行业的不同用例进行定制，包括连接的炼油厂、连接的油田和连接的管道。这些用例说明了如何在石油和天然气行业的操作工作流程中采用技术，以优化生产力、降低成本，并使运营决策过程更快、更全面。

1. 连接的油田

一个为支持油气行业上游业务而构建的物联网架构的典型用例是连接的油田，如图10-9所示。

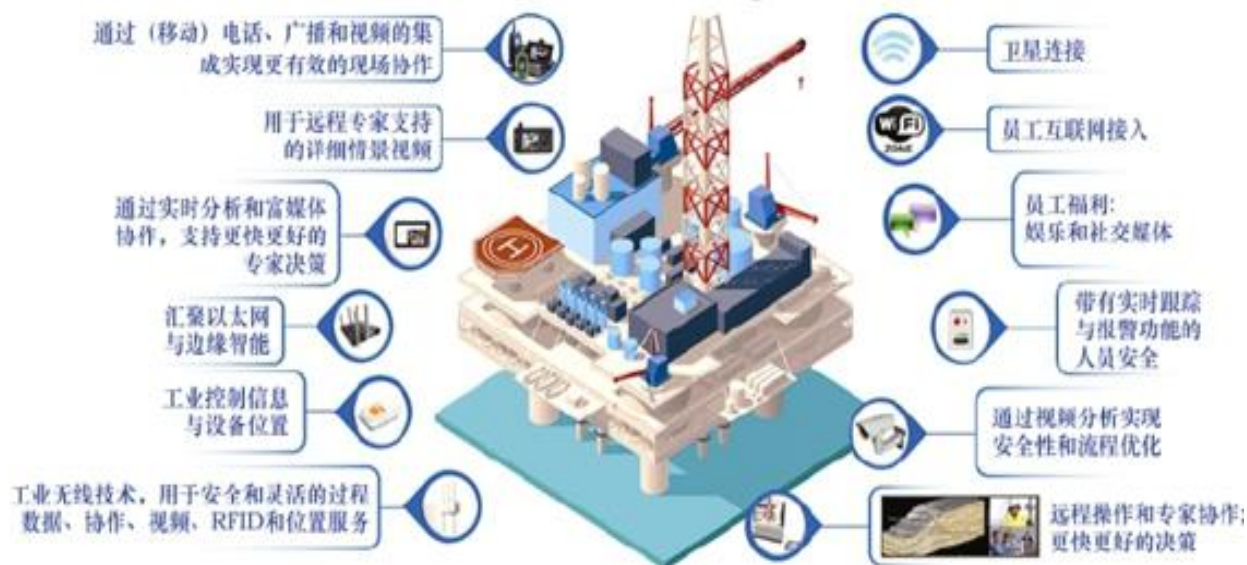


图10-9 连接的油田的物联网用例

无论是陆地还是海上，油田是一个从许多地下或海底油井提取原油的地区。通常情况下，海上油田位于偏远地区或海洋中部，因此很难进入和连通。因此，健壮且独立的通信基础设施是至关重要的。海上石油钻井平台的基础设施需要对钻井系统的运行、与总部地点的通信，以及健康、安全和环境监测系统提供态势感知支持，这只是其中的一部分。此外，由于在油田工作的人员长期居住在偏远地区，因此还需要进行娱乐和社交媒体交流。

由于油田地处偏远及其孤立性，大部分通信基础设施是基于无线技术。

2. 连接的管道

油气价值链中游的关键资产之一是管道。管道之所以重要，是因为它们是勘探、开采和精炼作业之间的纽带。管道需要确保产品以24×7全天候持续供应和精炼。运营挑战很多，而且性质各不相同。以下是一些具体困难。

■ 长距离和大面积的地理覆盖：管道可能非常长。例如，目前最长的天然气管道的世界纪录保持者横跨中国东西，最长的一段达9100

公里。

■ 恶劣的环境：管道可以在水下、沙漠、高山和其他恶劣的环境跨越很长的距离。

■ 与一般基础设施隔离：管道通常远离主要道路或高速公路，这使得与管道上的传感器和仪表的通信成为一个挑战。

■ 泄漏：石油和天然气管道传输的是高度易燃的物质。具有检测管道沿线的泄漏的能力很重要，这样可以避免火灾、爆炸和周围地区的污染。

■ 地震和山体滑坡：山体滑坡和地震会影响管道的完整性，因此必须监测管道周边的地震活动。

■ 盗窃和破坏公物：盗窃和破坏公物的现象在管道沿线司空见惯，盗贼利用管道获取产品。除了造成显而易见的经济损失外，还存在与盗窃和破坏有关的风险，这些风险可能对环境 and 基础设施造成重大破坏。

图10-10展示了联网管道的一些常见物联网用例。



图10-10 连接的管道物联网用例

实现这些用例的指导原则是确保连接的管道通信网络支持以下特性：

- 高可用性和冗余；
- 多层面安全（包括网络层面及物理层面）；
- 遵守开放标准；
- 多业务支持（用于控制室和使用连接管道通信网络的运营网络）。

3. 连接的炼油厂

精炼厂和加工厂通常是大型综合体，有多个建筑物、储罐和相互连接的地下和地上管道系统。与油田一样，炼油厂也是全天候运转，有复杂的系统不断监控操作参数，如流量、油箱液位、温度、振动、压力，甚至监测原油精炼过程中产生的危险或爆炸性气体的存在。

图10-11突出显示了现代石油或天然气精炼厂中一些常见的物联网用例。



图10-11 连接的炼油厂物联网用例

炼油厂是固定员工、外部公司和承包商的工作场所，他们在工厂周围从事各种各样的工作。过程控制操作员确保精炼过程按预期运行；他们在适当的地方监控和优化流程。炼油厂还包括维护人员，他们使炼油设备处于良好的工作状态，并在需要时进行维修。通过实施控制、安全和管理系统，所有这些系统和人员都以有效、高效和安全的方式工作。这些系统需要快速可靠的通信系统。

10.4 油气物联网架构

为了解决石油和天然气领域的各种物联网用例，本节将各种网络和安全功能映射到前面讨论的普渡模型。例如，图10-12所示的连接炼油厂参考体系结构演示了如何将有线和无线通信系统互连以提供快速可靠的通信。

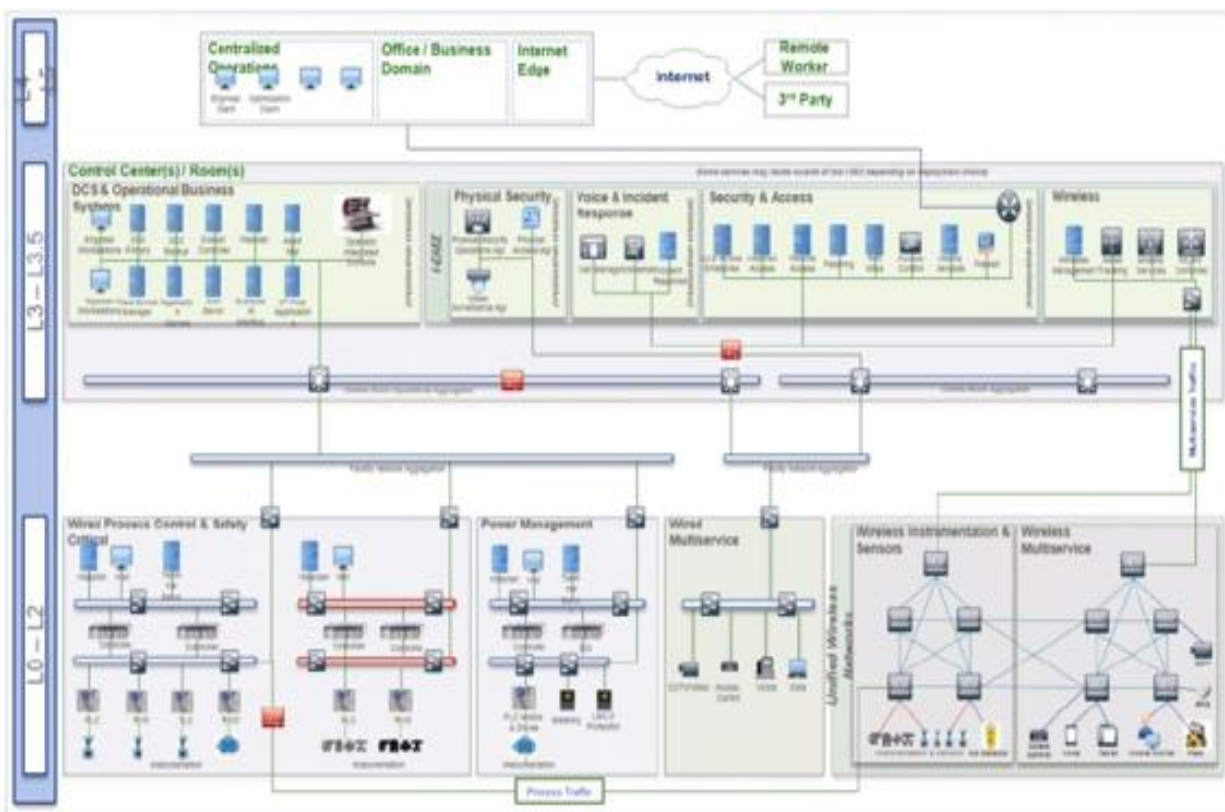


图10-12 油气参考体系结构

该体系结构使用炼油厂基础设施的不同系统构建，遵循ISA99/IEC-62443标准，该标准基于普渡控制层次模型。这些系统可以分为3大类：控制室网络、有线网络和无线网络。

10.4.1 石油和天然气控制室网络

控制室网络在炼油厂的控制室之外运行。控制室旨在为现场操作提供集中的可视性和控制。控制室网络的一些示例包括以下内容。

- 分布式控制系统：分布式控制系统使用自治控制器部署在整个工厂中，它们的操作控制集中执行。
- 物理安全：包括视频监控/闭路电视系统、门禁系统等。

■ **集中式无线管理：**描述用于管理工厂中部署的无线网络的软件应用程序，如网络管理应用程序、资产和人员定位服务等。

■ **安全和访问服务：**由于控制室是炼油厂和外部世界之间的连接点，这里的网络和服务通常需要入侵检测和预防系统以及防火墙。

10.4.2 石油和天然气的有线网络

精炼厂或加工厂的有线网络基础设施可以分为以下几类。

■ **有线过程控制：**有线过程控制网络支持过程控制设备，包括用于监控和优化生产过程的传感器、控制器和仪表。

■ **有线安全关键系统：**顾名思义，安全关键系统是负责正常关机或紧急停机的系统，或者是操作生产过程中特定关键功能的系统。

■ **有线能源管理：**这些系统负责生产设施的能源整合。

■ **有线多服务：**包括提供协作或物理安全的系统，通常使用的技术是语音和视频。

10.4.3 石油和天然气的无线网络

虽然有线基础设施（局域网和广域网）是实现这种体系结构的关键，但无线网络通常是炼油厂最常用的网络元素之一。石油和天然气环境中通常有两种主要类型的工业无线网络。

■ **无线多业务：**这些网络（包括IEEE 802.11/WiFi、LTE等）为许多协议设备提供了无线连接的平台。

■ **无线过程控制：**这些网络通常具有确定性的IEEE 802.15.4设备（如ISA100.11a或WirelessHART）。

这两种类型的工业无线网络可以组合成一个统一的架构，本章后文将会讨论。

1. 无线多业务：IEEE 802.11 mesh网络

IEEE 802.11无线mesh网络在油气环境中非常流行。802.11 mesh的主要优点之一是它不需要将每个接入点（AP）物理地连接到以太网。正如我们想象的，在石油化工精炼厂或石油钻机中安装电缆是非常昂贵的。安装活动非常耗时，有时非常复杂。例如，在石油钻井平台上安装光纤或铜缆时，通常需要钻透船体结构上的金属壁或舱壁，这通常是不允许的。在有爆炸性气体或粉末的生产工厂周围挖掘，则需要在安装过程中停止生产。通常，安装数据线的成本要比设备本身的成本高出几个数量级。

然而，对于mesh网络，AP只需要供电，它与其他AP形成无线回程连接。在802.11 mesh中，一旦部署了初始的基础设施，通过添加额外的接入点来扩展它的覆盖范围会相对简单。有关802.11无线mesh的详细信息，请参阅第14章。

2. 无线过程控制

无线场域网络（WFN）由一个自组式mesh无线设备（各种类型的传感器和制动器、现场移动设备和现场端点）和网关组成，它们服务一个小的连通区域（通常是以WFN网关为中点的50~100米半径区域），通过无线信道连接到局域网，以实现过程系统的监视和控制。

图10-13所示为一个WFN mesh架构。在无线现场网络中部署了传感器网状网络来测量和读取控制网络中PCN应用程序中的数据。传感器与传感器网关通信，后者负责将802.15.4（WirelessHART、ISA100.11等）协议转换为IP。

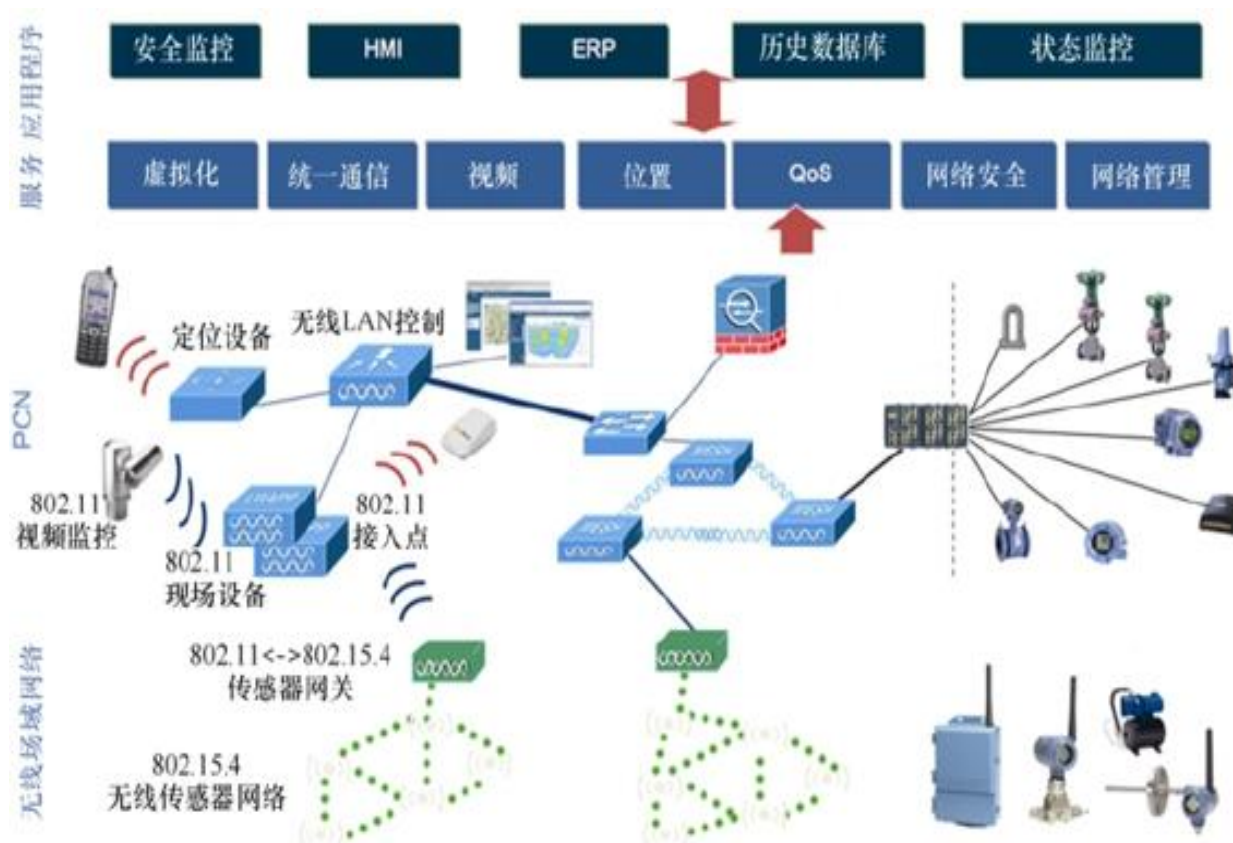


图10-13 802.11无线mesh中的WFN mesh架构

然后，传感器网关与无线网络基础设施通信，该基础设施负责向上游转发流量，消耗和报告传感器数据的应用程序驻留在这里。相同的无线LAN基础设施可以被并行地用于提供各种其他用例，例如语音和位置服务。

WFN mesh网络通常基于行业标准IEEE 802.15.4无线网络技术，而后者又为其他几种无线标准奠定了基础，包括WirelessHART（IEC-62591）和ISA100.11a。

基于IEEE 802.15.4的传感器可以提供重要的过程控制信息，如管道中的气体流量、炼油厂的锅炉温度、煤油罐的液位或压缩机的振动。这些类型的确定性网络也被用来以一种确定可预测的方式控制泵和马达，这是基于竞争的WiFi无法实现的。

要部署基于802.15.4的确定性无线网络，需要下面几个组件：

- 无线传感器网关，提供无线现场网络 and 控制系统之间的互连；
- 网络控制器，提供无线现场网络的业务流程；
- 协议网关，用于在无线现场网络和PLC中实现的协议栈之间进行转换。

WirelessHART和ISA100.11a无线现场设备在工业网络中以ISA95 0级运行。WirelessHART和ISA100.11a都实现了IEEE 802.15.4无线协议，其工作频率为2.4GHz。这些无线技术采用了直接序列扩频（DSSS）技术和信道跳变技术，以确保通信的安全性和可靠性，并采用时分多址（TDMA）技术来确保网络设备之间的通信延迟是受控的。

基于802.15.4的网络具有确定性，在过程控制网络中有广泛的应用前景。这意味着所有设备都是时间同步的，并在预定义的、预先安排的、固定的时间段内进行通信。这些时间段被分组在超帧中，这些超帧按照指定的速率重复。这样做的好处是，延迟敏感控制系统不必处理空中的拥塞，也不必等待传输帧。当控制器发送信号时，系统会立即发送。

无线接入的确定性控制对可靠性有重要影响。例如，WirelessHART能够在工业过程环境中提供99.9%的端到端的可靠性。这是通过使用信道跳跃和自愈能力的mesh网络实现的。当路径恶化或被阻塞时，网络会采取行动进行自动修复，并在阻塞路径的障碍点周围寻找替代路径。

WFN技术在2.4 GHz的ISM未授权公共使用频段运行。这些系统必须与其他无线系统共享相同的RF频谱，如WiFi、DECT、蓝牙和超宽带（UWB），而且它们还会受到2.4 GHz频谱中发出的其他设备的干扰（例如微波炉、USB 3.0设备和电缆、汽车报警器）。然而，WirelessHART和ISA100.11使用的确定性机制有助于将干扰、跳频、多路径mesh路由、信道白名单/黑名单以及其他可能影响无线领域网络性能和可靠性的因素的影响降至最低。

由于使用这些类型网络的应用程序只需要最小的带宽，但同时需要可预测的低延迟通信，因此基于WirelessHART和ISA100.11的系统比WiFi或类似的系统更适合于控制系统。802.15.4网络提供的典型最大带宽约为250kbit/s，与最新的WiFi标准相比非常慢。然而，相较于低带宽，它的传输范围更大，这是该类型系统的优点之一。

WirelessHART和ISA100.11a网关在工业网络的第1级运行（见图10-8）。无线现场网络必须连接到局域网，以提供无线传感器/控制设备、ISA95控制系统（如PLCs）和无线传感器网络控制系统之间的通信。

WFN与有线的基础设施之间的通信通过无线现场网络网关进行。无线现场网络的网关将无线传感器协议（如ISA100.11和WirelessHART）转换成适合与PLC通信的LAN路由协议套件。

无线现场网络也可以通过以太网双宿连接（即每个无线场域网络有两个无线传感器网关）到局域网接入交换机，为所有无线场域网络设备提供备用路径。当双宿连接到无线现场网络时，每个无线传感器网关必须连接到单独的局域网接入交换机，而单独的局域网接入交换机又连接到单独的局域网分布交换机，从而确保无线场域网络设备的双网络路径。

根据供应商的产品实现，WFN设备与PLC之间的通信可能以以下3种方式发生。

■ 无线现场网络网关可以直接与PLC以太网端口连接以控制流量。在这种部署模式下，无线现场网络的网关直接连接到PLC以太网端口。

■ 无线现场网络网关可以与双技术无线接入系统（例如WirelessHART和IEEE 802.11）集成在一个无线接入点。在这种部署配置中，双技术无线接入点必须向LAN接入交换机提供带有IEEE 802.1Q VLAN标记的以太网端口。目的地为IEEE 802.11无线局域网控制器（CAPWAP隧道；参见RFC 5415）的流量通过一个VLAN流向中央无线LAN

控制器，无线传感器的流量通过终接于端口LAN接入交换机中的一个独立VLAN流向直接连接的PLC控制以太网端口。另一种选择是双技术无线接入点指向现有的两个物理以太网端口，一个用于连接端口LAN接入交换机，该交换机用于将流量发送至IEEE802.11无线LAN控制器，另一个单独的以太网端口用于连接控制PLC。图10-14展示了炼油厂中与ISA100.11网络相结合的WiFi网络。在本例中，ISA100.11用于在传感器和执行器之间建立控制环路，同样的接入点也在设施中提供WiFi mesh服务。

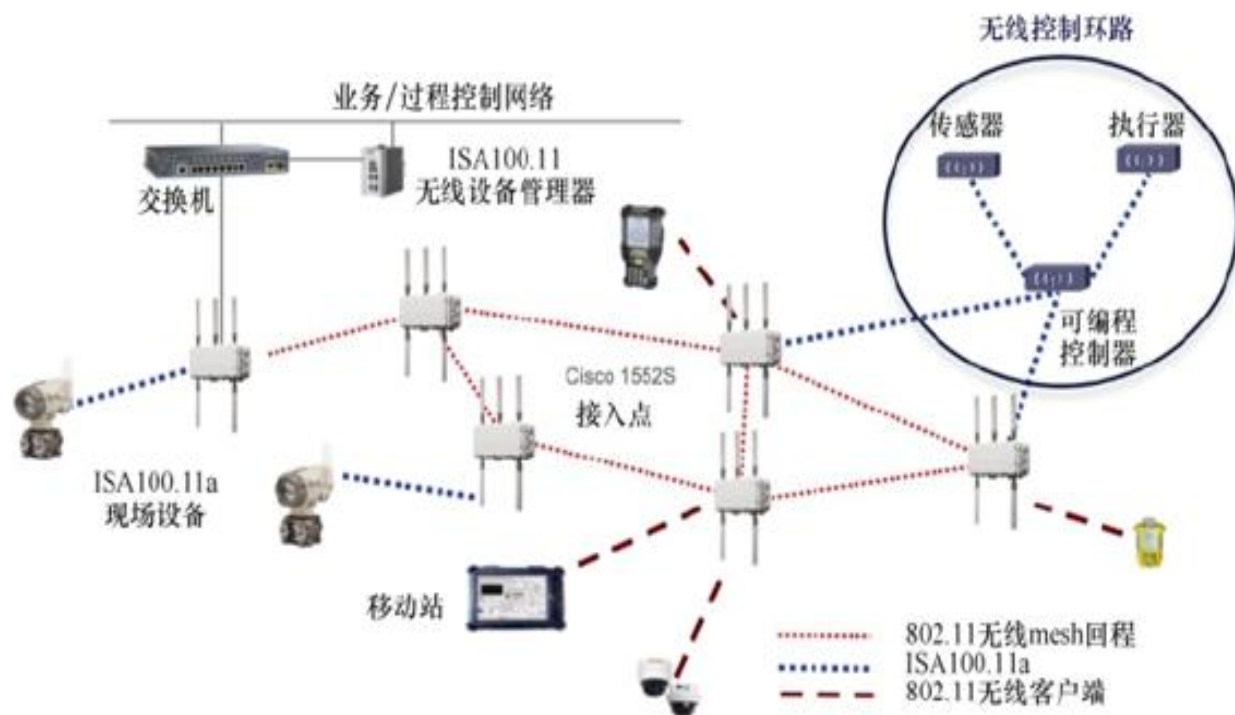


图10-14 结合了ISA100.11网络的WiFi示例

■ 一些无线现场网络供应商要求控制PLC流量的无线域网络设备通过协议转换器（如ISA100.11a IPv6到IPv4的协议转换）。协议转换后的流量通过入侵检测和防火墙功能进行转发，然后通过IEEE 802.1Q中继转发到接入交换机上的VLAN，最后通过PLC控制以太网端口转发给控制PLC。

10.4.4 石油和天然气行业的无线使用案例

下面将介绍基于802.11 WLAN技术的工业无线网络在石油和天然气行业中最流行的一些应用。

1. 移动过程控制网络运营商

在移动过程控制网络运营商场景中，设备（例如，工厂、管道、石油钻井平台）在给定位的战略区域具有无处不在的无线覆盖或只覆盖了部分。PCN操作员的职责之一是确保工厂的流程得到充分优化并可靠地运行。完成这项任务需要工具和应用程序来监测和管理现场所使用的信息系统。虽然这些应用程序运行的HMI位于工厂的控制室，但PCN操作员有时需要在工厂的不同区域进行户外工作，以便对不同的系统进行故障排除或维护。

可在危险区域使用的便携式运营商技术（如平板电脑、笔记本电脑、智能手机或可穿戴设备）与无处不在的WiFi覆盖相结合，有助于优化PCN运营商的工作效率。例如，通过无缝的WiFi覆盖，PCN运营商可以从工厂的任何地方访问工作单、示意图和操作手册。

2. 检修周期

检修周期是指工厂为检查和维护而停止生产的预定时间，这需要正常的停机操作。在此期间，工厂不是在精炼产品，这产生了明显的负面（甚至是重大的）财务影响，因此恢复运营的时间非常关键。

在检修期间，工厂员工、设备供应商和外部承包商昼夜不停地从事高风险和复杂的活动，以期尽快使工厂投入运行，避免发生任何HSE（健康、安全 and 环境）事故。根据检修的规模，在最繁忙的时候可能会有成千上万的工人同时工作。

传统意义上，检修是一个双向的过程，工程师在工厂范围内工作，通过无线电与中心工程师沟通，工程师为任务提供支持和验收。部署无线基础设施，为员工提供独立和远程工作的工具和流程，可以

节省时间和金钱。无线移动技术允许工程工具和工作任务应用程序直接链接到中央工作流和完井工具。

此外，大多数进行检修的工人通常不熟悉场地、批准流程等，因此，生产力受到影响，HSE风险因素显著增加。利用无孔不入的工业无线技术，结合项目工作范围、人力资源数据、门禁控制数据、工人信息等企业数据源，可以实时跟踪和优化生产效率，而不是在项目完成之后再进行改善。人员和设备的位置跟踪可以实时监控、管理和调整。还可以启用电子许可和设备跟踪，并分析和处理疲劳监测等人为因素。

工厂检修用例有助于极大地加快完成、工作流、活动记录、安全性和合规性。

3. 远程专家

炼油厂、管道或石油钻井平台面临的一个最大挑战是，由于不可预见的设备或电力停机，会导致生产力和盈利能力损失。由于劳动力年轻，缺乏经验，特别是对于老的系统和基础设施而言，要确保在适当的地点和时间提供适当的资源是一项具有挑战性的工作，而且通常是不可能完成的。公司可能需要许多来自不同学科的主题专家来实时实地协作处理各种情况，但是他们可能希望避免与之相关的费用。

利用视频、语音和协作技术，通过优化的通信基础设施使现场的工厂工作人员与远程专家联系，可获取所需的专业知识。有经验的操作员和具有特定技能的工作人员能够立即帮助完成支持任务、培训并处理紧急情况，而无论身处何处，他们可以立即与控制室或现场工作人员联系。

当需要咨询、指导和建议时，这就创建了一个集中的专家库。为了遵守风险管理和法规，可以通过数字化的语音、视频和消息记录在时间轴上捕获交互的所有方面。这些录音也可以用作培训工具。

4. 人身安全

除了用于工厂维护、废水处理和产品处理的化学品外，在精炼和加工过程中使用的许多化学品意味着如果工厂意外泄漏，则会造成潜在的安全风险，这些泄漏可能会影响到员工、承包商、急救人员以及工厂周围的当地社区。

在运输过程中，由于管道故障、储罐泄漏、设备故障和泄漏，可能会发生硫化氢（ H_2S ）、二氧化硫（ SO_2 ）和挥发性有机化合物（VOC）的泄漏。这类事件可能造成灾难性的影响，包括危害环境和生命。例如，在2010年5月的Deepwater Horizon石油泄漏事件中，有11人丧生，490万桶原油流入墨西哥湾。另一个例子是，1984年12月印度UCIL核电站的博帕尔灾难，一场事故导致该核电站的气体泄漏，导致超过50万人暴露在有毒气体中，死亡人数超过2000人，另有数千人受重伤。

此外，由于坠落或移动物体而导致的绊倒、跌倒而受伤，也是员工安全的常见风险。能够监测固定位置的气体泄漏和液体泄漏，以及监测流动工人是否有可能接触泄漏，是一项重要的安全功能。能够快速检测和隔离危险区域可以挽救生命，并有助于满足遵守法规。此外，准确了解核电站周围员工的实际位置，有助于确保泄漏区内受到影响的人员得到识别和疏散，并有助于防止泄漏区以外的人员进入。

固定无线气体传感器可以安装在泄漏有潜在危险的关键位置，工作人员可以配备便携式气体探测器，通过无线基础设施进行通信。员工的位置跟踪可以通过RFID标签实现，这些标签可以集成到一个设备中，如气体探测器或移动手持设备；也可以通过一个单独的定位标签实现。固定传感器和无线传感器都可以覆盖在工厂的地图上，以实时可见，信息可以通过无线基础设施传送到集中控制室。

对于工作中工人倒地的情况，可以在移动设备或标签中使用加速计来快速检测突然倒下的人员。信息可以被发送回中央监控位置，甚至可以与来自移动设备的实时视频连接，以显示这是一个真实的事

件，还是只是一个掉落设备。同样，信息是通过无线基础设施发送的。

5. 资产位置跟踪

通过WiFi网络上的RFID标签跟踪资产位置是许多工业应用的关键技术。通过集成的位置跟踪，工厂管理员、安全人员、用户、资产所有者以及健康和安全管理已经意识到基于位置服务的巨大好处，这使他们能够更好地解决工厂中的一些关键问题，包括：

- 快速有效地定位有价值的资产和关键人员；
- 通过有效的资产和人员配置来提高生产力；
- 通过便携式气体探测器和传感器，以及工作状态指示器，确保人员安全；
- 减少因未经授权从公司场所移除资产而造成的盗窃损失；
- 协调WiFi设备位置与安全策略实施，并确定恶意设备的位置；
- 监控其环境中关键资产的健康状况和状态，并及时收到变更通知。

管理整个工厂的关键资产和人员的位置是提高运营效率的关键。通过在设备、车辆和集装箱上粘贴有源RFID标签，并在整个基础设施中部署便携式气体探测器和传感器，工厂可以极大地提高其运行效率、员工安全性和合规性。

10.4.5 物联网网络安全风险控制框架

流程自动化团队的首要需求是正常运行时间和流程完整性。因此，网络安全最终是保护正常运行时间和完整性的一种手段；事实

上，流程自动化团队通常愿意为了流程正常运行时间和完整性而在网络安全方面达成妥协。石油和天然气以及几乎所有其他自动化工业历史上都依赖物理分离来保护其OT生产网络。历史上，SCADA网络和用于控制和监视制造业、公用事业、发电和其他系统的分布式控制系统（DCS）被设计为与所有其他网络物理分离。

人们认为，这种物理上的隔离可以防止网络攻击，而网络攻击可能起源于网络之外（这显然不适用于完全隔离的传统串行SCADA系统）。此外，由于所部署的系统没有系统地更新最新的防病毒签名，而且它们的操作系统没有针对已知的漏洞打补丁，因此几乎没有采取任何行动来阻止可能已经发生的网络攻击。

由于近年来以太网和IP技术的快速发展，这种物理上的隔离模式显然不再可行。随着石油和天然气公司不断采用新技术和新用例，新的和多样化的设备正在被连接到聚合网络。这带来了更广泛的安全攻击挑战（有意的、无意的、外部的和内部的）的潜在威胁，公司需要扩展其响应，而不仅仅在物理上隔离，它通常被称为隐匿安全。

物理隔离并没有帮助阻止Stuxnet，而且类似的攻击已经证明，即使是隔离最彻底的网络，也可能通过USB闪存驱动器上引入的恶意软件进行本地访问而变得脆弱。此外，为了更好地进行信息流和决策，需要工业网络与系统和数据应用的互联。报告、合规性监控和控制部署在PCN环境中的系统状态，可以在任何给定时间提供关于OT环境的风险级别和暴露程度的必要信息。

成本节约是一个同样重要的驱动因素，此外还有提升监控和通过安全、灵活和标准化的平台促进业务敏捷性的能力。能够安全地更新操作系统和AV签名，而不是雇用大量的现场技术人员在不同地点之间移动和使用固定的媒体，这样可以显著降低运营成本。所有这些发展都提高了网络安全的重要性，使之成为石油和天然气行业许多首席信息官的首要任务之一。

PCN采用风险控制框架，以更好地保护关键OT系统。这个框架映射了一组实践和控制来对抗PCN中最重要的攻击载体。这些控制和实践如

图10-15所示。

使用风险控制框架，可以实现一个更健壮的分层安全模式。这种模式试图在启用系统连接的同时，确保安全地处理连接，并限制攻击者利用系统的能力。

风险控制框架涉及的主要领域分为5大支柱。

■ **组织**：作为规划阶段的一部分，需要在网络或系统的整个生命周期中建立和遵循策略和流程，并使用必要的指示板和报告对其进行补充。组成各种系统的部件清单需要准确和详细。

■ **加固**：该支柱涉及网络分段的实现，它将IT和OT环境分开，并控制它们之间的通信流。系统补丁、防病毒保护和便携式媒体安全确保防范已知威胁，而物理安全防止未经授权的个人访问设备。

■ **检测**：这是监视阶段的一部分，在此阶段，读者将查找PCN中的任何异常行为，并识别用于检测恶意软件或其他安全威胁的控件。

■ **防护**：该支柱中包含的区域确保有足够的合法数据收集，可以分析这些数据来确定威胁及其应对措施。

■ **响应**：最后一个支柱负责确保必要的卫生措施到位，执行正确的备份和恢复策略以及灾难恢复。

组织	加固		防护	检测	响应
安全策略	网络分段 安全存储		安全日志的 收集和管理	主动监控	事件响应
处理库存	PCN访问 和控制	IPS/签名		安全监控	
资产盘点 和管理	防病毒	白名单和 黑名单		异常检测	灾难恢复
评估	系统补丁	便携式媒体安全	KPI与分析	恶意程序检测	
变更管理	加密	工业无线	威胁防御	入侵检测	持续改进
教育 及意识				虚拟化	
仪表板和报告	构建		运行	监控	管理
计划					

图10-15 PCN风险控制框架

PCN风险控制框架是一种新的模式，提供深度防御措施来组织、阻挡、收集、防御、检测和应对网络安全威胁。由于过程控制网络设备在该领域存在多年，因此该模式必须解决现有设备和新系统的问题。

10.4.6 保护油气PCN：背景

用于PCN的风险控制框架最重要的目标之一是就HSE（健康、安全 and 环境）事件以及网络事件导致的计划外中断的项目和/或产品损失而言，为了维系清白的历史而去支持行业的需求。

为了支持这一目标，需要满足一些详细的要求。这些特定的需求被设计来完成以下工作：

- 维护一个集中解决方案，以监控、管理和报告现场设备的合规状态；

- 提供跨业务的一个简化、标准化的解决方案；
- 在环境中引入更高的灵活性和敏捷性；
- 维持业务部门认为可以接受的操作安全级别。

通过满足这些需求，业务中的许多涉众都可以从安全架构中获益。对保密性、完整性和高可用性的强调突出了这一事实，即这些涉众运行的关键基础设施在任何情况下都不应该受到损害。要不惜一切代价避免可能造成人员伤亡和严重环境破坏的重大事故和灾害。因此，尽管现在需要连接这些控制系统（即使是那些几年前部署的安全性有限的系统），但同时需要将接口控制在最低限度，并始终严格控制。图 10-16 显示了一个应用于油气行业的 PCN安全参考体系结构示例。



图10-16 安全运营参考体系结构

这个参考体系结构包括两个主要组件：安全中心和安全站点（它们承载着有助于保护油气PCN的主要用例）。其指导原则是，不仅将安全中心用作查看PCN环境安全态势的中心点，而且还将其用作环境的单一入口点。合规性和报告的集中点有时可以使整个现场资产在全局范围内可见，从而可以从单一位置查看石油钻井平台、管道和炼油厂。这种方法的主要优点是大大降低了控制多个入口点所涉及的风险。

10.4.7 保护油气PCN：用例和要求

风险控制框架需要具有灵活性，并且能够执行控制措施并收集关于这些控制措施的信息和报告。主要的用例是资产盘点、远程访问控制、补丁管理、防病毒控制和安全智能。

1. 实时资产盘点

资产盘点提供了对整个油气设施中不同PCN系统中部署的OT资产的可见性。识别OT资产及其属性的能力为实现其他安全管理（如补丁管理）提供了基础。资产盘点功能还需要支持准确的维护记录。

资产信息应该合并到OT资产数据库中，并且使安装在每个组件上的软件可见，而且还要支持对事件和/或问题的主动管理和纠正性管理。为了支持其他业务实践或需求，可以收集其他信息。资产信息通常存储在关系数据库中，该数据库允许查询，并能够与外部报告工具集成。

2. 远程访问控制

对PCN的外部远程访问应支持来自组织内网和外部供应商的连接，访问应符合风险控制框架中定义的要求。实现PCN安全访问（包括远程访问）依赖于加密技术和强身份验证方法的组合，以确保用户或系统仅限于相应的PCN组件。

通过在PCN环境中强制设置中心入口点，并通过使用虚拟专用网络（使用诸如IPSec、RDP、VNC或SSH等分层技术）确保操作中心和站点之间的连接，可以严格控制访问，并且更容易管理。图 10-17 显示了一个第三方或远程工作人员到安全站点上的 PCN 资产之间的连接示例。

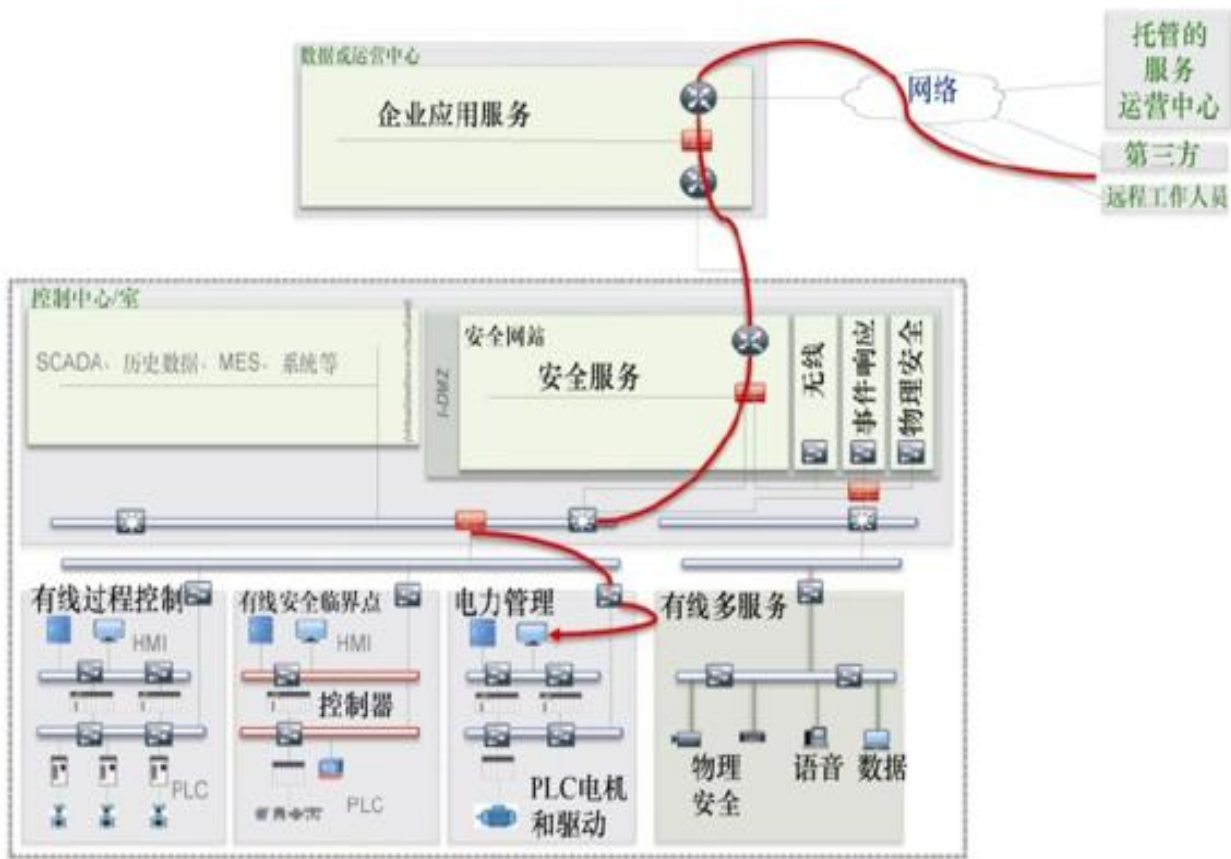


图10-17 远程访问会话流进入到PCN中

3. 补丁管理

操作系统补丁对于OT环境的整体安全至关重要，它们与部署在PCN中的IT组件密切相关。补丁管理确保已知的漏洞已得到解决，而不会成为未经授权的访问或用于进行恶意活动的潜在后门。

为了最有效地与基于Microsoft Windows的组件（主要用于PCN）进行交互，Windows Server Update Services（WSUS）应使用其他逻辑。

辑实现，以确保简化并能生成有意义的报告。这些报告有助于确定PCN的潜在弱点。

这种解决方案可以帮助交付准确合格的PCN供应商补丁，这些补丁往往会定期发布。该解决方案可以将合格的补丁列表（QPL）链接到补丁解决方案中的组，从而确保改进的补丁处理响应时间，并通过删除手动创建的QPL来减少出错的可能性。图10-18显示了部署在炼油厂并支持各种第三方工业系统的Microsoft WSUS补丁管理解决方案。

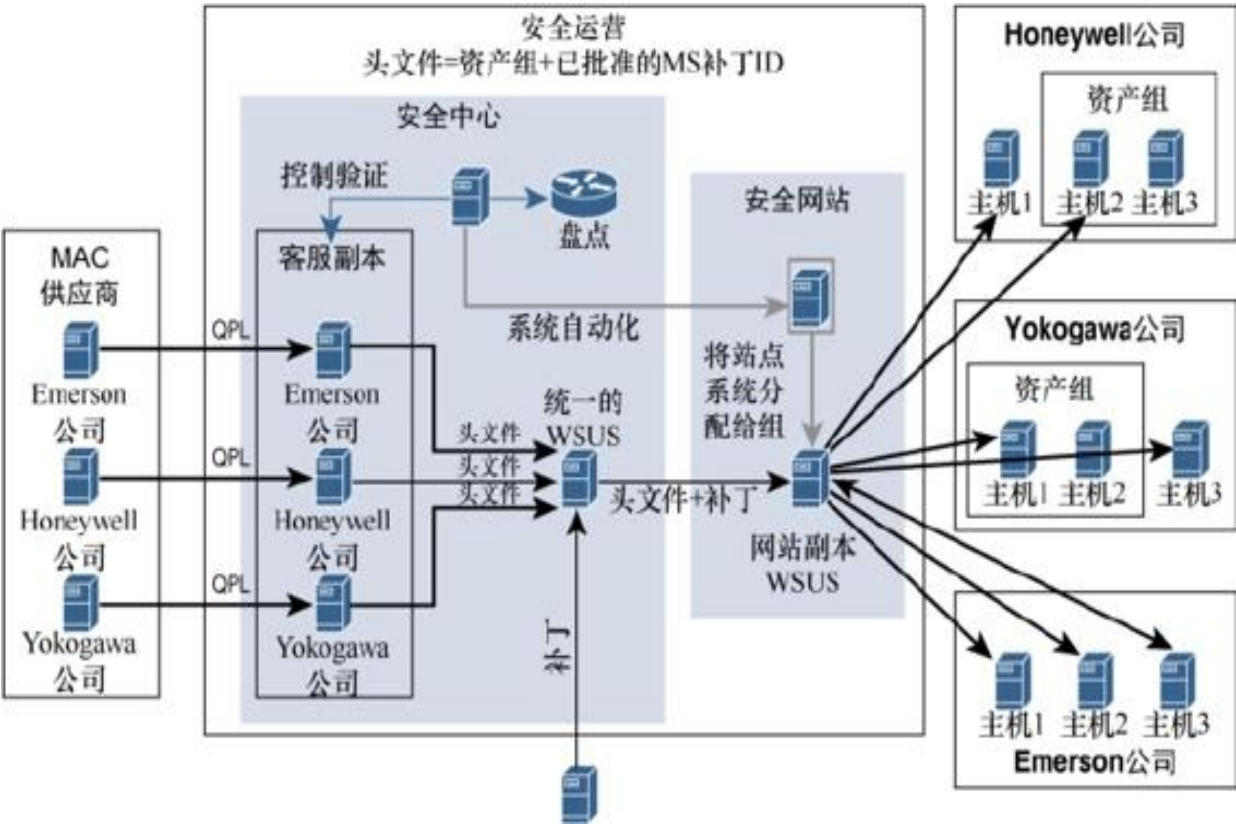


图10-18 微软工业补丁管理实现的示例

使用资产盘点功能收集的信息可以确定在PCN中的任何组件上安装了哪些补丁。了解建议安装的补丁程序（通过QPL）以及PCN中的给定OT资产当前安装了哪些补丁，可以将所需的和缺失的补丁映射到单个资产处。

4. 防病毒（AV）管理

就像刚刚为OS安全补丁提供的解决方案一样，AV签名更新也需要一个过程。标准AV提供商提供的管理解决方案可以结合资产盘点功能来部署已批准的AV签名文件更新。将特定设备匹配到签名更新要求后，AV管理解决方案可以推出AV签名。

一个健壮的AV补丁管理系统对于确保PCN中的OT资产免受已知威胁和漏洞的影响是非常重要的，特别是因为许多系统运行在著名的OS上，比如Microsoft Windows。在许多情况下，漏洞是通过已知的漏洞实现的，而这些漏洞恰好存在于资产没有安装补丁的地方。

5. 安全情报和异常检测

准确的资产盘点至关重要，因为正如人们所说“你无法确保你不知道的东西”。资产盘点允许我们监控PCN资产中部署的所有资产与所需的OS补丁和AV签名基线之间的差异，以及为了纠正任何不一致需要做些什么。然而，这并不是事情的全部。监控这些资产在网络上的活动，以及报告网络或设备行为中的异常或意外变化的能力，有助于对被动防御机制和防御网络威胁所需的流程和程序进行有意义的管理。

注释：被动防御是指不需要人工干预就可以提供防御机制的系统或组件。

由于PCN环境的性质，我们需要解决一些重要的挑战。例如，许多不同的PCN解决方案和系统被用于大多数油气设施，各种工业协议和访问方法已在不同的网络技术上实现。一个有效的系统需要能够避免这种可变性，并以清晰和简洁的方式呈现所有信息，以便能够及时地管理和操作它。如果集中的安全运营中心（SOC）也在监控设备，则必须同时收集并更新操作系统和网络日志，并上传到SIEM（安全信息和事件管理）系统中，以便进一步分析。

10.4.8 用于预测性资产监控的数据分析

对工厂机器和资产（如马达、阀门和泵）进行实时数据分析是优化性能和在问题发生前主动检测的宝贵方法。

传统上，设备的评估是基于预防性的时间计划进行的，或者在最坏的情况下，在出现问题后修复或更换设备。在许多情况下，即使设备或部件不需要根据估计的使用寿命来确定，也可以进行更换。例如，一个压力传感器可能处于完美的工作状态，并且可能还能再使用10年，但由于严格的更换计划，它在需要更换前几年就被更换了，从而导致了不必要的成本和效率损失。此外，物理检查可能会很昂贵，特别是在管道和其他难以到达的区域。缺乏设备状态的实时信息很容易导致设备故障、昂贵的计划外维护和处理时间的损失，更不用说设备故障导致的事故或紧急情况的危险。

分析可以使设备监控、管理和维护更加有效，可以为每种设备类型创建模型，以帮助预测组件故障并优化性能特征。无线传感器和工厂监控设备可用于实时测量温度、振动、校准、压力、粘度和润滑油状况等特征，并将这些测量数据与历史模型进行比较，以评估设备的性能和故障可能性。

从预测维护的角度来看，设备可以根据其实际情况进行维护或更换，而不是预先设定一个时间表或日程。这可以潜在地节省更换成本，也允许在计划维护窗口之前修复可能发生故障的设备，并防止事故或停机。此外，基于设备参数的实时反馈，可以实现设备性能的优化，即使是很小的效率改进也能节约成本（有关物联网分析的更多信息，请参阅第7章）。

10.5 小结

随着技术的进步，石油和天然气行业已经开始通过连接资产进行创新，并通过产生的数据获得洞见性。物联网解决方案有助于更好地访问现有的数据源，满足合规要求，并提高员工的安全性。许多人认为物联网技术是关键推动因素，特别是在采用无线技术的情况下。

我们必须认识到，单一的技术无法使石油和天然气工业满足这些要求。只有架构合理、安全的技术和应用程序集成，才能有助于降低成本、提高效率、保障员工的安全，并继续推动创新。

油气行业正在为连接的炼油厂、控制中心、管道和石油钻井平台构建新的物联网解决方案。这些解决方案遵循用于控制层次结构的普渡模型，该模型有助于识别体系结构级别和安全区域。

由于油气设施和工作环境的性质，无线技术被广泛用于连接传感器、工人和工业控制系统。WiFi和确定性无线系统（如ISA100.11和WirelessHART）在这个行业很受欢迎，它们解决了非常具体的挑战。

安全在油气行业中也是至关重要的，遵守风险管理框架可以提高安全性。安全性应该通过一个全面的深入防御策略来管理，该策略包括身份验证、加密、远程访问控制、AV和OS补丁管理。

第11章 公用事业

公用事业是现代社会的支柱。无论是电力、天然气还是水资源，公用事业公司为我们的城市、企业乃至整个经济提供服务。最近，一家电力公司的高管被要求用一句话解释公司的核心业务职能。他回答说：“我们提供电力是为了让客户享受。”“享受电力”听起来似乎有些奇怪；这是我们认为理所当然的事情，但这句话是有道理的：可靠的电力供应使我们能够享受生活中的许多事情。当停电时，我们突然无法使用心爱的电子设备，然后开始拼命寻找蜡烛和火柴。这感觉就像我们突然回到黑暗时代，试图弄清楚人们在使用电力之前是如何娱乐自己的。有些人开玩笑说，电力公司的功能就是让灯一直亮着。对我们大多数人来说，这正是我们所期待的，因为当灯光熄灭时，我们正常的生活就会戛然而止。当天然气和水服务停止供应时，我们也会遇到类似的挑战。

公用事业对社会基本功能的重要性是显而易见的，因为许多政府将其归类为关键的基础设施，而且大多数国家都有严格的法律来确保其安全、保护、持续运行和质量。

公用事业网络的规模确实是巨大的。每个连接到公用事业公司服务的家庭都需要一个电表。随着公用事业网络中的每一个电表通过IP和物联网实现自动化，该网络的规模变得巨大。想象一下，一个拥有50万户家庭和企业的中型城市，从不同的公用事业公司获得电力、水和天然气服务。如果假设每种类型的仪表都有一个IP地址，那么网络已经扩展到150万个端点，更不用说支持这些节点的网络基础设施了。然而，与一些现代智能电表网络动辄几千万的规模相比，这个数字实际上是非常小的。从纯IP的角度来看，很少有组织能够处理设计、部署和管理这种规模的网络所涉及的挑战。

本章的主要内容是电力公司的数字化历程，特别是物联网如何被用于构建智能电网网络。这并不是说天然气或水设施的重要性低，而

是反映了这样一个事实，即电力设施是第一个通过物联网实现电网自动化和分析的公用事业。此外，在电网中普遍存在的许多技术也很好发挥了物联网的自动化优势。尽管如此，本章讨论的许多原则也适用于其他类型的公用事业。

本章介绍了智能电网的概念，并探讨了正在改变发电、传输和传输方式的一些底层物联网技术，包括以下几个部分。

■ **电力行业简介：**本节描述电力行业，以及其业务模型和技术挑战。

■ **GridBlocks参考模型：**GridBlocks是智能电网的基础架构。本节将讨论该参考模型以及如何将其用于构建整体的智能电网策略。

■ **主变电站电网和变电站自动化：**变电站是电力传输和分配的场所。变电站内的设备正在往高度互联和自动化的方向发展。本节探讨自动化解决方案和目前正在变电站部署的物联网构件。

■ **系统控制 GridBlocks ——变电站广域网：**通用广域网允许变电站和控制中心之间的互连。广域网现在正从传统的时分多路复用传输向基于IP分组的网络过渡。本节将讨论使通用广域网能够承载任何行业中一些最敏感的应用程序的设计考虑因素。

■ **场域网（FAN）GridBlock：**本节将FAN作为连接智能设备（包括智能电表和配电网上的设备）的基础元件，允许公用事业公司利用自动化和数据分析的能力。

■ **保障智能电网的安全：**电网被认为是关键的基础设施。本节将探讨诸如SCADA安全性、NERC CIP以及配电网的安全最佳实践等概念。

■ **智能电网的未来：**物联网已经对全球电力设施产生了深远的影响，产生了新的流程和商业模式。未来，分布式能源发电、清洁能源和电动汽车将进一步颠覆电网技术。

11.1 电力行业简介

如果有人问你服务于你的家庭或公司的电力公司名称，你可能会回答给你寄账单的电力公司名称。然而，这只是答案的一部分，在许多情况下，计费公司只是电力供应链“最后一公里”的一部分。电力输送一般分为3个阶段，在世界上许多地方，这些阶段由完全不同的公司或至少是一家大型电力公司的独立部门提供支持。电力供应链的3个阶段是发电、输电和配电。

■ **发电：**发电是产生电力的地方。电力生产通常包括核能、水力发电、天然气和煤矿。高压（HV）电力一旦产生，会通过高压输电线路输送到输电系统。发电公司还负责对终端用户波动的电力需求做出响应。

■ **输电：**电力传输需要长距离的高压电力，一般为 115kV 及以上，传输距离为 50 公里及以上。输电线路包括架空线路和在水下长距离传输高压电力的海底电缆。输电系统负责将整个服务区的高压线路从发电站连接到变电站。当你看到大型金属塔沿着高速公路支撑着长长的电力电缆时，这些是将电力从发电厂输送到变电站的输电线路。

■ **配电：**配电包括从变电站到您的家庭或企业的公用事业网络部分。这包括中压（比如12.5kV）电力线，我们可以在附近的电线杆上看到，包括垫装变压器。请注意，在家附近的变压器上，电源降压至低压，通常以几百伏的电压向终端用户供电。需要注意的是，北美和欧洲的配电网络模型之间存在一些差异。例如，在欧洲，人们经常看到二次变电站。另外，欧洲的低压是240V，北美是110V。

图11-1说明了发电、输电和配电如何协同工作，为终端用户提供电力。

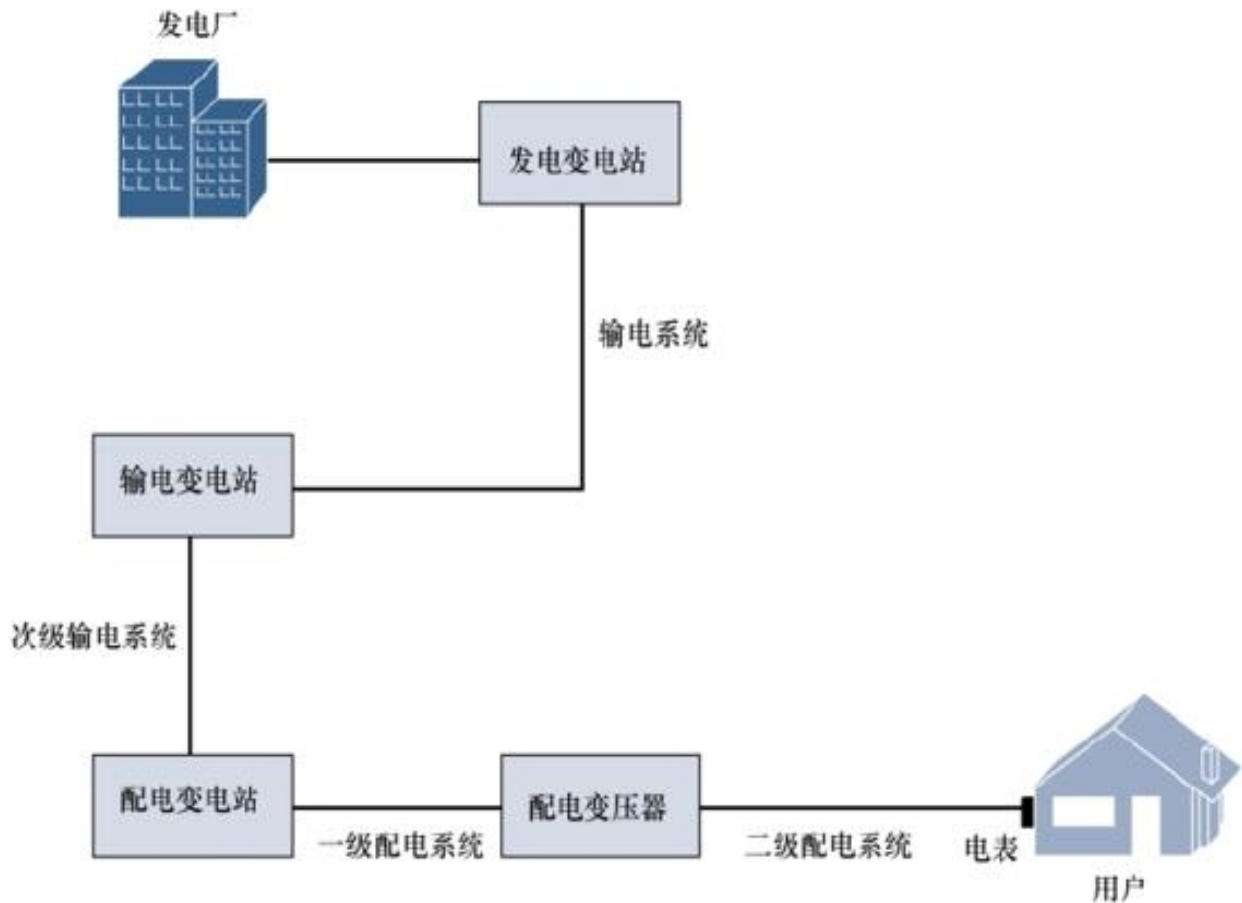


图11-1 电网中传统的发电、输电和配电阶段

注释：垂直整合的公用事业公司拥有并经营整个发电、输电和配电（以及零售或直销）的电力供应链，供应给所有类型的客户。根据不同国家的情况，政府和公用事业监管机构已将主要公用事业业务拆分为不同的公司，具体的拆分和运营战略取决于地区或国家。根据政府的规定，公用事业控股公司可以拥有多家公司的所有权，即使它们已被分割为不同的法律实体。因此，根据地区的不同，公用事业可以是垂直集成的，也可以是分离的。

IT/OT在实用程序上存在分歧

早在廉价的微处理器、工业通信标准和IP网络出现之前，电力工程就已经出现了。如果工程师需要从传感器收集数据并采取某种行动，该怎么办？早期的OT网络连接了远程的刻度盘和指示器，这样操

作员和工程师就可以不用去很远的地方进行读数。这使得他们能够从一个控制室方便地读取许多传感器的读数。如今的电网控制室呼应了这一开端，用图形显示器铺满整面墙。

随着廉价可靠的串行通信变得广泛可用，更多的功能以更低的价格出现，以允许广泛部署。当以太网第一次出现时，没有人想到它会比串行网络便宜，也没有人想到计算会变得如此廉价和强大，以至于可以在整个网络的几乎任何地方使用它，而不是在一个玻璃控制室中使用一个庞大的大型主机。

考虑到电气控制和监控系统的寿命，以及公用事业网络的巨大规模，当新技术可用时，替换所有传统的公用事业系统是不经济的。然而，随着具有新功能的新系统的安装，以及设备和系统价格的下降，它们为公用事业带来了更大的可靠性和成本效益。

虽然OT网络不像IT网络那样灵活，但OT工程部门一直在不断调整，以利用支持电网的新技术。这包括在新网络上开发并支持许多传统系统的方法。OT工程师总是在寻找更好、更具成本效益的方法来做事情，这通常包括尽可能利用IT技术。IT技术在业界得到广泛采用，这意味着很容易找到合格的人员来设计和支持网络和应用服务器。现在的挑战是理解OT物理系统并确保通用IT（主要基于IP网络技术）能够胜任这项工作（IT和OT在1章中介绍过）。

注释：术语OT并未在公用事业中普遍使用。在世界上的许多地方，运营电信工程的角色是由保护和控制工程师完成的，但是为了简单起见，在本书中使用了术语OT。

随着公用事业OT网络开始向IP通信和物联网架构迁移，OT网络的规模比IT网络大了一个数量级。以高级计量基础设施（AMI）为例，其中电表成为连接到单个网络的支持IP的智能设备。仅AMI网络就可能有数百万个节点，所有这些节点都可能成为IPv6可路由的端点。问题出现了：谁来设计、操作和管理AMI网络以及其他基于IP的OT网络？是具有理解实用程序技能的OT团队，还是具有IP网络经验的IT团队。

随着IT和OT网络的互联，这些挑战变得更加明显。需要解决的问题包括以下方面。

■ 如何为任务关键型OT应用程序（这些应用程序会让电灯一直亮着）提供网络弹性和冗余？

■ 谁将支持远程访问电网中的配电系统，而且访问必须通过OT和IT网络进行？

■ 如何管理OT网络之间和IT与OT网络之间连接点的安全？这是传统IT安全部门的责任，还是需要一个新的模式？

■ 变更管理是否将以与IT系统相同的方式进行治理，还是OT应用程序的关键性需要一组新的规则来确保业务的连续性？

不同的组织以不同的方式应对这些挑战。过去，IT和OT是完全独立的团队，几乎不需要相互联系。今天，随着网络的融合，OT和IT需要紧密合作。一些OT工程师正在学习构建和支持复杂OT系统所需的IP技能，而IT工程师正在学习公用事业核心OT系统的重要方面。然而，各方多年来积累的专业知识来之不易；这种知识不容易在短时间内在部门之间转移。一个IT工程师要花多长时间来学习复杂的电气保护和控制系统？同样，保护和控制工程师需要多长时间才能真正了解错综复杂的以太网弹性和IP路由？这些复杂的以太网和IP路由如今构成了他们负责的应用程序的网络传输。这些技能需要多年才能掌握。

这些挑战开创了智能电网的时代。智能电网是电网与运行电网的信息与通信技术（ICT）的结合，其目标是有效地提供可持续、经济和安全的电力供应。

公用事业公司现在正在努力应对IT/OT聚合的挑战，这可能是第一个面临如此大规模地将IT和OT整合到一个具有内聚治理的综合网络的主要行业。此外，公用事业行业目前正面临着制定新的行业标准的挑战，这些标准允许数百万变电站和配电装置安全地互连到企业IT网络。要成功实现这一目标，必须遵循体系结构方法。GridBlocks参考模型为公用事业提供了这样一种体系结构，下面将对此进行讨论。

11.2 GridBlocks参考模型

Cisco 是最早认识到需要一个系统架构来将电力供应链各个阶段的系统集成到现代通信系统中的公司之一。该架构必须考虑到智能电网技术的快速现代化，同时支持大量可能在未来多年仍将存在的传统技术。

为了满足这种需求，Cisco开发了GridBlocks参考模型。尽管存在其他参考模型，GridBlocks为在公用事业领域工作的新手和高级用户提供了一个易于理解的模型。如图11-2所示的GridBlocks参考模型描述了整个大容量电力供应链，从广域大容量电力实体到发电、控制中心、输电电网、变电站、配电网，再到电网边缘的分布式能源资源整合。该模型是前瞻性的，旨在成为一个通用的终端状态参考框架，可以帮助部署和设计电网各个方面的端到端安全能源通信解决方案，从而为公用事业提供新的和强有力的基础——智能电网。

GridBlocks参考模型为公用事业运营商提供了以下好处。

- 详细介绍了一个灵活的、基于层的模型，该模型支持对电网的逻辑部分（层）进行增量改进。

- 有助于实现新技术和传统技术的安全集成，提高网络元素的整体可管理性和可视性。

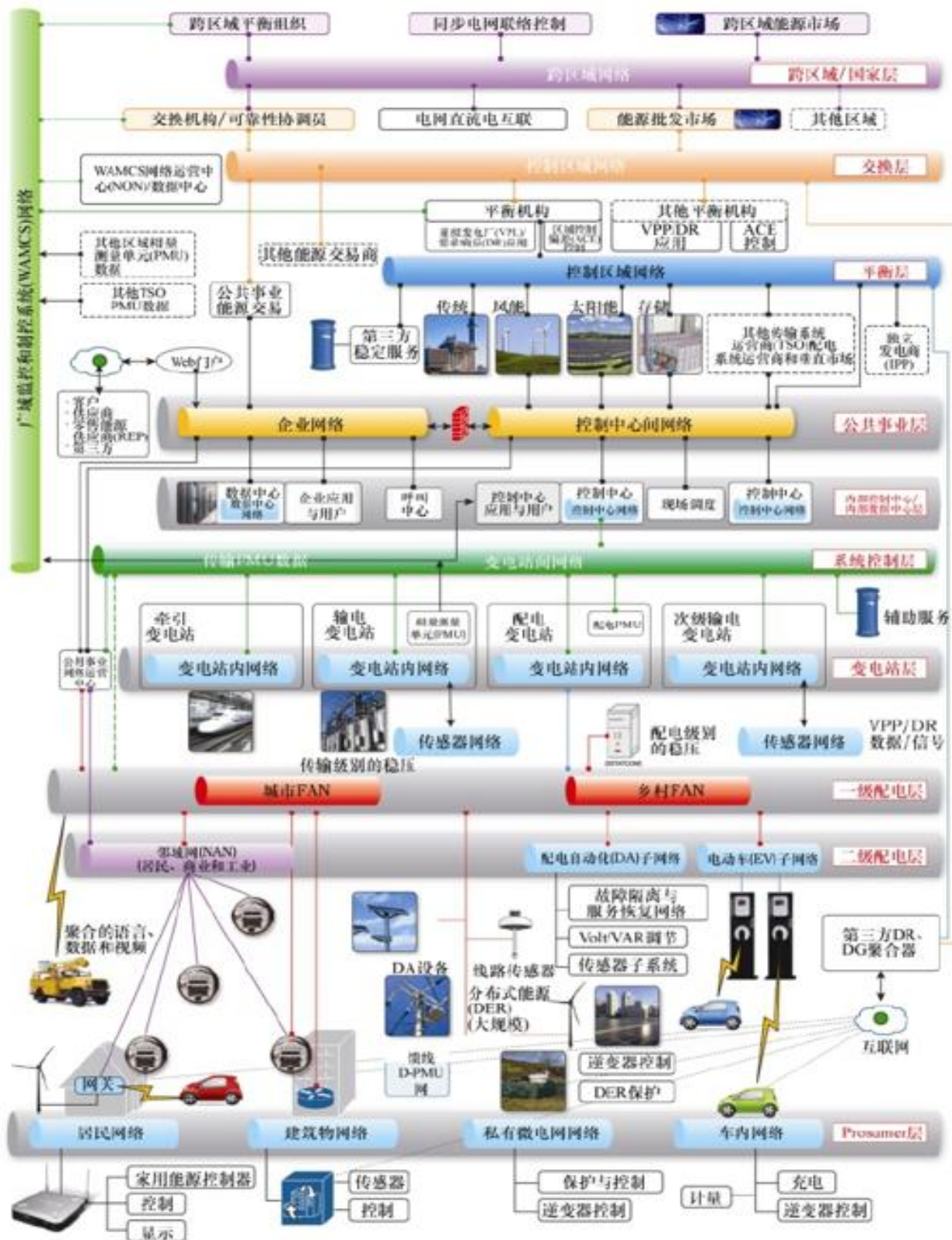
- 以开放标准（主要是IP）为基础，减轻对供应商的依赖，并支持互操作性，从而降低成本。

- 实现公用事业网络的融合和整合，其效果是简化运营，减少运营和资本成本，同时通过增加功能创造新的价值。

- 为公用事业提供数字化路线图，允许它们分阶段对电网的不同部分进行现代化。



Cisco GridBlocks™ 参考模型



GridBlocks：一个11层的参考模型

如图11-2所示，Cisco GridBlocks参考模型分为11个部分（或层），这些部分将电力供应链的各个方面联网。该模型的关键策略是通过网络通信将原来断开的电网功能统一为一个聚合的网络架构。电网的每一层可能由同一电力公司的不同部门拥有和运营，甚至由整个电力供应链上完全不同的公司来运营，同时支持各层之间的安全互连。

虽然基于层的GridBlocks模型允许将公用事业的功能和功能区域划分为层，但是它也支持将网络元素合并为单一的聚合架构。我们从图11-2所示的底层开始介绍各层。

■ **Prosumer层：**Prosumer层结合了能源生产者和消费者的双重角色，并包含可能影响电网的外部元素。这些设备既不属于公用事业公司，也不属于其基础设施的一部分，而是以某种方式与之交互。这包括分布式能源（DER），这些资源通过太阳能或其他方式产生本地电力。这也可能包括能源存储系统和电动汽车或工业设施的响应负载。智能电网技术的迅速成熟的这一部分有望成为未来一个主要的颠覆性元素，本章后面将对此进行讨论。

■ **配电层：**配电网络是电力输送系统的最后一公里。电网的这一部分位于配电变电站和终端用户之间。为简单起见，将其分为两个子层，如下所示。

■ **2级配电层：**这个较低的配电层是电力输送系统的最后一公里，或邻域网络（NAN）。智能电网的这一部分支持计量系统、需求响应系统、电动汽车（EV）充电站、配电自动化系统中的远程终端单元，以及许多其他类型的设备。

■ **1级配电层：**1级配电层将2级网络连接到配电变电站，并通过系统控制层向公用事业控制中心提供回程服务。

■ **变电站层：**该层包括所有变电站网络，包括输配电变电站。输电变电站连接多条输电线路，通常电压较高（115 kV及以上），并向配电站供电。配电变电站接收的输入电压一般为115kV及以上（或服务区内常见的电压），并向终端用户提供25kV或以下的供电。这一层的网络有各种各样的需求，从基本的二级变电站到提供关键电力传输功能的复杂一级变电站，如远程保护（本章后面将详细讨论）。在变电站内部，通常有严格的网络要求，包括弹性、性能、时间同步和安全性。这些变电站需求导致了功能的分离，每个功能都有独立的总线（例如，站点和流程总线功能）。一级配电变电站还可以包括配电集合体。

■ **系统控制层：**这一层包括连接变电站和控制中心的广域网（WAN）。这一层中的WAN连接需要满足最严格的延迟和弹性性能指标。变电站广域网需要灵活性和可扩展性，可能涉及不同的媒体类型，包括光纤或微波。系统控制层支持将远程SCADA设备连接到控制中心、事件消息传递和变电站内继电器之间的远程保护服务。

■ **内部控制中心/内部数据中心层：**这是公用事业数据中心和控制中心内部的层。数据中心和控制中心位于同一逻辑层，但是它们有非常不同的需求。数据中心对于IT工程师来说非常熟悉，因为它包含企业级应用程序和服务。控制中心包含操作和控制电网本身的实时系统，包括配电和输电系统、监控和需求响应。这一层需要通过系统控制层连接到变电站，以便收集重要数据并由变电站中的IT和OT系统使用。

■ **公用事业层：**这一层是企业网络的所在地（尽管该名称暗示这里有一些与电网相关的功能，但这是一个以IT为中心的层）。公用事业层是控制中心和企业网络之间的连接点，它使用带有适当安全策略的防火墙来确保只有来自企业网络的可信流量才能进入控制中心（注意，整个体系结构和层之间都使用了防火墙，这只是一个示例）。还需要注意的是，大多数公用事业运营着多个控制中心，并具有高度分散的企业网络，这意味着这些网络必须通过城域网络或WAN（可能重新使用WAN网络作为系统控制层）进行安全连接。

■ **平衡层：**该层支持第三方发电运营商与平衡机构之间的连接（以及与独立发电商[IPP]的连接）。在电力公司，发电供应不一定能满足客户的需求。为了管理负荷和需求，大多数公用事业公司与其他公用事业公司相互连接，在必要时可以相互买卖电能。有时，一家公用事业公司的电力可能过剩，而另一家公司的电力可能短缺。平衡机构的职责是管理电网的电力需求和供应。如果电力供需失衡，就会发生停电。平衡层的敏感特性突出了对通信网络的需求，它使不同的方面能够有效而安全地协作。

■ **交换层：**这一层的网络允许公用事业运营商之间进行电力交易。在公用事业领域，电力的交易方式与石油和天然气等其他大宗商品非常相似。电力的买卖需要实时进行。这一层网络不仅允许电力公司在需要的时候购买电能，而且在有机会的情况下，还可以通过将多余的电力卖给其他公司来获利。

■ **跨地区/跨国家层面：**大多数公用事业电网与更大的超级电网互联。这一层是同步电网之间的网络连接，用于电力交换、电网监控和电力流管理。

■ **广域测控系统（WAMCS）层：**这一层包括连接到电网的一个关键组件——电力管理单元（PMU），该单元负责整个电网的广域电力测量。由于这一层的范围巨大，它需要连接到其他几个层，因此在图11-2中将其描述为垂直层。

GridBlocks参考模型是一个有用的工具和蓝图，可以用作构建层内的网络元素并将它们链接到其他层的基础。它还提供了将网络功能分组为电网块的基本方法，可以对这些电网块进行更详细的扩展。以下是本章后文讨论的一些示例。

■ **主变电站GridBlock：**此GridBlock深入研究变电站自动化和变电站内过程总线和站点总线设备的互连问题。

■ **系统控制GridBlock：**GridBlock将变电站相互连接，并与控制中心连接。这个GridBlock的一个重点领域是对能够交付远程保护服务

的WAN架构提供支持。

■ 场域网（FAN）网络：FAN是一个快速发展的公用事业物联网领域，支持远程配电元件、智能电表、配电自动化、需求响应等的连接和管理。

11.3 主变电站电网和变电站自动化

托马斯·爱迪生和亚历山大·格雷厄姆·贝尔是同时代的人，被认为是世界历史上最有影响力的两位发明家。爱迪生发明了配电，被认为是现代电力工业之父。贝尔发明了电话，被认为是电信业之父。

如果给亚历山大·格雷厄姆·贝尔一部现代智能手机，他可能会惊奇地看着它。现代智能手机的功能与他在1876年发明的简单电话几乎没有相似之处，很可能被认为是与同时代的另一位科幻作家H. G. 威尔斯的发明。然而，如果把托马斯·爱迪生带到一个现代发电厂或变电站，他可能会告诉我们他能看到的几乎所有东西的详细功能。事实上，电力行业的技术进步速度比电信行业要慢得多。然而，这一状况正在发生改变，我们要感谢亚历山大·格雷厄姆·贝尔的技术开端。

在过去几十年中，电力行业最大的进步之一是通过电信网络连接和控制设备的能力，而物联网现在将这一飞跃提升到了一个全新的水平。

11.3.1 SCADA

SCADA是一个可以由中央服务器监控远程设备的系统。SCADA在变电站中起着至关重要的作用，它允许从远程设备（称为远程终端设备[RTU]和智能电子设备[IED]）进行控制和数据采集。RTU和IED是与电网硬件相连的微处理器控制设备，如继电器、负载控制器、断路器控

制器、电容器组控制器等。在SCADA的世界中，远程设备称为SCADA从设备，服务器称为SCADA主设备。

SCADA起源于20世纪50年代，那时计算机网络还没有出现。它的目的是成为一个操作人员可以从中心点（通常是大型计算机系统）管理远程工业设备的系统。在早期，SCADA系统是独立的，没有与其他系统的连接，它们几乎完全依赖于专有协议。随着时间的推移，远程WAN网络允许SCADA连接扩展到RTU，但这些连接通常是使用RS-232或RS-485接口并通过TDM电路传输的点对点串行链路。

随着时间的推移，SCADA传输开始采用基于标准的协议和开放的网络体系结构，不再依赖于连接每个SCADA从设备的专用串行链路，变电站LAN开始用于传输，每个变电站都有一个本地SCADA主设备。随着高速、弹性和灵活的IP WAN网络的出现，SCADA服务开始分散在整个网络中，并且可以在控制中心使用集中的SCADA主设备。

最广泛部署的传统SCADA通信协议是Modbus、IEC 60870-5和分布式网络协议（DNP3）。

注释：Modbus是这些协议中最古老的一种，于1979年为可编程逻辑控制器（PLC）设备开发，但最终被用于电力系统的SCADA。IEC 60870-5-101于1995年完成，旨在用于串行链路上的分布式SCADA系统。DNP3最初于1990年由加拿大的GE Harris公司开发，现在由DNP用户组管理。DNP3已被IEEE作为SCADA通信标准采用。从历史上看，DNP3一直是北美主要的SCADA协议，而IEC 60870则是欧洲主要的SCADA协议。如今，这些协议有TCP/IP变体，允许它们在IP网络上本地传输。

图11-3说明了一个传统变电站，其中电气继电器串行（RS-232或RS-485）连接到RTU，RTU又连接到一个SCADA网关设备，SCADA网关设备连接到变电站以太网。SCADA网关设备通常以两种方式工作。第一种方式是协议转换，例如将串行转换为IP封装。例如DNP3到DNP3/IP或IEC 60870-5-101（串行）到60870-5-104（TCP/IP）。网关设备的第二种工作方式是通过IP网络（例如，使用原始套接字）对串行流量进行隧道传输。要更深入地了解Modbus、IEC 60870-5和DNP3，以及协议转换和原始套接字的传输概念，请参考第6章。

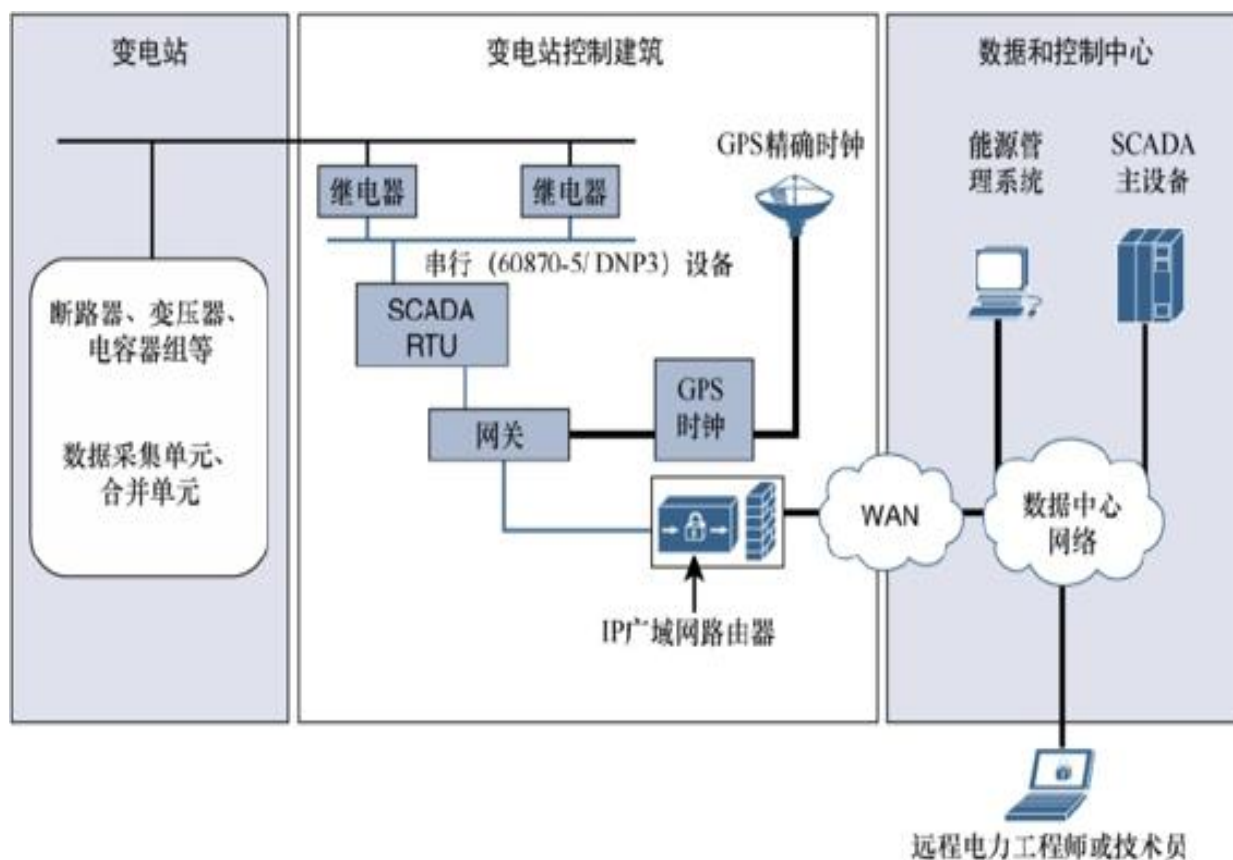


图11-3 带有串行RTU的传统变电站SCADA网络

虽然我们期望这些传统的SCADA传输机制在未来的许多年中仍然存在，但是从长远来看，传统的SCADA系统正在被一种新的技术标准所取代，这种新标准（IEC 61850）本身就利用了以太网和TCP/IP。

11.3.2 IEC 61850：变电站通信标准的现代化

现有的串行SCADA系统运行在Modbus、IEC 60870-5-101或DNP3上，无法支持现代IED的下一代功能。即使使用基于IP的协议转换服务，它们仍然缺乏部署灵活性，最终依赖于RTU上老旧的串行通信。为了使变电站通信现代化，并使用可以利用以太网和IP的协议，IEC技术委员会57（TC57）制定了IEC 61850标准。IEC 61850不仅仅是利用以太网和IP进行传输的串行协议的重新开发。相反，IEC 61850是在现代标准和技术的的基础上建立起来的，为变电站的IED提供了一系列新功能。

IEC 61850在变电站和其他方向克服了一些最具挑战性的供应商和网络互操作性的挑战。61850用以太网和IP代替了专用串行链路，大大减少了变电站内的铜缆。以太网固有的灵活性意味着IED可以轻松地直接与其他装置以及通信基础设施的其他元件进行通信。以太网的灵活性提供的另一个关键优势是接口价格低廉，而且设备供应商正在将接口添加到所有现代资产中，这意味着变电站中的无监督设备已经成为过去。

1. IEC61850变电站总线

IEC 61850定义了变电站两个关键区域（站级和过程级）的变电站通信，如图11-4所示。站级是需要与IED通信的设备（通常是SCADA通信）。站总线是站级设备和间隔层中IED之间的网络连接，在这里可以找到保护和电气控制资产、计量装置和其他关键系统。

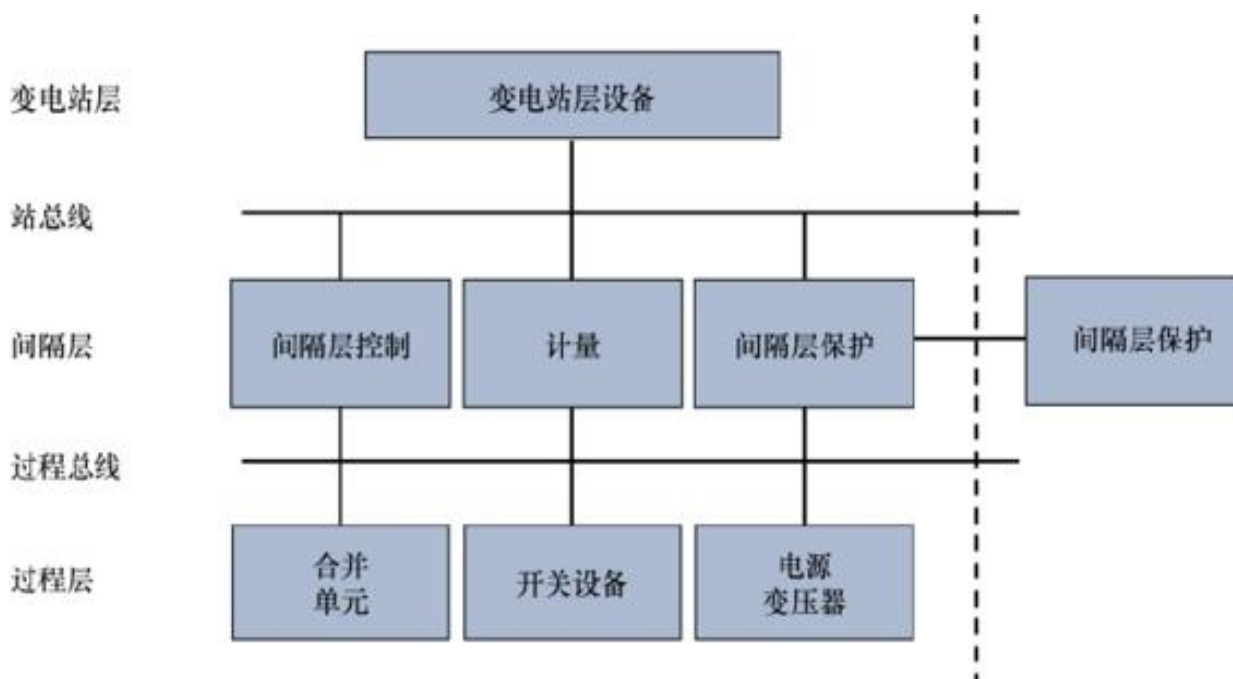


图11-4 变电站自动化层次结构

在图11-4中，间隔层与连接电源和电流变压器、开关装置等高压设备有关。这些装置连接到测量系统中进行保护和控制。间隔层的设

备通常有两种不同类型的网络接口：一种用于连接到站总线的SCADA管理；另一种用于连接到过程总线。

虽然站总线的主要焦点是通过以太网和IP进行SCADA传输，但IEC 61850远远不止这些。IEC 61850通信结构定义了3种主要的通信类型。

■ 制造信息规范（MMS；IEC 61850-8-1）：MMS支持IP上的客户端/服务器通信，用于SCADA。MMS流量通常出现在站总线上。

■ 通用面向对象变电站事件（GOOSE；iec61850 -8-1）：GOOSE采用基于以太网的多播（一对多）通信，其中IED可以互相通信，也可以在各个间隔层之间通信。GOOSE通常用于在保护继电器之间传递功率测量值，以及用于跳闸和互锁电路。GOOSE通常用于站总线。

■ 采样值（SV；IEC 61850-9-2）：SV通常用来在过程总线上承载电压和电流样本。SV的常见用途是母线保护和同步相量。

注释：同步相量是时间同步的电气编号，用来监测相位和功率。它们是由变电站中称为相位测量单元（PMU）的设备测量的。

在变电站自动化领域，GOOSE是一个非常重要的工具，因为它是电气保护和控制系统之间使用的主要61850消息类型。保护和控制系统是变电站中最重要的设备之一，它们被用来持续监控输电线路和馈线输送的电力。如果电力由于某种原因中断，则测量系统会在几毫秒内检测到它，并通过以太网将GOOSE消息传递给一个对等中继，该中继将电力传输切换到备用线路或馈线。如果GOOSE信息未正确传递，或者没有在规定时间内传递，则继电器就会变得混乱，电力可能被错误地切换，导致断电甚至更严重的后果。

注释：变电站GOOSE使用以太网多播消息，在IED之间传输。尽管最初的意图是仅在变电站内使用GOOSE（这意味着GOOSE的第3层VLAN间路由是没有必要的），但是IEC 61850-90-5最近的发展已经允许对协议进行修改，允许GOOSE在广域网的IP上进行路由。

2. IEC 61850过程总线

在撰写本书时（2017年初），全世界大多数61850实现仅限于站总线，但这只是IEC 61850实现的一部分内容。IEC 61850的另一个重点领域是过程总线。在过去，诸如电流互感器（CT）、电压互感器（PT）和数据采集单元（DAU）等设备会向测量系统传递连续的数据流。这些设备对变电站的功能至关重要，因为它们不仅能测量电力的平衡和质量，而且能有效地监控电网的整体功能。变电站的这一部分被认为是非常敏感的，原因是网络连接在历史上一直是硬连接的，并且与其他网络完全隔离。

IEC 61850-9定义了过程总线通信，其中关键的过程级设备可以通过以太网进行消息通信。任何上游测量、保护或测量装置都可以根据需要这些使用数据。

图11-5说明了一种可能的IEC 61850变电站自动化设计。图中使用了两个独立的以太网段：站总线和过程总线。站总线允许IED之间的通信，例如用于保护和控制的GOOSE消息，以及SCADA通信。根据61850，过程总线使用一套完全不同的以太网交换机来实现关键的变电站自动化功能。变电站的这个区域不能简单地使用与站总线上同一个交换机的独立VLAN；它必须为每个总线使用不同的物理交换机。原因之一是过程总线的网络弹性要求远远超出了标准以太网的能力，需要新一代的弹性协议，本章稍后将对此进行描述。

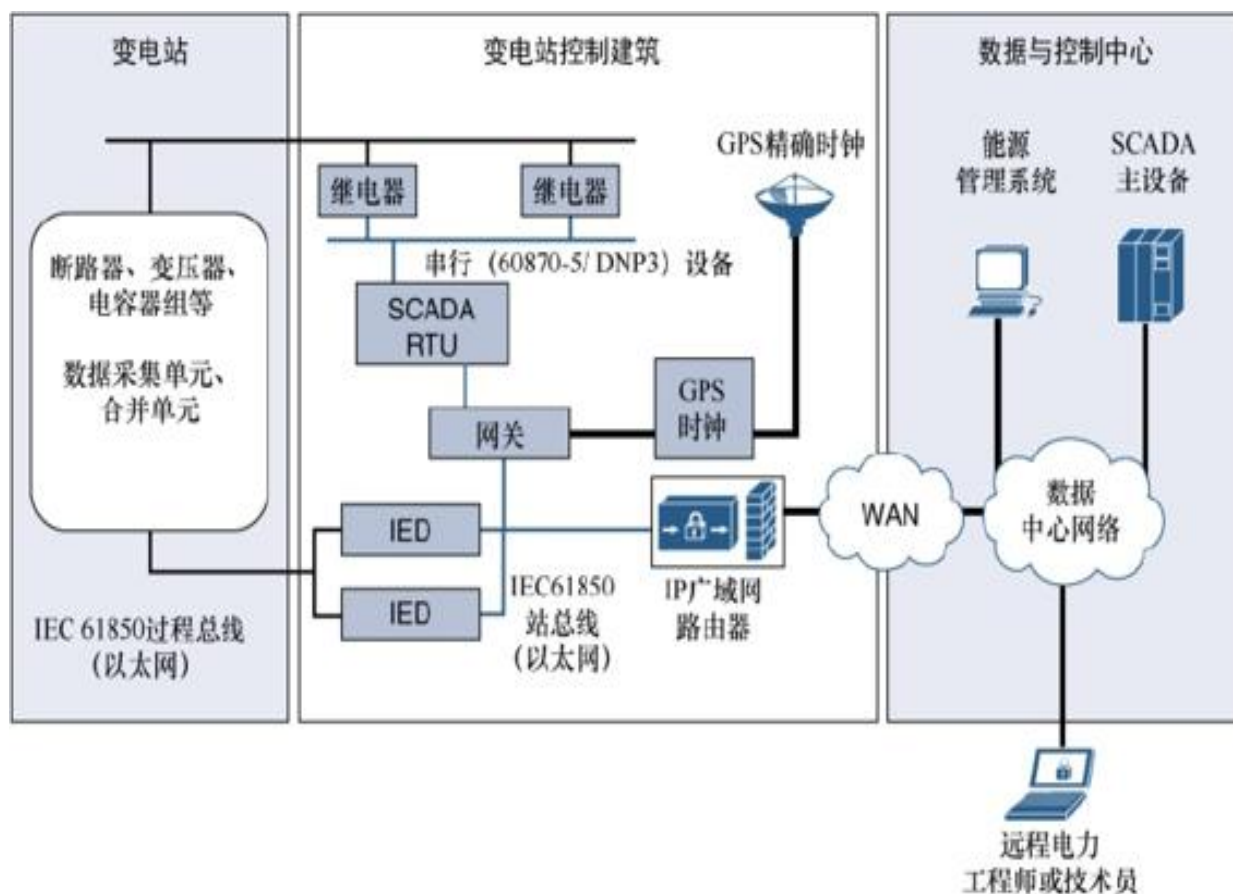


图11-5 基于IEC 61850的变电站体系结构

3. 迁移到IEC 61850

DNP3、Modbus和IEC 60870-5-101是依赖点对点串行通信的传统协议，似乎与现代网络技术不兼容。然而，它们仍然被广泛地使用，而且必须得到支持，甚至在现代变电站中也是如此。

IEC 61850仍然是变电站内通信的一个相对较新的标准。因此，不太可能立即从传统系统和协议进行迁移。公用事业资产通常有20~30年的更换或升级周期，迁移到更新的设备需要时间。在许多情况下，可以期望变电站中既有传统串行连接的RTU，也有现代的IED，它们可以利用IEC 61850提供的以太网框架。随着时间的推移，预计变电站过程总线也将开始采用61850功能。根据61850-90-5的定义，标准的最近发展也允许61850被路由到变电站外面。

图11-5显示了一个混合变电站，其中既有传统的RTU，也有更现代的61850设备。随着时间的推移，由于串行和TDM部件的可用性变得困难，预计IEC 61850解决方案将主导变电站所有部件的OT网络。

11.3.3 变电站中的网络弹性协议

IEC 61850过程总线在任何行业的任何应用程序中都有最严格的弹性要求。即使丢失一个包或以太网帧也不能容忍。具有快速重新收敛能力的现代以太网冗余协议，如快速生成树、ITU G.8032和弹性以太网协议（REP），不能处理这项工作（REP在第9章中进行了介绍）。这一挑战的解决方案是IEC开发的一种新型网络弹性协议，包括并行冗余协议（PRP）和高可用性无缝冗余（HSR），主要用于变电站。

1. 并行冗余协议（PRP）

PRP是一种IEC标准，用于实现高可用性的自动化网络，确保网络即使在中断情况下也不会丢失任何以太网帧。IEC62439 -3第4条中标准化的协议利用了并行冗余的原则。不同于仅仅发送一个帧到以太网段，使得网络在发生故障时快速收敛（如REP或G.8032），一个支持PRP的双连接IED能够在不同的并行以太网VLAN段上发送相同帧的冗余副本。

来自IED的以太网帧被桥接到两个网络接口，并被赋予一个序列号。然后这两个帧遍历两个并行的网络路径，直到它们到达接收IED（同样是在两个独立的NIC上）。接收IED选择一个首选（活动）接口并丢弃在非首选（备份）接口上接收的帧。当其中一个并行网络发生故障时，这种方法保证至少有一个包到达目的IED。

注释：在61850 GOOSE协议的情况下，增加了一个额外的弹性层用于电气保护系统，其中发送的IED将每一帧发送多次。这确保至少有一帧正确地到达目的地。

刚才的场景假设IED本身具有PRP能力，因此能够创建和删除每个帧的多个副本。这可能并不总是可行的，因为这不仅需要升级IED本身来支持PRP，还需要部署双冗余以太网网络。

一种类似但略有不同的方法是将一个现有的IED连接到一个支持PRP的接入交换机上。在这种情况下，PRP接入交换机充当冗余盒（或RedBox），对以太网帧进行两次复制，并通过网络两端的相同VLAN发送副本。然后，接收PRP交换机将以太网帧的一个副本转发给中继，并删除重复的副本。请注意，PRP的主要优点之一是中间交换机不需要具备PRP能力。在此场景中，只有发送和接收RedBox实际参与PRP冗余，如图11-6所示。

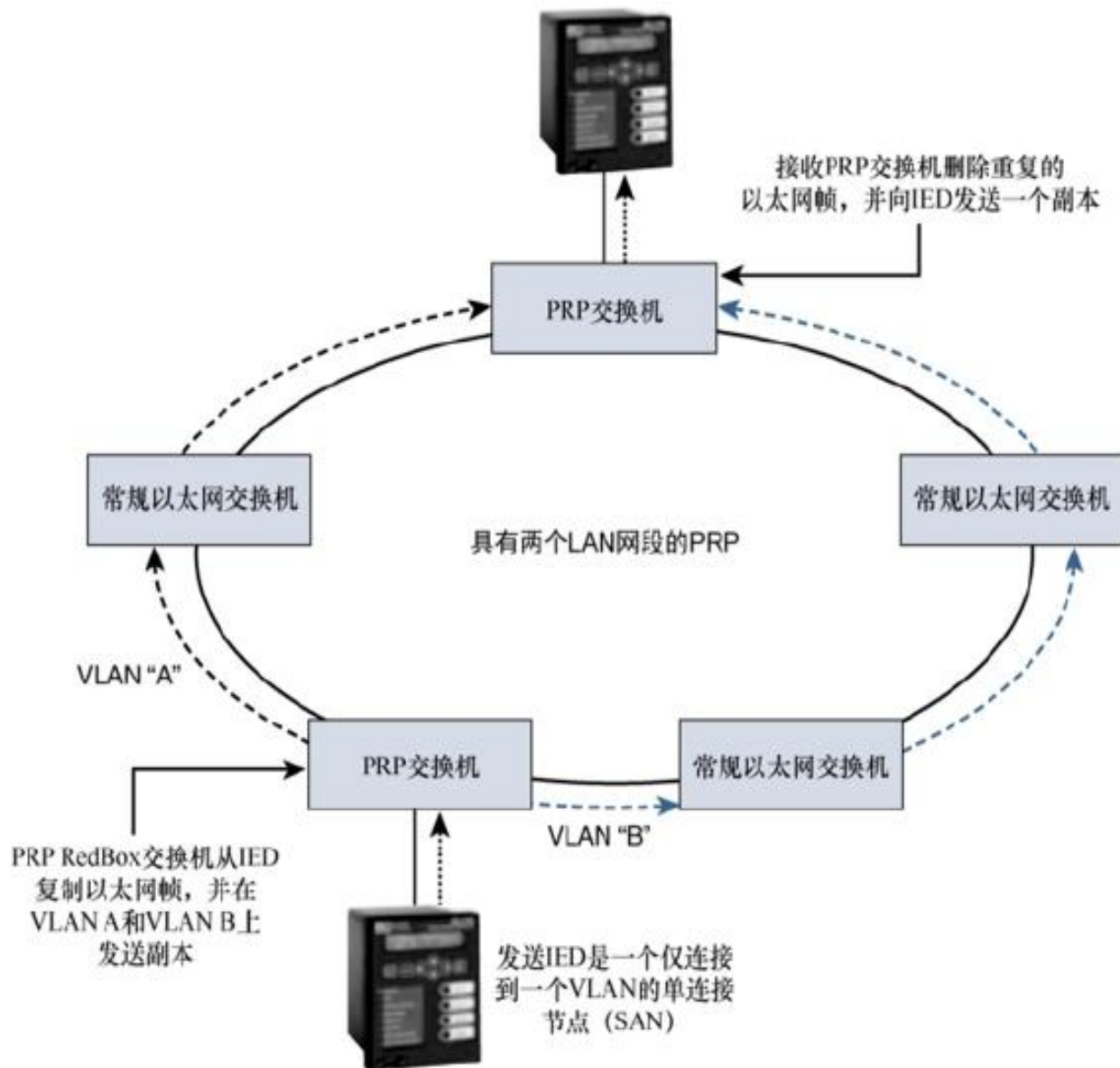


图11-6 PRP部署示例

2. 高可用性无缝冗余（HSR）

为公用事业开发的另一个弹性协议是HSR。与依赖并行网段的PRP不同，HSR是为以太网环型拓扑设计的。HSR与PRP有许多相似之处，并在IEC62439-3第5条中进行了标准化。虽然PRP非常灵活，可以部署在各种拓扑中，但是HSR是专为环型拓扑设计的。

与前面的PRP RedBox示例非常相似，借助于HSR，IED只有一个到HSR RedBox以太网交换机的连接。借助于HSR，HSR RedBox不是复制以太网帧并通过不同的VLAN发送它们，而是在相同的VLAN上向环的两端发送副本。HSR的一个关键限制是，环中的所有中间交换机必须能够理解HSR，以便在主帧被发送到目的地后删除副本。

11.4 系统控制GridBlock——变电站广域网

随着变电站自动化的兴起，广域网将变电站和控制中心连接起来，并负责承载本应由电力公司运行的应用程序。这些通信类型不仅包括传统的IT系统通信，还包括物理安全系统通信、SCADA和远程保护通信。在所有这些应用程序中，远程保护应用程序对延迟、抖动和包丢失最敏感，它需要精细的WAN设计。

根据IEC 60384，保护被定义为“在电力系统中检测故障或其他异常情况，进行故障清除，终止异常情况，并启动信号或指示”。远程保护是通过网络传输信息的机制。

世界上几乎所有的电力公司在输电变电站和一级配电变电站之间使用远程保护。电力公司使用远程保护来在保护继电器之间发送信号，以确保即使在电网部分断开的情况下也能持续供电。在物联网环境中，保护继电器是将重要数据数字化，然后由IP传输网络传输的端点。

11.4.1 定义远程保护

在实际应用中，有两种常见的保护形式：距离保护和电流差动线路保护。无论采用哪种保护方案，继电器之间始终需要通信系统。

1. 距离保护

距离保护监控在预定距离内电路阻抗不可接受的变量。如果继电器发现阻抗的变化超过了可接受的阈值，则继电器确定线路上有故障。继电器之间的通信网络传输测量的状态，不仅用于确定是否发生故障，而且用于确定故障发生的位置。在大多数情况下，此信息还用于清除故障和恢复电力。

距离保护使用了这样一个概念，即电路阻抗与其长度（线路的距离）成正比。因此，对于已知的线路距离，继电器只需要测量线路关键点的线路阻抗，然后计算出断点的位置。如果测量的阻抗与期望值不同，继电器可以向开关发出信号，以启用或禁用馈线。由于线路保护使用简单的阻抗测量，因此通信继电器之间的延迟或抖动不是主要问题。

图 11-7 说明了一个简单的多区域距离保护方案。继电器测量不同区域的阻抗，并以此来隔离故障的位置。区域可以重叠并延伸到区域线路长度以外，以提供100%的主跳闸保护，并为相邻线路提供备用跳闸保护。例如，在图11-7中，区域B1和B2重叠以提供冗余保护。

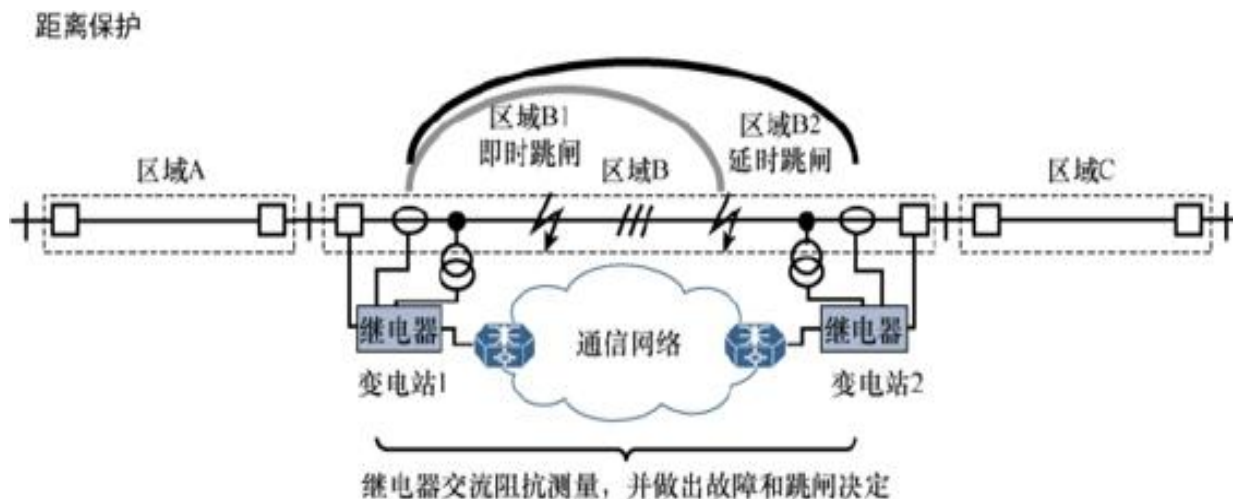


图11-7 距离保护方案示例

2. 电流差动（87L）保护

不同于距离保护，电流差动保护比较了不同变电站中两个相距较远的继电器之间的电流样本。例如，电流中的非零差动意味着线路上的某个地方出现了故障，将导致继电器跳闸。

当然，在交流电系统中，电流测量随时间变化，因此电流差动保护要求变电站之间同步计时。如果计时不同步，则继电器之间的电流测量在给定的时间点可能不同，错误地指示电流损失或电流过载，从而导致继电器向开关发出信号并断电。

同步继电器通常使用两种机制，以确保电流样本是一致。第一种是使用基于 GPS 的同步。第二种称为基于信道的同步，它基于双向时间传输，利用通信信道在继电器之间交换时间戳消息。基于信道的同步技术通常是继电器制造商的专利。

定时同步的常用方法有SyncE和IEEE 1588精确定时协议（PTP）。图11-8说明了测量电流矢量的电流差动保护方案。

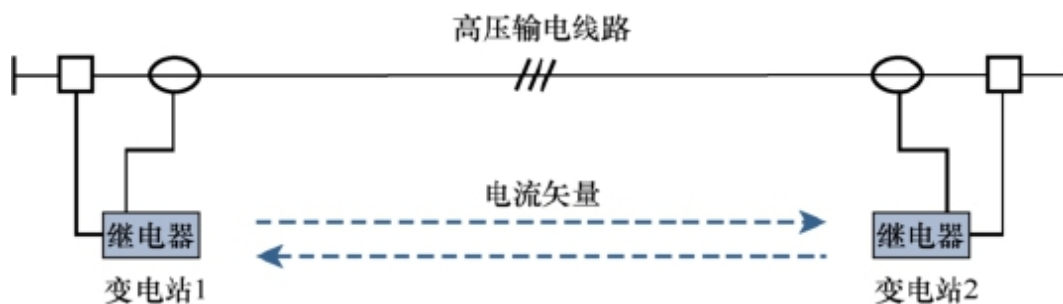


图11-8 高压输电线路电流差动保护方案

继电器之间的同步需求也意味着继电器之间的通信路径必须是确定和可预测的。由于时序同步的要求，电流差动保护对与分组延迟和抖动相关的通信要求非常严格，这意味着所有的方案都要求继电器之间进行对称的转发和返回路径通信。

在IEC61850之前，继电器通过TDM电路在变电站之间背对背连接。中继器之间通信的数据量实际上非常小，通常只需要一个DS0（或56kbit/s、64kbit/s链路）。

多年来，业界针对远程保护继电器制定了各种接口标准。其中包括用于铜线连接的ITU-T G. 703和用于光纤连接的IEEE C37.94。这些传统的接口类型是唯一的，并且是为远程保护应用程序定制的。此外，ITU-T X. 21和E&M接口也用于一些传统的远程保护继电器。E&M是一种监控线路信号的方法，我们可以从它在模拟语音中继的使用中了解它。近年来，各公司开始部署基于IEC 61850-90-12的现代保护系统（利用了以太网接口）。

电流差动保护的时间同步对网络提出了极大的要求。IEC 61850-90-12 规定继电器之间的端到端延迟不应超过 10ms。这包括中继内的接口处理延迟、路由器上的处理以及通过链路的光速时间。这种形式的远程保护还包括另一个挑战：管理路径对称性。正如管理单向延迟很重要一样，双向延迟的差异甚至更加敏感。典型的继电器可以容忍正向和反向通信延迟差不超过 $500\ \mu\text{s} \sim 1\text{ms}$ 。如果一个保护电路由于最优的IP路由问题而具有不同的正向和反向路径，则继电器可能会误读通信同步问题并跳闸，从而导致功率损失。实际上，管理端到端的远程保护延迟预算是保护和控制工程师工作中最具挑战性的方面之一。

11.4.2 为远程保护设计广域网

在过去的几年中，当保护和控制工程师使用TDM电路在不同变电站的继电器之间进行通信时，可以测量延迟，并且可以预测在两个方向上的延迟都是相同的。这些是简单的点对点电路。然而，大多数现代公用事业公司现在正在迁移到多用途分组网络，如MPLS，以传输几乎所有的应用程序，包括远程保护。基于MPLS分组的网络有巨大的好处；灵活、易于扩展、多租户和多服务；能够承载许多不同的应用程序；甚至可以通过通道模拟和隧道服务传输传统协议。

虽然基于IP的广域网在公用事业领域有非常积极的发展，但在远程保护方面，它们确实有一个缺点：虽然使用IP路由机制能找到最短的路径到达目的地，但默认情况下它们不使用已知有延迟的可预测路径。如果MPLS网络能够找到更好的路径到达目的地，它就会采用它，

而不考虑它所承载的底层应用程序的延迟敏感性。这里有一个微妙的平衡：虽然必须最小化端到端延迟，但它还必须是双向一致的。

为了应对这种需求，IETF和ITU于2008年开始联合研究MPLS的变体，该变体能够利用传统标签交换的所有优点，但同时也包含了载波交换和操作、维护、管理（OAM）的关键元素，这些元素允许远程保护等应用程序通过MPLS传输。MPLS传输配置文件（MPLS-TP）应运而生，它具备流量工程、自动保护切换（APS）和OAM的功能。

MPLS-TP通过规定的标签交换路径（LSP）传输点对点伪线（通过MPLS传输的虚拟电路）。逐跳的LSP由保护和控制工程师进行编程，以确保正向和反向LSP是精确相同的（见图11-9）。这样做的好处是使延迟可预测且具有对称性，并将抖动降到最低。伪线端点在远程保护继电器处终止。

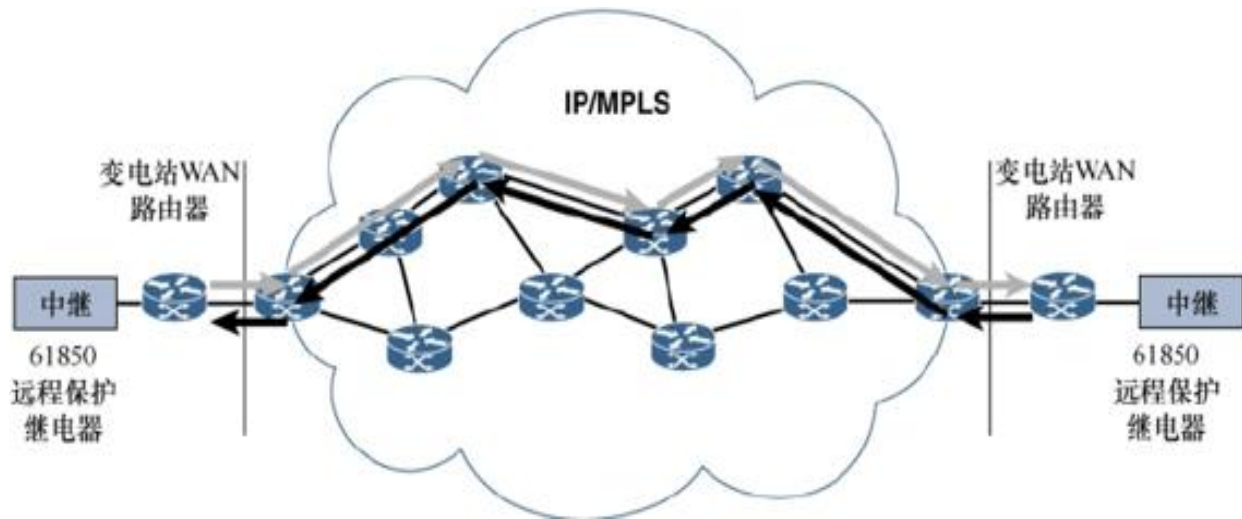


图11-9 用于远程保护继电器的对称前向和反向MPLS-TP LSP，提供了可预测的延迟和抖动

MPLS-TP还通过标识已知的备份LSP路径来支持APS，以防止主LSP发生故障。在本例中，还部署了备份LSP，以便在发生故障时具有可预测的延迟和路径对称性。

MPLS-TP的主要优点之一是它支持端到端的OAM。OAM允许在任何点对伪线路进行故障检测，并用作将故障转移到备用LSP的触发机制。MPLS-TP使用基于RFC 5085的通用关联信道（G-ACh）实现带内OAM功

能。带内OAM通道类似于点对点管理/控制电路，可以检测链路或节点故障，并可以在50ms或更短的时间内发出备份LSP故障转移信号。图11-10说明了MPLS-TP伪连接中的G-ACh。

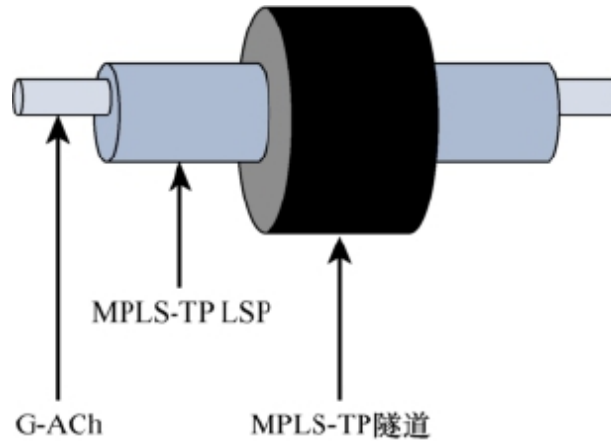


图11-10 MPLS-TP伪线路中的OAM通用关联通道（G-ACh）

MPLS-TP能够满足远程保护的要求，但其他类似的MPLS模式，如MPLS流量工程（MPLS-TE）呢？MPLS-TE是多年前开发的，用于通过MPLS网络显式动态地定义标签交换路径（LSP）。因此，它与MPLS-TP有许多相似之处。然而，尽管MPLS-TE可以用来满足可预测的延迟和远程保护的路径工程需求，但有一个缺点：MPLS-TE没有OAM功能。使用MPLS-TE，仍然可以创建确定的和对称的路径，以及提供对APS的支持，但MPLS-TP的实现往往要简单得多，并且与载波以太网交换有更多的相似之处。

与MPLS-TP相比，MPLS-TE有一个关键的优势：它具有呼叫准入控制（CAC）能力。使用CAC，边缘路由器能够确定路径上是否有足够的带宽来支持请求的电路。在大多数情况下，这种能力对于远程保护流量来说并不重要，因为带宽需求是最小的，但在实践中它很有用。

一种称为Flex-LSP的MPLS变体结合了这两者的优点。Flex-LSP支持MPLS-TP的所有优点，如用于伪线的APS和OAM，同时还支持CAC和第3层流量工程，很像MPLS-TE。随着技术的不断改进，其他MPLS方式（如段路由）可能也适用于未来的远程保护。

11.5 场域网（FAN）GridBlock

电力行业处于物联网的前沿。这一点在最后一公里的配电网中得到了最好的证明，该配电网被称为场域网（FAN）。

注释：术语邻域网（NAN）和场域网（FAN）之间有一些重叠。尽管这些术语几乎可以互换使用，但它们之间存在一些细微的差别。NAN严格地指最后一公里网络本身，而FAN包括连接到区域路由器的NAN和设备。图11-11显示了FAN区域所在位置的图形化描述。

FAN旨在用于实现对配电站和终端客户之间所有公用设施的全面监控。这部分电网包括客户和配电网系统本身的计量应用，还包括配电网设备的管理，这些设备有助于提高能力输送效率，建设低碳社会。

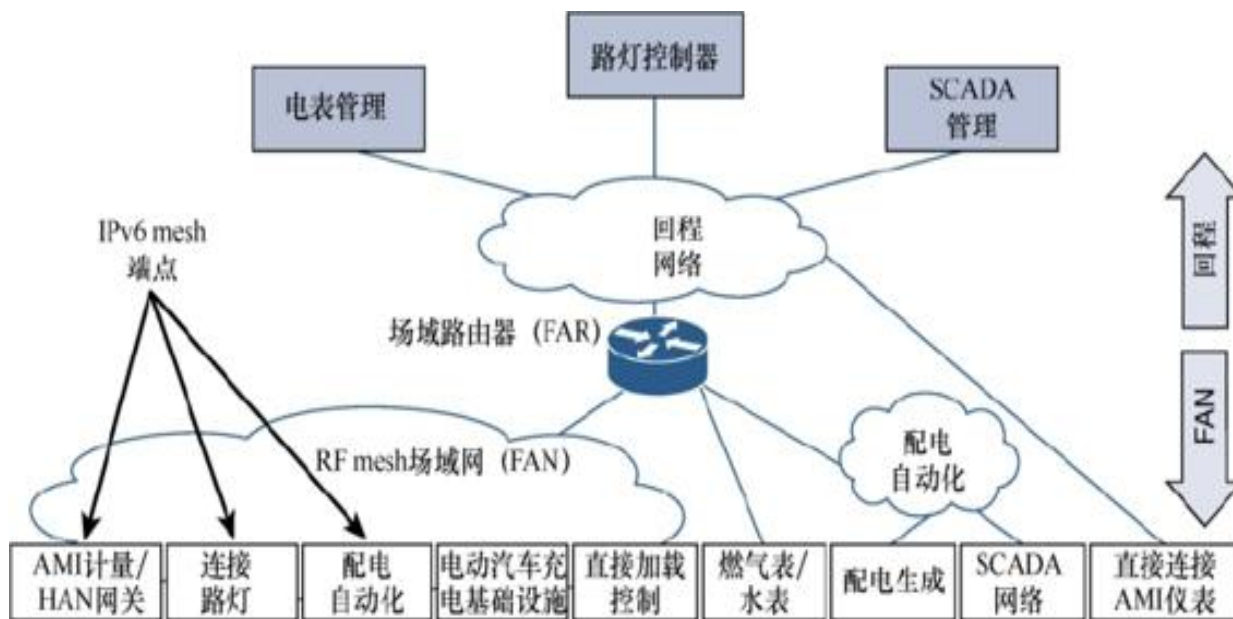


图11-11 风机多业务网格网络

FAN GridBlock被构建为多服务的，这意味着它不基于任何特定于供应商的专有技术，这些技术会限制其用途，就像许多传统的OT系统一样。过去，互联网标准根本不存在，在建立计量或配电自动化（DA）网络时，不存在基于开放标准的互联网标准。有必要为每个应

用程序建立一个专用的独立的网络。然而，现代开放标准和网络合规联盟（如Wi-UN和HomePlug联盟）帮助建立了互操作性标准，允许部署单个多服务网络，以支持广泛的应用程序和供应商。正如WiFi联盟帮助建立WiFi接入点和终端客户端的互操作性一样，这些联盟也在建立互操作性标准。很快就会有有一个全面运作的FAN网络，由不同的供应商提供各种组件，所有组件都使用相同的标准。

注释：Wi-SUN和HomePlug联盟都在本书的前面讨论过。关于Wi-UN联盟的更多信息，请参考第4章和第5章。HomePlug联盟在第4章中介绍过。

FAN GridBlock利用了第4章～第6章中讨论过的许多标准，包括IPv6、IEEE 802.15.4 mesh、CoAP和LTE。这种灵活和开放的标准方法通过对安全性、服务质量、弹性和网络管理服务的广泛理解，促进了多厂商即插即用的能力。这产生了一系列广泛的功能，远远超出了琐碎的计量用例。

图11-11展示了一个多服务电网FAN，它支持各种应用程序，如电动汽车充电站、连接的路灯、需求响应端点、智能电表以及与配电网中远程SCADA RTU的连接。

总之，现代FAN对于公用事业具有如下吸引力。

■ **开放和基于标准：**网络、传输和应用层的核心组件已经由IETF和IEEE等组织标准化，并且可以与其他兼容设备交互操作。

■ **多功能终端支持：**基于IPv6的物联网终端非常灵活，可用于多种地点，包括AMI（仪表）、街道照明模块、需求响应设备和SCADA RTU等配电自动化终端。

■ **灵活的前端部署选项：**因为FAN使用IPv6传输，所以前端聚合点和安全系统可以部署在本地，也可以托管在云端。

■ **灵活的回程选项：**FAN通常需要一个安装在电线杆或其他方便位置的场域路由器（FAR）。FAR是网状网络的终点。回程有很多种选

择，包括LTE、3G、WiMAX、光纤，甚至是非常偏远的社区的卫星回程。

■ 支持传统应用程序：通过使用网关，传统设备（如串行RTU）可以大规模连接到IPv6 FAN。

■ 可扩展：IPv6可以扩展到数千万个端点，方便地管理大型公用事业网络中的电表和路灯。

■ 高度安全：FAN GridBlock集成了多层安全性，包括应用程序和网络层加密以及端点身份验证。

■ 稳定和弹性：由于IPv6的灵活性，精心设计的FAN能够提供强大的网络可用性和弹性。例如，如果FAR通过WiFi进行主回程，LTE可以作为辅助备份，IP路由协议可以用来确定最优路径。此外，使用IP路由，远端可以形成到主端和次端站点的冗余连接。

下文将讨论FAN在两个关键领域的应用：高级计量基础设施（AMI）和配电自动化（DA）。

11.5.1 高级计量基础设施

截至2016年底，全球已安装智能电表约7亿只。智能电表是基于微处理器的传感器和控制器，利用双向通信过程来交换诸如设备认证、安全和管理等信息。在过去，电力公司不得不派遣技术团队来读取用户的电表，以便向用户发送基于使用情况的账单。在许多情况下，如果电表每年读取3~4次，电力公司会做得很好。此外，许多水表位于难以到达的地区，有时甚至对技术人员来说是危险的。

随着智能电表的出现，现在每天可以读取几次电表。对于商业和工业（C&I）仪表，每隔几分钟就可以进行一次读数，以了解最新的电力消耗情况。这对客户来说是非常有价值的，因为他们现在能够获得高度精确的每月账单报告。客户还可以通过门户网站查看每小时的电力消耗。一些公用事业公司已经实行了按日计费，这样一来，在高峰

时段可以收取较高的电费。几乎即时的反馈有助于家庭了解他们的消费模式，节省电费。这证明了物联网的力量。

图11-12展示了一个由加拿大公用事业公司发布的智能电表门户网站，该公司已经在其FAN中全面部署了IPv6智能电表。

智能电表还有其他几个独特的优点。例如，现在可以通过远程断开开关随意关闭一个仪表。虽然这可能被视为一个安全问题，但对这家公用事业公司来说，好处是在无须派遣工作人员的情况下，关闭或恢复那些尚未支付账单或正在偷电的客户的电力供应。这种减少的工作量节省了大量资金和劳动时间。

此外，大多数智能电表还带有一个内部家庭区域网络（HAN）无线电，可以通过ZigBee与家庭内部的电子设备进行通信（有关ZigBee的更多信息，请参阅第4章）。这允许家庭或企业所有者跟踪每台设备或每台设备的功耗。

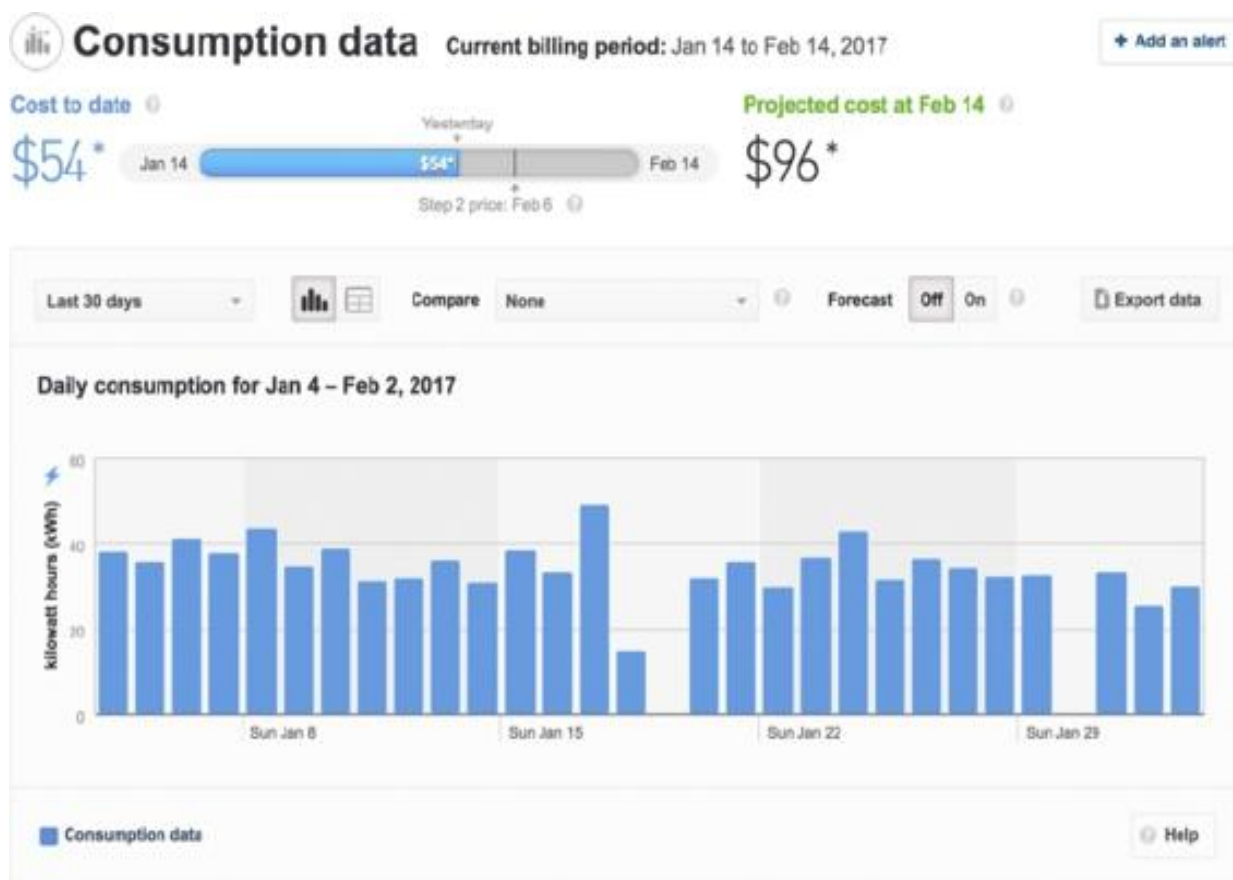


图11-12 智能电表门户网站的每日报表

图11-13展示了现代智能电表的结构。

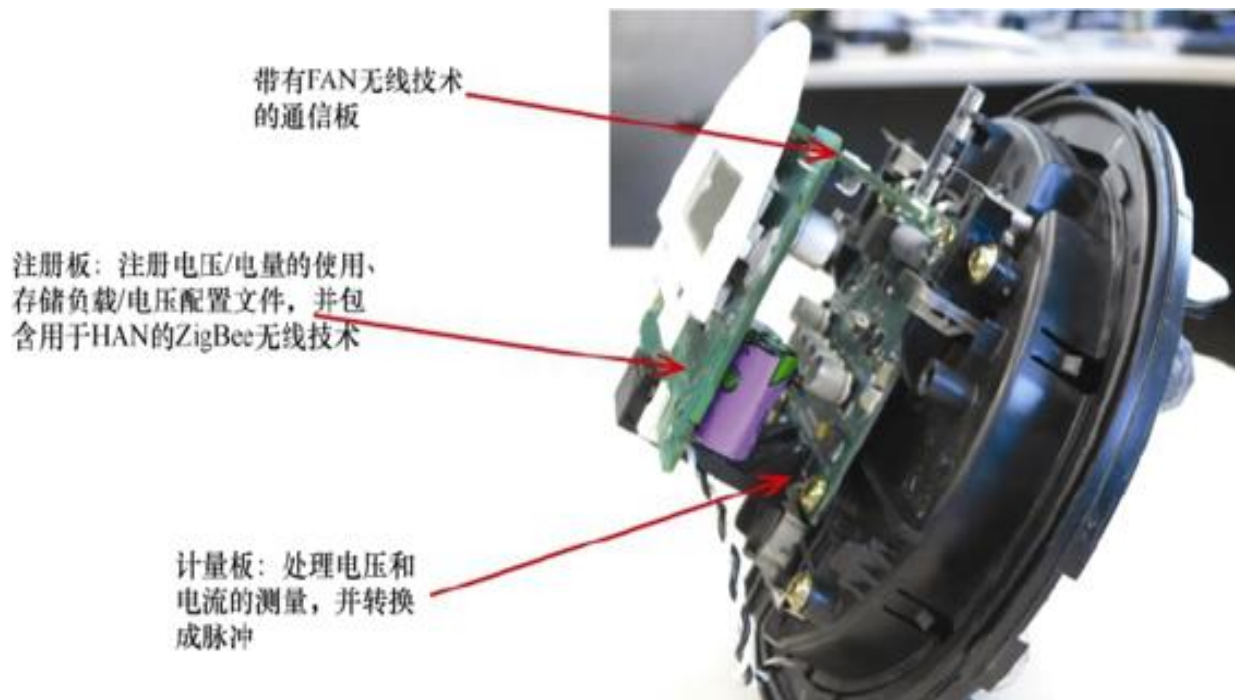


图11-13 智能电表的结构

在使用RPL mesh的IEEE 802.15.4网络中，仪表是网格节点，因此是中继器。有关802.15.4和RPL的更多信息，请参阅第4章和第5章。每个仪表运行IPv6协议栈，并努力通过RPL在网格中找到自己的位置。在一个大的mesh中，只有几个仪表直接连接到FAR。大多数是在更深的mesh中，并且相互之间有链接。在这种情况下，与大多数第2层网络不同，在第2层网络中我们试图限制广播域的大小，一个大的mesh实际上是一件好事，因为它加强了mesh的连通性。mesh越大，越密集，就越能把它推到周围。

以一个大型公寓楼为例，它的地下设备室包含该建筑的所有仪表（称为仪表场）。虽然整个建筑可能有数百个仪表，代表每个公寓或单元，但只需要有一个上游的RPL链接到通向FAR的父节点。其余的都是那个仪表的分支。图11-14所示为混凝土拱顶中的地下仪表场。这些地下电表只是在主mesh上形成一个分支。



图11-14 公寓楼中的地下仪表场

11.5.2 其他用例

FAN被设计为多服务，支持单一聚合网络上的广泛应用程序。然而，FAN有一些关键的限制，包括有限的带宽和节点之间的高延迟（每跳几百毫秒），这意味着它们不太适合媒体丰富的应用程序，如视频监控，当然也不适合远程保护。然而，有许多低带宽应用程序使FAN成为公用事业和其他行业（包括智能连接城市）的理想选择。

注释：Wi-SUN（无线智能公用事业网络）联盟是802.15.4 FAN最著名的供应商能力联盟。基于传统的数据编码调制方案，Wi-SUN 1.0兼容规范支持高达150kbit/s的链路速度。但是，我们应该注意到，使用性能更高的调制方案，可以显著地将其提高到几百kbit/s。

除了智能计量之外，还有无数的FAN用例，如图11-11所示。下面将更详细地讨论两个有趣的用例：需求响应和配电自动化。

1. 需求响应

平衡可用性和电力需求是公用事业的主要挑战之一。电力需要流动。它通常不会存储在整個配电网的巨型电池单元中，而是在需求突然增加时进行分散。如果需求超出可用性，就必须付出一些代价。例如，在炎热的夏天，大量的空调设备会使公共设施负荷达到极限，并可能导致停电。

随着时间的推移，公用事业工程师已经解决了这个问题，他们在用电高峰期控制不太重要的系统的用电量，从而使整个电网的用户仍然可以用电。这是通过一种称为需求响应（DR）的机制实现的，该机制涉及部署远程控制设备，该设备在用电高峰期间切断电网上某些设备的电力供应。例如，在用电高峰期，电力公司可以向使用某些类型的电力设备（如电热水器）的用户发送广播消息，自动降低这些设备的电力消耗，从而为电网的其余部分提供更多的电力。

在过去，DR控制器不过是简单的无线寻呼机，它接收DR管理系统的信号，然后根据指示自动关闭设备。当电源可用时，它将接收到其他信号，并将设备重新打开（使用二进制的开/关操作类型）。

虽然有许多方法可以连接到与电器连接的DR控制器（包括蜂窝式和1902.2 PLC），但FAN也可以用于此应用。在这种情况下，电力公司使用FAN的IPv6网络与需求达到峰值的电网特定部分的DR控制器通信，并可以根据需要集中控制其功耗。图11-15显示了一个装有FAN mesh DR控制器的电热水器。



图11-15 与FAN需求响应控制器相连的电热水器

2. 配电自动化

随着变电站通过网络连接实现自动化，从变电站到最终用户的配电网也在经历一场连接革命。配电网往往覆盖非常大的地理范围，网络连接成为一个重大的挑战。如果抬头看一根电线杆，注意到电气设备的种类和数量，我们可能会注意到数量相当可观。乘以公用事业服务区域的端点总数，这是一个非常大的设备数量。配电装置包括重合闸、负载开关和电容器组控制器。这些设备都在配电网服务中发挥着关键作用。由于将配电控制和自动化设备连接到中央网络的挑战，它们被设计成可以作为自治设备进行工作，在许多情况下，它们具有足够的智能，可以在没有任何监控的情况下运行。然而，随着无线网络的技术和可用性的提高，可以将感知电网运行状况的配电设备连接到通信网络，从而大大提高配电网状况的可见性。这也有助于显著提高配电网电力的可靠性和质量，并开创配电自动化（DA）时代。

DA致力于改善电网的状况、可靠性和电能质量，从而能够降低成本，增加正常运行时间并提升满意度。DA设备执行许多不同的功能，从测量电力质量到清除线路中的临时故障。临时故障的一个例子是树枝落在直线上，在树枝落到地面之前造成临时短路。清除这种故障是重合闸的功能。

将这些设备分层放置在通信网络上会使自动化水平显著提高。电力公司不仅可以通过SCADA获得确定配电网设备的状态，还可以对数千台DA设备生成的数据进行整理和分析，从而更好地了解整个电网的状态。

下面是一些使用基于FAN的DA的示例。

■ **配电SCADA系统：**本章前面介绍了变电站内的SCADA能够实现电网的自动化。通过使用FAN，现在可以对变电站外的设备进行相同级别的管理。虽然有几种技术适合连接这些物联网设备（包括LTE和WiFi），但FAN的可扩展性以及SCADA的低带宽要求，使FAN成为一个理想的网络平台。当SCADA终端是远程的时，通信可以在变电站聚合，然后发送回控制中心，或者直接发送到控制中心，完全绕过变电站。

注释：除了针对DA的FAN解决方案，还可以考虑其他几种无线技术，包括4G和NB-IoT蜂窝选项。

■ **故障定位、隔离和服务恢复（FLISR）：**在过去，有人打电话告诉电力公司，电力公司才会发现停电。这不仅浪费了宝贵的恢复时间，而且对查明系统故障实际发生的位置毫无帮助。FLISR系统的设计目的是识别、定位和诊断问题，以便电力公司立即了解发生了中断。在某些情况下，它们甚至允许电路自我修复。断路器、智能仪表和故障清除开关都是FLISR系统的一部分。由于这些装置都是远程的，只需要最小的带宽，所以FAN是传输FLISR通信的理想选择。

■ **集成电压/VAR控制（IVVG）：**电压/VAR系统用于配电网，以监测和控制高峰时期的电压水平，并有助于节约用电。过去，由于变电站外的通信挑战以及电网中电压传感器的可用性，电压/VAR优化（VVO）部署受到限制。近年来，蜂窝和FAN网状网络等通信系统使得

从电压传感器收集信息并利用这些信息实时调整电容器组等电压调节设备成为现实。

图11-16说明了这些不同的用例，它们连接到一个单一的多服务场域网络。在图11-16中，许多不同的应用程序都使用一个FAN。但是，控制SCADA、FLISR和IVVC功能的应用程序服务器都位于数据中心或控制中心的配电管理系统中。

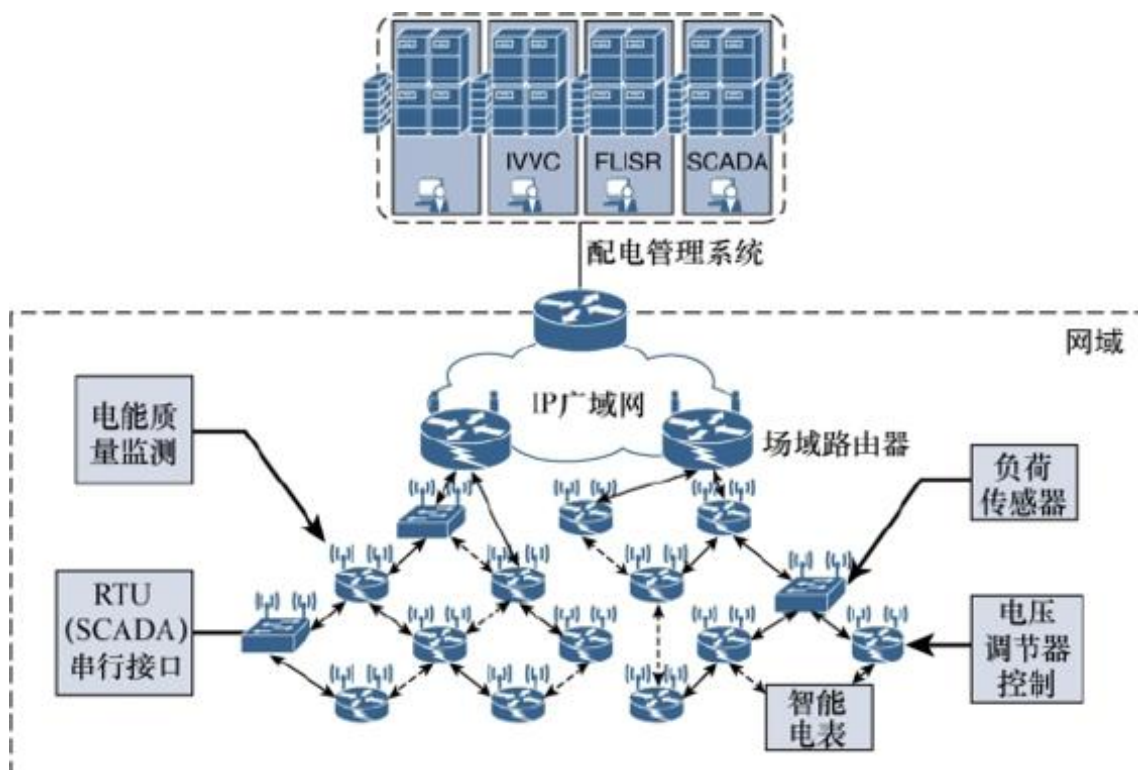


图11-16 使用单一的多业务FAN电网网络连接各种DA设备，包括SCADA、FLISR和集成的电压/VAR控制系统

11.6 保障智能电网的安全

初次开发SCADA协议时，几乎没有考虑安全性，因为SCADA是使用物理上隔离的专用串行连接与远程设备相连，并且与任何其他类型的网络没有连接。在过去的时代，网络黑客的概念甚至不是公用事业工程师考虑的问题。然而，随着SCADA的成熟并开始使用以太网和IP作为

传输技术，SCADA协议的性质导致了重大的安全问题，并最终为聪明的新攻击载体提供了机会。

第2章中讨论过2015年乌克兰的电力攻击，导致103个城镇断电（还有186个城镇受到影响），涉及对6家电力公司的复杂同步攻击。这次攻击影响了电网的SCADA网络，它从公司电脑上的恶意软件开始，蔓延到OT系统。今天，公用事业公司只剩下了这个具有几十年历史且在设计时没有考虑安全性的管理协议。

乌克兰的袭击给世界各地公用事业公司的安全团队留下了深刻印象。由于这一攻击和其他不为人知的攻击，公用事业公司都在争先恐后地尽快保护它们新的融合系统和传统系统。

根据Cisco安全能力基准研究，73%的公用事业IT安全专业人士表示他们曾遭遇过安全漏洞，而在其他行业，这一比例平均为55%。当然，公用事业是网络罪犯的高价值目标。2015年，伦敦劳埃德（Lloyds）保险公司模拟了一场针对美国东北部公用事业行业的大规模协同网络攻击的经济影响。据预测，影响将达到2.43亿美元到1万亿美元。虽然如此大范围的攻击似乎不太可能，但最近的网络攻击，如乌克兰电网的攻击，表明这种攻击在技术上是可行的，应该引起公用事业运营商及其客户的关注。

现在已经提出了不同的基于公用事业的安全体系结构。IEC 62351就是其中之一，它是由IEC TC57开发的，用于支持IEC 60870和61850的安全需求，其范围相当广泛。北美电力可靠性公司（NERC）的关键基础设施保护（CIP）是一个安全模型，是为了保护大容量系统而开发的，它仍然是北美公用事业行业最重要的安全主题之一。

11.6.1 NERC CIP

物联网是新一代公用事业安全的驱动力。为了应对针对电力公司的网络犯罪威胁，美国联邦能源监管委员会（FERC）要求所有电力公司在2016年7月1日前遵守NERC CIP v6标准。尽管NERC CIP是一个关注

美国公用事业（以及向美国出售电力的电力公司，如加拿大的电力公司）的安全标准，但是该制度制定的原则为全世界的公用事业提供了一个有益的参考模型。

NERC CIP采用风险评估安全方法。与使用一份详尽的说明性建议列表并通过审核强制执行它们不同，NERC提供了最终安全状态的清晰愿景。这是一种强大的方法，因为它通过检查所有正确的选项，而不是试图真正地保护网络，从而转移了通过审核的注意力。相反，NERC CIP v6帮助电力公司将重点放在真正重要的事情上：保护它们的网络免受来自内部和外部的攻击。例如，NERC CIP v6更注重原理驱动，需要恶意软件保护，而不是强制要求某种类型和级别的防病毒软件。

NERC CIP主要关注于建立安全策略、程序和过程。该模型中的一个关键概念是评估安全漏洞对公用事业资产的影响程度。公用事业公司需要正确地识别每项资产的影响级别，将级别定义为高、中、低或完全没有影响。范围内的资产被定义为“如果不可用、降级或滥用，将在折衷方案启动或执行后15分钟内对大容量电力系统（BES）的可靠运行产生不利影响的资产”。

NERC CIP v6还需要入侵检测/预防系统（IDS/IPS）或某种形式的深度数据包检查（DPI）。该标准还要求定义电子安全边界（ESP），其中EPS中的资产由两种不同的安全措施保护，如防火墙和IP。此外，还定义了物理安全边界（PSP），包括视频监控和建立访问系统等方面，旨在保护工作站免受物理攻击。

注意：2013年4月16日，加利福尼亚州圣何塞附近的太平洋天然气电力公司梅特卡夫变电站遭到狙击手袭击。在这次袭击中，持枪者向17个变压器开枪，造成1500万美元的损失。这是一次组织严密、计划周密的袭击，但罪犯至今仍逍遥法外。诸如此类的事件有助于塑造NERC CIP v6的PSP方面。

NERC CIP的一个关键方面是，无论BES网络系统是否与其他网络有外部连接，都必须为连接到可路由网络的所有高、中影响力的BES网络系统建立ESP。图11-17显示了一个主要的变电站网络，突出显示了ESP和PSP组件。

遵守一个标准并不能保证安全性，但是在提高人们对公用事业安全状况的认识和加强问责方面，它确实大有帮助。NERC CIP v6是一个庞大而复杂的主题，其细节超出了本书的范围。NERC CIP涉及恶意代码预防、配置和变更管理、漏洞评估和安全事件监视等领域。

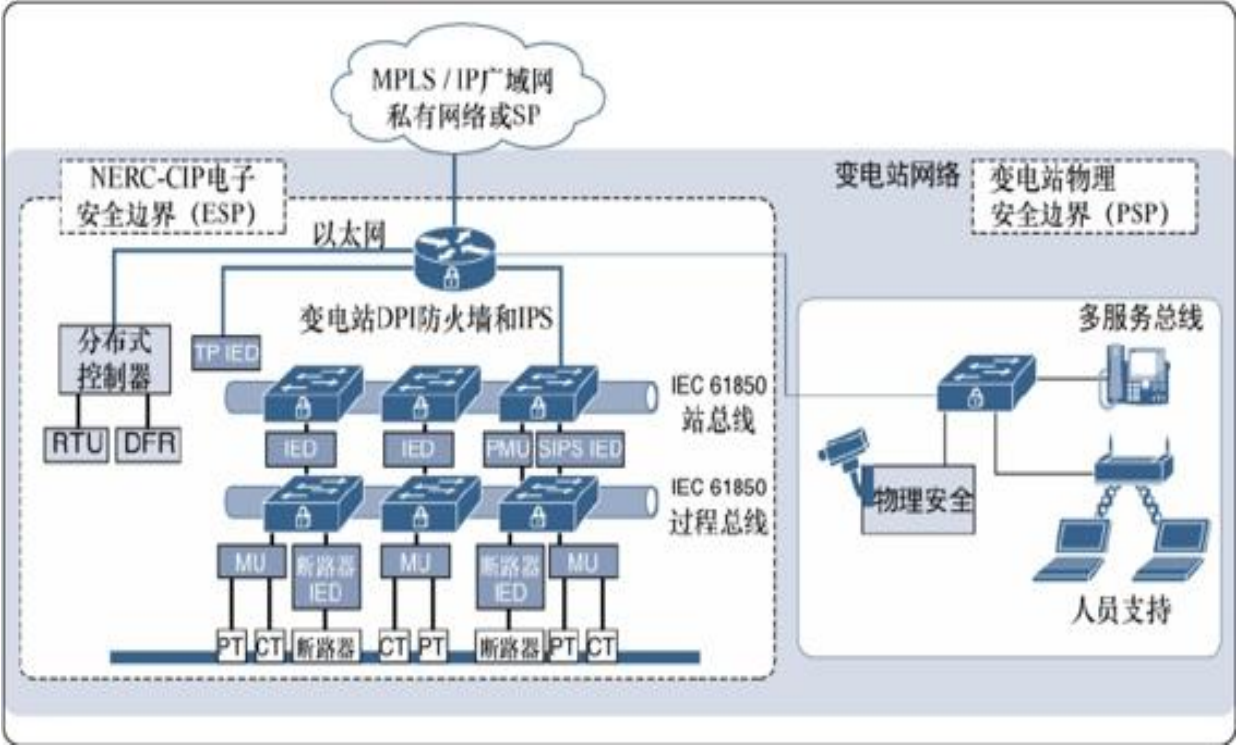


图11-17 具有NERC CIP v6电子和物理安全边界的主变电站网络

11.6.2 智能电网安全考虑

配电网络被认为超出了NERC CIP的范围，因此FAN不包含在这个符合标准的范围内。然而，配电网仍然是一个需要安全保护的关键区域，特别是因为这部分电网的资产分布非常广泛，而且通常处于不受保护的区域。

FAN安全性符合以下原则。

■ 访问控制：FAN设备通常驻留在不安全的位置，因此设备本身需要具有高度安全的访问控制。如果一个电网物联网终端被恶意添加

到FAN，它可能是网络的后门。为此，建议使用FAN端点和路由器来支持X.509证书，一旦设备注册到网络中，则同时提供工厂级别的证书和实用程序特定的证书。ITU-T X.509标准定义了一种用于处理安全证书和密钥的结构，我们可以识别到它，因为它通常用于保护Web和电子邮件通信。

■ **数据完整性和保密性：**FAN设备需要加密。“最后一公里”的FAN经常使用未经授权的无线技术，很容易被发现。强烈建议对堆栈的每一层进行加密。此外，应该加密FAN设备（如FAR）中的配置文件，以防止黑客从被盗设备获取信息。

■ **威胁检测和缓解：**实现单向威胁检测和缓解的一种方法是，将FAN前端组件和系统与变电站或控制中心的其他关键系统进行逻辑分离。与前面提到的NERC CIP v6要求一样，遵循深度防御模型并使用一层以上的深度数据包检查是一个好主意，例如理解工业协议（如SCADA）的防火墙和IPS（注意，如果FAN端点应用层加密，这将限制深度数据包检查的可见性）。

■ **设备和平台的物理完整性：**现场区域的资产，如FAR，需要尽可能进行物理保护。路由器应该是防篡改的，并有门铃。此外，IEEE 802.1AR（安全唯一设备标识符）正在成为远程路由器的标准，不仅可以加快部署速度，而且可以确保电力网络上的设备是可信的。保护智能电网是一项复杂且不断发展的任务，特别是在高度分布式和公共环境中，如配电网络。尽管NERC CIP主要关注于保护发电站和变电站资产，但公用事业的安全最终需要一个更广泛的视角。这必须在GridBlocks体系结构的每一层都得到解决，要特别关注于特定于公用事业的协议，如SCADA，这些协议在设计时没有考虑到安全性，但是现在通过高度互联的网络进行传输。

[11.7 智能电网的未来](#)

自电力行业诞生以来，这种涉及大规模发电、输电和配电的模式一直是向客户提供可靠电力的最具成本效益的方式。然而，在这一过程中也存在一些挑战，包括对发电厂排放的污染的担忧、消费者对电力的无止境需求，以及不断扩大电网基础设施的相关成本，更不用说日益复杂的电网的脆弱性。

如今，这个行业在多个方面都面临着前所未有的挑战。其中一些挑战具有破坏性，并威胁到该行业的未来。这些挑战包括要求整合由可再生资源产生的电力，比如风能和太阳能，以及集成的分布式能源资源（DER），如太阳能光伏（PV）电池，它是由客户而不是公用事业公司安装和拥有，但是向电网销售电力。

夏威夷就是一个有趣的例子，那里的平均电费是北美其他地方的三倍多。高昂的电力成本促使许多夏威夷人安装太阳能光伏板，以利用充足的阳光。事实上，到2016年，超过12%的夏威夷人在家里安装了太阳能电池板。虽然太阳能是一种生产清洁能源的好方法，但要将这些家庭生产的电力整合到一个与其他电网隔离的岛屿电网中，这是一个极其困难的挑战。此外，随着越来越多的人在家中安装太阳能，电力公司的付费用户也越来越少；连接到电网的太阳能家庭成为分布式发电节点，电力公司必须向客户支付电费。付费用户越少，维护系统的收入就越少。2016年，这些经济现实导致夏威夷停止在岛上进一步部署太阳能电池板。

一些分析人士预测，随着时间的推移，客户拥有的发电量的增长可能会破坏公用事业的经济基础，到一定程度，它们将被打乱秩序，就像我们在互联网、音乐、零售和其他行业所看到的情况一样。一些人认为，公用事业公司不拥有的DER可能造成的破坏是一种威胁。其他人则认为这是电网在高可靠性、低成本和低碳排放时代需要进行的变革。

分布式发电和可再生能源的时代为智能电网提供了强有力的支持。如果不控制和监督可再生能源，特别是在中/低压层，就不能引进它们。例如，公用事业公司面临的一个有趣的挑战是，在电力高度分散的电网中，如何平衡和控制电力。

例如，太阳能电池产生直流电源。然而，电网运行在交流电上，电流频率和电压/电流相位都是提供高质量电力的关键因素。为了向电网提供能量，直流电源需要通过电源逆变器转换为交流电源。虽然这看起来很简单，但仍有一些挑战需要考虑，比如如何在整个电网中平衡如此分散的第三方发电。这就需要一个可靠的网络系统，能够在电力公司的电网和DER的物联网设备（如逆变器或智能电表）之间进行通信。

另一个颠覆性的变化是电动汽车的兴起。随着越来越多电动汽车的推出，它们将需要更多来自电网的电力，也有可能将这些充满电的汽车电池作为远程电力存储单元。工程师正在寻找使用这些电动汽车电池作为DR解决方案的方法，以支持电网在高峰时期的供电。这完全改变了需求响应的概念以及如何有选择地使用电力。同样，汽车电池是直流供电，所以电力需要转换成交流电，这样的系统将需要逆变器和系统计量来跟踪电力的流动，包括电力的输入和输出。所有这些都凸显了可靠的物联网通信网络在智能电网中的重要性。

不管世界各地的颠覆和转型如何发展，未来10~20年，电力行业将经历比过去一个世纪更大的变化。

11.8 小结

可靠的电力对现代文明至关重要。虽然世界各地的公用事业公司严重依赖传统技术和协议，但颠覆性技术和对电网的新需求使电力公司成为最早采用物联网的公司之一。

物联网技术正在推动电网从发电到输电、再到配电各个方面的数字化转型，开启智能电网时代。一个独立于供应商的整体参考模型是GridBlocks，用于将电网的所有元素联网到一个单一的架构中。GridBlocks将电网的各种功能划分为11层，使得电力公司能够系统、有条理地进行数字化。

本章讨论了GridBlocks体系结构的几个元素，包括主要的变电站GridBlock，并讨论了变电站自动化技术，其中重点是SCADA的使用以及通过IEC 61850标准推动标准化。这种标准化的重点是支持变电站内的站总线和过程总线，以及各种以太网交换设计，以满足IEC 61850的严格要求。

本章还研究了系统控制GridBlock，特别关注MPLS广域网上的远程保护系统。远程保护继电器具有世界上最敏感的应用层延迟和抖动要求。本章讨论了满足这些需求的不同设计建议。本章还介绍了场域网GridBlock，包括多用途FAN如何驱动多业务配电网。本章还介绍了AMI、DA和DR等用例。

智能电网安全是电力行业许多人最关心的问题，特别是在电网设备通过IP进行连接的情况下。本章介绍了NERC CIP v6的关键概念，以及保护NERC范围之外的要素（如配电FAN网络）的策略。

本章对公用事业行业的未来做出了展望。分布式发电、微电网和电动汽车等颠覆性技术不仅以新的方式挑战现有电网，而且是数字化颠覆的主要力量，将为21世纪智能电网的创新创造新的机遇。

第12章 智慧互联城市

世界正在迅速城市化，而且这一趋势将持续下去。1950年，世界上只有不到1/3的人口居住在城市；到2050年，地球上2/3的人口将是城市居民。非洲和亚洲目前拥有世界农村人口的90%，预计将分别有56%和64%的人口实现城市化。今天，北美、欧洲、拉丁美洲和加勒比地区居住在城市中的人口比例已经超过了70%。从原始数据来看，世界城市人口已从1950年的7.46亿增长到近40亿。到2050年，这个数字将再增加25亿。

大多数城市都是从小城市中心发展起来的。这些城市在最初设计时，都没考虑过能立即容纳大量人口。人口的快速增长通常会给城市基础设施带来压力。道路、桥梁和下水道系统往往达到最大容量，使城市服务面临挑战。如何在提供水和住房等基本生活必需品的同时减少碳排放，已开始列入世界各地城市规划者和城市领导人的主要议程。

随着世界人口的增长，排放和消费也在增加。当人口集中在有限的地理区域时，环境吸收排放和废弃物的能力就受到挑战。排放和浪费的增加加剧了气候变化的诱因。今天，城市的能源和温室气体排放量占世界的60%~80%，消耗了所有饮用水的60%，水资源的渗漏损失高达20%。世界各地城市的领导人关心的关键问题是优化资源（水、电力、通信基础设施效率等）、废弃物和排放处理。

然而，城市的领导人也知道，城市人口的增长提供了一个利用城市潜力的机会。在每天每时每刻涌入城市的新人口中，有拥有技能、天赋和奉献精神的人，他们将成为他们最终生活在那个城市的有价值的资产。大的人口密度将为所有居民创造更多的商业机会。麻省理工学院的研究预测，未来城市将占全球人口增长的90%、财富创造的80%、能源消费总量的60%。我们的目标不是限制人口增长，而是更有效地控制人口增长。提高管理效率意味着提供更好和更有效的城市服

务，简而言之就是确保城市居民有更好的生活体验，能利用大量城市人口的经济利益，同时减轻随之而来的社会和环境困难。

未来的城市将在哪里找到维持自身所需的资源呢？没有简单的答案，但有明智的解决方案。本章将在以下几节中介绍这些解决方案。

■ 面向智慧城市的物联网战略：本节定义如何利用物联网技术改善市民生活和城市中心的有效管理。

■ 智慧城市物联网架构：本节描述智慧城市物联网集成的4个主要层次。

■ 智慧城市安全架构：本节从通信和收集数据的可接受用途两个方面考察智能城市物联网安全的主要制约因素和考虑因素。

■ 智慧城市用例示例：本节详细介绍了物联网在智慧城市中的4个用例：街道照明、智能停车、交通和智能环境。第13章和第15章提供了另外两个应用于智能城市的用例。

[12.1 面向智慧城市的物联网战略](#)

管理一个城市与管理一个企业有一些相似之处。随着对效率的需求增加，新的工具有助于提高运营效率。对城市来说，就像对企业一样，数字化改变了运营的视角。新思想的出现，带来了解决管理问题的不同方法。利用信息和通信技术（ICT）的可扩展解决方案，可以通过提高效率来缓解当今城市中心面临的许多问题，从而降低成本并提高生活质量。采用这种方法的城市通常被称为智慧城市，这是一个在世界范围内的城市规划和城市政策领域经常讨论的概念。

12.1.1 智慧城市的垂直物联网需求

城市管理有许多不同的方法和解决方案。所有这些解决方案通常是从街道层面开始的，传感器可以捕捉从停车位可用性到水纯度的所有数据。数据分析也被广泛使用，例如，减少犯罪或改善交通流量。市民可以利用他们的智能移动设备来报告问题，提出改善城市生活的建议或找到可用的停车位。通过互联互通，这些智能解决方案可以对生活质量产生变革性的影响。信息和通信技术将人、数据、事物和过程连接在一起，形成数十亿甚至数万亿的连接网络。这些连接产生了大量的数据，其中一些数据以前从未被访问过。当这些数据被智能化地分析和使用时，关联、分析和优化服务和流程的可能性实际上是无限的，从而为人们提供更好的生活质量。然而，城市中心物联网应用的增长不仅为其解决的每个问题带来独特的好处，而且还增强了城市开发高效服务的能力。

未来10年，城市将为物联网带来全球近2/3（63%）的总体民用收益。为了实现价值最大化，智慧城市可以通过共享收入的商业模式与特殊的合作伙伴结合使用案例，为零售和旅游、城市规划、停车和水资源管理等城市定位服务创收。

Cisco最近的一项研究（见图12-1）预计，物联网在10年内将产生以下经济影响。

■ **智能建筑：**智能建筑通过高效集成采暖、通风、空调（HVAC）和其他建筑基础设施系统来降低能耗，从而降低运营成本，这些举措有可能节省1000亿美元。请注意，财政收益只适用于城市拥有的建筑。然而，无论谁拥有这些建筑，减少的排放都会使城市受益。

■ **天然气监测：**监测天然气用量可以节省690亿美元，因为可以减少抄表成本，提高市民和市政公用事业机构的抄表准确性。当公用事业由城市管理时，对用户和公用事业公司产生的经济效益是显而易见的。无论谁经营公用事业，物联网在安全方面都有非常重要的优势。在消费量突然增加的情况下，及时发出警报可以更早地派遣应急响应小组，从而提高城市环境的安全性。

■ **智能停车：**智能停车可以通过提供整个城市停车位可用性的实时可视性，创造多达410亿美元的经济效益。居民可以识别并保留最近的可用停车位，交通管理员可以识别违规停车，市政当局可以采用基于需求的定价方式。

■ **水资源管理：**智能水资源管理通过IP网络连接家庭水表，提供远程使用和状态信息，可节省390亿美元。这样做的好处是显而易见的，它具有实时消耗可视性和泄漏检测等功能。此外，智能水表可以用于协调和自动进行私人与公共草坪浇水，在用水量较低或符合市政当局的用水限制时启动浇水计划。在城市范围内，物联网可以用于管理供水设备和报告状态（例如，打开或关闭、水库水位、输出和输入速度对比）。根据各种流量输入和输出分析数据，可以远程和实时地自动打开和关闭闸门或泵。可以通过测量设备的振动，以检测和预测潜在的设备故障。在设备发生故障之前，可以提前派遣维修小组。这些效率收益将直接转化为经营收益。

■ **道路收费：**当车辆进入繁忙的城区时，城市可以通过实施自动支付来创造180亿美元的新收入，同时改善整体交通状况。实时交通状况数据是非常有价值 and 可操作的信息，也可以用来主动地改变公共交通服务或私人用户的路线。

谁受益？

通过建立新的和更有意义的联系，世界各国政府和其他公共部门机构可以受益，并最终为公民创造可量化的利益。

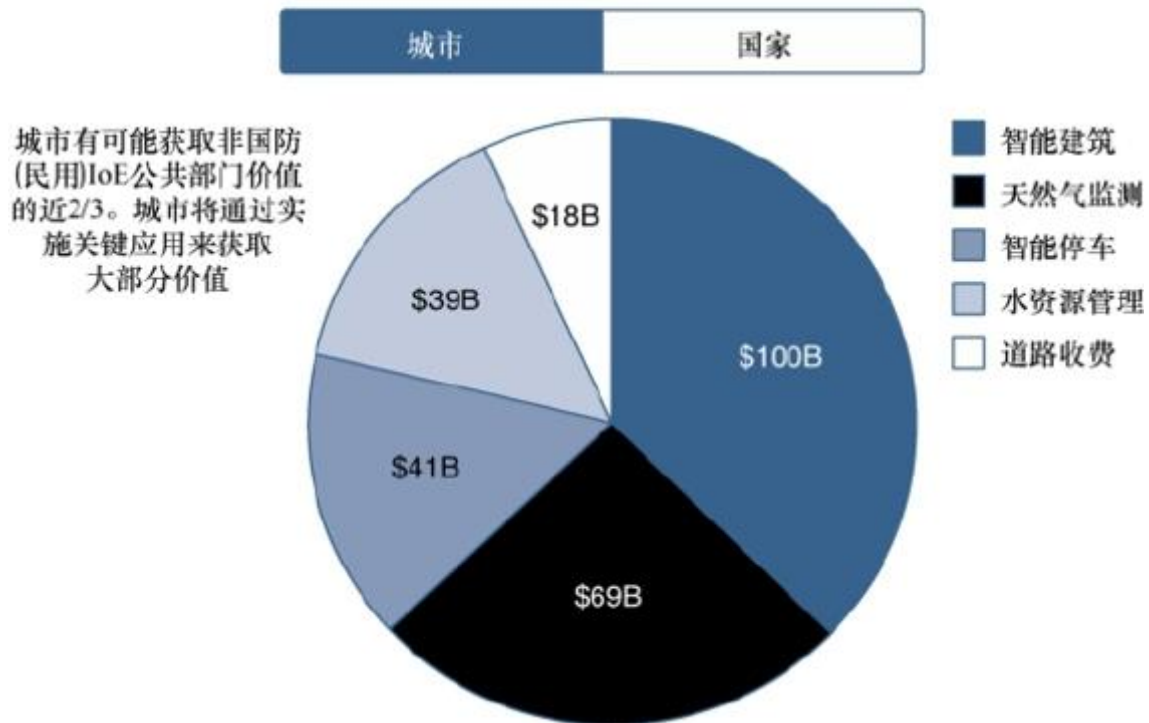


图12-1 智慧城市的关键用例

为了最大化能源和环境投资的投资回报，智慧城市可以采用水管管理、智能电网、废物管理、颗粒物监测和气体监测的策略。

智能城市可以利用这些技术进步来提高宜居指数，这有助于在竞争日益激烈的劳动力市场中吸引和留住人才。就业机会和人才数量的增长影响着国外投资的数量以及有多少顶级公司来一个城市落户，这进而导致更大的经济影响和提高未来投资的潜力。

12.1.2 全局和局部战略

在当今的传统基础设施中实施智能解决方案的主要障碍是城市运营、融资、监管和规划的复杂性。城市在试图升级基础设施以满足市民日益增长的需求时，往往一次只对一个问题进行投资，而且是独立

进行的。即使是使用物联网技术的城市，也会将城市资产和服务管理划分为多个隔离区域，这些区域通常无法相互通信或相互依赖。

独立投资模型存在以下问题：

- 隔离基础设施和IT资源；
- 不共享情报和信息，如视频和传感器数据；
- 投资和工作会造成浪费和重复；
- 难以扩展基础设施管理。

这种支离破碎的方法不具有可扩展性、高效性或经济可行性，并且无法从数据和服务的跨功能共享中获益。例如，在传统的城市基础设施中，停车、照明和交通部门在管理上都是独立运行的，它们各自的预算用于升级各自的基础设施。这导致了在相同基础设施上的重复投资，且只针对特定部门的疏忽定制了一些小细节。这是一种非常低效的资金管理方式，浪费了本可以造福社会的公共资源。然而，将不同的物联网系统与不同的供应商和数据协议集成与扩展会带来挑战。

城市需要从一个可以跨供应商、技术和数据类型扩展系统的解决方案开始，并且它们应该通过一个通用的解决方案来处理基础设施投资问题。可以将其与公路系统进行比较：城市没有针对汽车、卡车和紧急车辆建设不同的道路系统，因为使用统一的道路网络更有效率。这种思想可以应用于网络上的数据流：多个网络的效率低于单个统一网络。一个城市需要一个开放的物联网解决方案，允许所有公共服务（垃圾、停车、污染等）使用一个公共网络，并可能交换数据进行交叉优化。

城市问题通常是大规模的。它们需要实时收集大量不同的数据集。例如，要管理城市中的交通流和拥堵，就需要实时了解交通模式。这意味着必须实时收集和分析来自交通传感器、交通摄像机、停车传感器等的的数据，以便围绕信号定时、重新规划路线等优化决策。

所有这些需求都带来了技术挑战，包括以下方面。

■ 如何收集数据？包括硬件端点和软件在内的各种数据来源是什么？

■ 如何确保在不增加成本的情况下维护任何数据收集设备（如传感器）？

■ 在哪里分析数据？将哪些数据发送至云端，以及在本地分析哪些数据？

■ 哪种网络连接最适合收集每种类型的数据？

■ 需要什么样的电源可用性和其他基础设施，比如存储？

■ 如何聚合来自不同来源的数据以创建统一的视图？

■ 如何发布数据并使其可供应用程序使用？

■ 如何在智慧城市专业人员（例如交通指挥员、停车执法人员、街道照明操作员等）的逻辑决策点上提供最终分析？

■ 如何向城市规划者提供长期分析？

每个智能城市都需要一个定制的、结构化的计算模型，该模型允许对数据进行分布式处理，具有一定的弹性、规模、速度和可移动性，使得生成的数据在经过网络处理后得到价值，并能高效有效地交付这一价值。

在这种情况下，云计算和雾计算的结合是有意义的（第2章介绍了云计算与雾计算的更多架构细节）。需要在本地处理的数据位于网络的边缘。例如，关于可用停车位的本地和实时信息仅在本地可用。有关交通的指标也可以在本地处理，以调节和同步交通信号灯，或使公交车辆在交通拥堵的情况下改道行驶。相比之下，关于峰值时间和结构的全局统计和分析可以发送到云端，在整个城市的范围内进行处

理。这使城市规划者能够更好地组织城市中各种活动中心的发展，并计划增加公共交通的可用性、收集废物的轮换班次等。

12.2 智慧城市物联网架构

智慧城市物联网基础设施是一个四层架构，如图12-2所示。数据从街道层的设备流向城市网络层，并连接到数据中心层，在那里数据被聚合、规范化和虚拟化。数据中心层向服务层提供信息，服务层由向城市提供服务的应用程序组成。

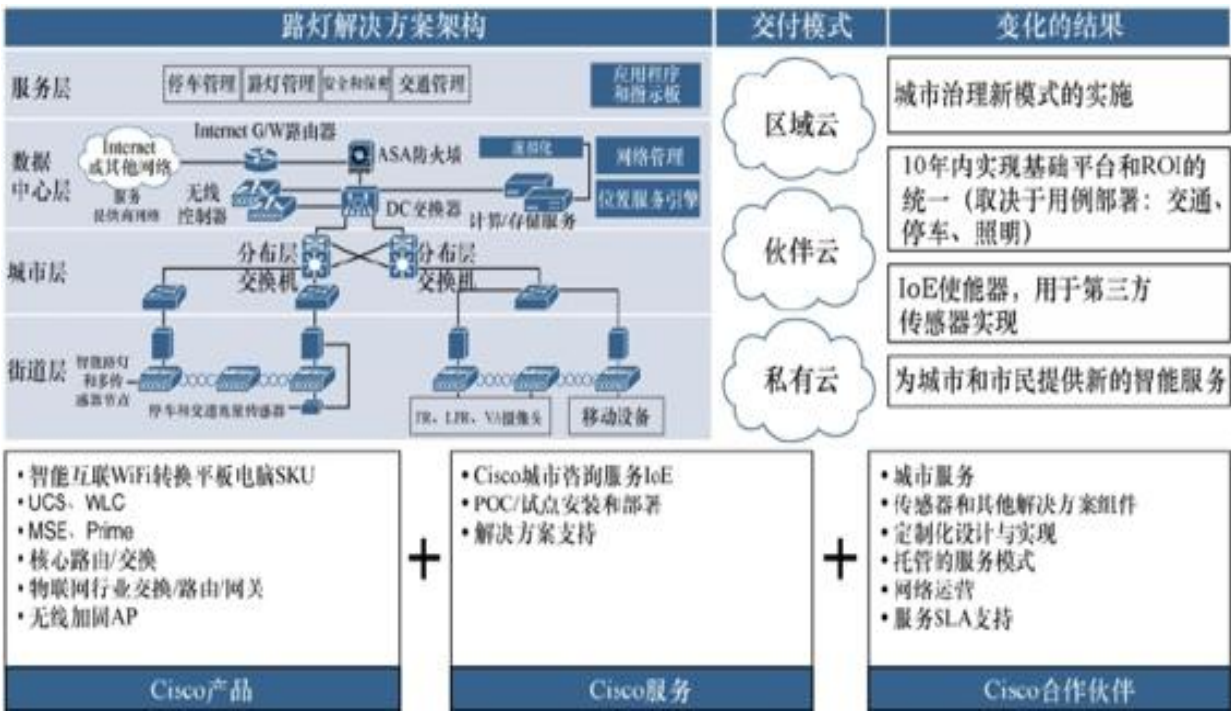


图12-2 智慧城市分层架构

在智慧城市中，多种服务可能会将物联网解决方案用于许多不同的目的。这些服务可能使用不同的物联网解决方案，使用不同的协议和不同的应用程序语言。因此，从传感器到应用程序的数据流涉及将其转换为规范化语言的过程，该过程可以通过API公开，以供其他服务应用程序使用。这种转换确保云端的所有设备使用同一种语言。这种通用语言简化了通信和数据管理，并允许解决方案相互交互。利用这

种交互，智能城市可以开发跨服务的新解决方案，而不需要进一步的基础设施，并且可以使系统适应未来的需求。有了标准化的语言和开放的API，城市可以投资于新的解决方案，因为它们知道新的解决方案很容易与现有的解决方案交互。相比之下，封闭的格式将限制交换以及利用一部分解决方案来改进另一种解决方案的能力。

下文将讨论针对特定应用选择传感器的各种注意事项，并提供技术网络需求的示例，以支持传感器并通过信息和通信技术（ICT）连接来驱动实时解决方案。

12.2.1 街道层

街道层由设备和传感器组成，这些设备和传感器收集数据并根据整个解决方案中的指令采取行动，以及整合和收集数据所需的网络组件。

传感器是一个数据源，用于生成理解物理世界所需的数据。传感器设备能够探测和测量物理世界中的事件。ICT连接解决方案依赖于传感器来收集周围世界的的数据，以便对其进行分析并用于城市的用例操作（参见第3章）。

多种传感器用于各种智能城市用例的街道层。以下是一个简短的清单。

- 当一辆汽车或一辆卡车等重金属物体靠近停车场（或停在其上）时，磁性传感器可以通过分析周围磁场的变化来检测停车事件。

- 照明控制器可以根据时间和环境条件的组合对光线进行调暗和变亮。

- 结合视频分析的摄像机可以检测各种交通和安全用例中的车辆、人脸和交通状况。

■ 空气质量传感器可以检测和测量气体和颗粒物的浓度，从而对特定地区的污染提供超局部的视角。

■ 设备计数器对该区域内的设备数量进行了估算，从而大致了解在街道、公共停车场移动或停放的车辆数量、人行道上的行人数量，甚至是公园或公共纪念碑上的鸟类数量，鸟数量的控制在城市中已经成为一个问题。

对于要收集的每种类型的数据，都有各种各样的解决方案和可能的方法。传感器技术的选择取决于问题的确切性质、与之相应的准确性和成本的权衡，以及物理环境造成的任何安装限制。另一个需要考虑的问题是，需要与同一物理空间中的其他物联网系统进行交互。例如，停车位可用性传感器可能是用户通过应用程序可以使用的封闭系统的一部分，或者它们可能必须通过开放API与其他系统（如拖车公司、公共执法机构、停车计时器等）进行交互。整体解决方案使数据是开放的和集成的，并通过单一和开放的平台将不同的系统整合在一起。

选择传感装置时要考虑的一个关键方面是它的终身维护成本。一些传感器安装在城市基础设施上，如电线杆。这些传感器可以从其安装位置的电力（可能还有网络连接）中受益。但是，其他传感器可能安装在地面或其他无法到达的地方。一旦安装好，为了处理一个问题而将它们取出来的成本是非常高的。在安装时，将电源线连接到传感器位置通常也是非常昂贵的。因此，这类传感器通常是由电池供电，并且是节能的，因此它们有很长的寿命，而且它们是加固的，以避免维护成本。

为智能城市选择合适的技术时要考虑的另一个关键方面是边缘分析。许多传感器及其数据必须通过网络以一种安全地处理数据的方式进行管理，这种方式的延迟最小，而且通常是实时的。为了只发送相关的数据，区分不同事件是智能城市设计中大数据输入的关键组成部分。例如，一个车辆计数传感器不需要为检测到的每辆车发送更新；它可能每分钟只发送一个累计计数。同样，污染传感器可以随时处理化学传感信息，但仅在一定时间间隔发送状态报告。为了最大化处理

速度和最小化服务器需求，通过云服务器的数据量必须是基于事件的（参见第2章）。

事件驱动系统允许城市基础设施具有前后关联的智能，因此只有目标事件才能触发数据传输到云端。这种灵活性允许基础设施监控大量的系统，而不会因状态更新消息不正常使网络超载。边缘处理分析为云分配了计算和存储需求，从而最大化地提高了数据传输速度，并将服务器需求和成本降至最低。

最后，对于传感器特性而言，存储是一个关键的考虑因素，这取决于数据必须存档的方法、位置和时间长度。这根据每个国家的法律要求以及用例而有所不同；将视频存储数周与使用一组基于事件的触发器之间的区别非常明显，这对设备有限的物理容量中可能包含的分析有很大的影响。此外，考虑到城市部署的规模和与长期规划相关的需求，存储需求可能比传统部署更高，而事件驱动方法有助于避免对支持网络造成压力。城市必须找出解决存储需求的最佳做法，并确定需要多长时间来保存数据，并根据这些标准适当地选择设备。

数据收集和存储对隐私也有重要影响。一个用来计数实体的视频传感器可以读取汽车登记号码或记录行人的面部特征。法律和隐私方面的考虑在选择系统时起着重要的作用。出于公共安全的考虑，可能会要求记录这类数据。另一方面，可能有一个有条件的规定，即设备只能在无法单独识别的情况下计数（隐私是一个要求）。在最后一种情况下，由于传感器的图像分辨率有限或无法识别超出其一般形状或轮廓之外的物体，因此可以专门选择传感器。通信系统也可以被设计成禁止超出设备计数的传输（例如，低带宽）。在设计时，必须清楚地了解和界定隐私要求的范围。

无论选择哪种类型的系统，传感器数据都由物联网系统进行传输和处理。虽然物联网系统使用云中的通用API和规范化语言，但它们可能使用不同的网络协议。为了物理地连接来自如此多设备的数据流，关键是要有一个网络基础设施，它可以使用在街道级别运行的各种通信协议与设备进行通信。蜂窝技术是信息通信技术的核心，因为城市通常允许简单和密集的蜂窝连接。然而也有其他技术进行连接。

注释：第2章更详细地讨论了物联网的总体架构考虑因素。第4章对智慧城市中遇到的不同类型的范围和应用可能使用的各种协议进行了深入研究。本章的最后一部分还提供了有针对性的示例和具体的智慧城市用例。

在所有情况下，一个智慧城市的网络必须加固以适应户外条件，必须能够承受恶劣的天气条件。为了支持智能城市部署的ICT解决方案，网络必须满足户外电子设备的标准，并提供故障维护以简化问题隔离。

网络规划必须考虑的另一个问题是智慧城市网络所需的不可知论的程度。LoRaWAN正在成为跨多个垂直领域的智慧城市传感器的主要协议。LoRaWAN很好地适应了城市环境所需的范围类型以及大多数智慧城市传感器所需的数据交换类型（第4章提供了关于LoRaWAN的详细信息）。然而，多个用例意味着可以部署多个协议。不同领域和来自不同技术供应商的异构传感器阵列利用不同的通信协议来实现某些优点和特性。许多传感器都有自带与特定硬件兼容的网关。然而，网络需要足够广泛且不受供应商限制，以使这些网关能够与更大的网络和终端节点进行通信，这些终端节点可以桥接低功耗协议（如ZigBee到IP），并满足主机的其他通信需求。所有这些协议和系统必须协同工作，并通过相同的网络基础设施进行传输。

智慧城市网络还必须实现本地分析和闭环决策，这也意味着终端节点的计算能力需要高于典型的部署。网络的规模和复杂性随着智慧城市部署的规模以及城市使用的传感器的数量和类型而增长。物联网网络基础设施是城市融合智能解决方案的支柱；设备连接是实现数字化公共服务的关键。

12.2.2 城市层

在位于街道层之上的城市层，必须部署网络路由器和交换机，以匹配需要传输的城市数据的大小。这一层将传感器和终端节点网络收集的所有数据聚合到一个传输网络中。

城市层可能是边缘设备和数据中心或互联网之间的简单传输层。然而，城市层的一个关键考虑是，它需要传输多种类型的协议，用于多种类型的物联网应用。一些应用程序对延迟和抖动很敏感，而另一些应用程序则需要采用确定性的方法来传递帧。丢失的数据包可能会产生警报或导致无效的状态报告。因此，城市层必须围绕弹性构建，以确保来自传感器或网关的数据包总是能够成功地转发到前端站。图12-3显示了实现这一目标的常用方法。

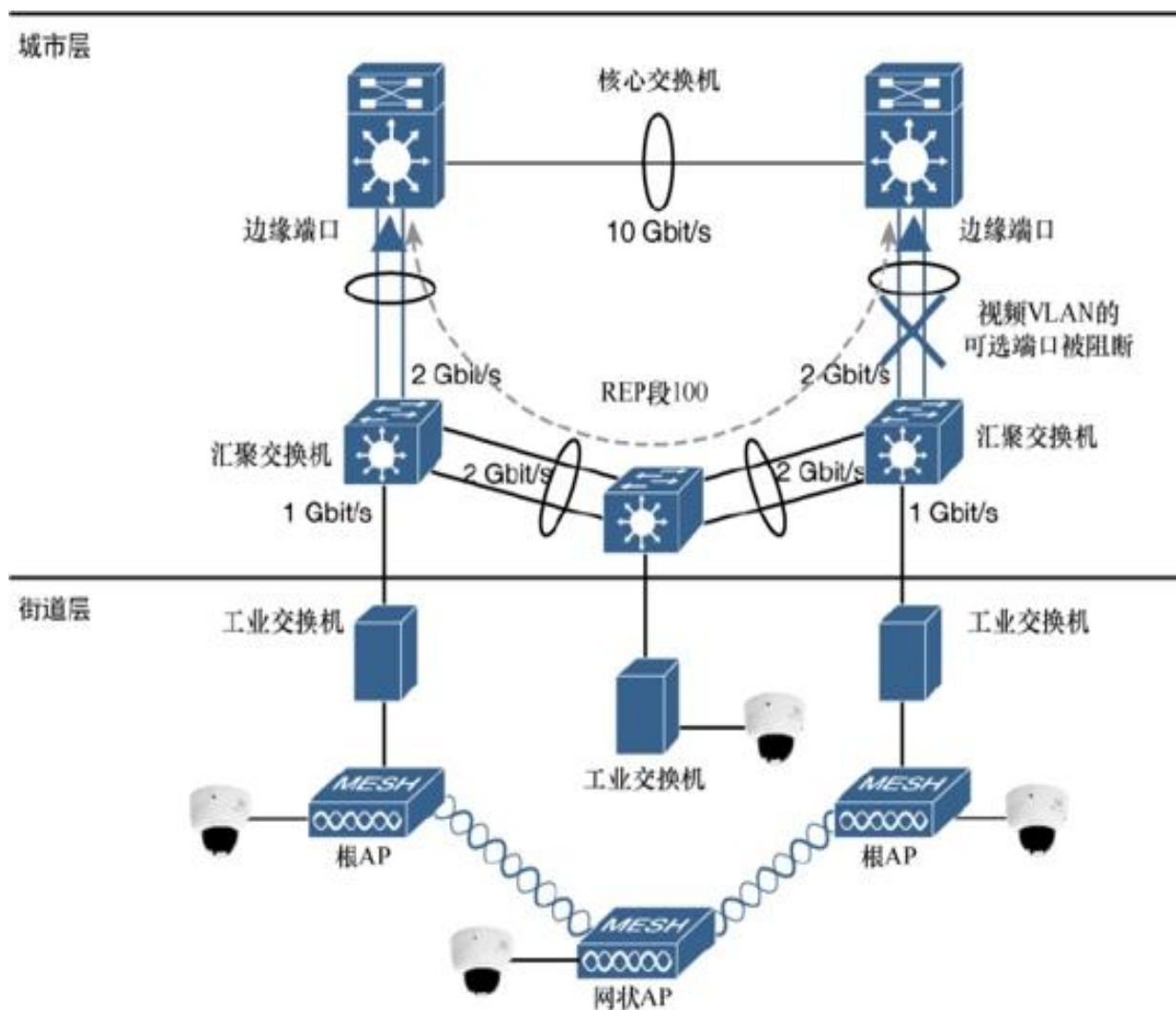


图12-3 街道层弹性

在此模型中，从任何汇聚交换机到数据中心层至少存在两条路径。一种用于确保这种弹性的通用协议是弹性以太网协议（REP，在第9章中进行了详细讨论）。

12.2.3 数据中心层

最后，从传感器收集的数据被发送到数据中心，在那里可以进行处理和关联。在这种数据处理的基础上，可以得到有意义的信息和趋势，并提供相应的信息。例如，数据中心的应用程序可以提供城市交通的全局视图，并帮助主管部门决定是否需要更多或更少的公共交通工具。同时，可以生成自动响应。例如，可以处理相同的交通信息，自动调节和协调整个城市范围内的路灯持续时间，以限制交通拥堵。

创建任何全面的智能服务解决方案的关键技术是云。使用云基础设施，数据不会存储在城市当局直接或间接拥有的数据中心。相反，数据存储在与通过互联网访问的租用逻辑容器中。因为容器可以根据需要扩展或缩小，所以存储大小和计算能力是灵活的，可以适应不断变化的需求或预算条件。此外，多个承包商可以同时存储和处理数据，而不需要考虑专有空间。这种接近性和灵活性也促进了智能系统之间的信息交换，并允许部署新的应用程序，利用来自多个物联网系统的信息。

云模型是实现存储、虚拟化、适应性和分析技术的主要方式，而城市需要借助这些技术在智慧城市中实现信息的技术融合和协同作用。传统的城市网络无法满足智慧城市的实时数据需求；它们受到物理限制的阻碍。云支持将数据分析带到具有大型和可扩展处理能力的服务器场。

图12-4显示了在城市智能解决方案中使用云的远景。云提供了一个可伸缩的、安全的、可靠的数据处理引擎，可以处理通过它传递的大量数据。

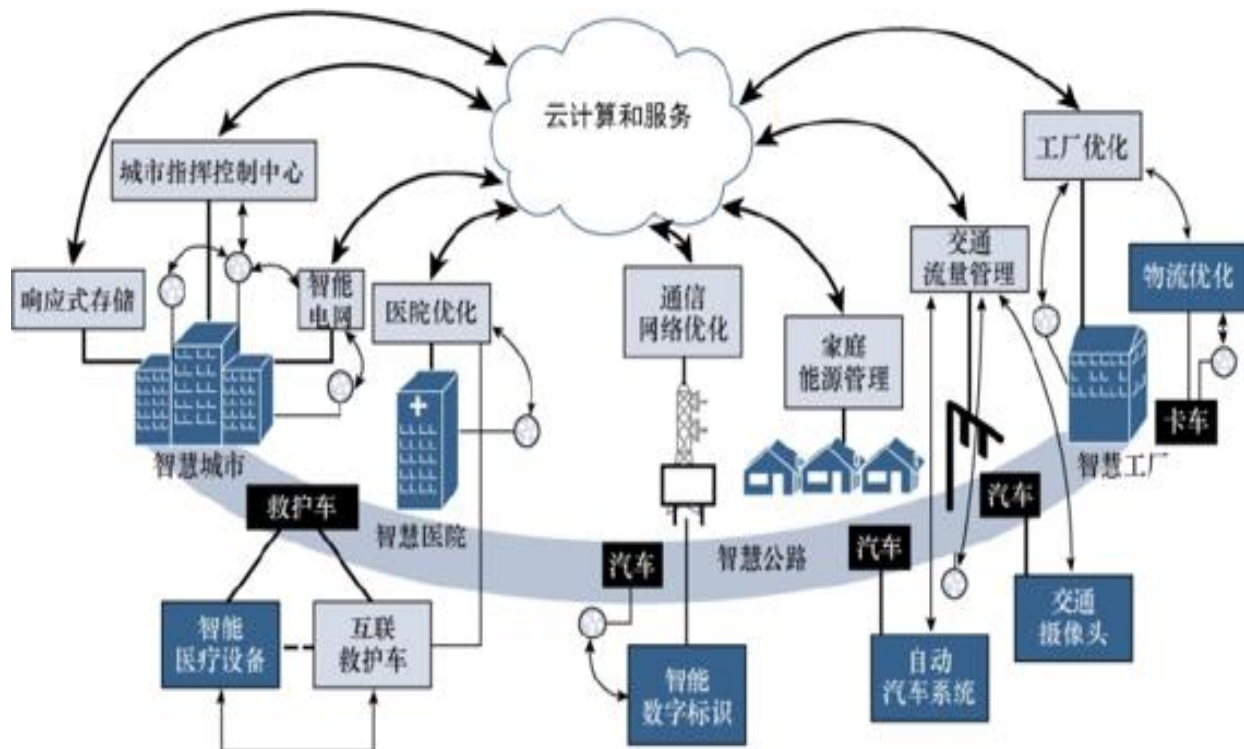


图12-4 云在智慧城市应用中的角色

智慧城市问题不仅需要高效利用基础设施（利用云计算实现），还需要新的数据处理和管理模型。例如，云服务允许创建周期性投资回报的软件即服务（SaaS）模型。通过图12-4所示的云计算方法，智慧城市还可以利用基于运营费用的消费模型来克服任何财务障碍，从而为其最关键的问题提供解决方案。关键数据，如空调（湿度、温度、污染）水平监测，可以进行初步处理。然后，随着物联网效率的提高，在云应用中可以实现更丰富的数据处理。例如，湿度可以用来调节路灯的颜色和亮度。在城市预算紧张时，数据处理可以缩减到基本服务。

在刚刚讨论的分层架构中，可以通过云服务启用平台；该平台将通过驱动服务的应用程序所使用的API来聚合、规范和公开城市数据。

然而，并不是所有的数据都在中央云数据中心处理。大多数实时和本地重要数据可以在网络边缘利用雾架构直接处理，在这个模型中，处理和分析功能在网关运行的街道层的顶层可用。通过这种方式，来自多个传感器（同一类型或多个不同类型）的数据可以在边缘

进行本地处理。决策在本地很重要，可以在不与云进行不必要交互的情况下做出。本地处理数据的结果随后被发送到云，以提供更全局的视角。

12.2.4 服务层

归根结底，ICT连通性的真正价值来自于测量数据可以为城市内的不同用户提供的服务。智慧城市应用程序可以为各种用户类型（包括城市运营商、市民和执法部门）提供价值和可见性。收集到的数据应该根据每个数据使用者的特定需求、特定的用户体验需求和个别用例进行可视化。例如，显示停车位是否被占用的数据可以驱动市民使用停车位应用程序、加强执法人员对公共停车位的状态（使用和支付）的了解，同时帮助从城市运营商的角度去审视特定时间的停车问题。相同的数据具有不同的粒度和规模，可以为3个不同的用户执行3个不同的功能。在同样的路线上，交通信息可以被单独的汽车司机用来寻找最不拥挤的路线。公共交通工具使用者可以利用相同的信息来估计出行时间。公共交通系统，如公交车，可以在已知的拥堵点附近改变路线。地铁列车的数量可以动态增加，以应对交通拥堵加剧的状况。在道路非常拥堵的日子里，预计成千上万甚至数百万通勤者会选择乘坐公共交通工具，而不是私家车。同样，不同类型的用户根据其特定的用例以不同的方式使用相同类型的数据（第13章提供了更多关于这类交通信息处理的示例和细节）。

通过本节描述的架构，智慧城市可以合并任意数量的应用程序，这些应用程序可以使用来自云托管平台或雾应用程序的规范化数据。因为整个体系结构都使用兼容的API，所以这些应用程序甚至可以带来跨域的好处。作为这种跨域好处的一个示例，在已知的交通拥挤点，可以从可用性地图上删除停车位，可以适当地改变废弃物管理路线，可以增加街道照明。因为存在水平级别的聚合和规范化，这些类型的跨域数据关联可以由系统在分层体系结构中开发和改进。

该体系结构为应用程序开发人员和传感器供应商提供了必要的工具，通过开放API、软件开发工具包（SDK）、城市信息模型等来创新

和发明新的社区体验，以开发符合城市标准的应用程序，从而驱动高价值的智慧城市服务。这使得量身定制的智慧城市解决方案也可以由市民自己为他们的城市开发。

12.2.5 本地与云端的对比

根据安全或法律政策，不同的城市和地区有不同的数据托管需求。在开发ICT连接解决方案时，一个关键的考虑因素是一个城市是否对数据的存放位置有要求。数据可以托管在本地或云端。雾架构提供了一个中间层。雾处理产生的数据可以发送到云端或本地操作的数据中心（本地）。内部环境包括传统网络及其所有限制，而如果不采取适当措施保护公民数据，云托管则包含大量的安全风险。当数据被发送到云端时，数据主权法律可能会限制数据实际存储的物理位置。

理想情况下，一个利用ICT连接的智慧城市将使用云计算架构，但如果这是不可能的，这个城市需要在城市层的网络组件（例如，交换机、路由器）上投入更多，并且仍然可能无法在其设计中实现相同的跨域价值主张和可扩展性。

一个城市可以从传统的网络设计和内部托管开始，目的是保护数据，但是它可能很快就会得出结论：本地数据中心的能力落后于云托管数据管理为城市提供的能力。在这种情况下，可以实现一种混合的托管方式，其中一些数据可以迁移到云端，而其他数据则保留在本地。例如，来自单个街道摄像机的图像可能存储在本地，而关于行人或车辆流量的分析和相关元数据可能托管在云端。

12.3 智慧城市安全架构

数据安全是大多数智慧城市及其居民担忧的一个严重问题。大量的敏感信息在一个分层的实时的架构中被共享，城市有责任保护其公民数据不被未经授权地访问、收集和篡改。

一般来说，当城市本身（而非私人实体）拥有公共或与城市相关的数据时，市民对数据安全的感觉更好。如何利用这些数据取决于城市和管理城市的官员。当私人实体拥有与城市相关的数据时，所有权的范围最初可能非常明确。但是，私有实体策略中的后期考虑或更改可能会改变数据的使用方式。这样一来，市政当局或市民可能更难以反对这一新方向，因为他们在私营实体的决策过程中没有任何利害关系。此外，私人实体可能有经济利益和政治动机，他们可能没有市政府通常拥有或通过公共审查和投票获得的安全标准或责任机制。例如，假设一个私人承包商负责收集和管理停车传感器数据。提高这类数据的盈利能力的一个可能方法是将其卖给保险公司，保险公司希望向在街上（而不是在有遮盖和安全的车库里）停车的车主收取额外的保费。当城市拥有这些数据并且市民有权利投票反对这种用途时，这种偏离最初规定的情况就不太可能发生。

传统上，网络部署使用隔离方式，并不总是遵循开放安全标准。机构可能在公共云上运行应用程序和服务，实施有限的安全保护措施，并且在没有适当安全的情况下使用基于云的协作工具。因此，需要一个集中式的、基于云的、基于合规性的安全机制来满足服务提供商和最终用户的需求。安全性显然是一个端到端的问题，从数据收集的位置和方式开始，并贯穿整个数据处理生命周期。

智慧城市的安全架构必须利用安全协议来加强架构的每一层，保护城市数据。图 12-5显示了一个参考架构，其中突出显示了特定的安全元素。安全协议应该对各个组件进行身份验证，并在整个过程中保护数据传输。例如，劫持交通传感器向控制信号灯的系統发送错误的交通数据可能会导致严重的拥堵问题。对违规者来说，好处可能是可以在旅行时畅通无阻，但总体结果通常是危险的，会危害城市安全。安全架构应该能够随着最新的技术而发展变化，并与区域指导方针（例如，城市细则、县或区域安全法规）相结合。网络合作伙伴也可能有自己的合规性标准、安全策略和治理需求，需要添加到本地城市需求中。

- 10 Day PowerPC - 10 Day
- 10 Day Power
- 1 Day Power
- 10 Day with Copper

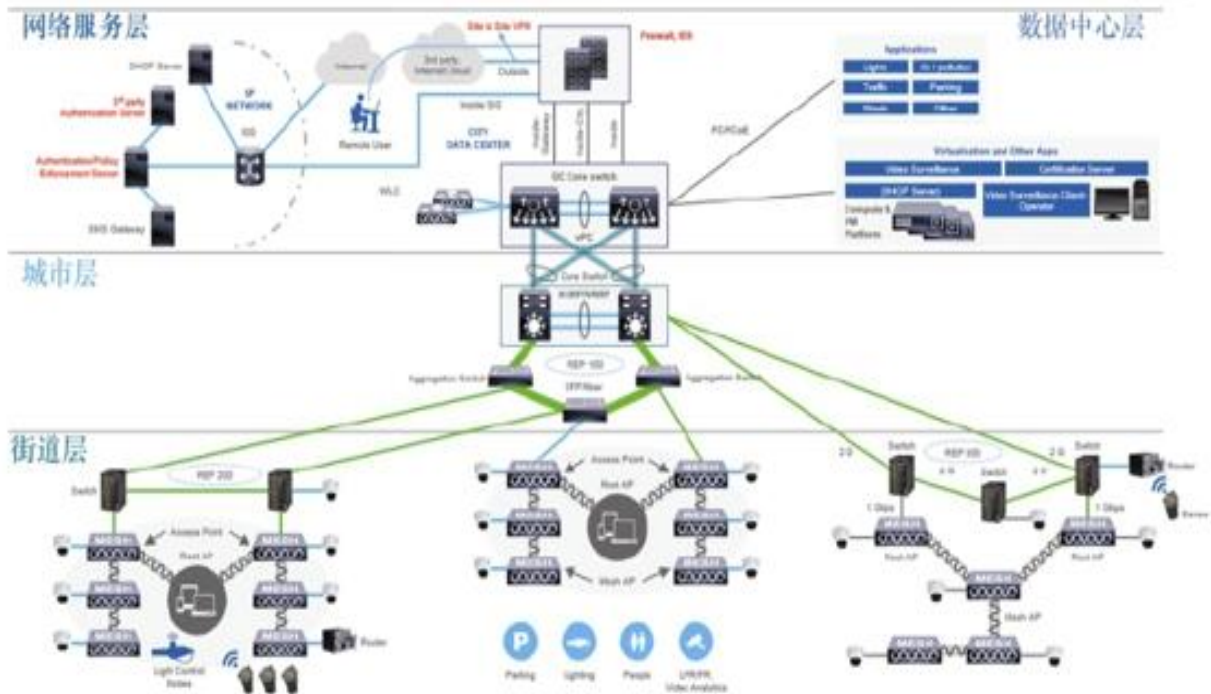


图12-5 智慧城市互联互通参考架构

从街道级别开始，每一个传感器应该有自己的安全协议。一些行业标准的安全功能包括设备/传感器的识别和授权；设备/传感器数据加密；可信平台模块，当传感器被物理处理时，允许自毁；用户ID身份验证和授权。传感器识别和授权通常需要在组织级别预先安装工厂X.509证书和公钥基础设施（PKI），其中通过零接触部署过程安装新证书。这种额外的处理可能会降低部署速度，但可以确保交换的安全性。

另一个考虑因素可能是传感器能够收集和处理的类型。例如，路边的汽车计数器可能包括一个蓝牙传感器，可以识别唯一的司机或行人。安全考虑应该决定是否收集这些信息。如果收集该数据，则应该决定是否使用在线处理过程（在该过程中，信息用于分析，但个人识别数据未被存储，因此立即忘记）或更传统的分析流程（临时存储数据，要么是因为该算法需要避免重复，要么是因为轨迹确定是数据处理的一部分）。数据在静止和移动时都应该受到保护，但在存储数据时，需要设置额外的安全措施，以确保信息不会被篡改、滥用

或窃取。无论数据存储网关（雾）或云中的位置如何，保护数据安全都是正确的。

城市层在街道层和数据中心层之间传输数据，它充当网络层。以下是用于网络层安全的常见行业元素。

■ **防火墙：**防火墙位于边缘，应具备IPSec和VPN功能，并包含基于用户和角色的访问控制。它还应该与架构集成，以便城市运营商能够远程访问城市数据中心。

■ **VLAN：**VLAN提供端到端的数据传输分段，进一步保护数据不受恶意干扰。每个服务/域都有一个专用的VLAN用于数据传输。

■ **加密：**保护从传感器到应用程序的通信是避免数据篡改和窃听的常见需求。在大多数情况下，加密从传感器级别开始。在某些情况下，传感器到网关的链路使用一种加密方式，而网关到应用程序的链路使用另一种加密方式（例如VPN）。

每个已部署的物联网解决方案可能需要多个特定元素（如交换机到交换机加密）来提高系统的可靠性。在数据中心层，拥有安全的虚拟私有云是一个常见的需求。围绕应用程序、客户端、主机和共享资源创建动态边界会进一步混淆窥探者的数据。集成最新的技术框架，如用于设备认证和基于身份进行访问的相互传输层安全（mTLS）或OAuth 2.0，是确保城市解决方案完整性的关键。

注意：mTLS是双向的，这意味着在身份验证阶段同时确定客户端和服务端身份。这种双向性可以防止未经授权的客户端访问网络，并且允许每一方充当客户端或服务端，从而增加了系统的灵活性。例如，传感器可以是连接到云应用程序的客户端，也可以是网关或其他传感器的服务端。

OAuth是一个授权框架，它允许应用程序使用HTTP获得对目标服务的有限且受控的访问。

在分层架构中，遵循和优先考虑安全逻辑，可以减少严重的网络安全破坏或城市数据隐私侵犯的机会。

12.4 智慧城市用例示例

智慧城市可以通过多种方式提高效率，改善市民生活。下面将介绍在智慧城市中实施物联网的一些常用应用：互联路灯、智能停车、智能交通控制和互联环境。虽然这些解决方案中的每一个部分都可以用整个章节描述，但是为了简单起见，我们将这些讨论与本章中讨论的概念架构相关联。其他章节涵盖了公共安全（第15章）和交通（第13章），这些主题也适用于智慧城市。此外，建议读者参考本书第2部分的其余章节，以获得更多关于各个层的智能对象的深入信息，以及支持这些用例所需的一般架构和协议。第3部分的其他章节也提供了关于在城市层面实施的应用程序的有价值的信息，比如公用事业（第11章）。

12.4.1 互联路灯

根据纽约州环境保护部的数据显示，在所有的城市公用事业中，街道照明是市政公用事业支出中最大的开支之一，占总额的40%。鉴于路灯数量众多且广泛分布在各处，路灯的维护是一项运营挑战。

1. 互联路灯解决方案

城市通常寻找解决方案来帮助减少照明费用，提高运营效率，同时尽量减少前期投资。安装智能路灯解决方案可以节省大量能源，还可以提供额外的服务。在这方面，发光二极管（LED）技术引领了传统路灯向智能路灯的转变。

■ LED比传统灯需要更少的能量来产生更多的光，而且它们有更长的寿命和更长的维护周期。

■ 一家领先的照明公司估计，完全转换到LED技术可以减少高达70%的个人照明费用。

■ LED非常适合于智能解决方案用例。例如，LED的颜色或光照强度可以根据现场要求进行调整（例如，在城市中心，LED有温暖的颜色和较低的亮度，在高速公路上有阳光般的清晰度，有与时间和天气相适应的强度和颜色）。

图12-6所示为电力价格上涨，而LED价格下降，但其单位销售额上升的情况。

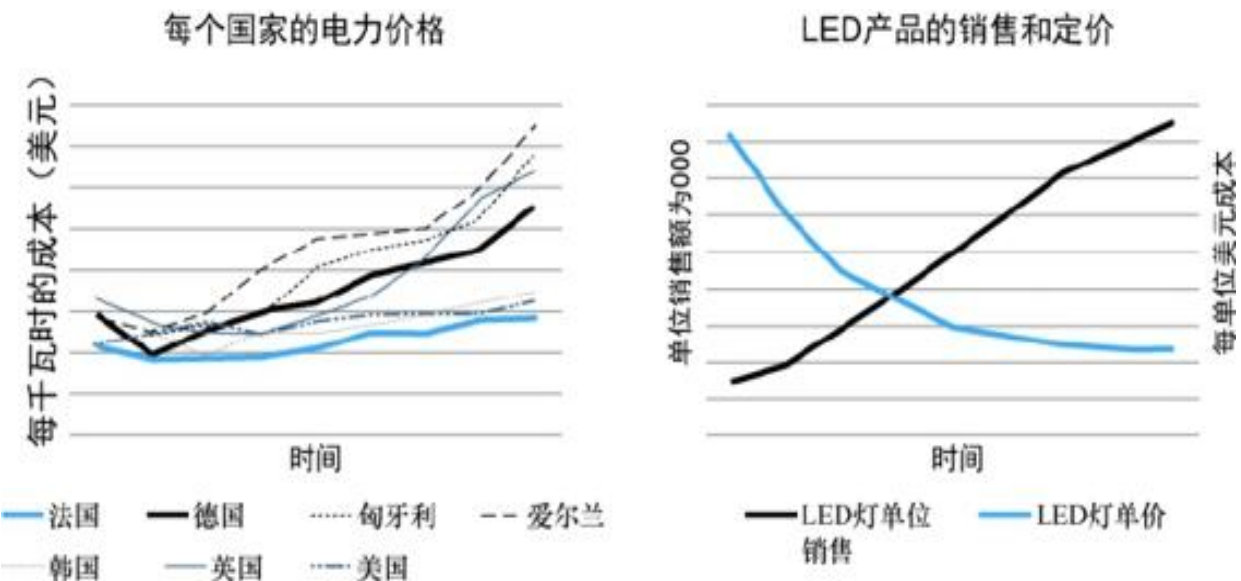


图12-6 电力成本与LED成本及销售

全球向LED的过渡是智慧城市开始向ICT连接解决方案迈进的关键因素。随着电费的上涨和LED灯价格的下降，这种硬件的转变可以为一个完整的智能照明解决方案打开大门。

一个全面的智能照明解决方案能够实现一个融合和网络化的系统，该系统集成了基于LED的灯具和动态照明控制，由本章前面讨论的分层智能城市架构提供支持，该架构易于扩展，可以支持其他用例和解决方案，从而使城市受益。

2. 路灯架构

互联路灯使用灯光管理应用程序，通过连接到智能城市的基础设施来远程管理路灯。这个应用程序连接到LED灯，监控其管理和维护，并允许查看每个灯的运行状态。在大多数情况下，传感器网关充当应用程序和路灯（灯光控制节点）之间的中间系统。网关将来自应用程序的指令中继到路灯并存储本地灯光事件以供应用程序使用。控制器和LED灯使用云连接到智能城市的基础设施，如图12-7所示。

人工或自动操作员可以使用云应用程序来执行灯光的自动调度，甚至根据需要使光传感器执行自动调暗或调亮功能。还可根据环境条件、天气、一年中的时间、一天中的时间、城市中的位置等因素影响光的强度水平和颜色。

照明节点在行业中差异很大，特别是在它们使用的通信协议（例如，WiFi、cellular、ZigBee、802.15.4g [Wi-SUN]、LoRaWAN）、强度级别和车载传感器功能等方面。这些功能针对不同的环境和条件进行了优化；没有一个单独的照明节点能够理想地支持所有环境。例如，城市中心可能很容易部署WiFi（由于靠近以太网或互联网干线，覆盖范围约为100米，城市设施密度高，提供了大量中继和网关选项），而高速公路可能要求提供更大范围的解决方案，如cellular或LoRaWAN。许多解决方案利用有线连接，或者使用现有的城市电缆基础设施，或者在电力电缆旁边添加一条电缆。在布线不实际的情况下，无线技术可能会带来有趣的功能。例如，802.15.4g的控制器可以用来形成网状网络并扩展网络。这种扩展不仅可以用于连接其他的灯杆，还可以从邻近房屋的灯光控制节点连接智能电表。在所有情况下，图12-2所示的四层体系结构所提供的内置多功能确保了所有不同类型的技术都可以灵活地整合到解决方案中，以适应任何城市拓扑结构。

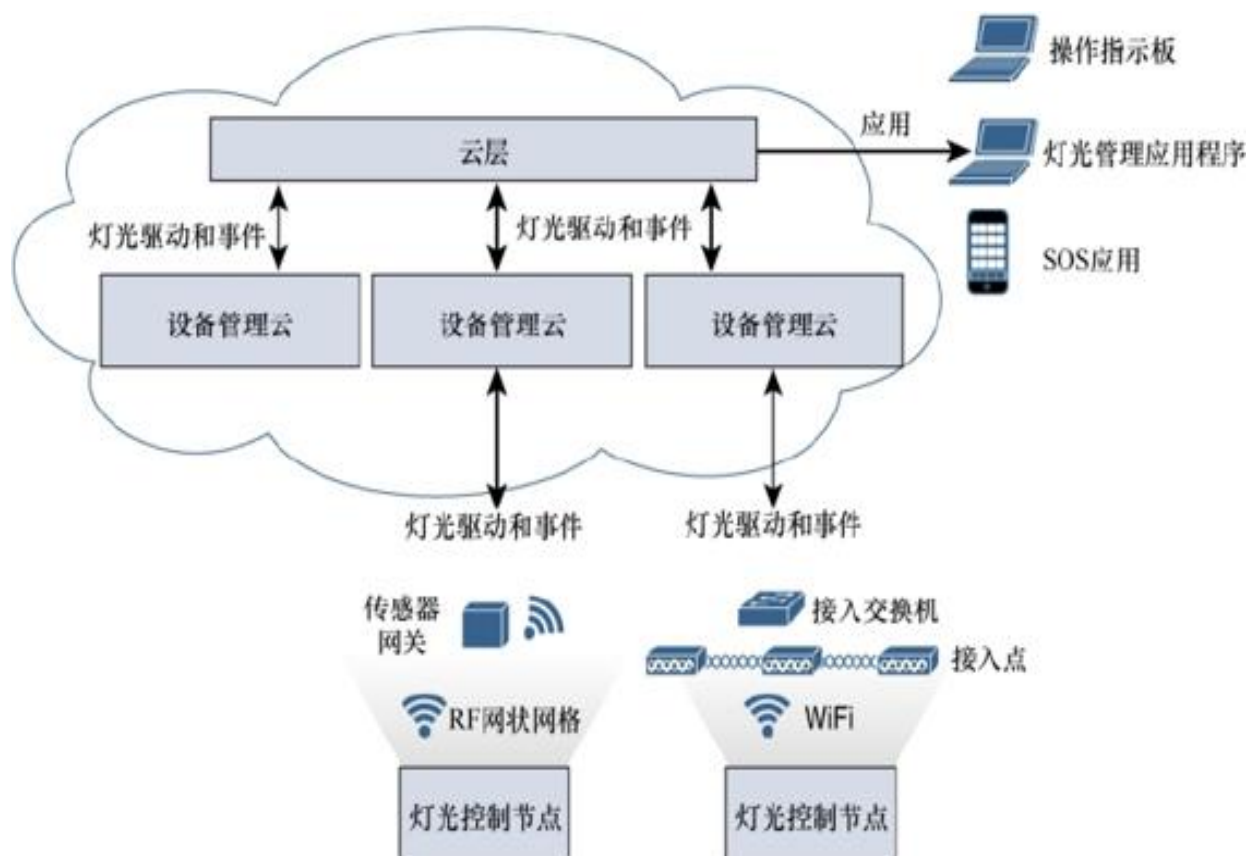


图12-7 互联路灯架构

路灯作为一种ICT连接解决方案，充分利用了现有的城市资产和现有的电源。使用ICT连接技术的资产不仅可以增加收入，还可以通过成为不同技术用于运营的资产来驱动ICT连接解决方案。例如，LED灯泡通常配备有基本传感器，可以检测光（驱动本地开/关和调光动作），还可以检测许多其他环境参数，如温度、运动、压力或湿度。在传感器上增加这些功能通常只会增加边际成本。最大的好处是路灯也可以成为当地的天气预报站。这些信息对当地居民和需要检测实时驾驶情况的都市交通系统都很有用。还可以添加监测功率、测量氧气和二氧化碳浓度、测量污染或颗粒物的数量、检测长波紫外线的水平（UVA）和短波紫外线B（UVB）辐射水平等功能，以提供额外的价值和服务（例如，污染监测、花粉警报、电网监控）。还可以嵌入更专业的功能，比如基本的音频或视频功能，以及过滤和分析功能，以实时检测交通拥堵或车祸。在这种情况下，随着使用量和带宽消耗的增加，网络连接技术越来越重要。效率是智慧城市的一个关键特征，包括互联路灯。例如，在没有检测到汽车的高速公路上，可以减少照明量。灯

光可以设定为特定的闪烁模式，以帮助警方快速定位特定的GPS位置。将物联网用于路灯可以提供大量有用的应用，因此，路灯通常被用作智慧城市部署的入门级物联网功能。市政当局通常将节约能源成本作为首要任务，并很快意识到，在已经部署的物联网路灯基础设施上增加传感器，可以为城市管理带来重大效益和优势。

3. 智能停车

停车是全球城市面临的普遍挑战。据城市规划研究人员称，在拥堵的市区交通中，多达30%的汽车在寻找停车位。无效的停车通道和管理使城市停车成为一场持续的斗争，并在许多方面影响城市。

4. 智能停车用例

司机寻找停车位时造成了以下后果，交通拥堵是其中之一。

- **造成污染：**大量额外的碳排放被释放到城市环境中，原因是汽车在本可以停车的地方到处寻找停车位。

- **造成司机的失望感：**在大多数城市，停车位不足会导致司机失去耐心，导致路怒、注意力不集中和其他压力因素。

- **增加交通事故：**寻找停车位的司机增加了街道的拥堵，进而导致更多的交通事故。收入损失是司机寻找停车位失败的另一个后果，它也有以下各种负面影响。

- **经济损失：**由于停车计价器执行不力以及违反停车、装载区规定，会造成经济损失。

- **停车场管理员工的工作效率受到影响：**员工们在大街上巡视，试图找出违章停车的人。

■ 可停车性影响收入：由于停车位短缺导致可停车性降低，当地商店和企业失去了顾客。当我们考虑如何应用技术来解决当今城市面临的一些最紧迫的问题时，停车是一个显然需要改进的领域，而且可以很容易进行量化。随着城市在数量、规模和复杂性上的不断增长，城市基础设施和服务的压力也越来越大。随着城市人口和密度的增加，上述问题变得更加紧迫。城市地区的停车困难影响了市民的生活质量，由于出行时间增加、压力、噪声、污染等原因，城市生活变得不那么理想。

解决城市中心交通问题的一个选择是重新利用密集的城市空间，创建额外的停车基础设施。然而，这种选择通常是具有挑战性的，主要是因为成本、财务和其他方面。城市往往可以通过优化现有停车位的使用效率来更好地满足市民的需求，而不是利用宝贵的城市地产来创造更多的停车位。这一方案通常能最快地缓解停车问题，同时最大限度地减少对新投资的需求，并限制对城市建筑的影响。

5. 智能停车构架

市场上有各种各样的停车传感器，它们采用不同的方法来检测停车位的占用情况。例如，地面磁传感器，它使用嵌入式传感器在停车位上创建一个磁场探测场；基于视频的传感器，用于检测基于视频计算的事件（车辆移动或存在）；感知车辆存在的雷达传感器（体积检测）。大多数安装在地面的传感器必须依靠电池供电，因为使用电力线通常太昂贵。这些传感器通常对变化做出反应，比如磁场的变化，触发传感器唤醒并发送事件报告。因为这些事件不是太频繁，电池可以持续很长时间。基于每个报告所消耗的能量，在一个典型的停车传感器的生命周期内可以报告600000条记录。在一个非常繁忙的停车位，每10分钟就有一辆车进进出出，电池续航时间可以达到10年。在高密度环境中（例如，室内停车场），每层有一个或多个网关可以使用ZigBee或WiFi等短程协议连接到停车传感器。然后，网关可以使用另一种协议（有线或无线）连接到控制站。在较宽阔的（例如室外）

环境中，较长范围的低功耗广域（LPWA）协议比较常见，如图12-8所示。



图12-8 互联的停车场架构

技术创新层出不穷，这使得整体的ICT连接架构更加重要。例如，新的检测技术依赖于检测来自车辆的无线电辐射（蓝牙和其他无线设备）。采用这些新技术意味着通信体系结构足够开放，可以满足这些新系统的需求（有关这种开放架构的详细信息，请参阅第2章）。以创新的方式结合这些技术也拓展了物联网系统提供服务的可能性；这当然适用于智能停车场。例如，传感器可以安装在残疾人停车位上。司机可以用一个应用程序登记他们的身体状况，以便于更容易找到这些地点。当用户停车时，传感器可以与司机的智能手机上的应用程序通信以验证其身体状况，并限制这些停车位的欺骗性使用。

不管使用什么技术，停车传感器通常都是事件驱动的对象。传感器检测事件并基于时间或分析对其进行识别。事件通过设备的通信协议传输到接入点或网关，网关通过城市层转发事件数据。网关将其发送到云或雾应用程序，在那里进行规范化。一个应用程序在操作员仪

表板或个人智能手机上显示停车事件，在那里可以采取操作。例如，司机可以预订附近的停车位，或者停车场操作员可以将其从目标位置的可用停车位列表中删除。此操作将触发数据发送回停车传感器，以便根据接收到的指令修改其可用状态。反之，传感器可以与附近的系统交互。例如，根据这些指示，停车位上方的灯可以变成红色、橙色或绿色，以显示空闲、已预订或已占用的停车位，从而方便司机搜索可用的停车位。同样地，停车传感器可以将状态发送到停车平台入口处的通用停车位计数器，以显示给定区域（如停车平台的特定楼层）中有多少停车位可用。这种通信可能是直接的，但通常通过网关、网络 and 应用程序进行，该应用程序通过API与其他系统通信。用户还可以访问来自云或基于雾的应用程序的数据，以查看特定城区或社区中可用的位置列表。智能数据也可以被嵌入，例如增加较远的停车位的折扣，或者在特定时间增加离场馆较近的停车位的成本（如体育赛事或音乐会）。

正如本章前面所述，智能停车场有3个应用程序必须通过聚合数据支持的用户：城市运营商、停车场管理员和市民。数据规范化的真正价值在于，所有停车数据，无论是技术还是供应商，在这些应用程序中都是可见的，以便支持不同用户的特定体验。以下是这3种用户的一些潜在需求。

■ 城市运营商：这些用户可能希望获得城市停车的高级地图，以保持对城市当前停车状况的看法。他们还需要关于历史停车数据模式的信息，以了解拥堵位置，以便能够有效地影响城市规划。

■ 停车执法人员：这些用户可能需要实时更新某个区域的停车变化情况，以便能够立即采取执法行动，例如向时间即将到期的市民发出罚单或警告。他们的重点是为城市创造收入，并通过大规模实施停车监控和执法来尽量减少浪费的时间（也就是说，不需要查看每一辆车的情况，因为只有小部分被检查的车辆实际上需要采取行动）。

■ 市民：这些用户可能想要一个带有地图的应用程序（比如车里内置的停车应用程序），显示可用的停车位、预订功能和在线支付。他们的重点是尽量缩短停车时间，避免停车罚单。该应用程序可以在

接近停车时间限制时发出警告，允许司机在计时结束之前移动车辆，或支付延时费用而不必移动车辆。

12.4.2 智能交通控制

交通是任何城市最容易理解的痛点之一。它是全球意外死亡的主要原因，造成了巨大的损失，并严重加剧了全球的污染。一个智能城市交通解决方案将结合人群数量、交通信息、车辆数量等，发送与道路事故相关的事件，以便街道上的其他控制器可以采取行动。

1. 智能交通控制架构

在图 12-9 所示的架构中，视频分析传感器基于视频计算交通事件，并仅通过网络推送事件（车辆数量或元数据，而不是单个图像）。这些事件经过架构层，到达能够驱动交通服务的应用程序。这些服务包括交通灯协调和收费公路的车牌识别。一些传感器还可以识别异常模式，如车辆行驶方向错误或驶入保留车道。在这种情况下，视频可能会被上传到交通执法机构。

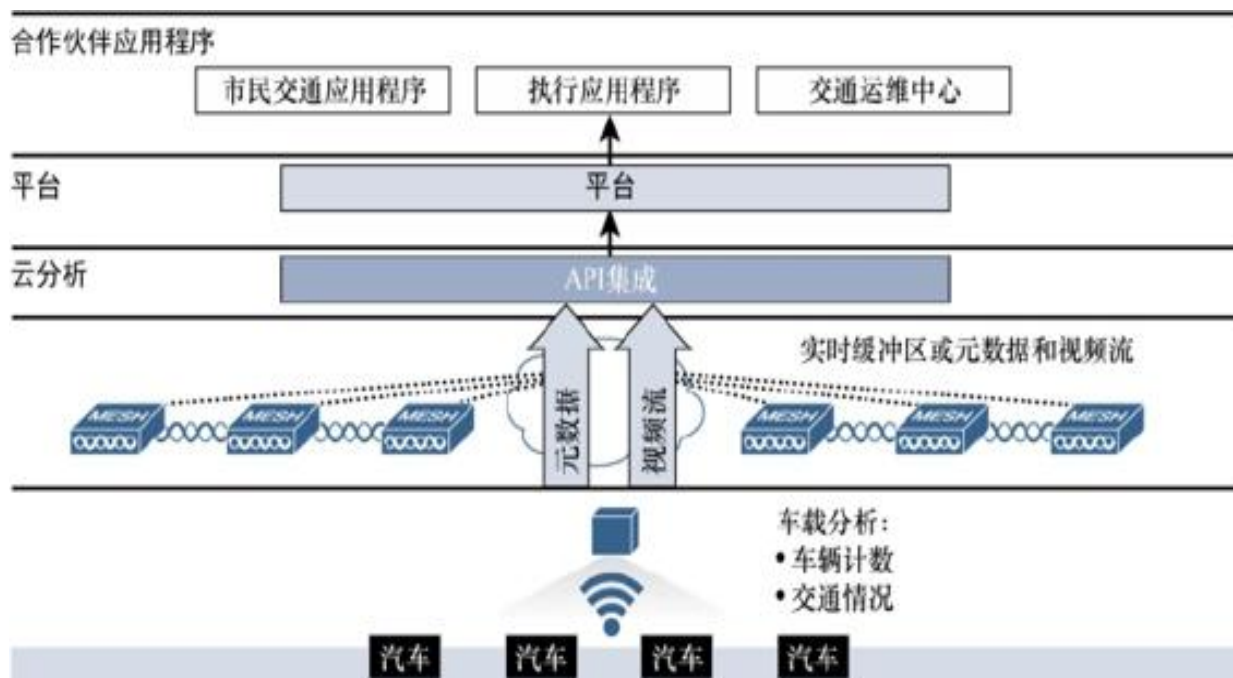


图12-9 智慧城市交通架构

交通控制解决方案中的其他类型的传感器包括蓝牙车辆计数器、实时速度和车辆计数器，以及照明控制系统。这些传感器提供实时视角，同时还为历史数据趋势和相关目的提供数据收集服务。通信技术因多种多样的传感器形式而有所不同。例如，安装在路灯或红绿灯上的计数器可以使用有线或无线技术和任意数量的通信协议。当一个传感器没有与另一个物联网城市应用程序耦合时，通常会使用无线技术。

2. 智能交通应用程序

交通应用程序可以与其他传感器一起立即采取行动来管理车流量并减少痛点。历史数据可以用来制定更有效的城市规划，以减少城市的交通量。一个常见的交通痛点是车辆走走停停，即交通流突然停止，然后再次流动。这种波浪状的交通模式是交通速度不可预测的自然结果，长期以来一直由公共和私人组织进行研究。这种交通波动的后果是局部交通事故大量增加，尽管通常是轻度的，但会加剧整体拥堵。

对于走走停停的交通，一个众所周知的补救方法是根据车辆密度来调节标准的车流速度。随着密度的增加，汽车速度被迫下降，以避免波浪效应。一个实时测量交通密度的应用程序可以通过调节路灯的周期持续时间来控制增加到主干道上的车辆数量，从而限制或抑制波浪效应。从司机的角度来看，在上高速公路或主干道之前有一段等待时间，而且主干道上的交通缓慢但稳定。这给人的印象是交通缓慢但移动，结果是通勤体验更好，减少了通勤时间，减轻了压力，减少了事故数量。

信息也可以与司机共享。无数应用程序利用外包或传感器提供的信息来提供实时的出行时间估计，建议重新选择路线以避免拥堵点，或简单地找到两点之间的最佳路径，同时考虑到交通、道路工程等。

了解一个城市的实时交通模式，并能够有效地缓解交通问题，可以为一个城市带来巨大的价值。许多部署在街道上的物联网系统，即使用于其他目的，也可以处理交通信息；具体来说，垃圾、停车、照明和环境都会影响交通结果。传感器计数设备或汽车、检测运动的传感器、测量空气中气体浓度的传感器，都可以用来估计交通状况。由此得到的评估结果可以在很多方面发挥作用，比如在城市级别调节交通流量，使市民获得更好的驾驶体验。

12.4.3 互联环境

截至2017年，全球50%的人口居住在地球表面积不足2%的地区。这种人口密集的封闭空间可以随时看到危险气体的峰值。超过90%的世界城市人口呼吸的空气污染水平远远高于建议的阈值，全世界每8例人口死亡中有1例是由空气污染造成的。

1. 互联环境的需求

大多数大城市会监测它们的空气质量。数据通常来自巨大的空气质量监测站，这些监测站造价昂贵，已经存在了几十年。这些监测站

的测量精度很高，但范围也很有限，一个城市很可能有许多盲点。考虑到空气质量监测站的价格和规模，城市无法负担所需数量的监测站，以便在局部水平上提供准确的报告，并跟踪污染物在城市中随时时间流动的情况。

为了在短期和长期内全面解决空气质量问题，智慧城市需要在任何特定时间以超本地化、实时、分布式的方式了解空气质量。为了获得这些指标，智慧城市需要在以下方面进行投资：

- 开放数据平台，利用现有的空气质量监测站获得当前的空气质量测量数据；

- 传感器的精度与空气质量监测站类似，但价格要低得多；

- 通过跨领域的行动来改善空气质量；

- 为消费者提供可视化的环境数据，并维护历史空气质量数据记录，以跟踪排放随时间的变化情况。

2. 互联环境架构

图12-10展示了一个架构，在这个架构中所有连接环境元素都覆盖在本章前面介绍的通用四层智慧城市物联网架构之上。

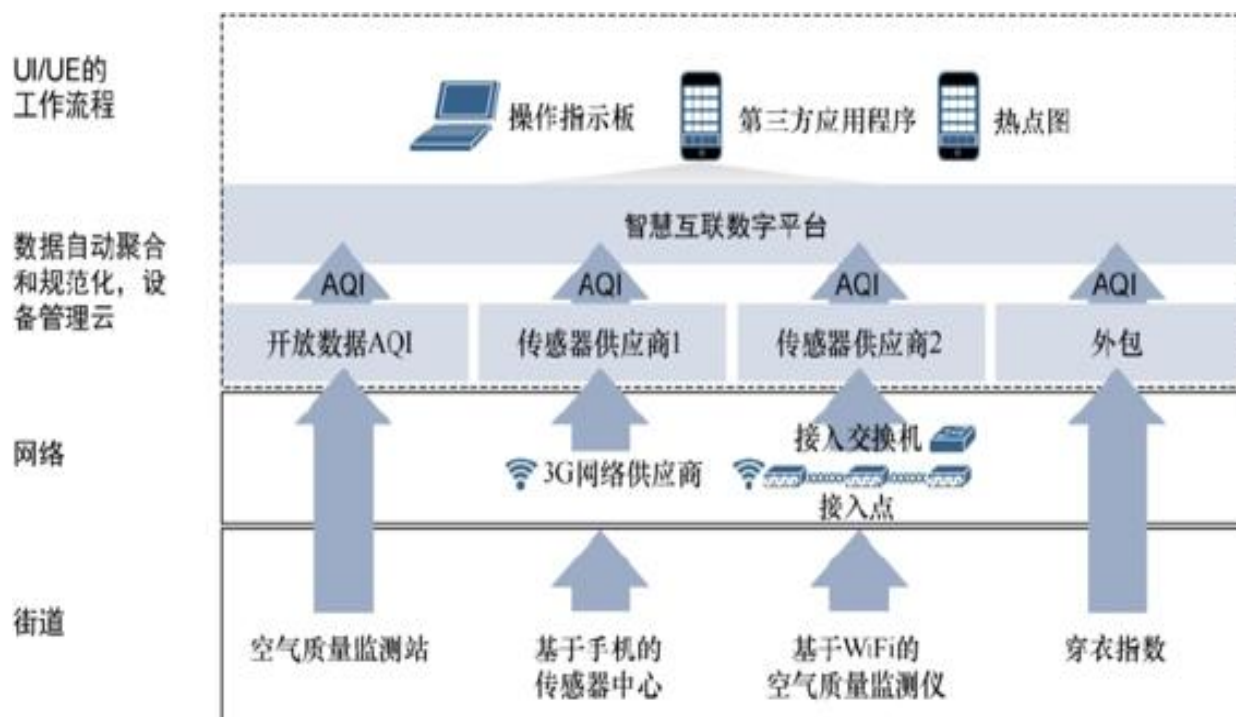


图12-10 互联环境架构

如图12-10所示，在街道层有各种多厂商传感器产品，它们使用各种通信协议。相互连接的环境传感器可以测量不同的气体，这取决于城市的特定空气质量问题，可能包括天气和噪声传感器。如前所述，这些传感器可能位于各种城市装置（如路灯）中。它们也可以嵌入到地面、其他架构或智能城市基础设施中。即使是移动信息源，也可以通过可穿戴设备接入，市民可以选择购买这些设备并随身携带，随时了解周围的空气质量。采用众包可能会将这些信息提供给全球系统。

通信技术取决于传感器的位置。可穿戴设备通常通过短程技术（如蓝牙）与附近的收集设备（如电话）进行通信。然后，该设备将收集到的数据转发给基础设施（例如，通过蜂窝数据）。安装在城市设施中的传感器也使用多种通信技术。街道照明系统中包含的传感器可以利用与路灯控制应用程序相同的通信基础设施。

独立的传感器通常使用无线技术。在密集的城市环境中，ZigBee和WiFi很常见。然而，由于WiFi需要保持802.11连接，这会消耗电池资源，因此，WiFi并不能很好地适应报告零星出现的网络（不过，新的WiFi实现，如Wi-Fi联盟物联网低功耗和802.11ah，可以解决这个问题）。

题)。在更大的环境中，使用的是LPWA技术，如NB-IoT和LoRaWAN，除非传感器能够使用有线技术（例如，连接到有线照明基础设施时），但由于成本的原因，这种情况非常罕见。

除了所有的空气质量传感器和可穿戴数据外，图12-10左侧的数据中心层或应用层也接收来自现有气象站的开放数据作为额外的数据输入。所有这些数据输入汇集在一起，可以在任何特定时刻提供对城市空气质量的高度准确的感知。这些信息可以在应用程序中可视化，包括微粒、浓缩物的热图，以及关于这种气体异常危险的具体信息。可以传达不同的污染水平，可以跟踪气体在城市中的扩散，无论是由于风还是因为气体源的运动（例如，早上和晚上通勤者的钟摆式运动，密集的交通路线形成了污染模式）。

通过这些污染和环境数据以及应用于这些数据的分析，城市可以跟踪问题区域，并在长期城市规划中采取行动，以减少空气质量扰动的影响。这种行动可以采取多种形式，从污染更严重的线路上增加可用的公共交通，到鼓励企业迁往居住区，以限制每天通勤的需要。有了这些污染信息，市民还可以采取短期行动，比如在某一时刻打开空气净化器，或者在污染物浓度变得严重时直接进入室内。还可能采取战略协调的联合行动，例如限制某些路线或特定日期的交通，鼓励公民共用车辆或使用公共交通系统。

12.5 小结

本章回顾了智慧城市物联网的主要组成部分。当城市中心利用技术来改善公共资源的管理（比如街道空间或垃圾收集），并改善市民的城市生活质量时，它们就被贴上了智能的标签。随着城市密度的增加，必须找到新的更有效的解决方案来维持或提高快速增长的城市中心的宜居性。

物联网技术在街道层面部署传感器，收集本地数据。城市层将收集到的信息传送到数据中心，在数据中心对信息进行处理。然后可以

自动或基于机器学习来采取行动。信号被发送回街道层，以修改传感器状态、调整路灯工作模式等。此外，市民还可以访问过程信息并采取行动（例如，找到停车位或采取备用路线以避免交通堵塞）。

这种智慧城市解决方案的一个关键问题是安全性。智慧城市的一个要求是隔离和保护与街道设备的数据交换，并保护与数据库和处理数据的交换。另一个需求是为多个服务使用公共传输体系结构，并使用公共云基础设施来促进应用程序之间的交换。这种交换的一大优点是相同的信息可以被多个用户利用，每个用户都有不同的关注点或观点，比如市民个体、应急响应人员和城市规划者。平衡安全需求和交换需求是一个持续的挑战。

智慧城市物联网应用的典型例子是互联路灯；物联网可以显著降低城市能源成本，同时利用现有的路灯基础设施，并与其他智慧城市应用（例如污染或交通检测）相结合，从而产生非常小的溢价。智能停车是物联网带来巨大效益的另一个例子，它可以减少城市拥堵，提高市民驾车的生活质量。与停车相关，智能交通控制是另一种智慧城市解决方案，可以用来调节车流，提供最佳的路线选择。控制交通和改善停车也有利于环境。互联环境智慧城市解决方案可以通过分布式传感器或众包直接测量、管理和监测空气质量和污染。

第13章 交通运输业

高效的交通工具彻底改变了人们交流和互动的方式。有了更强大和更便宜的发动机，商用车、客车、公共汽车、火车（包括地下、地上、轨道和有轨电车）和各种型号的飞机的数量在20世纪都呈指数级增长。这增加了交通堵塞、事故和污染。如今，影响交通运输业的主要问题不再是发展和增长，而是管理过度增长和旅途体验不佳。物联网和自动化技术可以通过提供车辆性能和预期行车条件的实时信息来帮助司机个体。物联网还可以帮助整个城市和国家优化交通和运输。

本章包括以下部分。

■ 交通和运输业系统：本节提供运输行业及其分子行业的观点。

■ 交通运输业的挑战：本节描述影响公路和铁路出行的挑战，包括个人和公共交通工具。

■ 运输业物联网用例：本节提供了多个例子，用于说明物联网如何显著改变运输行业和出行体验。

■ 运输行业的物联网架构：本节详细介绍本章涵盖的运输行业的物联网架构——道路上的个人车辆、公共交通巴士和火车。

13.1 交通和运输业系统

交通运输业包括多个子行业：公共交通（包括地铁、轻轨、电车、轮渡和公共汽车）、铁路、公路、航空、海运、货运和物流以及客运车辆。每个子行业和运输方式也可以包括多个专门领域。例如，航空运输包括机场、地区或国家空中交通管制当局、航空公司、各种

维修公司。当然，还有飞机制造商。图13-1所示为常见的交通运输子行业。



图13-1 交通运输子行业

其他章节中涉及的一些考虑因素也适用于这些子行业。例如，大多数用于制造业的物联网解决方案可以应用于汽车制造商（有关制造业物联网的深入讨论请参见第9章）。同样，智能互联城市利用许多物联网解决方案来建设交通基础设施和应急交通体系（有关公共基础设施物联网的详细讨论，请参阅第12章；有关应急服务物联网的详细讨论，请参阅第15章。）整个交通行业规模太大，本书无法涵盖。本书侧重于特定的垂直领域和交通运输业的具体方面。我们用交通运输的3个子行业来说明物联网如何改变这个行业。

■ **道路：**道路涉及单个车辆、管理车队和整个道路基础设施——红绿灯、路边摄像机、道路传感器、收费停车场、数字标牌等。由于物联网对个人生活有着强大而直接的影响，因此改善道路的物联网产生的影响是巨大而明显的。

■ **公共交通：**公共交通将个人交通工具扩展到公共交通工具。这个子行业是其他子行业发生变革的催化剂。

■ 铁路：虽然公共交通包括地铁和轻轨，但城际火车交通也包括货运，这是铁路活动的一个重要部分。

针对这3个例子所描述的改善可以成功地应用于其他运输子行业（如航空、乘客海运和货运/物流）。但是，请记住，每个子行业都有特定的特征，这些特征可能适用于其他行业，也可能不适用于其他行业。

同样，本章重点关注运输物联网的各个方面，这些方面会影响乘客体验、劳动力优化和运营效率、安全性和保密性。由于物联网的优化，交通运输的许多其他方面也发生了巨大的变化。例如，智能传感器可以根据检测到的路况调整汽车轮胎的刚度，从而直接延长汽车轮胎的寿命。通过物联网来优化轮胎寿命是一个很有吸引力的领域，物联网与车辆之间的所有关系需要一本书来讲解。在道路的背景下，本章重点介绍车辆和道路基础设施之间的相互作用如何改善出行体验，以及如何提升车队管理团队的运营效率。

13.2 交通运输业的挑战

随着交通工具的增多，与规模相关的挑战也出现了。随着车辆的增多，公路和铁路的管理和维护变得更加困难。当交通密度增加时，保持较高的安全水平需要优化管理效率。在只有一个用户时，维护一辆车是相当容易的。在大型企业或公共交通机构中，维护整个车队更具挑战性。跟踪每辆车的位置和维护状态需要主动监控每辆车。所有车辆和运输媒介（航空、海洋、铁路或公路）都面临这些挑战。然而，每一个运输子行业都面临独特的挑战，下文将详细介绍。

13.2.1 道路

道路面临的挑战可能是最常见的，因为大多数成年人都可能是司机，以及道路问题经常出现在新闻报道中。如今，道路运营商面临的

最大挑战在安全、流动性和环境方面。

■ **安全：**根据美国交通部的数据，2015年美国共报告630万起交通事故，造成超过3.3万人死亡，240万人受伤。

■ **流动性：**全球有超过10亿辆汽车在路上行驶，交通拥堵已经成为一个主要问题。据世界卫生组织估计，交通拥堵在世界范围内造成了55亿小时的出行延误。这些延误仅在美国就造成了1010亿美元的损失。这些后果可能是极端的。

■ **环境：**根据美国公共交通协会（American Public Transportation Association）的数据，在美国，每年因交通堵塞而产生的燃料浪费超过30亿加仑。此外，交通运输造成了近1/3的温室气体排放。

这些大范围的挑战是显而易见的，但对于个体驾驶员来说挑战也同样存在。在夜间或恶劣的天气条件下开车是危险的。缺乏可见度、车辆行驶缓慢、意外的障碍物以及其他司机都增加了挑战。这些问题并不新鲜。然而，汽车已经成为21世纪一种公认的交通方式。人们希望汽车和摩托车具有与智能手机或导航系统相同的智能水平。汽车被认为是聪明的工具，而不仅仅是由引擎驱动的四轮工具。在这一领域，物联网可以通过提供有关车辆状态的详细信息并预测任何零件的损耗或故障来帮助改善旅程体验。智能物体还可以帮助车辆及其驾驶员与更大的道路基础设施进行通信，以预测障碍物或更好地了解行驶状况。这种增强的可视性有助于提高机动性，并通过绕过拥塞路段来减少污染，同时通过避免碰撞和故障预警机制提高安全性。

这种对车辆智能的期望也适用于任何管理车队的组织。在部署了成百上千的车辆和人员的情况下，组织需要能够了解每辆车的位置，查看机械问题的预警，简而言之，可以查看和管理整个车队，而无须依靠每辆车的司机的简单汇报。在此，物联网提供了强大的工具，将单个车辆监控（为车辆工作人员的利益）与中央报告相结合，以帮助车队管理团队自动化维护需求警告、帮助定位每辆车并优化团队轮换，并使用大数据有效地管理车队的运营。

13.2.2 公共交通

公共交通通常是城市内部的。它是一个集体运输系统，连接着一个城市特定区域的不同位置。“城市”这个词可以指一个城市，也可以指一组邻近的城市，它们之间的距离足够近，可以共用公共交通基础设施。公共交通可以指公共汽车、电车、地铁、地上列车和轻轨。因此，公共交通包括火车。然而，铁路子行业在本章中有一个单独的小节，因为城际列车包括货物列车和客运列车（而城际列车通常主要载客），以及城市轨道交通通常面临的挑战并不总是适用于铁路运输。

■ 火车总是在轨道上运行。公共交通（公共汽车、有轨电车）可能与其他车辆共用一条街道，因此经常面临与交通拥堵相关的挑战。如果把车停在家里搭乘公共汽车，而公共汽车也像私家车一样堵在路上，那么对乘坐公共交通工具的激励就非常有限。

■ 火车能够涵盖多种现状。一些列车运行于城市之间。公共交通系统（包括轻轨、地铁、公共汽车等）运行的距离更短，但频率更高。一条公共交通线路上的事故可能会对其他多条线路上的乘客造成干扰，从而可能影响数百万人的出行。相比之下，城际轨道上的事故可能只影响该轨道上的交通。

■ 公共交通乘客在出行时可以使用多个公共交通系统或一条公交线路。例如，乘坐郊区火车和公共汽车（反之亦然）可能是日常通勤的正常组成部分。基本上，出行人员关心的是在两点之间找到最快的路线。当有事件影响一个系统的效率时，出行人员必须能够评估备选解决方案并实时做出调整。相比之下，城际线在两个指定地点之间提供的选择较少。

■ 规模是一个问题。每天往返于两个城市之间的火车可能每天拥有相同的货物和/或乘客数量，高峰和低谷是可以预测的（比如工作日、周末和假期）。相比之下，一个城市内的公共交通系统也会有众所周知的高峰（商业高峰时间），但是外部事件会突然改变系统的负荷。在一个特定地点举行的音乐会可能会带来成千上万的新乘客。另

一个公共交通系统的中断可能会使成千上万的旅客重新进入一个并行的系统。在这种情况下，对载客量和班次的规划比城际列车要困难得多。运输管理部门必须实时做出反应，以保持系统的效率。

13.2.3 铁路

从外部看，铁路行业的规则似乎相当简单——铺设轨道并连接地点。一旦铁轨铺设好，就可以在特定的方向上有规律地安排列车班次。正确的时间安排是确保客户满意和安全所需要的全部保证。

然而，现实情况比较复杂。例如，美国人更喜欢坐飞机而不是火车。然而，美国有 22.5 万公里的铁路贯穿全国。这些是城际轨道（不包括城市交通），每天有数千列火车在上面运行，属于多个公司，运载乘客或货物或两者兼用。即使有最合理的时刻表，一旦意外事件发生，事情也会变得复杂（例如，轨道上有动物或树木、损坏的设备迫使列车停止运行）。即使不考虑意外情况，协调时间和位置也很复杂。当轨道相交时，复杂度会增加更多。

一列火车也会显示这种复杂性。假设你负责每天在两个相距不远的城市之间运营一列火车。乘客或货物应准时到达，准时离开。货运客户或乘客不应担心天气状况。当下大雨时，或者铁轨被冰雪覆盖，又或者当龙卷风或飓风吹过轨道时，火车应该能保持同样的性能。他们也不应该担心有人在轨道上放置物体或窃取信号或电缆。

只要火车还在运行，铁轨上就会一直使用信号。工程师可以通过这些信号了解火车是否正在接近交叉路口，不同的信号颜色表示交叉路口的障碍物是向上还是向下。利用磁力计，这些信号还可以探测到一辆经过的火车，并在特定的时间内发出“其他列车正在靠近”的警告。

确保火车安全、准时到达目的地涉及多个信号和系统的协调。一个主要的挑战是确保所有这些系统的效率，并确保以协调一致的方式提供信息。如果信号丢失或有缺陷，维修团队如何知道？机车司机该

怎么办？如果一列火车因为轨道上的问题不得不停车，后面的火车是否应该得到这个信息以便停车？如果轨道问题需要修理，能否使列车改道至受影响路段附近的另一条可能路径？为此，物联网可以极大地提高运营的安全性和效率，跟踪列车的位置和速度，收集轨道状态、信号、电力线和轨道沿线其他基础设施的数据。实时查看铁路基础设施的状态可以大大降低延误或事故的风险。

如果这些担忧只出现在一列火车上，想象一下，当它们上升到整个旅程的水平时，会变得多么复杂。铁路通常只是货物运输的一部分。货物需要按时交付，否则整个供应链都会受到影响。

同样地，乘坐火车的乘客希望有一个最新的、准确的列车时刻表（考虑到当天可能发生的无法挽救的意外事件），并在必要时选择最佳方案。一旦上车，乘客还希望得到各种服务，而不仅仅是简单的交通工具（例如，清洁的厕所、食物、舒适的温度、互联网连接）。因此，铁路行业面临着多重挑战：确保乘客安全，在任何意外情况下按时运行列车，提供足够高质量和舒适的乘客体验，使乘客愿意再次乘坐火车。物联网可以用来追踪货物，提供旅程的实时视图（延迟、预期到达时间等），同时通过跟踪和报告机载设备状况（从厕所故障警报到售出的三明治数量）帮助优化出行体验，以便进行有效的、有针对性的维护。

13.2.4 交通运营商和用户面临的挑战

考虑公共交通和私人交通的挑战时，我们会发现有不同的参与人员，在不同的规模上运作，有着不同的需求。

用户是第一个现场级参与者。我们开车时，想要享受一段舒适、可预测、高效的旅程。汽车必须正常工作（不管浪漫的电影告诉我们什么，一次汽车故障通常都不是愉快的经历）。当汽车的部件磨损或濒临故障时，我们希望在故障发生前得到通知。传感器可以清楚地看到汽车的状况。智能算法可以预测磨损，并提前发出警告。在计划出行时，还需要了解出行时间和条件，包括交通、道路状况和天气。汽

车必须能够在（几乎）任何天气条件下运行并提供舒适的体验。如果交通影响了你的旅程，汽车系统应该能够通知你（在交通变得拥挤之前），并提供其他选择。简而言之，汽车需要提供关于其自身运行状态的信息，预测其性能，并补偿外部条件的变化。你还需要了解关于旅程和旅程发生的环境的信息。借助物联网，汽车可以与道路基础设施进行通信，对任何即将出现的问题（事故、路障等）发出警告，并提供预期旅程的视图（出行时间、天气状况等）。

对于单个驾驶员来说，正确的事情在整个车队的范围内也是正确的。想象一下，你正在经营一家有线电视公司、一家电力公司，或者任何其他拥有车队的公司。你还需要告诉客户，卡车需要多长时间才能到达他们那里，并根据出行的时间和地点，将交通密度纳入每个工作人员的日常工作量的考虑中。在管理的车辆数量增加的情况下，个体司机的担忧会成倍增加。能够实时或近乎实时地跟踪每辆车解决了这个挑战。有了智能对象，车辆还可以报告工具和设备的水平，以确保机组人员总是处于最佳状态，以便执行下一个任务。如果所需的工具丢失，可以将车辆送至集合点，或改派一名附近的工作人员前往，而另一队人马将被派遣到另一个任务，对此任务而言车辆有适当的设备。

作为一个单独的出行人员，踏上公共交通旅程的时候也会出现相同类型的需求。在这种情况下，我们不需要关心车辆。运输公司负责这次出行。虽然车辆的状况会影响行程，但我们不必直接留意车辆；如果操作人员没有对其进行维护保养，导致车辆抛锚，你可以直接投诉。但是我们仍然希望获得关于旅程的信息（比如时间和条件）。

对于车辆状况和一般交通状况，公共交通运营商也有同样的担忧。他们也有自己的车队，和私人组织一样关心车队的管理。不过，它们的运营水平也高于个体司机。驾驶条件的恶化不仅影响到他们所驾驶的许多车辆，还可能产生更多的污染，降低客户满意度。由于公共交通比单个车辆效率更高（在单位道路或轨道空间上运送的乘客数量方面），这些运营商必须平衡道路上的车辆数量和运营车辆的成本。他们还必须平衡交通线路，尽可能多地吸引乘客，从而在对城市

居民有用的同时，提供一个经济合理的解决方案（如果这是他们的任务）。

在更高的层次上，城市要么直接运营公共交通系统，要么与公共交通组织有密切关系。因此，市政当局（通常是对公共交通的新资金进行投票的市民）有权决定需要修建哪条新轨道，哪条街道可以使用，哪条道路可以通行，以补充其他交通系统。在这种规模下，交通管理不是针对单个车辆的，它是关于拥挤和共存的。更多的公共交通线路减少了拥堵，但前提是它们满足了市民的需求（在没有市民关心的地区之间修建一条交通线路纯粹是浪费资源）。利用收费系统和公共交通票价的收入，可以制定使用公共交通系统的激励措施。当交通堵塞发生时，应急车辆必须有一个通道通过。之后，公共交通工具应该能够更好地进入基础设施的通道，从而使公共交通比单独的交通工具更受欢迎。

同样的问题在火车上也可以看到。主要的区别在于出行的距离和其他交通方式。如果一辆公共汽车坏了，你可以乘坐另一辆公共汽车或乘地铁。如果一列火车在两座城市之间抛锚，乘客和货物就会被困，有时长达数小时。这会给乘客带来很差的体验。与城市轨道交通相比，乘客对火车的满意度更为关注，因为一旦出了问题，没有立即的替代方案。然而，对于出行人员来说，下次选择驾车或乘飞机出行要容易得多。货运客户不像乘客那样灵活，但如果货物在某条路线上被严重延误，他们也可以考虑其他的运输方式。在城市公共交通中，出行人员可能会选择开车而不是乘坐公共交通工具，但是直接的替代选择（另一辆公共汽车或地铁）通常更容易获得，以改善糟糕的出行体验。因此，铁路运营商通常对客户体验和出行可靠性非常敏感。当然，这并不意味着公共交通运营商对乘客的体验不敏感。他们每天都在与其他交通工具竞争，同时也非常注重乘客体验，以维持和改善他们的收入来源。

13.3 运输业物联网用例

对于上述所有需求，物联网带来了强大的优势：收集本地数据，在任何范围内共享这些数据，并提供工具来处理收集的数据，以便更好地优化车辆和整个交通基础设施。

人们可以优化可用的资源，但是拥有单个驾驶员的本地化信息并不够。通过无线技术和其他通信手段共享这些信息仍然只能掌握有限的整体状况。

一个众所周知的故事发生在南美洲的一个大城市（在一些独立的公共交通优化专家圈子里），这个城市的当局考虑将优化公共汽车出行效率的任务委托给个体司机。他们认为，因为司机在街上，所以他们比任何一个更高层的官员都能更好地了解当地情况。因此，公共交通管理局制定了一项规则，将司机的工资与其工作表现关联。绩效将通过每辆巴士从起点到终点所花费的时间和沿途运送的乘客数量来衡量。这样做的理由是，该系统将鼓励司机帮助加快乘客的上下车速度，并寻找解决当地交通拥堵的办法。

但是，这样做的效果与预期效果不同。仅仅几周后，公共汽车就停止了按照预定路线行驶。司机只走捷径，绕过拥挤的街道，还绕过乘客较少的车站（不关心乘客期望在绕过的车站上下车），争相在客流量大的车站载客，因而引发道路纷争和竞争。司机们确实完成了规定的任务，但总体上提高公共交通效率的目标并没有实现。

物联网在这个方面提供了更好的解决方案，因为信息可以同时是本地的和全局的，可以提供给多个利益相关者，他们都可以从系统获得的知识中受益。

13.3.1 联网汽车

物联网能够缓解交通挑战的一个对象显然是车辆本身。现代汽车高度计算机化，有数百个传感器来评估从轮胎压力到一个松动的油箱盖等所有部件。这些信息显示在仪表板上，以帮助司机获得更好的出行体验。这是一个智能对象的例子，但不是物联网。不能称之为物联

网的一个限制原因是信息仅在本地可用。因此，它不能与来自其他车辆的信息相关联，从而描述更全面的场景。如果你的轮胎漏气了，这只是局部的不幸事件。但是如果过去一小时内有20辆车在同一区域爆胎，那么这段路就会出现大问题。如果你要前往该区域，你会希望提前得到预警，并可能有一个车载系统建议走另一条路线。当你的车在冰面上打滑，车上的雷达探测到一小团雾时，或者当了解其他当地情况对其他司机有利时，同样的逻辑也适用。

物联网允许智能对象进行通信，并基于通信提供有价值的服务。汽车传感器发现的任何信息都可以与汽车外部的系统共享。当信息在局部有效时，应该在局部提供。当其他车辆驶近某一特定区域时，他们就会收到由当地事故引起的交通堵塞、由于路面溢油而造成的湿滑状况，或由于路灯损坏或铁路枢纽系统故障而造成的交通困难的警告。这种通信意味着必须有一个车对车（V2V）、信息交换系统（在提供有用信息的同时保护您的隐私）和一个车对基础设施（V2I）信息交换系统，以便在相关的地方提供本地信息。

当信息仅与您的汽车相关时，可以在局部提供，但可以与第三方系统共享。例如，当你得到一个提示说你的车需要更换机油，这很好。但是如果你的仪表盘上同时也出现了当地汽车护理公司可能提供的预约时段，这样会更好。同样，如果你的汽车制造商召回一件有缺陷的设备，你的汽车受到影响，在仪表盘上显示是否有用？这样的通信需要车辆和互联网之间始终保持连接。

手机上的应用程序之所以能够提供最佳导航，是因为我们的手机连接到互联网，交通数据实时更新。然而，手机并没有连接到车上的系统。将汽车直接连接到互联网或手机，将为我们的出行体验带来所有的连接优势。应用程序层出不穷。例如，汽车制造商可以将天气预报映射到一个非常细粒度的级别，并动态调整汽车引擎设置以适应当地条件并节省燃料。初创公司已经开始生产智能挡风玻璃和智能前灯。灯光闪烁非常快（每秒50次），比眼睛能察觉到的速度还要快。对司机来说，道路上有连续的灯光。与此同时，挡风玻璃上覆盖着一块透明的屏幕，可以变成黑色。当两辆车面对面时，它们的灯光和屏幕会同步。当从对面驶来的汽车灯光亮起时，你的屏幕会变暗；对面

的光线消失时，屏幕会重新变得透明。因为闪烁的频率高于视觉暂留，结果是两个司机都能看到道路被光线照亮，但他们两人都不会被迎面而来的灯影响视线。该技术为你的眼睛优化驾驶体验，可以大大提高安全性。类似性质的发明数不胜数，但它们都有一个共同的概念：你的汽车可以与基础设施和其他汽车通信，交换信息，使出行体验更轻松。

13.3.2 互联车队

联网车辆比单独的司机出行更能改善交通状况。想象一场风暴让成千上万个家庭断电。正如在第11章中所解释的那样，电力公司能够实时了解所有电力线中断的地点，并为此部署了数百辆修理车。通过物联网解决方案，调度中心还可以实时了解每辆维修车的位置。它知道维修车是否正在向故障点移动，或者吊桶是否已经打开，工作人员是否正在进行修理。每辆维修车的状态都受到严密监控。有了这些信息，电力公司就能准确地掌握紧急维修工作的进展情况。摄像机还可以监控维修车周围的环境，以帮助评估是否需要额外的调度（清理道路、增加标杆等），并确保操作的安全性。调度中心可以将维修车调配至最需要的地方，进行管理维修和供人员休息，以及供应或更换电缆或其他设备等。同样的模式也适用于任何其他车队。出租车公司可以根据客户密度、天气和出行模式，在整个城市范围内优化出租车密度。汽车租赁公司可以跟踪车辆以优化停车场的运营，甚至可以找回丢失的车辆。同样的模式也适用于公交运营商或其他管理车队的公司。

13.3.3 基础设施和公共交通

在更广的层面上，信息交换系统意味着基础设施可以与车辆通信，收集基于数百个传感器的车辆信息（例如位置、速度、车辆运行状态），并将其传送到互联网，还可以向车辆发送有关当地情况的信息。当基础设施本身包含传感器时，信息可能更加丰富（包括天气、检测到的预期的交通密度、事故等）。目前已经有多种寻路应用程序

可以提供这些信息。这些应用程序从多个用户收集信息。这些信息被发送到云端，在那里可以得到有用的模式。拥堵区域和时间可以测量，并返回到应用程序以显示预期的出行时间。然而，这些应用程序对本地用户的好处是有限的。它们可以告诉你当前的交通状况，并且它们可以结合预测的交通状况变化并相应地修改它们的预测，但是它们不能修改道路的状态或协调发送给多个用户的响应。有了物联网，每辆车的信息，以及每辆车上每个导航系统的程序化出行，都可以在云端以协调的方式进行分析。其结果是更好的流量预测，也可以返回不同的信息给不同的用户。如果1000个用户都在朝同一拥堵路段导航，物联网可以动态地向不同用户推荐不同的路线，从而在第一时间避免拥堵（而不是简单地告诉你已经发生拥堵，并建议重新规划路线）。这种动态系统可以与动态自适应收费和高载客率车辆（HOV）规则相耦合（在许多城市，HOV车道是为搭载两名或两名以上乘客的车辆保留的）。对于每天开车上班的司机来说，其结果可能与导航系统每天建议的路线略有不同，但总体而言交通更顺畅，拥堵也更少。

这种智能物联网也会对公共交通用户产生直接影响。当你走向公共汽车站时，一条发送到特定号码（包括公交ID信息）的短信或一个手机应用程序可以显示最近的公共汽车站位置和预计的等待时间。当在公共汽车站等车时，智能面板可以显示下一辆公交车的预计等待时间和到任何目的地的估计行程时间。这种估计是实时的、智能的（基于当前的交通状况，并考虑到未来几小时内交通密度的预期变化）。从一个城市的层面上讲，出行规划应用程序会告诉你关于整个城市 and 所有交通系统的出行条件，可以提供最佳路线建议。许多其他物联网用例可以更好地缓解城市拥堵（更多例子参见第12章）。

物联网对车辆与基础设施通信的另一个影响是提高了安全性。例如，在拥挤的交通中造成车祸的一个主要因素是车辆走走停停的状况（当车辆以中速或高速行驶，然后突然停止，然后又加速）。走走停停的原因是众所周知的：交通密度（合并车道）、路边的干扰（交通事故、路边的异常现象）、恶劣的天气（雨或雾）、交通灯，以及车道变窄。有些元素是道路部分的结构性因素（合并车道、车道变窄），而其他因素则是偶然的。这些因素的综合效果可以在数公里内引发走走停停的状况。

减少走走停停的交通状况的一个常见方法是仔细地调节进入道路各路段的车流量。一个最优的进入速度会加速整个道路交通，从而产生更大的流协性（以及单位距离和时间内更多的汽车驶入和行驶在道路上）。物联网与机器学习是实现这一目标的强大组合。从车辆和基础设施上的传感器收集的交通密度信息，例如，车辆计数摄像机、记录车辆和速度的压力电缆，或者沥青中的光纤电缆可以通过估计当地车辆对沥青的压力变化而产生的光束偏差来测量交通密度，可以动态地适应当地情况，协调灯光，解决停车和通行问题，增加整体交通流量。同时，交通流量的突然下降（这可能意味着发生了事故）可以在交通管理中心触发警报。这个警报可以转发给应急组织，从而更快地调度应急车辆。同时，可以围绕事故区域标识出一个感知范围，这具有多重好处：

- 附近的司机会收到关于事故区域的警告（基础设施反馈到车辆智能系统）。

- 调整道路入口匝道交通灯，以减少每分钟进入受影响路段的车辆。

- 故障区域外的附近司机可以动态地接收备选路线建议。这必须以一种集中且智能的方式来完成。如果道路前方减速，你的导航应用会提醒你。然而，如果周围成千上万的司机收到完全相同的信息，选择完全相同的建议替代路线，会导致没有整体效益。集中系统允许实时监控和智能分配替代路线；为了平衡交通流量，可以分布几个备选路线。

- 应急服务车辆可以忽略它们接到的报告事故的冗余电话。当交通繁忙的道路上发生事故时，成百上千的司机会打电话给紧急服务中心报告事故，紧急服务中心必须确定每个电话是与一个新的事故相关还是与一个已经派出救援队伍的事件相关。感知范围可用于将来自范围内的类似和重叠调用关联到同一事件。同时，智能传感器可以检测到附近是否发生了另一起事故，从而简化了消除重复事件的过程。

路边传感器能做的不仅是汽车计数，还可以测量空气质量以及天气状况。这些信息可以转发到中央系统进行监视和警报。其他传感器可以应用到道路基础设施和物体上，以改善维护和安全。例如，道路上的传感器可以测量沥青渗透的水量，并评估路面的磨损。在桥梁上，结构传感器可以评估钢结构构件的应变和应力，倾斜仪可以测量桥梁的沉降和相对位移以及桥墩和桥台的倾斜度。加速度计可以测量振动和对交通、风，甚至地震活动的动态响应。图13-2显示了应用于桥梁的这些传感器的示例。



图13-2 监控桥梁的智能对象

所有这些信息都可以报告给道路维护中心。在那里可以在破坏性事件导致事故或道路堵塞之前进行主动维护。同样类型的传感器可以

安装在山路两侧。简而言之，物联网使交通部门不仅可以监控和优化交通状况，还可以主动监控基础设施。

这些信息也意味着雾计算和云计算。一座桥可以包含多个传感器。并不是所有传感器都需要报告详细信息。在大多数情况下，一个简单的“绿色”状态就足够了。同样，一辆标准的现代汽车有多个传感器产生数据。部分数据只对司机有意义，应该留在车里。部分数据只在局部有意义，应由路边雾计算系统处理。只有与大型系统相关的部分信息（例如，制造商的汽车数据）应该被转发到云端（在雾中进行预处理或不进行预处理）。

借助物联网，个体司机可以以更安全、更可预测的方式出行。交通部门可以更好地控制车辆流量，更好地管理道路基础设施。这些物联网解决方案还通过提供准确的交通信息、智能地图和旅程规划，使城市内的公交乘客受益。

将物联网应用于大型交通工具也能极大地改善出行体验。监视公共汽车的性能是一个明显的用例，它类似于汽车的预防性维护。同样的逻辑也适用于铁路。例如，许多列车是由悬挂在轨道上的电缆供电的（对于地铁来说，电缆则位于轨道附近）。电缆或电力线上任何物体的损坏最终都会导致列车停车。快速通过的列车会增加破坏程度（或损坏物体，然后成为轨道上的危险）。在过去，传统的铁路维护都是目视检查，这需要时间，而且可能会导致部分铁路无法使用（因为检查人员需要缓慢而仔细地检查每一米电力线）。通过物联网，智能传感器安装在列车顶部的电源棒上（称为受电弓）。一旦与电力线的接触超出了可接受的范围（以作为基线的多次跳闸为基础），传感器就会自动发送带有精确GPS坐标的警报，允许在损坏变得严重之前派遣维修人员。

基于同样的逻辑，智能传感器可以安装在机车和汽车的车轮上，以处理车轮在轨道上的声音，并识别任何可能表明车轮或轨道磨损的异常。机车性能是实时测量，并对前后两次行程进行比较，以满足轨道维护需求。车厢间连接系统测量下一车厢的牵引力，以跟踪异常情况（接合断裂、货物装载异常等）。在轨道的一侧，探测器可以读取

安装在车厢上的标签发送的信息。火车通过时，火车的每列车厢连同其顺序被确认（往往车厢从一列火车换到另一列火车时会有变化，使单独跟踪一列车厢成为非常具有挑战性的任务），同时还有一些有用的数据，如列车上厕所储水池中的可用水位、出售食品的详细信息，或运载货物的标识符。这些信息被实时传达给控制中心，在那里可以采取主动的行动（例如，检查列车、在下一站补充厕所水箱、补充食品供应、跟踪货物位置）。

轨道旁的其他传感器可以观察环境，并将其与已知参数进行比较。这种系统可以测量地下水位（如果地面积水，会影响铁路路堤）和山体滑坡，还可以将过往列车的图像与平均值进行比较，从而检测出异常的侧弯或其他异常。交叉口也是物联网的关键位置，传感器可用于交叉口，探测正在靠近的列车（及其速度）、故障信号或障碍物，或轨道上的车辆，并生成主动报警或紧急停车。

物联网也可以扩展到车厢本身，这些应用能够覆盖所有公共交通系统。与大数据处理引擎相连接的摄像头可以检测人群密度，预测高峰时段，还可以检测到自动分类的异常动作（不稳定的货物装载、攻击、事故、坠落等），并可以面向对象触发警报。与社交媒体的交互经常被用来预测特定线路和路段的交通流量。在更简单的层面上，这些数据可以用来提供最佳的出行计划。这些规划帮助预测的不仅是出行的持续时间；它们还可以预测影响客户满意度和业务的出行条件。在火车上没有座位，或者在地铁或公共汽车上被迫挤在人群中，都可能对公共交通产生负面影响。能够使用大数据和分析来规划合适的火车或公共汽车密度是改善出行条件的关键。但是，能够提前告知旅客已经是一个巨大的进步。一般来说，如果提前得到警告，出行人员不太可能对他们的出行条件产生负面情绪。

对于所有这些用例，以及每天发明的更多用例，物联网有助于提高出行途中的安全性和舒适度。

13.4 运输行业的物联网架构

很明显，用于运输行业的物联网涵盖了不同的需求，因此需要不同的架构，这取决于运输方式等因素。这些架构在以下几个地方相互交叉和重叠。

■ 单个车辆需要一个架构来与其他地区交换信息。范围大小不限，信息可以是本地的，也可以是云端的。在大多数情况下，根据不同的目的，可以使用短程和远程通信。同样，有些信息是在本地处理的（雾计算），而有些信息是发送到云中进行处理的。车辆之间、车辆与基础设施之间也需要进行通信。

■ 使用道路（公共汽车、电车等）的公共交通系统受益于单独的车辆架构。这种架构可以在全局范围内标记为道路物联网。道路公共交通组织还需要一个更全局化的架构来管理车队（例如，一个维修站），并在更大范围内管理或应对不断变化的道路状况。

■ 铁路需要有自己的体系结构来考虑交通、安全和车队管理。城际铁路对乘客体验表现出特殊的敏感性，因为出行时间比市内出行时间长。

13.4.1 道路物联网技术

用于道路的物联网架构从车辆层面开始，允许与路边系统和其他车辆进行通信。在物联网领域，这种通信被称为V2V（车对车）和V2I（车对基础设施），有时也称为V2X（车对一切），包括V2P（车对行人）、V2N（车对网络）和其他不同形式。由于车辆的移动不受限制（例如在轨道上），这种通信必然依赖于无线技术。下面几种技术是可用的，它们涵盖了不同的用例。

1. 蓝牙技术

对于短程通信（例如，车辆到乘客的智能电话），蓝牙是首选技术。大多数时候，使用的是二类无线电。

注释：1类无线电的最大覆盖范围为1米，2类无线电的最大覆盖范围为10米，3类无线电的最大覆盖范围为100米。

在一些罕见的情况下，需要安装3类无线电以允许V2I通信。在这种情况下，一个常见的应用是红绿灯与公共交通系统（应急车辆或公共交通工具）交互，并使这些车辆优先于其他交通工具通行。这个应用程序称为交通信号优先化（TSP）。虽然TSP可以使用蓝牙，但更常见的技术是DSRC，本章稍后将详细介绍。另一个应用是安装在路边的3类蓝牙无线电，它可以探测和读取过往车辆中蓝牙系统的唯一MAC地址。这样就可以在装备齐全的路段进行车辆计数和速度估计。虽然3类蓝牙允许这种类型的交换，但蓝牙在车辆外部是一个次要设备（最初是由于范围限制）。

2. 蜂窝技术/LTE

蜂窝技术用于一些V2X应用程序，但更常见于道路到基础设施的通信（安装在道路或路边物体上的传感器和对象与网络进行通信，汇报其状态）。有关适用于该领域的蜂窝技术的详细讨论和示例请参阅第4章。请注意，应用于物联网的蜂窝技术通常使用低带宽来实现更长的范围。

另一个值得一提的技术是WiMAX（802.16e）。尽管WiMAX确实在物联网的最后一公里或回程应用中占有一席之地，可以很好地适用于道路空间的物联网（见图13-3），但它最初未能在这一领域得到广泛采用。随着其他技术的竞争优势日益明显，WiMAX在V2X上的前景并不明朗。

3. DSRC和WAVE简介

V2X旨在促进车辆到基础设施的通信，并利用多个元素和协议，如DSRC、IEEE P1609和WAVE。本章稍后将解释这些协议。这些协议对3个协同工作的元素进行了区分。

■ OBU（车载单元）：车载系统。

■ RSU（路侧单元）：与OBU通信的路侧系统。

■ WAVE接口：无线电和通信系统。

OBU和RSU都包含一个WAVE接口，便于进行通信。

V2V和V2I通信是可能的，如图13-3所示。DSRC还允许车辆将另一辆车的信息转发到附近的RSU。

通信可以通过几个可能的信道进行。以每小时90公里的速度，在车辆和路边系统之间进行通信可能比较困难。在大多数情况下，车辆首先需要意识到路边RSU的存在。为了简化操作，RSU使用一个预定义的静态信道（美国DSRC的178信道），以100毫秒的间隔通知OBU它支持哪个通道上的哪些应用程序。有两种类型的应用程序：安全的和不安全的（本章后面将详细介绍）。OBU监听静态信道（178），验证RSU数字签名，首先执行安全应用程序（如果有的话），其次切换信道并执行不安全应用程序，最后OBU返回178信道收听下一个RSU通告。

OBU将从RSU和其他车辆OBU接收到的信息与自己的GPS位置和轨迹进行匹配，从而计算RSU或发出OBU信息的其他车辆的位置。RSU还可以发送专门的消息。典型的常见消息如下。

■ 游客信息：弯道速度、高度限制、路面结冰、前方碰撞、红灯、穿越铁路、工作区域警告、道路危险警告等。

■ 非DSRC车辆接近：非智能车辆不会对其他车辆的位置和轨迹发出警告或被警告，这意味着需要留有一定余地。

■ 行人警报：检测到行人持有具有DSRC功能的智能手机。

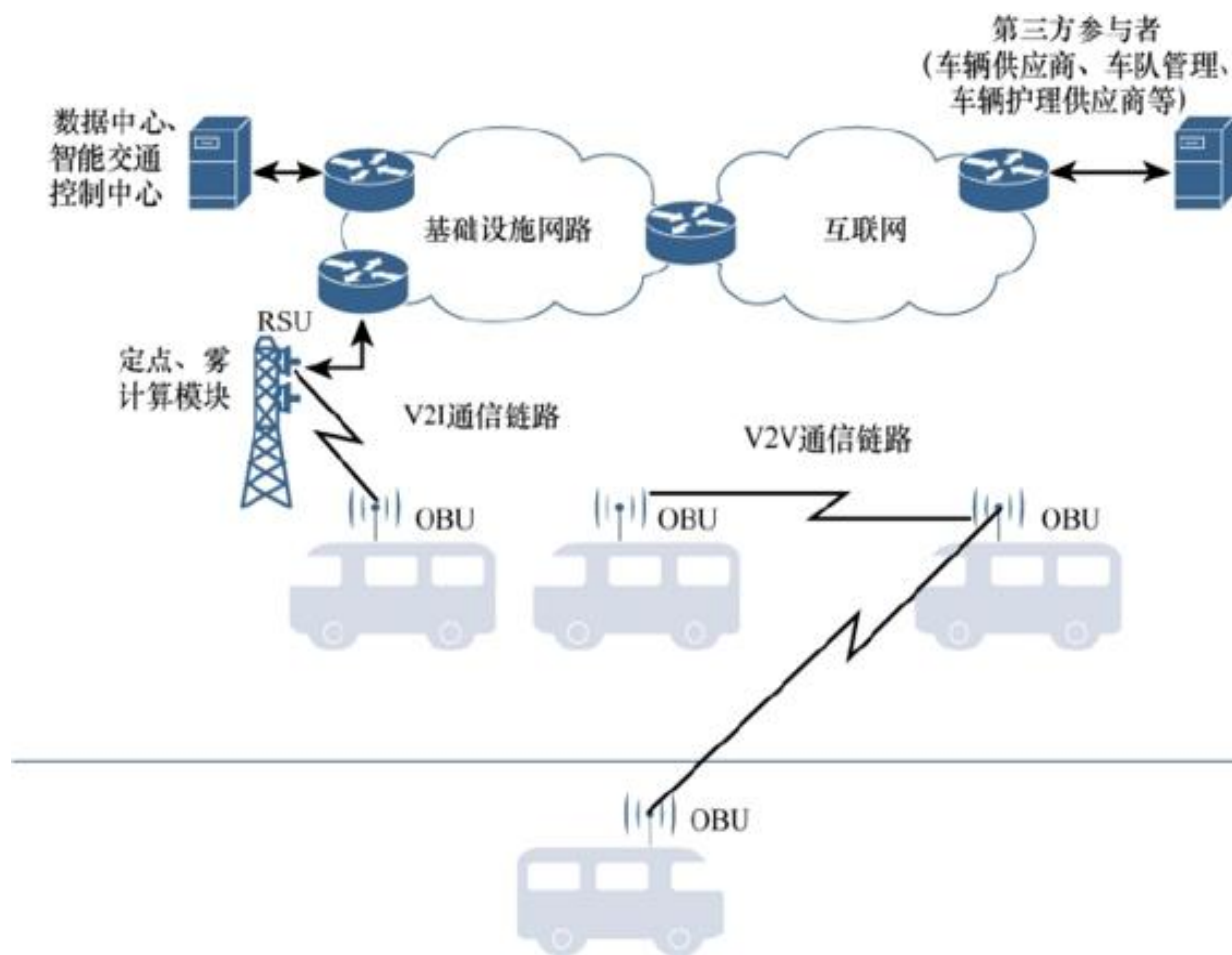


图13-3 DSRC通用通信架构

每个信道都被指定给特定的用例。例如，184信道专门用于大功率、长距离的公共安全通信。

应急服务机构通常使用184信道向其他车辆发出警告。公共安全车辆也使用这一通道将半公里外的路灯设置为绿灯。这种情况要求车辆配备DSRC设备，并且通信发生在小于半公里的范围内。在DSRC中，172信道专门用于V2V安全通信（避免和缓解事故）。在172信道，每辆车以每秒10次的基本安全信息（BSM）广播其核心状态信息。在接收到BSM后，路程内的其他车辆建立每个邻居的轨迹模型，评估潜在的碰撞风险，并在紧急情况下警告驾驶员（或采取控制措施）。典型的应用如下。

■ 前面的车辆（直接在你前面或前面几辆车）停车或刹车。该车的OBU会广播停车或刹车状态，从而使后面的车辆可以评估距离和碰撞风险，并自动刹车，即使司机还没有看到停下的车辆。这种情况如图13-4所示。

■ 你想更换车道。通过附近汽车的OBU信息使你的车知道有一辆车在你的视觉盲区，当你转动方向盘时会显示一个警报。

同样，如果你想要超过一辆较慢的车，然后转动方向盘来改变车道。你的OBU可以探测到另一个方向上正在接近的车辆信号，并发出警报（或控制车辆避免碰撞）。这种情况如图13-5所示。

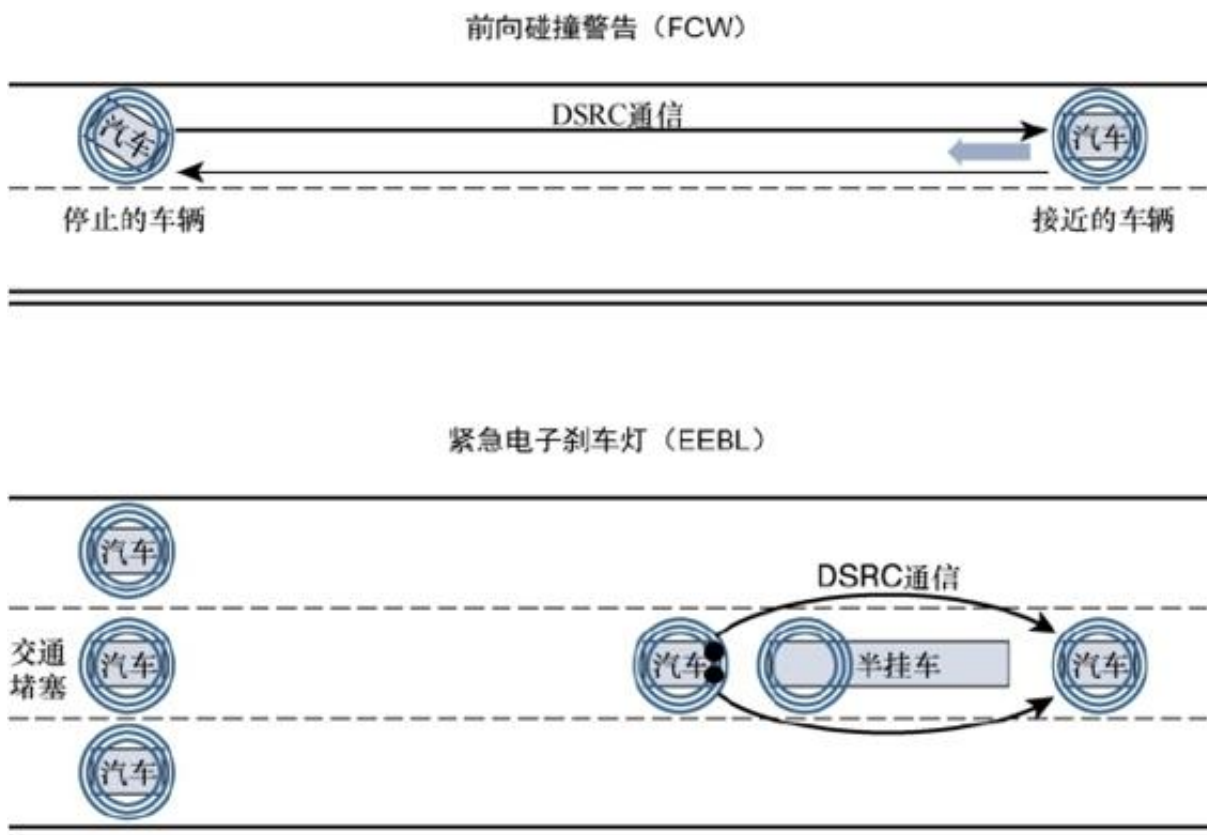


图13-4 DSRC紧急刹车警告

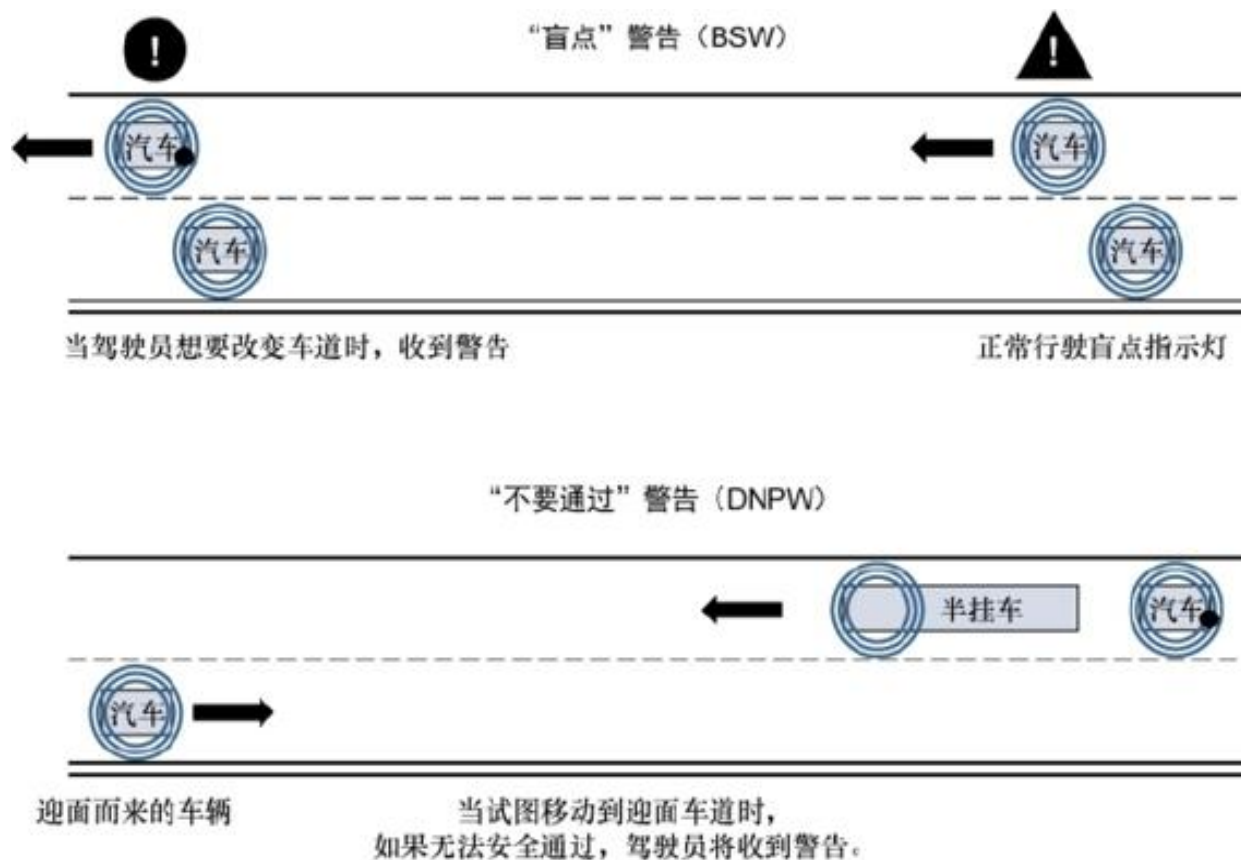


图13-5 DSRC盲点和不通过警告系统

■ 由于建筑物的原因，你在接近一个能见度低的十字路口。你的OBU已经获取其他车辆的位置和轨迹图，可以帮助避免碰撞。

这些应用对于道路上车辆的安全影响是显而易见的。然而，联网道路的物联网不仅仅关乎安全问题。我们可以执行私人应用程序，要求RSU将数据转发到互联网。在这种情况下，RSU只是一个IP转发器（它不需要处理数据）。前一节介绍了转发给汽车制造商的车辆诊断示例，但是还有许多其他应用程序。V2I应用程序能够满足车队管理的许多要求。在上述公用事业公司在暴风雨后调度车队的示例中，V2I允许卡车通过路边的RSU与公用事业公司控制中心进行通信，以补充直接的蜂窝通信。当车辆被送去维修时，它会自动上传状态和日志数据（服务记录、召回、过去的维修记录等），以便更好地执行现有维修任务。当返回基地时，卡车可以上传它们的记录（速度、装载细节、行驶时间等）。识别驶近的车辆对于限制停车、门禁控制甚至自动收

费都非常有用。同样，租车公司可以跟踪停车场上的每一辆车，以及里程、燃料油位和许多其他相关信息，从而加快租车运营。

4. DSRC/WAVE协议和架构

上一节主要讨论DSRC。然而，V2X的主流解决方案也使用802.11。我们还将接触到不同的术语，如WiFi、802.11p、WAVE、DSRC和ASTM标准E2213-03。理解以下术语之间的关系可能会有所帮助。

■ 专用短程通信（DSRC）：这是全球监管机构为满足汽车行业的需求在5.9 GHz频段内分配的频段名称，供智能交通系统（ITS）使用。美国的带宽是75MHz（由美国联邦通信委员会[FCC]分配）。在其他调控领域，带宽大小略有不同。然而，世界范围内的分配在相同的频谱范围内，并且相同的无线电和天线可以用于这些监管领域的任何实现。

■ ASTM标准E2213-03：美国材料试验协会（ASTM）开发了该标准。虽然这个名称表明它起源于美国，但ASTM实际上是一个创建标准的世界性非营利性组织。ASTM意识到FCC在1999年为DSRC分配的频谱区域也被WiFi使用。因此，ASTM修改了802.11使之适应于车辆通信。这项工作的结果在2006年以ASTM标准E2213-03发布。

■ WAVE（802.11p）：这是对802.11标准的一个修订版。802.11是由IEEE定义的，因此ASTM工作不可能直接集成到802.11中。2004年，IEEE 802.11工作组创建了802.11p任务组，以使802.11适应车辆通信。这个名为车辆环境无线接入（WAVE）的组织在2010年发布了修订版。

■ IEEE P1556和P1609：这是一系列与车载通信相关的协议。当802.11小组致力于研究WAVE时，在车辆和基础设施之间传输信息的想法引起了人们对隐私的担忧。另一个IEEE小组创建了P1556（包括智能卡通信在内的车辆/路边通信的安全和隐私标准）。这个标准被重新编

号为 IEEE 1609.2，并被整合到表 13-1 所列的更大的P1609系列WAVE协议中。

表13-1 与DSRC相关的IEEE P1609系列标准

标准编号	标准名称
IEEE P1609.0	WAVE 标准草案：架构
IEEE P1609.1	WAVE 试用标准：资源管理器
IEEE P1609.2	WAVE 试用标准：应用程序和管理消息的安全服务
IEEE P1609.3	WAVE 试用标准：联网服务
IEEE P1609.4	WAVE 试用标准：多信道操作
IEEE P1609.11	智能交通系统（ITS）空中数据交换协议

这些标准之间的关系有点复杂。例如，WAVE基于802.11p，但是它的P1609方法涉及一般车辆环境的无线接入，而不仅仅是前两层。图 13-6总结了这些标准和OSI模型之间的相互作用。

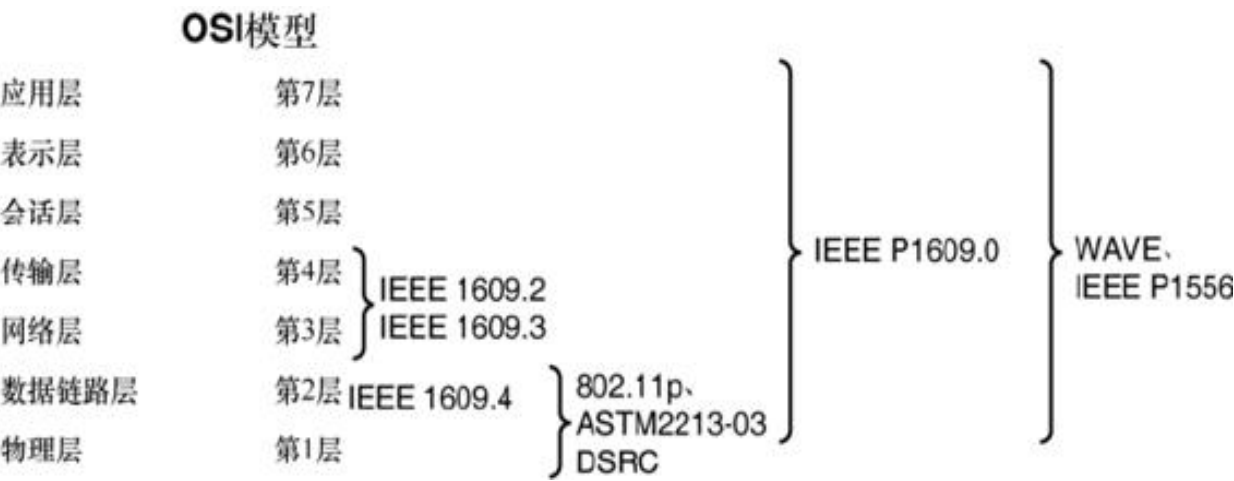


图13-6 DSRC、WAVE、802.11p、IEEE 1609和OSI模型

美国汽车工程师协会（SAE）也定义了适用于WAVE的标准。SAE J2735定义了通过DSRC实现的消息传递模式，以支持V2I和V2V数据交换，SAE J2945定义了DSRC系统的最低性能要求。

基于802.11的DSRC/WAVE通信是半双工的。802.11物理和数据链路层针对高达90公里/小时的速度进行了优化。对于车辆通信，802.11也进行了修改，以允许不需要接入点的通信。当车辆快速行驶时，不需要依赖接入点和强制身份验证/关联消息。因此，没有关联的通信是可选的（也是允许的）；如果需要，单元或基本服务集（BSS）的概念仍然存在。802.11p建立在802.11修订版的基础上，集成了QoS的概念和不同帧类型的各种统计优先级（在2005年由802.11e定义）。

DSRC是由地方监管机构推动，例如美国联邦通信委员会（FCC）等；与欧洲标准化委员会（CEN）合作的欧洲电信标准协会（ETSI）；以及日本无线电工业和商业协会（ARIB）。每个管理机构都定义了DSRC允许的频率和无线电输出功率。

例如，在美国，可用频谱被划分为7个10 MHz宽的信道（信道172、174、176、178、180、182和184），在典型的300~1000米范围内允许6~27Mbit/s的数据速率。如前一节所述，通信178位于频带的中间，被设计为控制信道，有些信道是为特定的通信需求保留的（例如，信道172用于基本的安全消息传递）。

其他监管机构决定道路规则。例如，在美国，国家公路交通安全管理局（NHTSA）决定哪些车辆设备在美国公路上得到授权或被强制使用。在政府的推动下，该机构正在制定新规则，可能要求DSRC在2020年之前在所有车辆上运行。

DSRC是V2I通信的主要协议，但它不是在车辆和道路交换中涉及的唯一协议。表13-2比较了DSRC与其他用于互联道路的协议。

表13-2 互联道路协议

特点	DSRC/WAVE	WiFi	蜂窝网	移动 WiMAX
数据传输速率	3~27 Mbit/s	6~54 Mbit/s	<2 Mbit/s	1~32 Mbit/s
移动速度	>90 km/h	<10 km/h	>90 km/h	>90 km/h
标称带宽	10 MHz	20 MHz	<3 MHz	<10 MHz
运行波段	5.86~5.92 GHz (ITS-RS)	2.4 GHz、 5.2 GHz (ISM)	800 MHz、1.9 GHz	2.5 GHz
IEEE 标准	802.11p (WAVE)	802.11a	N/A	802.16e

13.4.2 互联道路网络架构

公路物联网的基础在于两个要素：车辆设备和路边设备。

车辆携带OBU。OBU不是独立工作的，它需要从其他传感器收集信息，如车辆定位单元（VLU），也称为自动车辆定位单元（AVL）。车载计算机需要处理有关车辆的数据，并将其发送到云或其他车辆。计算机辅助调度（CAD）是该函数的通用名称。CAD最初是为调度车辆和技术人员设计的，但后来扩展到包括任何车辆数据和应急管理软件。通常需要一个加固的路由器来连接这些不同的元件。

路侧设置有RSU。由于RSU也是一个IP转发器，它通常还包括一个加固的路由器。RSU可以通过无线技术与主干网络通信。然而，以太网和光纤是常见的选择，因为道路、街道和路边装置越来越普遍地配备了有线通信设施。RSU还可以连接路灯。在这种情况下，可在RSU或路灯处安装具有交通信号优先权（TSP）能力的交通信号控制器（TSC）。该功能允许应急车辆在RSU范围内通过DSRC控制路灯。

一些RSU路由器可以连接到一个普通的加固的交换机（仍然在路边层）。然后通过城域网络传输数据。MPLS是这一领域的一种常见技术。聚合路由器从多个街道级交换机收集流量。电信级路由器是互连网络的核心。

然后将数据转发给不同的参与者（汽车制造商、车队管理控制中心、交通管理部门、应急服务部门等），在这些参与者的数据中心中对数据进行处理。图13-7总结了联网道路的物联网网络架构。

请注意，OBU/RSU架构与V2X物联网相关。当传感器直接集成到路边的物体中时（也就是说，路边的物体不是用来与车辆通信的，而是用来收集它们自己的数据集，如桥梁振动监测），要转发的数据量更为有限。此外，传感器可能位于有线连接不实用的地方。在这种情况下，像LoRaWAN这样的远程技术更为常见。第4章详细讨论了LoRaWAN。

1. 互联车队架构

图13-7所示的架构也与车队管理相关。与单个车辆相比，车载CAD/AVL VLU模块更是一个关键元素。自动车辆定位（AVL）系统依赖于卫星GPS信号，有时还依赖于低频的地面无线网络。车辆的位置需要传送到操作中心。这种通信通常使用GSM。一些组织（如公用事业和紧急服务）可以强制建立双GSM连接，以确保总是可以发送车辆信息，即使是在一个服务提供商的低覆盖区域。

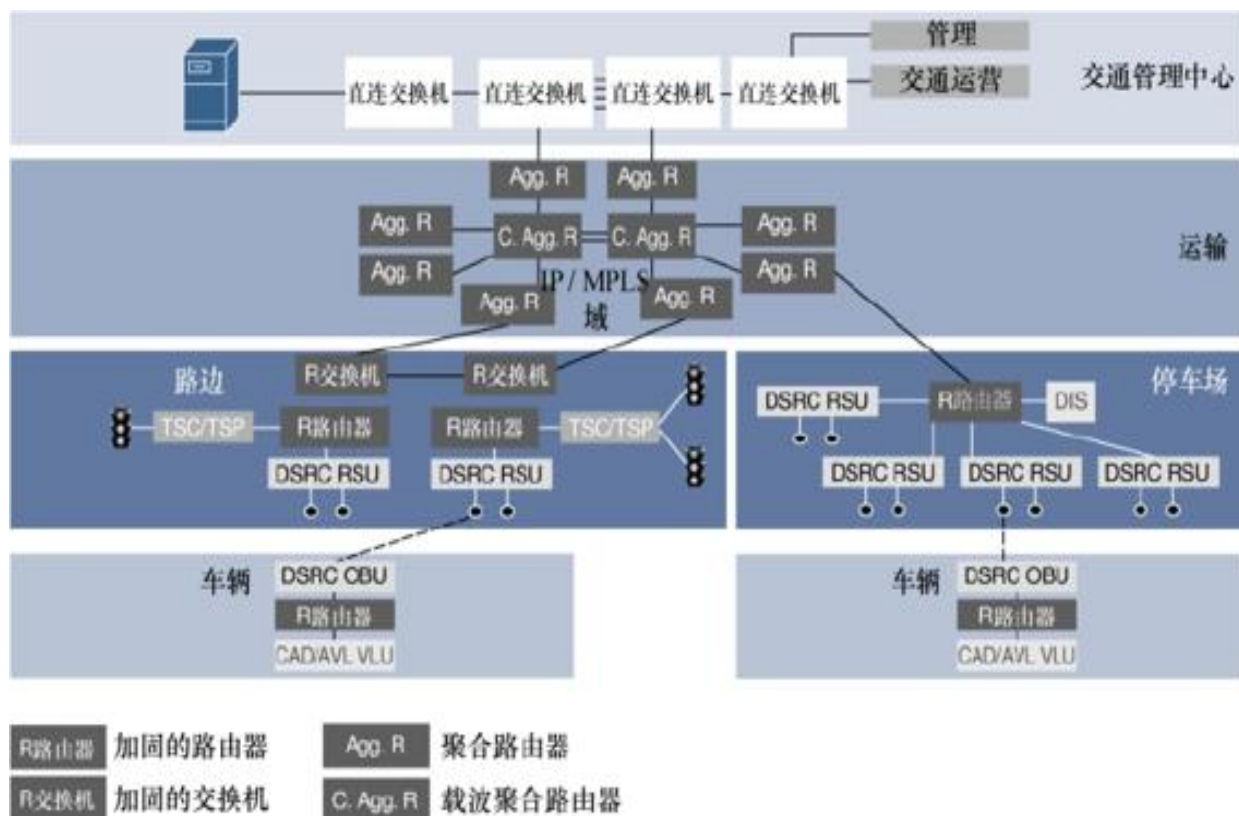


图13-7 互联道路物联网网络架构

通信必须是双向的。也就是说，控制中心还需要与司机沟通当天的任务。该功能是通过车辆上的计算机辅助调度（CAD）模块来实现的，该模块允许乘员和控制中心之间进行信息交换。这种实时交流可以更好地利用机组时间表，将发生的事件纳入时间表。计算机辅助设计还减少了通信成本，并通过允许机组人员向控制中心报告任何异常事件来提高操作安全性。一些车队可能还会安装监控摄像头。例如，快递公司可能会在车辆周围安装摄像头，以便在车辆停放和司机递送包裹时监控偷窃行为。同样，当公用事业的卡车停在路边时，公用事业公司可能需要捕捉其他车辆的行为。在这些情况下，有一个或多个摄像机用于捕获和存储数据。当车辆返回基地时，使用WiFi将录音上传到存储服务器。

根据这个逻辑，车辆包括一个连接摄像头和机组CAD系统的交换机（通常是一个平板电脑或笔记本电脑，可以安放在车内，当驾驶员需要处理车辆外部的信息时，可以将其卸下）。路由器包含蜂窝模块和

WiFi客户卡。这张卡是用来连接停车场里的WiFi系统的。路由器还可以作为连接平板电脑或WiFi手机的接入点，如图13-8所示。

因此，车辆在路上时的通信架构与车辆在停车场里时的通信架构略有不同。总体架构如图13-9所示。

当车辆在路上行驶时，大多数情况下通过蜂窝连接进行通信。移动服务提供商网络连接到操作中心，操作中心会存储和分析数据、位置和CAD系统，并与每辆车交互。

这种结构对于任何类型的车队都是相同的，包括公共交通工具（例如公共汽车），本章后面将进一步讨论。在公共汽车上，公共汽车站也配备了蜂窝网络连接（或在密集的城市环境中配备WiFi）以向运营中心提供信息（例如，在公共汽车站基于视频自动对乘客计数），并将信息返回到汽车站（例如，带有等待时间的智能面板）。

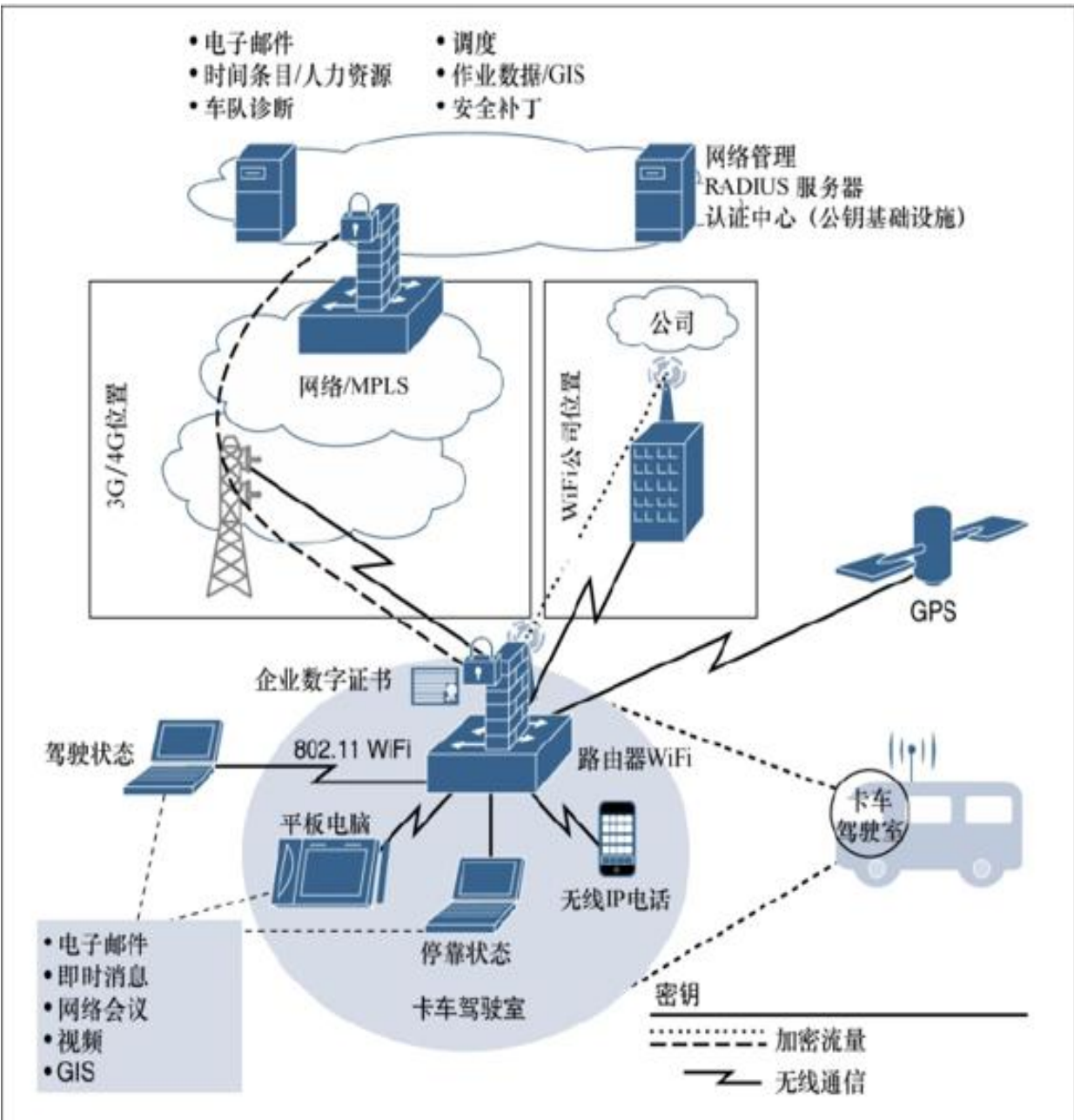


图13-8 车队管理架构

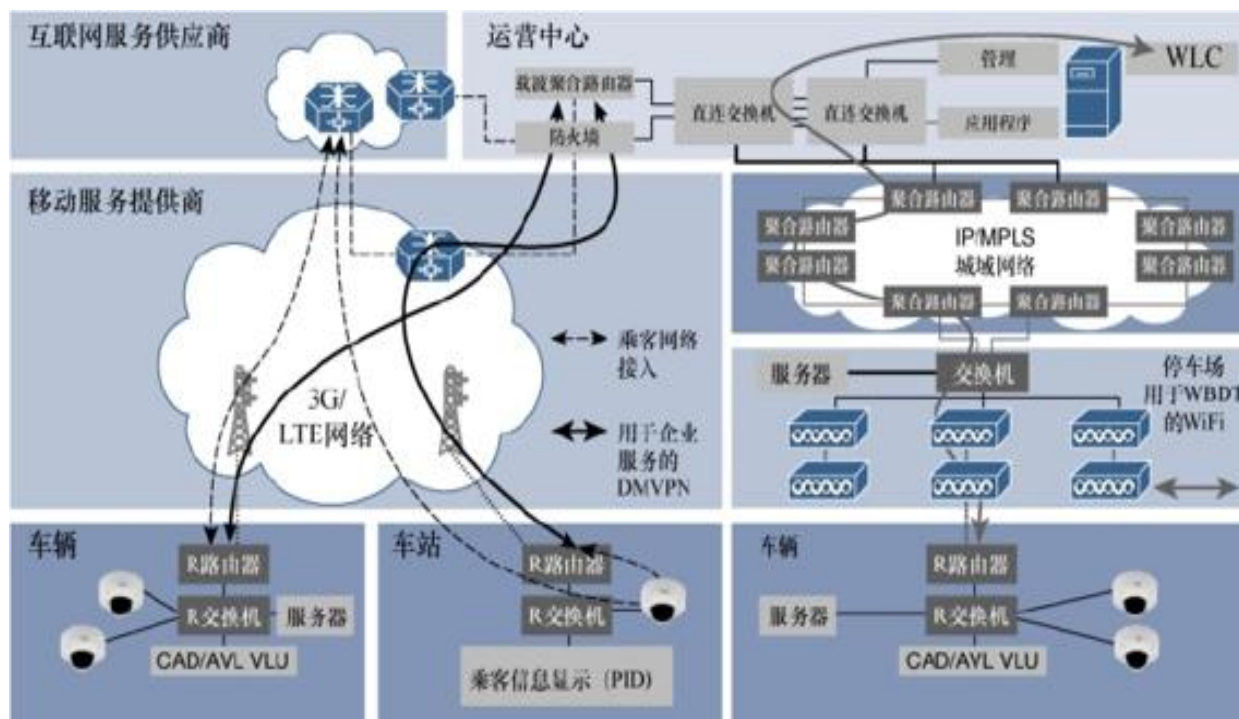


图13-9 互联车队架构

当车辆停在停车场中时，允许通信使用WiFi上传记录的数据（车辆参数、车载摄像头记录等）。每个停车场的WiFi接入点通常通过IP/MPLS城域网与中央运营中心进行通信，在中央运营中心，由一个中央无线LAN控制器负责管理通道、电源和单独车辆的WiFi连接（认证、防火墙等）。

控制中心的运营管理是物联网的关键要素。系统需要安全地连接到每辆车的车载系统，并检索有关车辆的信息（燃料、各种设备的状态、位置等），也可能连接到数以百计的其他系统（客户交互中心、票务或计费、日计划、燃料或零件供应链，以及专业的设备管理系统，如卡车车斗、车载摄像头等）。管理系统还可能与智能系统交互，智能系统分析从现场收集的特定数据，为系统提供可执行的分析结果。轮胎和油压是明显的例子，但该系统也可以监控车辆上还有多少米的电线可用，或监测执行危险任务的司机的生命特征值。

虽然车辆主要与控制中心通信，但互联网连接也允许与第三方（例如，车辆部件制造商或各种维修承包商）进行通信。

车队管理也受益于V2V通信。越来越多利用这些交换的示例是排队。大型18轮卡车没有针对空气阻力的问题进行形状优化；相反，它们的形状针对最大货物装载量进行了优化。因此，它们消耗大量的能量只是推动卡车质量通过空气，空气以湍流的形式回流到卡车后面几十米处，而卡车后面的空气则以卡车的速度流动，排好队后，几辆卡车近距离地彼此紧跟着。这种结构有以下几个优点。

- 只有第一辆卡车消耗空气穿透能量。后面的卡车停在安静的区域，并受益于第一辆卡车的空气轨迹。

- 这些卡车占用的路面空间较少，它们形成一个紧密的块而不是一条长线。

- 使用V2V通信，整个车队实现零反应时间。当第一辆卡车刹车时，后面所有的卡车也以完全相同的方式立即刹车。这为整个车队提高了行驶过程中的安全性。

- 由于后面的每辆卡车都是根据前一辆卡车的速度来设定速度，所以不需要每个司机主观判断前一辆卡车的速度，在油门踏板和刹车之间交替切换，以适应变化和地形。协调的交流允许跟随者简单地模仿第一辆卡车的速度模式，从而降低燃料消耗。

卡车排队不是自动驾驶，因为每辆卡车都有一个司机。卡车之间通过V2V通信的协调优化卡车之间的行程。在控制中心，每辆卡车以及司机的行动都会受到监控。然而，整个车队可以作为一个单一的块。

2. 连接道路安全

当司机或个人信息被传输时，安全性迅速成为首要问题。P1609.2讨论了DSRC与其他车辆和基础设施通信的安全性。虽然每辆车都有一个标识符，但该标识符仅在局部有效；周围的车辆不会将某辆车的车辆标识符与汽车制造商、车型或驾驶员相关联。RSU也不转发此标识符。同时，OBU识别RSU（信道178上使用基于证书的身份验证的消

息），以避免恶意消息的注入。驾驶员与汽车制造商之间的通信是加密的。在车里，传感器至控制单元越来越受到协议的保护，如802.1 Xbx（一种协议，为基于端口的网络访问控制提供MACsec密钥协议[MKA]协议扩展），以避免任何第三方连接到汽车内部通信系统，从数据中获取出行或开车的方式。

13.4.3 将道路物联网架构扩展到公共交通

前面描述的道路解决方案也可以用于公共交通，本节以公共汽车为例。特别是DSRC可以用于维修厂，以优化和加快车队的维修。DSRC还可以在行驶过程中用于将位置和轨迹（以及运行数据，如燃料水平、轮胎压力和其他可能指示公共汽车需要维修的元件）传递到控制中心。这些位置和轨道数据可以用来评估交通拥堵和估计到达公共汽车站的时间。

然而，公共交通已经不仅仅局限于公共汽车（下一小节将讨论火车的体系结构）。此外，公共汽车需要扩展DSRC所提供的功能之外的功能。

公共汽车并不总是在配备有RSU的城市中行驶，它们也并不总是被其他配备有OBU的车辆所包围。因此，将物联网应用于公共汽车归根结底是满足一种需求，而不是实施特定的技术。

- 公共汽车需要传达有关其位置的信息。这是基本的GPS数据。还需要关于公共汽车状态的技术信息。

- 公共汽车通常使用摄像头以确保安全。这些摄像头可以在本地存储录像，并在公共汽车返回车站时通过WiFi上传录制的内容。但是在发生警报或紧急情况时，也应提供远程访问功能。

- 用户喜欢在旅途中上网。

定期发送GPS坐标或基本车辆状态信息不需要DSRC架构。一个简单的蜂窝式发射机就足以满足这种需求。当车上装有摄像头时，蜂窝网

络还可以向中央监测站提供实时访问（或发送警报信息）。中央车站还可以关联其他公共汽车的信息来计算乘客或道路交通负荷，并在适当的时候建议拥堵点周围的替代路线。这里的目的不是要跳站（尽管中央管理系统可以计算出跳站可能是有价值的），而是避免由于事故或异常高负荷的阻塞点而造成的障碍。

公共汽车内可以安装WiFi接入点，为乘客提供互联网接入服务。蜂窝数据连接可以在需要的距离上中继通信。在某些情况下，当WiFi沿着公交线路部署时，可以使用工作组桥（配置为客户端的接入点）将公共汽车连接到市政WiFi基础设施。即使当公共汽车在维修站时，也可以使用这种WiFi连接。

公共汽车司机可能还需要与基站保持联系。这种通信可以使用专用的无线电设备或智能手机，也可以直接连接到蜂窝网络或通过公共汽车WiFi连接。因此，与图13-8和图13-9所描述的车载架构相比，公共汽车的车载系统如图13-10所示。

在公共交通方面，物联网并不局限于公共汽车本身。公共汽车站可以配备加固路由器，允许WiFi连接（在市政WiFi接入的情况下）或蜂窝网络连接。雾计算平台接收来自云的更新，屏幕显示下一辆公共汽车的到达时间，以便乘客可以决定他们是应该乘坐拥挤的公交车还是等待下一辆。也可以显示公共汽车负载信息。智能面板也可以连接到控制中心系统来显示行程信息。该面板可以显示城镇地图，以及当前的拥堵点。该面板还可以提供两点之间的最佳路线建议，以帮助乘客优化他们的出行时间。

最后，公共汽车站还可以配备一个基本的状态检测器，用于近似估计等待公共汽车的人数。这有助于控制中心决定是否需要沿着这条路线调配更多车辆。当一个站点位于一个非常拥挤的区域时，该计数器还可以帮助正在驶近的巴士司机判断是否走捷径和跳过一个站点。

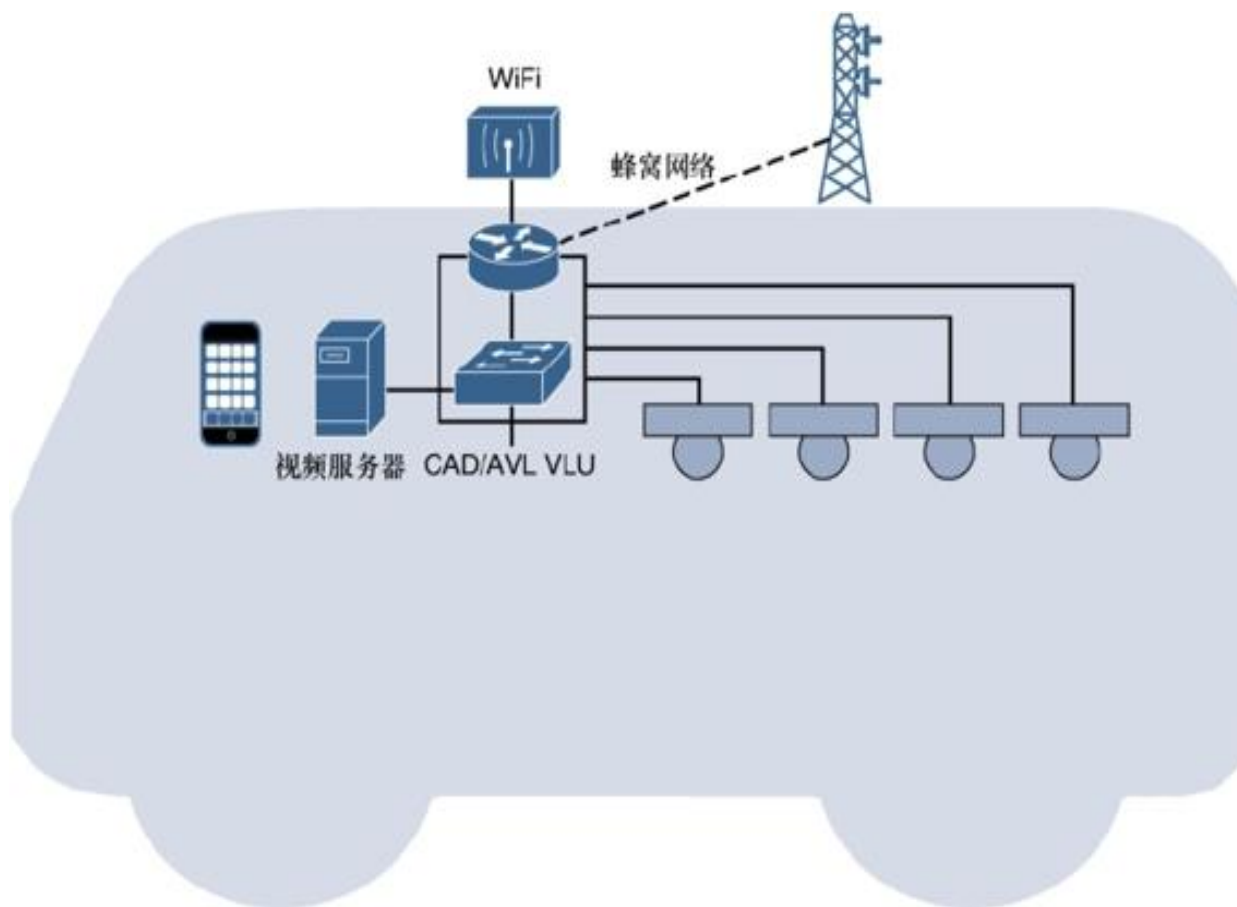


图13-10 公共交通：公共汽车车载系统架构

公共交通安全

乘客通常直接通过蜂窝网络上网。在某些情况下，公共汽车（和车站）可以配备内容防火墙和过滤器。特定于公共汽车的数据（视频监控、停止和出行管理、与司机的通信）通常是加密的，并通过VPN连接传输到运行中心。第15章详细介绍了校车视频监控的架构。同样的逻辑和架构也适用于市政公共汽车。

13.4.4 将公交物联网架构扩展到铁路

铁路的物联网通信架构在很多方面与公交系统相似。在这两种情况下，车辆位置跟踪都是在云端处理的，并传送到车站或车站的智能面板上，这可以帮助出行人员找到最佳的交通方案，并了解城市的拥

堵点。对于货运客户，货物位置可以实时跟踪。当然，铁路通常不拥堵，但事故可能会扰乱交通。对于乘客来说，智能面板可以显示所有的出行选项（地铁、电车、公共汽车），而不仅仅是铁路选项。

火车上的系统与公共汽车上的系统略有不同。尽管WiFi连接类似，火车也使用传感器，然而，火车传感器位于不同的位置，并监控来自公共汽车传感器的不同元素。火车是较大的交通工具，因此包含更多的部件，如图13-11所示。

图13-11中的顶层汇总了火车和公共汽车的需求。由于火车出行时间可能比巴士出行时间长，乘客通常更希望在火车上获得信息娱乐等客运服务。这些客运服务显然不适用于货运。

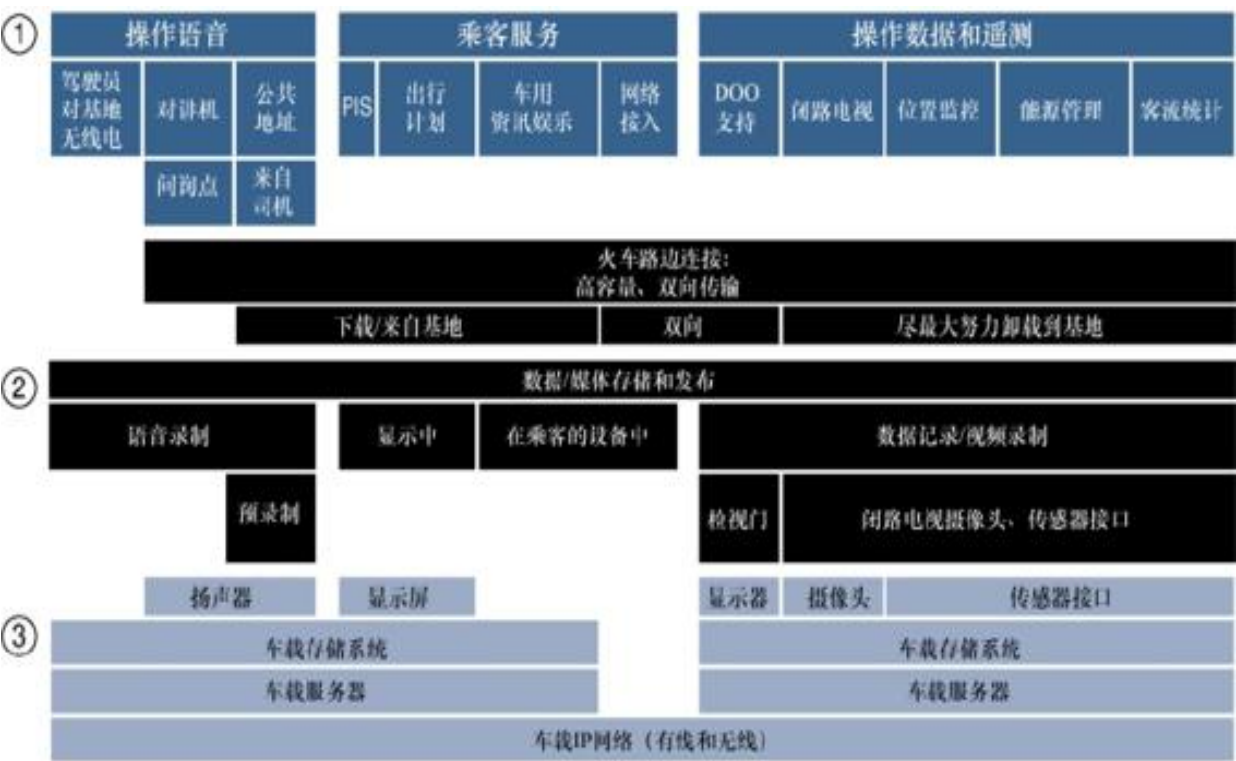


图13-11 列车物联网技术组件

图13-11的第二层描述了用于满足火车需求的通信基础设施。这一层与公共汽车的对应层不同。火车是在轨道上运行的，这意味着它们的路径是可控制和可预测的，从而允许更多的确定性连接。可以在铁路沿线建造专用的通信系统，供所有过往火车使用。闭路电视录像

（全流程或触发片段）和传感器信息可以上传，预先录制的信息（匹配目标事件）可以在需要时推送到列车上。旅客上网流量也需要通过铁路线路中转。这需要高容量的双向传输。

图13-11的第三层描述互联列车架构中涉及的对象，从传感器、摄像机和显示器到车载服务器和存储系统。所有这些都需要连接（因此需要一个IP网络）。

最终的物联网网络架构如图13-12所示。

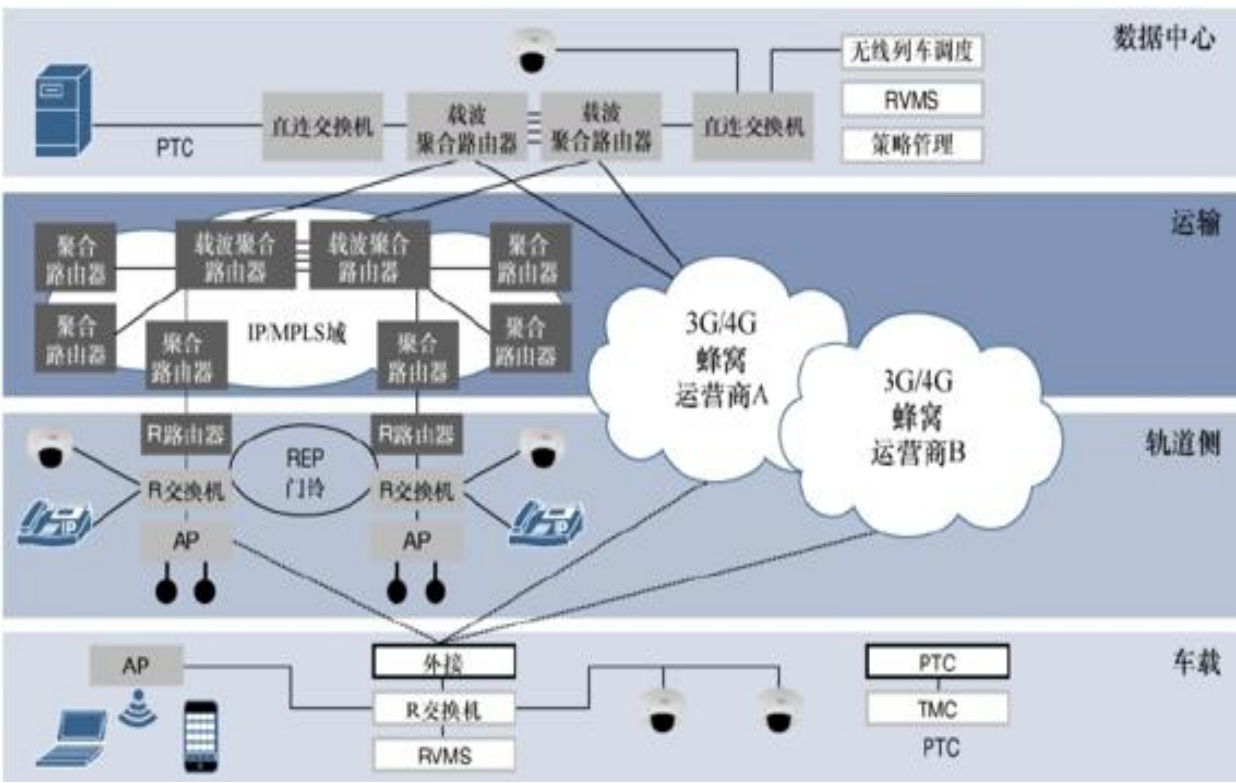


图13-12 互联铁路物联网架构

在列车内部，列车主动控制（PTC）和列车管理计算机（TMC）系统集成成了控制列车运行的命令、控制、通信和信息网络。列车车辆管理系统（TVMS）提供详细的维护信息和设备状态。这些系统与其他传感器、摄像机和WiFi接入点一起，通过一个以太网交换机进行连接，该交换机应该是加固的。根据环境的不同，列车与位于轨道沿线的蜂窝网络或WiFi户外AP进行通信。这些户外AP连接到交换机，通常围绕健全的冗余链路协议组织（如弹性以太网协议）；铁轨侧的摄像机也

可能与其他设备（具体的传感器、IP电话等）连接到相同的交换机。坚固耐用的路由器连接到网络传输端，其结构在概念上与其他大规模运输系统相似。在大多数情况下，数据被直接发送到铁路公司的数据中心。但是，有些数据可能会重新路由到第三方数据中心（例如，货运客户、食品或部件供应商、其他承包商）。

公共汽车和火车公共交通架构的主要区别在于与基础设施网络的连接。公共汽车通常包括一节车厢。相比之下，火车由多节车厢组成。每辆车都有传感器、摄像头、WiFi接入点和通信系统（例如，扬声器、员工电话）。他们需要与铁路沿线的基础设施以及在彼此之间进行通信。一个完全分布式的系统可以实现每辆车的完全自治。每辆车都有自己的摄像头、交换机、传感器、AP、通信模块、加固的服务器（用于视频监控、传感器数据存储等）和路由器，与铁路边的基础设施独立通信。然而，这种分布式模型的成本高昂。半分布式模型更为常见，如图13-13所示。

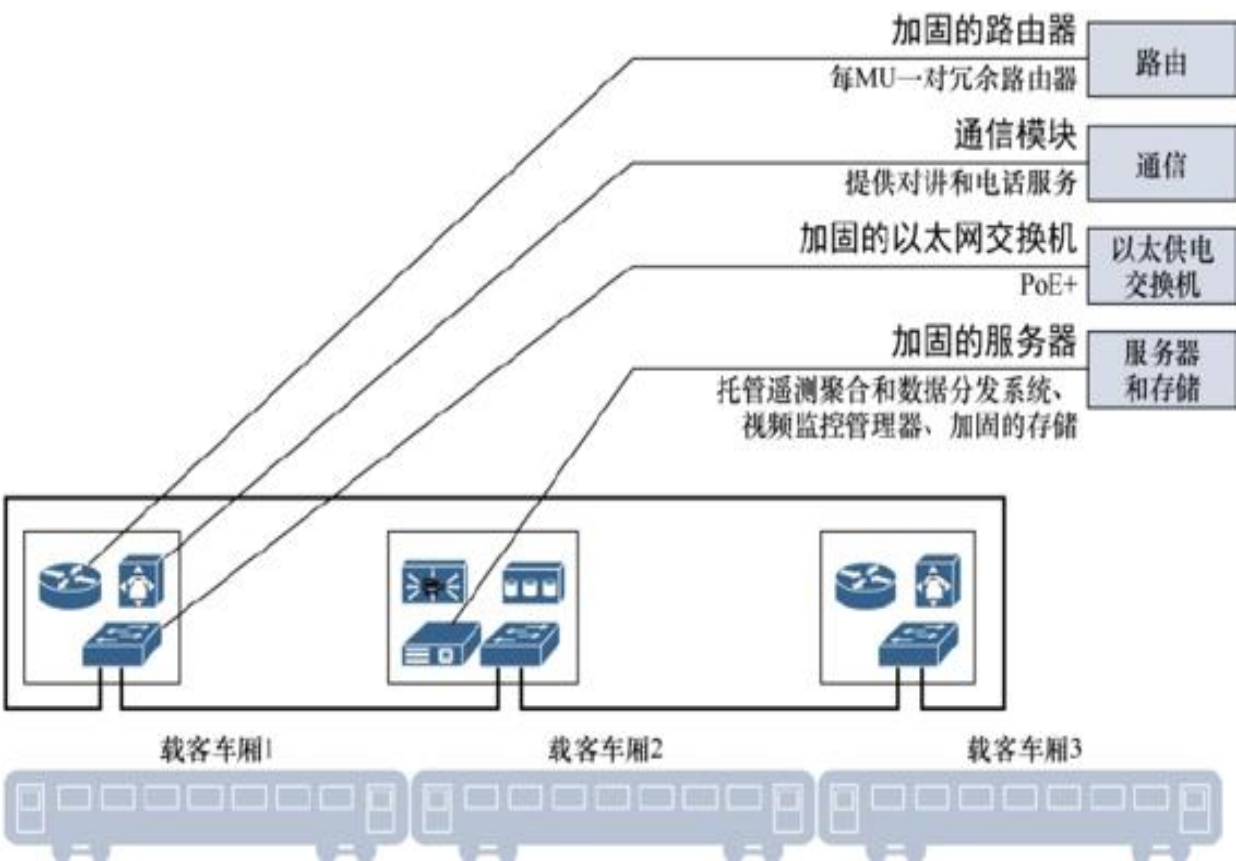


图13-13 列车半分布式车载物联网模块化架构

在这种半分布式模型中，每个车厢都有自己加固的交换机、摄像头、传感器和AP，用于实现其监控和连接功能。但是，火车车厢有不同的类型（图13-13中的示例中有3种），每种类型都添加了一个特定的组件，而不是在所有火车车厢中都存在的组件（例如加固的路由器、通信模块或服务器）。火车车厢之间的连接允许火车车厢共享这些功能。当列车组装完成时，铁路运营商需要确保每一种类型的车厢都是足够的，以实现列车的全部功能。

车厢与车厢之间可以用电线连接。然而，WiFi连接也很常见。在这种情况下，网状WiFi网络是一个非常灵活的结构。其中一个AP（通常是与包含路由器的车厢相关联的AP）充当根接入点（RAP），而其他车厢中的AP是网状接入点（映射），如图13-14所示（关于网状WiFi的详细讨论，请参阅第14章。有关网状网络拓扑的详细信息，请参阅第2章）。

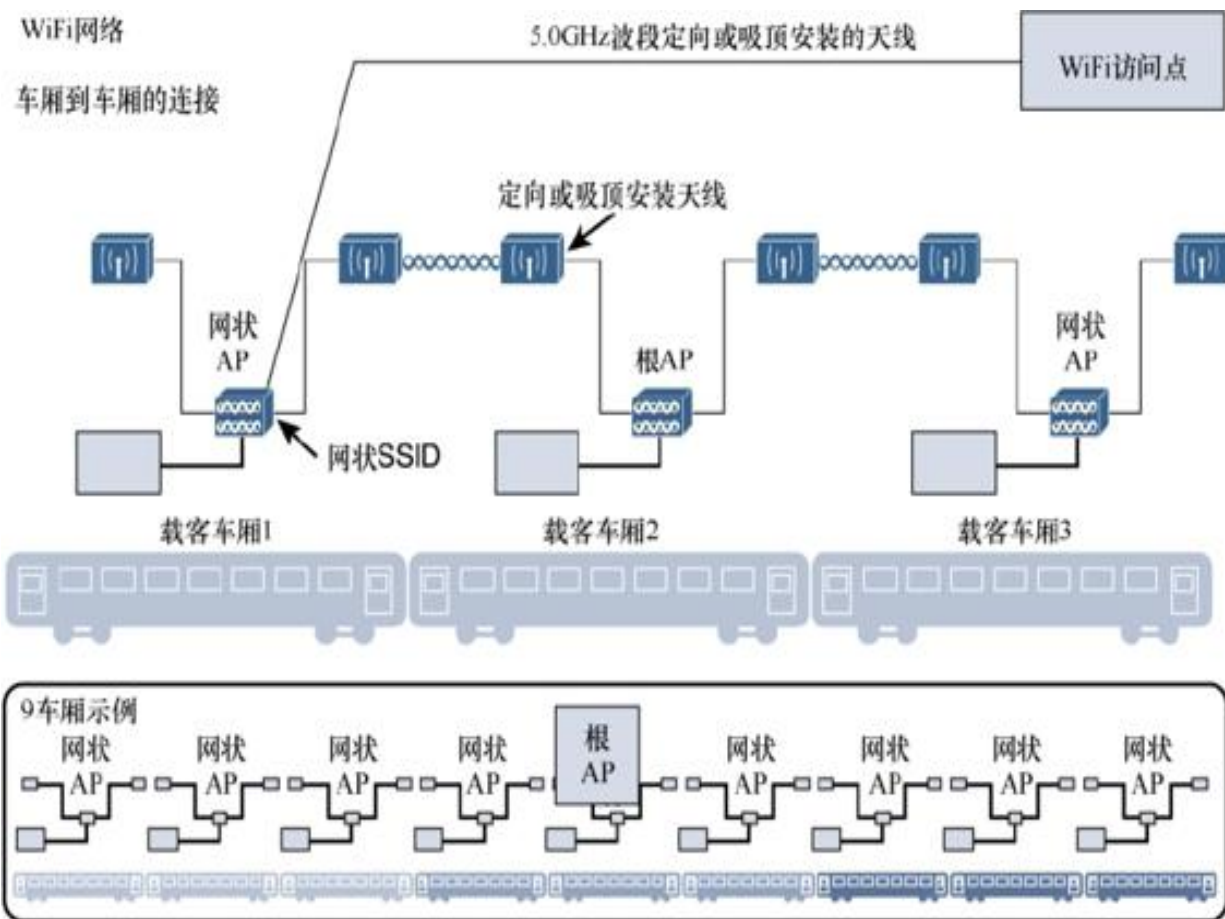


图13-14 互联列车的车厢到车厢WiFi

无论车厢上是否提供WiFi，都可以实现车厢间的WiFi连接。当提供WiFi接入时，2.4 GHz频段通常用于乘客接入，5 GHz频段用于网状回程连接，如图13-15所示。

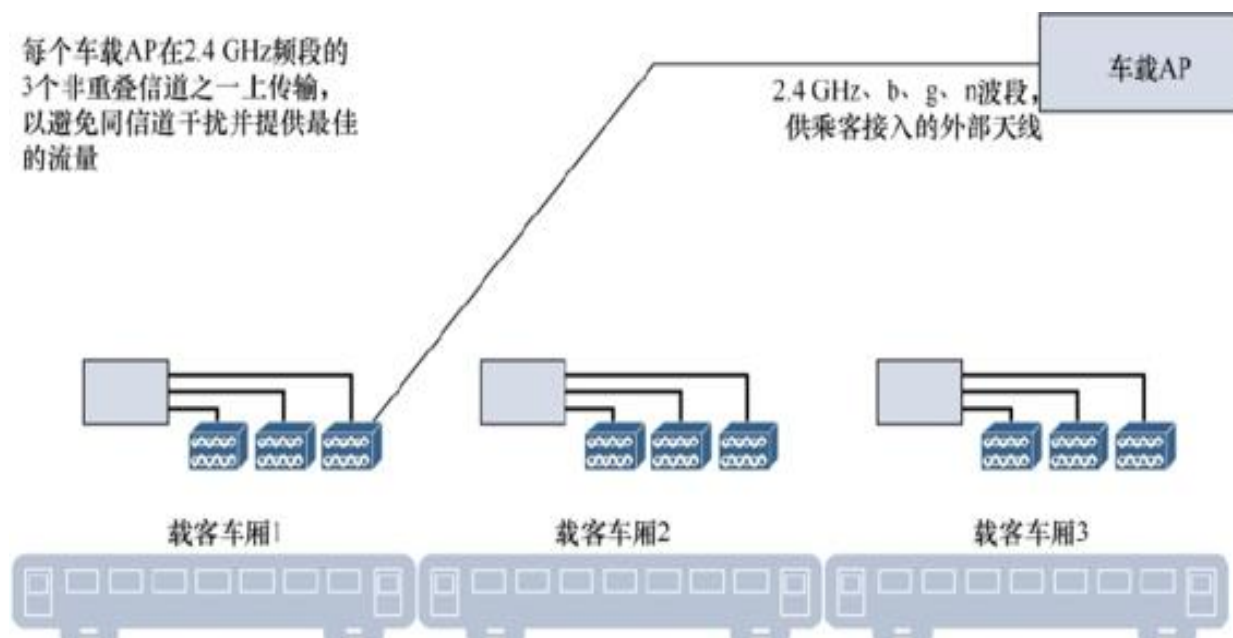


图13-15 车载WiFi

每节车厢包括一个或多个AP，以在整个车厢中提供一致的覆盖范围。流量被聚合并传递到网状网络，然后沿RAP转发。RAP可以通过路由器连接到路轨无线系统（蜂窝）甚至卫星连接。当轨道沿线有WiFi连接时，RAP可以连接到另一个配置为无线客户端的AP（例如，工作组网桥[WGB]）。

利用轨道旁的WiFi功能，可以在列车内提供不同的吞吐量。更高的吞吐量要求部署更多的WGB。每个WGB都连接到轨道旁的WiFi基础设施，如图13-16所示。

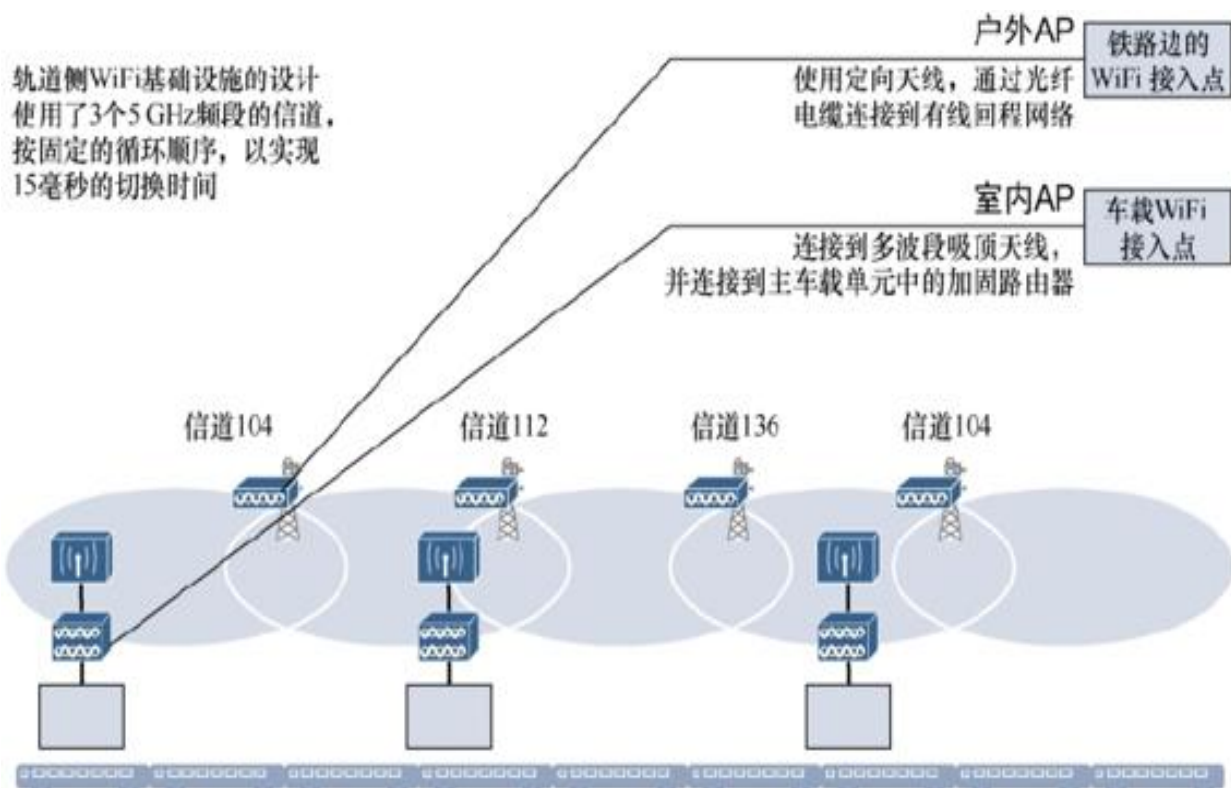


图13-16 轨道侧WiFi网络连接

其中一个挑战与列车运行的速度有关。每个WGB需要从一个钢轨漫游到另一个钢轨。漫游需要保持在15毫秒以内，以避免通信中断。这一要求规定了轨道侧AP的位置、间距和天线类型。

1. 连接站点

用于交通运输的物联网不会仅限于火车或公共汽车，它还延伸到车站或货运站。公共汽车站是小型实体，物联网涉及智能面板、为等候的乘客提供WiFi，以及为安全和乘客计数提供摄像头。火车站要大得多，需要允许多种服务的连接，包括智能面板和数字标牌、票务系统、照明和空调系统、视频监控以及多个第三方系统（ATM、停车场、商店等）。车站还需要包括公共广播系统和一套丰富的传感器来监测列车和车站的活动。货运站还包括货运跟踪和调度系统。

所有这些系统都需要通过共享的IP基础设施进行通信。此外，火车通常会在车站上传一次核心数据。车站操作需要接收这些数据并进行处理。因此，车站也需要连接到操作员数据中心。

2. 互联火车的安全

由于聚合的IP网络上存在多种类型的数据，因此安全性是首要考虑的问题。第三方终端通过VPN与其相关的数据中心进行通信。虽然传感器和票务系统的安全性可能共享相同的基础设施，但物理安全性与流量隔离相结合（例如使用802.1AE之类的协议）。802.1AE也称为MACsec，是一种协议，它通过独立于媒体访问的协议和实体指定无连接的用户的用户的数据保密性、帧数据完整性和数据来源真实性，而且这些协议和实体对MAC客户端是透明的。802.1X还应用于控制对网络的访问。唯一的例外是车载WiFi系统，它通常使用Web身份验证，而且没有加密。然而，尽管有些难以管理，使用额外的预共享密钥（PSK）越来越普遍。

13.5 小结

随着私人 and 公共交通系统的爆炸式增长，与安全性、出行体验和出行可预测性相关的挑战也越来越多。

为了应对这些挑战，汽车制造商以及交通和安全部门采取了几种方法。通过物联网可以提高这些方法的效率，从而实现车辆互联、道路互联、公共交通互联和铁路互联。

在单个车辆级别，多个传感器可以提供车辆状况的主动性视图，从而限制意外故障的发生。与此同时，智能车载系统允许车辆动态反应并适应周围环境，从而提供更好的出行体验。

基于802.11构建的技术（比如DSRC）允许车辆与路边的基础设施交换信息。这种交换对车辆是有益的，它现在可以接收本地的重要警

告。专用车辆（如应急服务）也可以使用这个通信系统，在通过交叉路口时获得特权访问。私有应用程序可以利用该系统进行车队管理或车辆监控。

这些单独的车辆物联网也有利于公共交通工具（如公共汽车和电车）。物联网使交通管理局对交通状态有一个全局的、动态的、适应性的看法，预测维护需求，并根据网络中不断变化的用户密度调整运输方案。

旅客可以通过更高效的交通系统直接看到这些好处，也可以通过公交或火车站的智能面板看到这些好处。列车也可以利用这些系统，增加车辆在固定轨道上行驶的细节。

第14章 采矿业

“采矿”一词常与黑白老照片联系在一起，老照片中，勤劳的工人扛着镐和矿灯进入黑暗的地下隧道，将矿石或废石装入小型轻轨车辆中。虽然这些照片准确记录了历史，但技术已经使采矿业取得了重大进展，特别是在安全、生产优化和降低运营费用方面。

在最基本的层面上，采矿就是从地球上提取矿物的过程。今天有许多种类的矿物被开采，包括铜、金、银、锂、钼、铁、盐、钾、煤、铀和宝石。大多数矿物，尤其是贵金属，很少集中在地表下某个位置，等着别人来捡。相反，它们与地表下的其他物质混合在一起。以铜矿石为例，其平均体积量不到1%。

为了分离和提取所需的矿物质，我们必须分解大量的土壤并将其运送至加工厂，在那里泥土被进一步分解，并使用各种技术来分离所需的材料。采矿作业中使用的技术和技艺同其他制造业和运输业有许多相似之处。因此，本章讨论的许多物联网原则除了与采矿相关外，还有其他的意义。

采矿一般可分为3大类：地面采矿、地下采矿和水下采矿。本章主要讨论前两类。在这3个采矿类别中，也有3种主要的矿物类型：煤、金属和非金属。

在大多数国家，采矿活动受到管制。例如，在美国，采矿由美国劳工部管理，隶属于矿山安全与健康管理局（MSHA），并且在每个州都有监管。在矿山工作通常需要国家监管机构（如MSHA）的专业培训和认证。在其他国家，采矿类型和开采过程也受到管制。

矿山的生命周期远远超出了矿物质的开采周期，如图 14-1 所示。矿山的勘探、规划、建设、运营、环境监测、关闭和复垦等方面都需要投入大量的时间和工作。然而，本章主要关注的是运营，这是矿山生命周期中最长的部分，通常以数十年为单位进行衡量。

本章包括以下部分。

■ **当今采矿业及其挑战：**本节概述采矿业，并将帮助您了解该行业的工具、规模、限制和挑战。

■ **物联网在现代采矿业中的挑战：**本节探讨在采矿业环境中部署物联网解决方案的具体挑战。

■ **采矿业物联网战略：**本节详细介绍物联网改善采矿作业的多种方式，从提高安全性和效率到雷电和危险气体安全、坡度和环境监测以及定位服务。

■ **采矿业物联网体系结构：**本节详细介绍用于采矿业的物联网网络的体系结构，从客户端到访问层，再到核心网络及其安全性。本节还将讨论应用层，并举例说明大数据如何改变采矿业的运营方式。



图14-1 采矿业的生命周期

14.1 当今采矿业及其挑战

在过去50年中，采矿作业的规模有了巨大的增长，与此同时，开采矿物的工艺和效率有了很大的改进。现代采矿业的安全性是有史以来最高的。然而，现代采矿业经营者仍然面临许多挑战。

14.1.1 规模

对于外行人来说，关于现代采矿业最难以理解的概念之一是许多采矿作业的规模巨大到难以想象。如果你曾经有机会参观美国大峡谷国家公园，你可以联想到这个概念。无论你读了多少遍，听了多少遍，看了多少张图片，你都只能亲身体会它的大小和规模。同样的概念也适用于采矿业。在采矿业，场地可能覆盖数百平方公里，可能有深度超过700米的矿坑，宽度跨越数公里（见图14-2），类似于一个大峡谷。

许多露天矿都有几个相邻的深坑（见图14-3），这些深坑都有长长的、蜿蜒的运输道路，这些道路都是供被称为“牵引卡车”的巨型自卸卡车通过的。如图14-4和图14-5所示，相比之下，这些运输卡车使大尺寸皮卡看起来像玩具车。一些较大的运输卡车能够一次运输350吨以上的材料，这些车使用近4米高的轮胎和4000马力的发动机。用于填充这些卡车的电铲车（见图14-6）具有相同的大小。



图14-2 亚利桑那州的一个露天矿



图14-3 有大型运输卡车的露天矿坑



图14-4 一辆典型的用于铜矿开采的运输卡车

这种巨大的规模并不是地表采矿作业所特有的；地下矿井有数百公里的隧道，也被称为“漂移隧道”，大到可以容纳两辆城市公共汽车，这些隧道在地表以下垂直方向延伸很长的距离。如此巨大的规模也意味着，可能需要很长时间才能到达矿井内的地点。从物联网的角度来看，这意味着技术人员可能需要几个小时才能到达现场的设备位置。

矿山往往位于物理和电子技术难以到达的偏远地点。这意味着支撑一个大型矿场所需的基础设施（电力、水、通信、铁路/公路/海运）往往不到位，或无法达到促进采矿生产活动所需的规模。这些基础设施必须由矿山经营者或代理人建设。有时，整个城镇，包括住房、购物、学校、医疗设施、保安和娱乐，都是由矿业公司建造和运营的，以满足那些与现有城镇之间距离太远的地方的工作生活需求。此外，许多采矿地点所处的位置必须控制高度、湿度和温度等极端环境条件，而且疾病和动物也可能造成危险。



图14-5 运货车与普通车辆的对比



图14-6 在露天矿中的电铲车

14.1.2 安全

采矿本身是危险的，安全是这一领域最重要的考虑因素之一。地下采矿的危险已经在许多电影中被曝光，不幸的是，世界各地的突发新闻也在不断曝光这些危险。坍塌的风险一直是人们关注的问题，而监测隧道结构始终是首要任务。爆炸也是风险之一。采矿作业过程中从地下释放出的各种气体可以快速达到爆炸浓度。在坍塌的情况下，隧道内有限的空气量只能为被困工人提供一个非常短的救援窗口。虽然已经开发了各种技术以消除气体泄漏并使新鲜空气在矿山所有部分流通。然而，监测空气质量和隧道结构的稳定性是地下采矿每天面临的重要挑战。

露天矿可能看起来比地下矿安全。然而，移动数吨泥土的力量和开采矿物所需的过程可能是非常危险的。山体滑坡可能是致命的，监测露天矿的斜坡是一项关键的安全要求。此外，在巨大的引擎周围工作也很危险。在这些大型车辆的驾驶室里，司机可能看不到行人，甚至是小货车。灰尘使问题更加严重，即使是配备了雷达的车辆。控制所有工人和车辆的位置并发出信号是必要的。

天气状况也会带来挑战。许多矿井位于极端气候地区。突如其来的暴雨可能会很快填满矿坑和矿洞。当雷暴来袭时，工人们暴露在雷雨之下，可能距离能够提供遮蔽的安全建筑物有数公里远。

14.1.3 环境

采矿公司有义务保护环境不受其经营活动的影响。这些影响包括地面和水污染，当然，还包括噪声、灰尘和采矿作业对动植物的影响。在矿井生命周期结束时，必须对现场进行管理，以避免任何污染，并将现场条件恢复到开采前的状态。

矿难，比如尾矿坝溃坝，会对广大地区造成破坏，其影响可能持续数十年甚至数百年。如果不能成为一个良好的矿业企业，政府将不会发放新的矿业租约。采矿作业关心作业对环境的影响，需要密切监测天气（例如，灰尘或水污染的可能后果）、空气、水质等。

14.1.4 安全

现代社会依靠采矿来供应几乎所有东西都会需要的矿物质：建筑物中的电线；电子设备中使用的元件；小工具使用的电池；建筑物、汽车、飞机、轮船、桥梁、珠宝中的金属和许多其他东西。对于几乎所有现代工业和一个从制造业中获益的社会来说，矿产处于全球供应链的最底层。

虽然普通消费者不了解矿物位于何处，甚至不关心矿物是如何开采出来的，但靠近矿藏的人往往知道。由于各种原因，采矿可能是一个非常两极分化的话题。矿业经营者拥有大量宝贵资产。显而易见的资产是被开采的矿物和用于提取和精炼它们的设备。勘探数据和其他知识产权等资产可能不那么明显。

一些矿藏位于世界上政治不稳定或环境不敏感的地区。如果考虑到由于操作距离遥远、规模庞大、固有的安全考虑因素以及使用大型重型设备和炸药所产生的额外风险，物理安全和网络安全通常是煤矿经营公司最关心的问题。

14.1.5 震荡的市场

大多数矿山的产出是在商品市场上出售的原材料。因此，现代矿业运营公司的盈利能力取决于市场力量。产品的差异化对大宗商品来说通常是不可能的。例如，在2011-2017年期间，高品质铜价最高升至每磅4.50美元，最低跌至每磅1.96美元。大宗商品市场的波动是无法控制的，但拥有一个高效、适应性强的供应链，可以在价格升高时实现利润最大化，在市场低迷期将损失降至最低。

14.2 物联网在现代采矿业中的挑战

现代采矿业中的许多挑战都可以通过物联网解决。然而，在采矿环境中部署物联网解决方案具有挑战性。

14.2.1 OT在采矿业中发挥的作用

与其他行业一样，矿业行业对传统企业IT网络的目标和要求与OT有很大不同（IT和OT的概念在第1章中介绍和讨论）。矿业的技术作用通常集中在OT方面（见图14-7）。

■ **矿长：**矿长负责矿山的运营，并最终负责矿山的盈利能力。他负责平衡投资（物联网、引擎和人力）和矿山产出。矿长对任何能提高盈利能力和安全性或降低成本的物联网解决方案都感兴趣。

■ **工程经理：**矿长与工程经理协调工作。工程经理负责矿山的设备。因此，他对任何能够提高设备可靠性（通过提供更好的监测，允许预防性维护）和减少与采矿作业有关的能源消耗的解决方案都感兴趣。

■ **IT运营经理：**IT运营经理负责IT网络。任何需要通过IT网络连接的设备都需要经过IT经理团队的审核和批准。

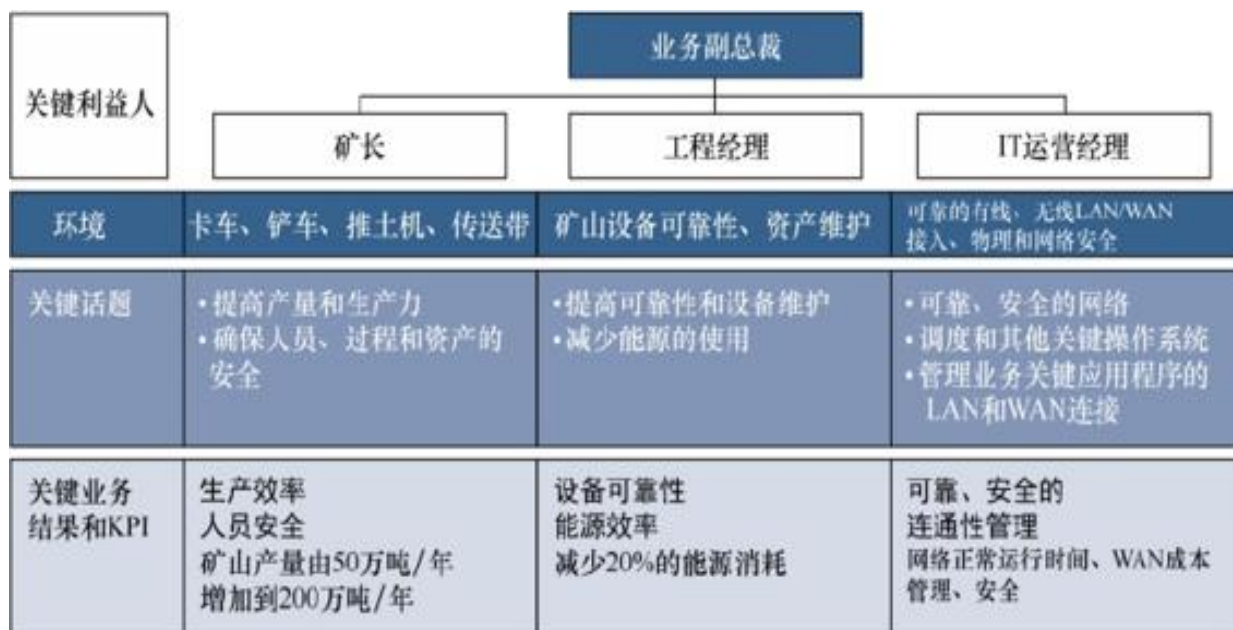


图14-7 采矿业中的关键角色

14.2.2 连接

物联网依赖于网络连接，在采矿业，网络连接尤其具有挑战性。采矿的本质意味着物理层具有极强的动态性，网络可以处于不断变化的状态，以满足不断变化的矿山的需求。总的来说，这些挑战通常可以分为3类。

■ **远程性：**在许多矿山运营的偏远地区，WAN连接可能很难获得，而且往往非常昂贵，带宽相对较小，通常出现高延迟和高丢包。特别是在无法利用传统的地面电路，必须使用卫星通信链路的情况下。对于许多应用程序，这些问题可以通过WAN加速和压缩技术来解决。然而，这些技术通常不适用于实时通信应用，如VoIP和IP视频会议。此外，许多矿山所在的地方甚至没有蜂窝网络覆盖，这意味着矿山运营商往往需要部署自己的无线通信基础设施，并可能依赖卫星通信提供一些数据服务。

■ **极端的环境条件：**矿山存在各种各样的极端条件，设备必须在这些条件下工作。其中一些条件与矿藏的偏远位置有关，另一些则与采矿过程的性质有关。地面上的采矿作业通常遇到极端的湿度和温

度，包括热和冷，以及极端的天气，例如闪电、风暴和雷雨。许多矿井，特别是南美洲的矿井，通常在4500米以上的高海拔地区作业，那里的空气密度要低得多，必须考虑设备的冷却效果。有些采矿过程涉及腐蚀性化学品或易燃易爆环境。为了保证设备的安全，防止火灾和爆炸，需要适当的设备认证或防护罩。重型机械，尤其是推土机等履带式车辆，会产生极大的振动，几乎可以振开附近的设备。这种环境要求在安装设备时具有创造性，比如使用橡胶垫圈来隔离振动，使用钕磁铁来简化设备的安装和拆卸。

其他环境方面的考虑包括在爆破过程中定期和有意控制的爆炸。表14-1总结了采矿方面的一些环境挑战和可能的解决办法。

表14-1 环境因素及可能的解决方案

环境因素	可能的解决方案
水分和灰尘	使用防护等级合适的设备或防护罩，如 IP54 或 IP68
腐蚀性	使用保形涂层设备或具有适当等级的防护罩
闪电	使用适当的防雷设备（如避雷器、适当的接地），并通过光纤互连进行电气隔离
极端热/冷/海拔	使用用于扩展温度范围的设备和/或能使设备保持在操作规范范围内的适当防护罩
振动	使用减振底座和防护罩
易燃易爆环境	对于获得 HazLoc 认证的特定危险（例如，Class 1 Div2），使用安全的设备或防护罩

■ 规模：采矿业的规模与大多数行业完全不同。这通常意味着网络需要提供数百平方公里的连接。更复杂的是，一些挖掘应用程序不是基于IP的，无法进行路由。第2层连接有时必须在广泛的地理范围内可用。与其他行业不同的是，采矿业的性质意味着地面在不断地移动。今天作为网络分发点的物理位置可能明天就会消失。矿业的地形每天都在变化，这往往意味着网络的逻辑和物理拓扑必须相应地进行调整。由于工作环境中网络拓扑的高度流动性，无线连接通常用于访

问层的“最后一公里”。即使是这种灵活的“最后一公里”接入方法也必须经过生命周期的修改，以适应矿井不断变化的环境。

14.3 采矿业物联网战略

从提高运营效率到生命安全和环境监测，物联网在矿业领域有获得广泛应用的机遇。图14-8提供了几个示例。物联网解决方案为采矿业带来了巨大的好处，有些方案的投资回报时间非常短。

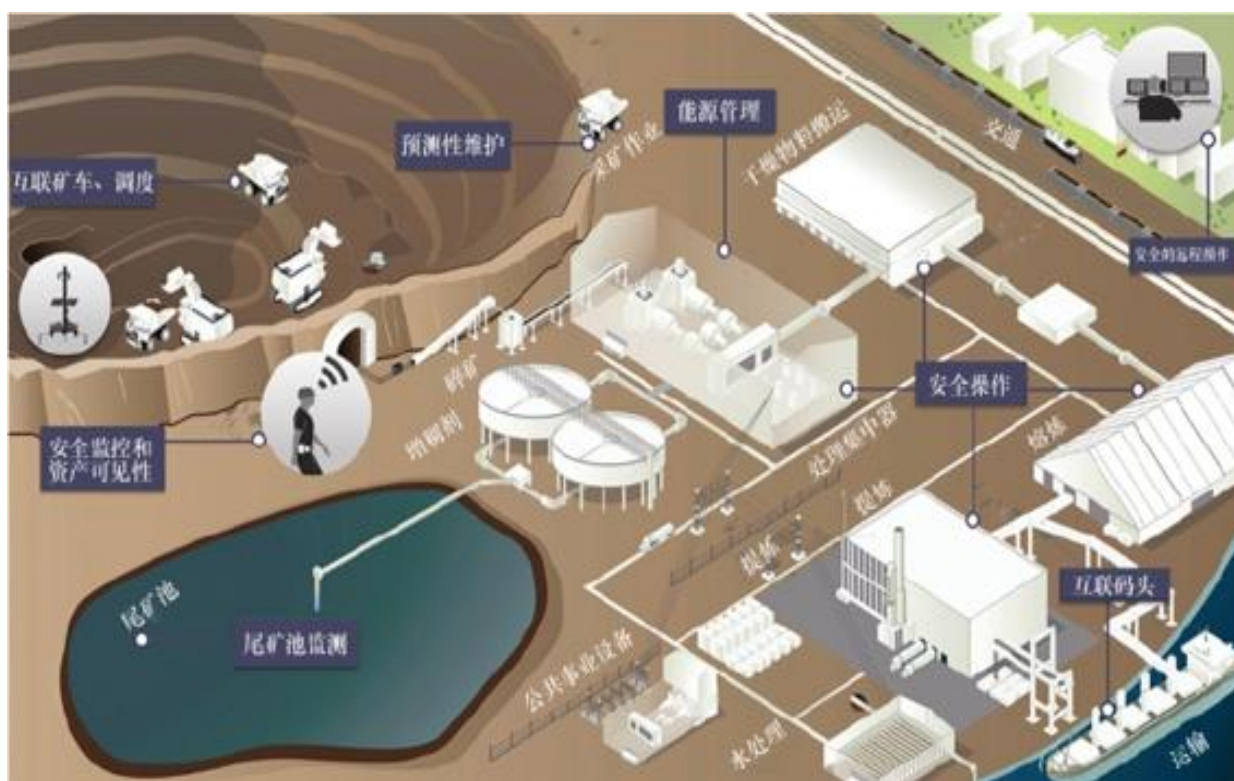


图14-8 物联网应用于采矿业的示例

14.3.1 改善安全和定位服务

在用于采矿作业的所有可能的物联网应用中，对于所有采矿经营公司来说，首先想到的是安全。长期以来，采矿业一直以危险著称，

因为它所处的环境和大量的材料是由非常大型的车辆运输的。物联网在多个层面上为提高采矿安全性提供了非常强大的手段。

1. 司机的安全

矿山本身就是危险的地方，但物联网解决方案正在全球各地的矿山现场部署，以帮助提高矿工的安全性。例如，如果司机感到困倦，运输卡车的安全性就会大打折扣。运输卡车事故可能造成设备损坏和采矿作业停顿，甚至可能对在矿场的司机或工人造成伤害或死亡。为了解决这个问题，物联网系统可以用来测量运输卡车司机的身体状况。这些系统可以基于3种类型的度量进行操作。

■ **生理测量：**司机可能会被要求佩戴腕带（类似于健身追踪器），测量心率、呼吸模式和其他因素，当这些模式提示司机困倦时，就会发出警报。

■ **行为测量：**安装在仪表板或后视镜上的摄像头可以测量眼睛闭合、眨眼模式（入睡后眨眼会变慢）、打哈欠、头部位置等。

■ **车辆轨迹测量：**卡车上的传感器可以测量方向盘的运动、车道上的位置、加速踏板上的压力等因素。突然的变化会反映出司机的精神状态。

当检测到睡意时，可以在卡车或控制中心触发警报，卡车可以自动停止。

在一些地形相对稳定的露天矿中（即采掘区与处理机器之间的路径不会每天发生改变），开始使用自动驾驶卡车。图14-9显示了其中一个自动引导车辆（AGV）的示例。

这些卡车是无人驾驶的，没有驾驶室。因此，它们没有正面或背面，可以在任何方向卸载矿石。它们被编制在矿区地图里，并被配置成前往装载地点，在那里装载矿石。当装载量达到一个确定的阈值时，卡车驶回处理区，将矿石倾倒入机器中。传感器和摄像头以及矿

藏地图可以帮助卡车在现场导航。操作方面的优势是，一个远程操作员可以监控多辆卡车，而卡车永远不会疲倦。然而，就目前的技术水平而言，这种解决方案在拓扑结构经常变化的站点并不实用，因为卡车控制系统需要经常重新编程。这些自动驾驶卡车非常复杂，通常需要多个传感器，包括计算机视觉、高精度GPS定位、导航系统和防撞机制。说到安全问题，把人从一辆300吨重的汽车的方向盘后面解放出来是一个严重的风险。大多数自治运输系统严重依赖IP连接，对网络可用性有严格的容错。



图14-9 小松AGV拖车展示

2. 天气和闪电

在露天开采中，雷电和恶劣的天气构成了严重的风险。雷击监测系统 and 小型气象站可以部署在整个矿区，并与网络相连，为矿区运营商提供实时天气信息。当在5公里范围内发现闪电时，工作人员可以通过手机收到警报，指示他们在风暴到来之前寻找掩体。

3. 边坡监测

露天矿尤其面临矿山边坡失稳的风险，边坡失稳可导致大规模的致命性滑坡。有几家公司已经开发了监测坑壁完整性的系统，通常称

为边坡监测系统。这些系统可以使用多种传感器。

例如，监测系统可以安装在拖车上，并定位在露天矿坑的一侧。该系统在180度范围内发射三维激光束或雷达脉冲，测量信号响应模式，并将其与基线进行比较。图案的变化表示坡度的变化（通常是由于地形稳定性的变化引起的）。有了这样一个系统，就可以在实际山体滑坡事件发生之前发出警报，提供数小时甚至数天的预警。这种较高的安全水平还允许在更陡峭的斜坡上进行采矿作业，并对这些斜坡进行安全监测。

将边坡监测系统有战略性地安装在露天矿中，需要通过网络连接将信息传递给采矿运营公司。

14.3.2 定位服务

由于采矿作业规模庞大，因此很难在矿山内准确定位特定的资产或工人。虽然陆地移动无线电（LMR，又称为对讲机或手持式对讲机）解决方案已经取得了进展，其中包括通过内置GPS传感器跟踪无线电的能力，但这些解决方案在室内或地下都不起作用，而且可能无法为每个矿工提供定位资产的能力。

无线定位服务的优点是不需要GPS信号，可以通过矿山网络报告设备或工人的位置。其中的一些解决方案需要使用关键点和信号灯（以检测资产何时接近或离开给定位置），其他解决方案则使用网络设备的信号强度或信号传输时间（如到达时差[TDoA]），通过三边测量（圆的交点）来确定位置。虽然这些解决方案可能无法提供与GPS相同的定位精度（根据环境和建筑，三边定位精度在3~25米之间变化），但它们有助于在无法获得GPS信号的情况下定位资产或工人。这在紧急情况下是非常重要的，因为它可以使急救人员立即获取工人的位置（无须人工呼叫和计数），并根据事故的位置和工人与该位置的距离，将他们的努力集中在最需要救援的地方。

除紧急情况外，工人跟踪可能还有助于在地面上发现工人时向卡车司机发出警报（卡车通常装有传感器和雷达，当在附近发现车辆或人等较小的物体时，这些传感器和雷达会发出警报）。当工作人员在危险场所操作时，控制室也可以显示特定的警告。

一氧化碳（CO）是一种无色无味的有毒气体，由煤或木头等含碳物质不完全燃烧而产生。它是地下矿山的主要危害之一。多年来，工人一直携带着检测一氧化碳的设备。如今，物联网传感器可以实时地向操作人员通报矿井内任何地方是否存在一氧化碳，并显示一氧化碳的积聚趋势。物联网系统还可以根据检测到的一氧化碳来调节通风，并根据卡车（产生一氧化碳的卡车）和人的存在来进一步调节通风。这些定位系统通常需要连接到网络和/或利用现有的WiFi网络。

1. 有害气体检测

在地下和地表采矿中，可能存在各种各样的致命或有害气体，这取决于所开采的矿物及其加工方法。工作人员接触这些气体的危险地点通常有固定的气体探测系统和工作人员进入这些地区的便携式解决方案。其中有一些便携式系统能够直接连接到网络，或者利用能够支持工业无线协议（如ISA100.11a和WirelessHART，两者都在第4章中定义）的网关连接到网络。当检测到有害气体时，系统会发出警报，但连接的存在也使得系统可向控制室报告危险及其详细信息。

2. 环境监测

如本章前面所述，采矿经营公司必须接受严格的环境监测。具体的环境监测类型可以有很大的不同，这取决于矿山类型、位置和区域法规。然而，将这些系统连接到网络是非常常见的。其中包括空气质量监测仪、监控灰尘和颗粒物以及水质的摄像机。

与采矿有关的重大环境问题之一是确保尾矿池的完整。尾矿池非常大，用来存放采矿过程中产生的废物，通常是细碎的岩石、水和采

矿过程中使用的任何化学物质。图 14-10显示了一个示例。



图14-10 土坝外（上）和尾矿池与土坝的景观（下）

最近的一个例子说明了为什么监测尾矿池的完整性是重要的，即2014年8月的波利山矿灾。在这场灾难中，尾矿池的故障导致了大约63.4亿加仑的矿山废料污染了加拿大不列颠哥伦比亚省莱克利镇附近的湖泊和河流。为了提高尾矿池溃坝检测的平均时间，同时降低人工检查尾矿池大坝完整性的劳动成本，许多矿山运营公司现在都安装了物联网系统来监测尾矿池的情况。这些系统通常使用沿尾矿池的土坝有策略地放置的地面探测传感器来检测故障的迹象和症状（见图14-11）。这些系统通常与矿井的IP网络进行无线连接，以报告状态和潜在的故障。



图14-11 带有传感器的尾矿池土坝（左）和压电式地面监测传感器的特写（右）

14.3.3 提高效率

物联网在采矿业领域最令人兴奋的用例之一是提高效率。本章的开头部分提到，采矿作业是跟随商品市场进行的。成本是至关重要的，任何可以获得的效率都会直接影响矿山的盈利能力。

大多数矿山都有几百人，甚至几千人从事各种工作。当设备发生意外故障时，这些人往往无法履行职责。有时这些故障对矿山的整体作业来说是无关紧要的（例如，轻型卡车的故障）。有时故障非常严重，会导致生产的重大中断。在露天铜矿开采中，当一辆满载的运输卡车发生故障时，会使电铲车到破碎机的矿石流中断。另一个类似的重大事件是，主破碎机被卡住，因为电铲车的齿进入了破碎机。这类事故可能会使矿山在劳动力闲置和恢复、修理和重新启动工作方面损失一大笔钱。

提前预测设备故障并不是什么新鲜事，但利用物联网和大数据分析来实现故障预测却是新鲜事。许多矿山经营公司已经在重型设备上安装IP连接的传感器，以便在故障发生之前预测和预防故障。如果这

项工作做得好，投资回报会很快，这不仅可以防止意外故障导致的停工，还可以优化设备的预防性维护成本。

一种非常常见的矿山设备是电动绳铲（见图14-6）。在前面，一个装有金属齿的大桶在土壤或矿石堆中挖掘。当齿轮脱落时，有系统可以监控和自动检测铲斗的钢齿，并通知操作员，脱落的钢齿可能进入破碎机。然后，矿山操作员可以停止装载，防止钢齿对破碎机造成损坏并停止相关的工作。

以电力和燃料形式存在的能源是矿山最大的运营成本之一。矿山中几乎所有的设备都消耗能源。这种消耗包括每小时50加仑柴油的重型设备（取决于设备类型和负载）、为地下矿井通风的设备，以及运行破碎机和将矿石加工成可用矿物所需的大量电力。

许多物联网应用试图解决这些能源挑战。在燃油效率方面，应用程序可以为运输卡车建议最省油的路线（计算最短路线，并避免检测到的斜坡和颠簸），或监测司机的行为，并报告次优驾驶模式。这些系统还可以记录和报告任何违反标准操作程序的行为，如过度空转。对车辆性能和维护的详细跟踪也可以确保最佳的燃油效率。

在地下采矿中，加压气流系统需要大量的电力。通过物联网监测和分析，可以优化性能以及寿命和能源消耗。同样的原理也适用于矿井中许多依靠电动机的系统。

14.3.4 改进的协作

前往矿山和矿山内的特定地点可能非常耗时且成本高昂。传统上，矿山中的主要协作方法是基于无线电的语音通信。虽然半双工LMR系统和语音电话服务仍然是采矿作业的一个重要部分，但现代技术和连通性极大地增强了这些系统的功能，允许使用更丰富的通信方法提高效率。例如，技术人员在矿区可以使用IP连接的加固计算设备的视频功能发送设备图片甚至实时视频，以获得工程师的远程协助，从而大大减少维修时间。

沉浸式视频系统还可以减少矿藏的审视时间。虽然基于房间的视频系统不太可能应用于活跃的矿区，但它们经常用于矿山的业务办公室，并允许进行远程面对面会议。这项技术可能并不适用于所有的会议情况，但对于时间敏感的会议来说是一个很好的选择，否则就需要人们长途跋涉。

14.3.5 采矿业物联网安全

如前所述，安全性是采矿业的一个重要主题。与许多工业和制造业的物联网系统一样，采矿业系统应该而且通常遵循普渡控制层次模型或ISA99/IEC-62443框架，将工厂网络划分为逻辑区域（有关控制层次的普渡模型的更多信息，请参阅第2章）。将单个过程区域分组到其自己的单元/区域中并不罕见，但是使用适当的DMZ（有时称为数据二极管）将这些区域与业务或企业网络分隔开来，可以保护工业系统免受外部威胁，这一点非常重要。

除了物联网系统的DMZ，传统的安全最佳实践还包括网络认证、基于角色的访问控制、定期打补丁、控制平面监控、系统日志审核以及其他相关行业的最佳实践。虽然不可能完全保护系统免受所有可能的攻击，但是分层安全和遵循行业最佳实践可以显著提高在不断变化的威胁环境中免受攻击的概率。

除了对IT和OT系统的网络安全威胁外，物理安全是一个主要的关注领域，必须根据与矿山物理位置相关的风险适当地加以解决。在世界某些地区，资产盗窃和物理性破坏（包括物联网基础设施）是一个重大问题。最初出现的远程设备故障实际上可能是盗窃。

网络设备盗窃、物理损坏或清除（为了不同功能而借用的物品，因为借用比新设备运送时效快）也会对采矿作业的功能产生重大影响。例如，与从简单的远程设备故障中恢复相比，从无线网状网络根接入点及其所有相关组件的失窃中恢复要困难得多。为了解决这一问题，矿山运营公司经常设置重要的物理安全防护，以防止设备被盗，如图14-12所示。



图14-12 矿山现场无线网状网络设备的物理安全防护

14.4 采矿业物联网体系结构

智能对象位于物联网网络堆栈的入口点。在采矿环境中，大型物体，包括运货卡车和电动铲车，正在成为智能物体。由于这些大型对象通常由本地人员操作，因此传感器通常通过有线接口连接到人机界面（HMI）。操作员可以直接利用所提供的信息。然而，在许多情况下，智能对象还需要向远程操作人员提供信息。在这种情况下，网络连接是必不可少的。

由于其不断变化的地形环境，大多数矿山选择无线技术来连接人和智能对象。许多矿山地处偏远，不大可能受到附近系统的干扰。然而，由于大规模的无线技术部署在采矿现场，因此强大的定向天线是常见的。由于射频（RF）的特性，以及其他系统有可能产生无意的有害干扰，协调在特定站点上实现的所有无线通信技术是极其重要的，无论无线通信的类别、技术或应用是什么。建议各矿区积极跟踪和管理其RF频谱。

同样，该建议不仅限于特定的无线技术。事实上，采矿作业中可以使用多种无线技术来实现物联网通信。无线技术对于大多数矿山来说是极其重要的，因为它能够连接固定设备、移动设备以及人员。大

多数无线网络技术都工作在微波频段。在微波频段，通常需要视距通信以保障可靠的通信，并且RF路径消耗相对较高。

无线技术可以分为两大类。

■ **获得许可：**顾名思义，无线频谱需要经过政府许可才能在指定频率或频段上操作设备。这些许可通常与物理站点位置或地理位置相关联。在采矿作业中，获得许可的无线经常用于LMR（又称对讲机或手持对讲机）、长距离无线回程链路（又称微波链路）和传统的3G/4G/LTE。一些站点（如澳大利亚的多个远程站点）使用私有LTE，而其他站点则依赖与移动运营商的协议来部署通向矿区站点的基本蜂窝网络连接。

■ **未经许可：**未经许可的无线频谱受到政府机构的监管，但此类设备的所有者或运营商不需要单独获得使用设备的许可。在美国，联邦通信委员会（FCC）是监管机构，未经许可的发射机必须遵守FCC Part 15规则。这类技术包括IEEE 802.11a/b/g/n/ac/ah和IEEE 802.15.4，其中包括ISA100.11a、ZigBee和WirelessHART。

注释：第4章中介绍了许可和未经许可的无线频谱的概念，还介绍了LTE、IEEE 802.11、IEEE 802.15.4等用于采矿业的无线技术。

由于成本相对较低且易于使用，未经许可的无线技术在采矿业应用程序的数据通信（包括物联网）中非常常见。虽然未经许可的频率很方便，但在矿山中必须注意协调频率的使用，以防止干扰。矿山中无线通信故障最常见的原因之一是由两个不同团队安装的基础设施造成的干扰，这两个团队没有协调他们计划使用的频率。例如，一个2.4GHz的无线视频发射机（非WiFi）可以影响到附近的2.4GHz 802.11无线网络流量，并且在没有RF频谱分析仪的情况下很难检测到。

14.4.1 IEEE 802.11作为物联网接入层

在矿山提供无处不在的网络连接非常具有挑战性。与语音通信使用的许可LMR相比，未经许可的数据频率允许的RF输出功率与正常路径

损耗的比率相对较低。在IEEE 802.11（包括IEEE 802.11ah）中使用的未经许可的无线电频谱不会穿透土层、岩石或金属，并且容易受到多信道的影响。然而，一个合理设计的IEEE 802.11网络可以提供到整个矿山所有资产的高流量、低延迟、低损耗的连接。要成功做到这些，需要对射频（RF）和物理学中的电磁场（EMF）原理有很好的理解。除了需要传统的IEEE 802.11无线局域网的技术外，设计和维护矿山中的IEEE 802.11无线网络还要求精通路径损耗计算、读取天线主平面图、理解菲涅耳效应，并熟悉监管规则。

14.4.2 802.11室外无线网状网络

在没有蜂窝连接的地上矿山，提供可靠无线网络访问的最佳方法之一是使用802.11P户外无线网状网络。图14-13提供了这种部署的一个示例。与传统的每个无线接入点都通过网线连接到网络的室内无线应用不同，网状网络允许没有有线网络连接的接入点通过无线回程连接为客户服务。客户端设备可以使用自己的802.11 WLAN适配器连接到无线网状网络，或者通过有线以太网连接到工作组网桥（WGB），工作组网桥又连接到无线网状网络、工作组网桥是配置为客户端的访问点。与传统的WLAN客户端接口相比，工作组网桥具有显著的优势，包括集中式管理、高RF输出、能够通过单个WGB连接多个有线客户端、可选的远程安装和外部天线，以及附加的第2层/第3层功能（取决于WGB的型号）。

从架构的角度来看，WiFi网状网络由以下5个组件构成，如图14-14所示。

■ **根接入点（RAP）：**网状接入点与网络具有有线连接，以进行回程传输。在地下矿井中，这些节点往往靠近交换机连接点。在露天矿场，RAP往往更接近控制中心。

■ **网状接入点（MAP）：**网状接入点通过无线接口回传客户端流量，理想情况下是在与客户端设备不同的频段上。许多MAP支持通过本地以太网接口将有线客户端连接到网络。所有网状接入点（MAP和

RAP) 都可以配备GPS模块, 以使控制操作员能够在矿山地图状上精确地定位它们。图 14-15 所示为部署在露天矿场的地图。

■ **工作组网桥 (WGB):** 工作组桥网是一种专用设备, 用于将移动采矿设备的有线以太网流量传输到无线网络。一些模型提供了附加功能, 例如支持多个以太网设备、多个VLAN和网络地址转换 (NAT) / 端口地址转换 (PAT)。NAT和PAT通常用作安全特性, 允许多个设备共享一个IP地址, NAT和PAT允许在设备传输数据包时转换IP地址和/或端口。

■ **串行回程:** 回程链路遍历多个MAP; 客户端流量通过多个2层无线跳数到达RAP。

■ **背对背或菊花链:** 对于没有为每个功能包含足够专用无线电的接入点 (一个2.4GHz的无线电用于客户端连接, 两个5.8GHz的无线电用于回程), 可以使用两个连接在一起的接入点创建一个虚拟的串行回程映射。



图14-13 露天矿场的WiFi部署实例

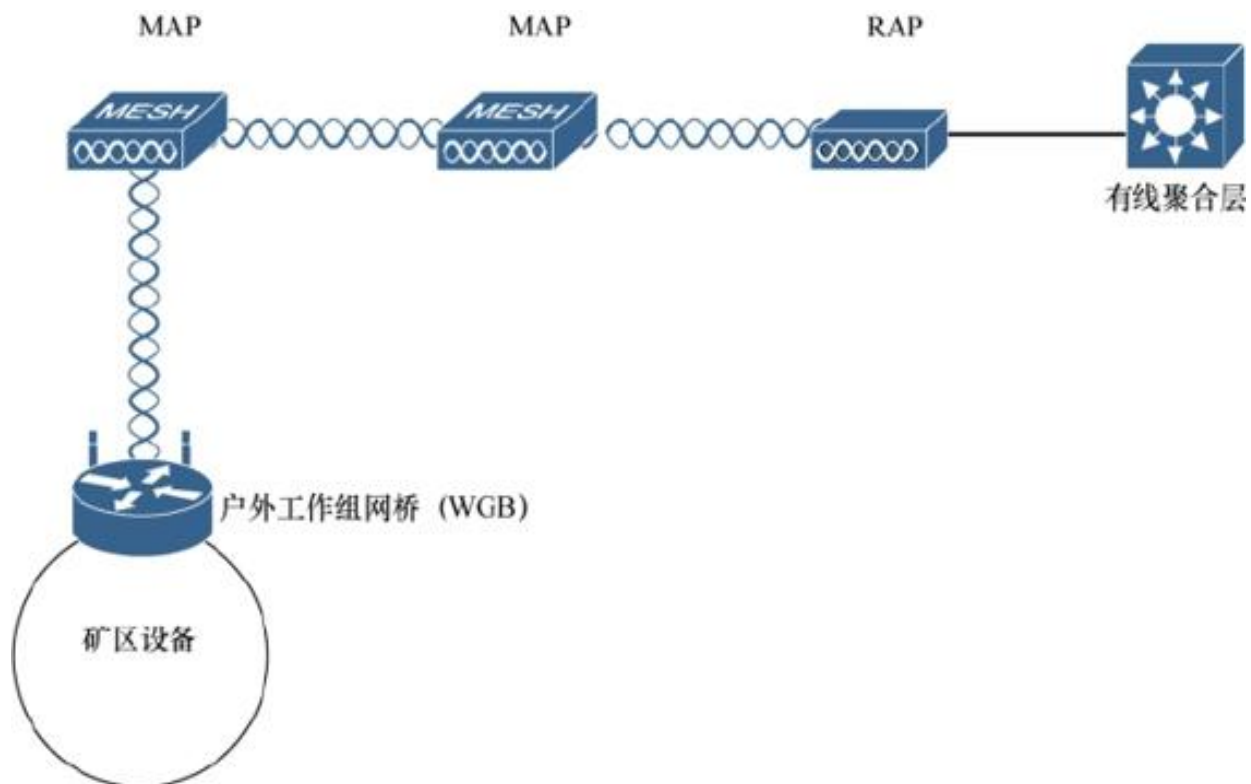


图14-14 用于采矿的WiFi网状结构



图14-15 移动无线MAP示例

1. 802. 11无线网状网络回程注意事项

采矿环境，包括地下矿山，对电子设备来说是非常恶劣的。因此，所有的接入点都需要进行温度强化、防震和防水处理。在无线网状网络中，一种常见的部署方法是将5 GHz无线用于回程，将2.4 GHz无线用于客户端连接。许多802.11无线网状网络可以部署在MAP上，每个频段只支持一个无线电。但是，在这种模式下部署时，不使用串行回程或背靠背菊花链，会影响性能和流量。如第2章所述，大多数网状网络是用树状结构构建的。RAP连接到有线基础设施，并使用其5 GHz无线电连接构成第一跳的一个或多个MAP。在更远的地方，其他MAP通过第一跳MAP来回程。本场景中的所有网状MAP都位于相同的5 GHz信道上。一个标准的网状网络可以包含这样的多个跳数。

因为WiFi是半双工的，所以MAP无法同时与上行的RAP或MAP（指向RAP的MAP）和下行的MAP（离RAP更远的MAP）进行通信。MAP将花一些时间用于中继上行业务，部分时间用于中继下行业务，还有一些时间用于其自身2.4GHz连接的客户端。因此，每一跳都会产生额外的延迟。与转发来自另一个MAP流量的MAP相比，转发来自另外3个MAP的流量的MAP将花费更多的时间进行中继，而且用于转发自身的客户端流量的时间更少。在多跳网状网络中，当使用单个无线电同时连接上行RAP和下行MAP时，每一跳都大大减少了可用带宽。

单一的5GHz回程无线电架构也缩小了范围。设想这样一个部署场景，其中有一个RAP和两个MAP，且这两个MAP是按直线方式组织的（即两跳部署场景）。第一跳MAP必须使用全向天线在一侧到达RAP，而第二跳MAP在另一侧到达RAP。全向天线的增益比定向天线低。这样的架构减少了AP间的距离。理想的配置应该包括为链路的每个方向提供专用的定向天线。例如，使用窄波束天线作为到RAP的上行连接，并使用同样合适的天线为下行MAP提供服务。

在设计和部署需要多个MAP跳数的网状网络时，更有效的架构是为上行链路提供一个5GHz的专用无线电，为下行链路提供另一个5GHz无线电。这可以通过包含两个5GHz无线电的AP或使用菊花链或串行回程来实现。在这个拓扑中，两个MAP通过它们的有线接口连接，如图14-16所示。

上行业务通过一个称为主设备的AP 5GHz无线电进行处理，下行业务通过另一个称为从设备的AP 5GHz无线电处理。每个AP都有一个定向天线，用于增加范围。通信量通过以太网连接从一个MAP传递到另一个MAP。结果是在更大的范围内获得更好的总体吞吐量，如图14-17所示。

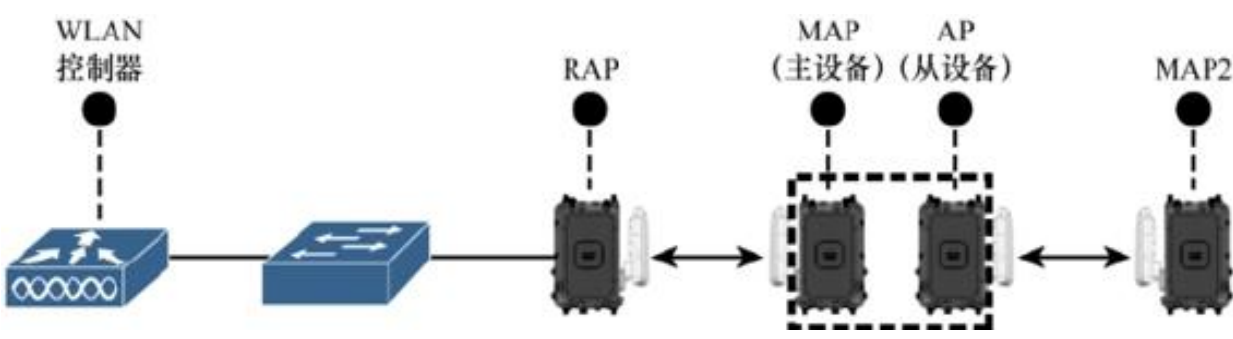
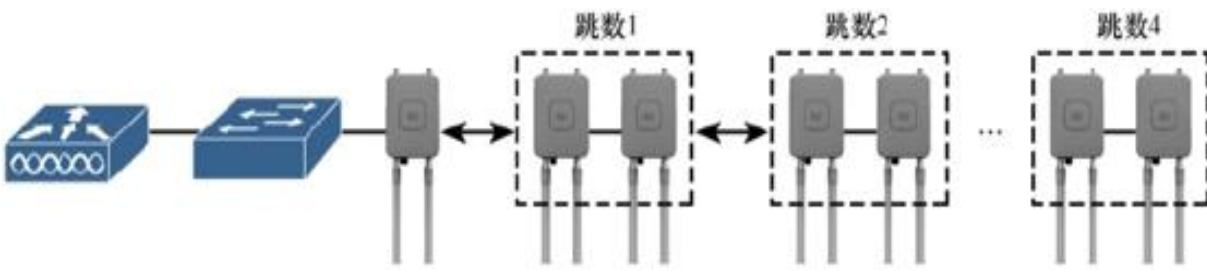


图14-16 MAP菊花链拓扑



性能比较	跳数1	跳数2	跳数3	跳数4
最大20 MHz信道速率 (802.11n、无菊花链)	83 Mbit/s	41 Mbit/s	25 Mbit/s	15 Mbit/s
最大40 MHz信道速率 (802.11n、无菊花链)	111 Mbit/s	94 Mbit/s	49 Mbit/s	35 Mbit/s
最大40 MHz信道速率 (802.11n、带菊花链)	241 Mbit/s	241 Mbit/s	241 Mbit/s	241 Mbit/s
在每一跳中，测量菊花链延迟 (ms)	2.9	6.1	8.8	13.3

图14-17 无线网状网络部署中的菊花链MAP

在标准网状树拓扑中，单个RAP连接一个MAP树。通常情况下会安装第二个RAP作为备份。在第一个RAP发生故障的情况下，MAP会自动扫描所有信道以寻找另一个RAP，并发现备份RAP。安装第二个RAP会增加初始成本，但中断连接的成本通常比安装第二个AP更高。使用多个RAP通常也会平衡MAP负载。由于WiFi是半双工的，所以无论跳数是多少，

每个附加的MAP都会减少其他MAP的可用带宽。一般来说，与任何给定RAP连接的MAP不超过20个。深度超过4跳也是不常见的。

2. WiFi客户端

大型机械（例如，电动铲车、运输卡车、推土机、轮式装载机、钻孔机、牵引索）包含大量传感器。例如，一个新型的长途卡车包含32个引擎传感器、40个车轮传感器和120个负载传感器。所有这些传感器都能完整地显示卡车的工作状态及其在空间中的位置、行驶特性（轨迹、倾角和在矿山中的位置）和负载信息（重量、体积和每个车轮上的压力）。卡车还可能有多达6个外部摄像头，用于监控周围环境（当在卡车附近检测到特定形状时，可能会发出警报）。该信息由驾驶员使用（当有驾驶员时），并反馈给控制室。在大多数情况下，一组专用传感器连接到一个模块（例如，轮胎监测模块、负载监测模块、位置和行程监测模块）。每个模块都连接到一个普通的加固路由器，该路由器还包含一个配置为无线客户端（如WGB）的无线AP。驾驶室内有一个小型系统和人机界面。WGB将关键数据传输回网状网络。

收集的信息可以以多种方式使用。例如，在干旱的天气条件下，粉尘是露天矿山的的一个关键问题。传感器可以帮助装载机穿过尘雾（参见图14-18的左侧）也能感知到运输卡车的位置，使装载机司机（或无人驾驶装载机的计算机）在开始装载卡车之前到达正确的范围和角度。水平指示器和精细的可视化（见图14-18的右侧）也可以告知装载机装载到卡车上的矿石量。卡车传感器还可以向装载机提供反馈（当负载达到定义的阈值时发送停止消息）。此时，装载完成信息可以发送回装载机（和采矿作业控制室），通知监控人员装载完成，卡车开始向矿石加工区移动。这种解决方案甚至可以在干燥的天气条件下进行装载，在这种情况下，装载机司机根本无法透过粉尘看到卡车。

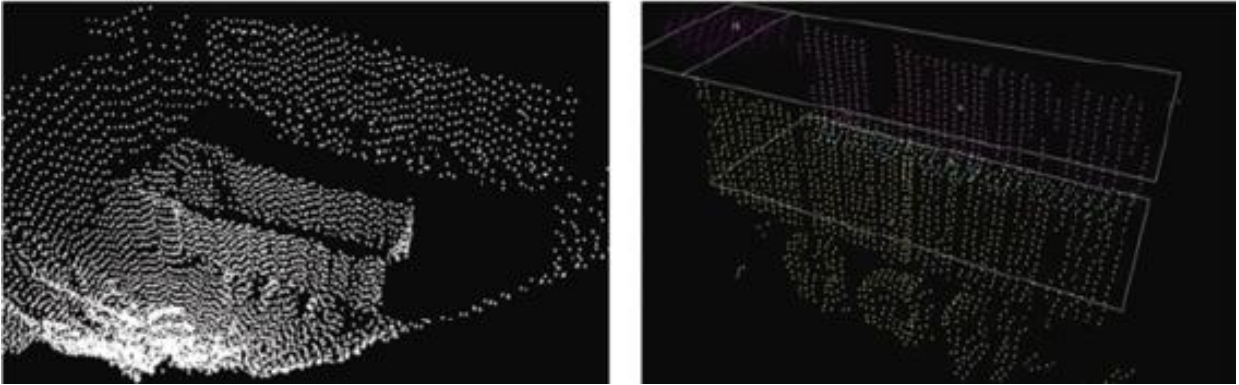


图14-18 用于卡车装载的传感器

WGB是配置为无线客户端的AP。它们可以安装在装有电池的车辆上。工作人员通常还携带无线设备，如智能手机、平板电脑或专用无线IP电话。所有这些设备都有WiFi功能，可以通过三边测量跟踪它们的位置。RFID标签也很常见，尤其是在地下矿场。一个RFID标签包括一个WiFi卡，该卡被配置成在一个固定的时间间隔内发射一个基本的信号，从而可以方便地跟踪每个工作人员的位置。越来越多的RFID标签具有高级功能，如传感器（振动、加速计、气体或其他）、紧急按钮或多功能信号。

3. 无线网状网络的天线考虑

对于所有的802.11无线网络，需要适当的无线电和网络规划以及工程设计来获得最佳性能。这对于采矿环境中的室外无线网状网络尤其如此。例如，高增益的全向天线并不总会产生更好的客户端连接，特别是在海拔有显著变化的情况下。

天线是无源器件。它辐射的能量取决于进入到天线中的能量。不同的天线可以向不同的方向发送能量，但发送的能量总和保持不变。一个经典的比喻是一个充气的气球。你可以按一个方向放大它，但里面的空气总量保持不变。使用增益更高的天线意味着向一个方向发送的能量更多，向其他方向发送的能量就会更少。

常见的高天线增益将辐射能量的形状从球体改变为扁平的饼状，如图14-19所示。结果产生了一个较大的水平范围，但垂直范围较小。当客户端和MAP天线处于相同的海拔时，这不是问题，但在露天矿中会造成巨大的覆盖缺口，因为在露天矿中往往存在较大的海拔差异。

在图 14-19 所示的示例中，运输卡车的全向天线增益过高，客户端无法与下面的MAP或上面的RAP进行通信。可见，天线规划是有效连接的必要条件。天线类型取决于矿场的拓扑结构和WiFi系统所连接的设备。

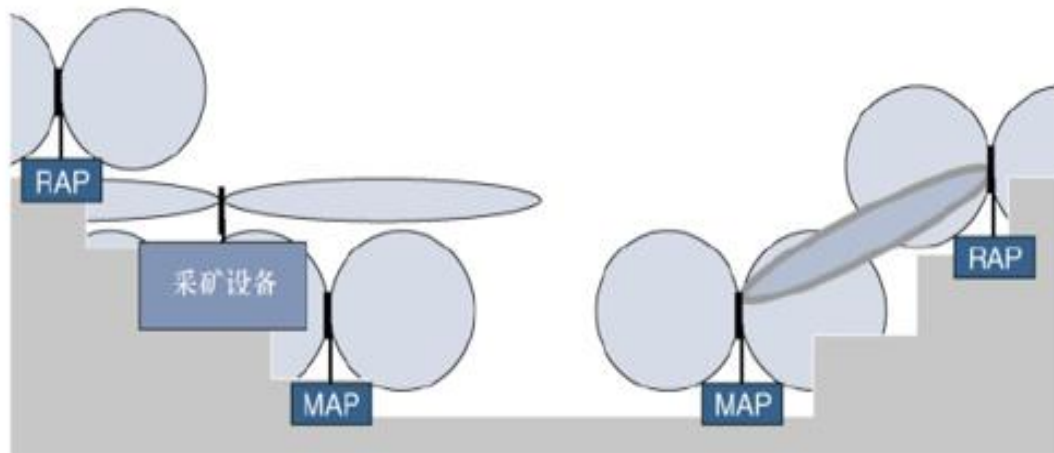


图14-19 三维空间中的天线和覆盖限制

天线的安装位置也是一个重要的考虑因素。802.11天线需要有清晰的视距来进行通信，但是也需要保护它们以免遭到破坏。必须在视距与防止岩石坠落和其他危险之间取得平衡。许多装置利用多个天线来达到最佳效果。

14.4.3 4G/LTE

由于大多数采矿作业地处偏远，商用的4G/LTE服务通常无法使用，而且在这些服务可用的情况下，它们的速度、成本和可靠性可能无法满足采矿运营公司的要求。然而，在一些监管领域（例如，澳大利亚中部的许多矿山，以及加拿大的一些地方），矿山运营公司可能

会选择安装和运行私有4G/LTE服务。离大城市更远通常也意味着频谱成本更便宜。与传统的WiFi解决方案相比，该解决方案提供了令人印象深刻的性能和范围。

与商业LTE相比，私有LTE的另一个优点是可以根据矿山的需要进行定制，包括QoS、无线网络的同步维护调度等。采矿业有特定的要求，如双向实时视频或车队自主管理，这与传统商业LTE的要求有很大的不同（例如，LTE更适合单向视频流）。然而，需要注意的是，私有4G/LTE解决方案需要大量的规划和资源投入。在很多情况下，采矿运营公司要么必须从政府监管机构购买LTE频谱，要么必须与另一家拥有频谱的私营公司合作。该解决方案通常与WiFi和无线网状网络（例如，ISA100.11a、WirelessHART）服务结合使用，为矿场中的所有资产提供适当的覆盖范围。

14.4.4 地下采矿中的无线

地下采矿作业给无线通信带来了一系列独特的挑战。矿井地质、施工、车辆运动都会影响地下无线环境。用于蜂窝或WiFi通信的无线电频率不能穿透土层或岩石。这对于降低整体射频噪声水平非常有利，但是如果使用传统的地面无线设计，则会产生不利影响。解决这一问题的解决方案包括泄漏同轴电缆（充当长天线的电缆）和传统的分布式天线系统，以及无线网状设计，在这个无线网状设计中，通过射频或有线以太网整合了数据电缆或菊花链。后者也是提供WiFi定位服务进行资产和人员跟踪的有效方式。

注释：有关泄漏同轴电缆的话题争议很多。原因是泄漏同轴电缆相当于很长的天线。在标准的WiFi部署（例如，室内办公室部署）中，天线很小，客户端移动速度较慢。由于帧传输最多持续几毫秒，所以在传输期间客户端和天线被认为是静态的。

在隧道中，有一个移动的客户端和一个很长的天线，情况有很大的不同。在天线上接收信号的开始点和接收信号的结束点之间可以存在物理距离。这可能导致多普勒效应，即信号被扭曲（压缩或膨胀）。这种改变可能足以使帧产生错误。此外，一根长电缆可能会发

生这样的情况，即在隧道的两个不同部分，两个客户端可能同时将流量发送到同一根泄漏电缆，从而导致未检测到的冲突。

因此，泄漏电缆并不是所有矿井的最佳解决方案。车辆的速度和电缆的路径必须仔细设计，以提供覆盖范围，且不会产生过度的失真或碰撞，同时要意识到泄漏电缆也不提供定位服务。

14.4.5 工业无线

无线局域网和4G/LTE在高速双向传输数据方面做得很好，但它们的覆盖范围有限，功耗较大。IEEE 802.15.4无线网络（在第4章深入讨论过）可以提供更好的覆盖范围和更低的总功耗，代价是数据吞吐量不大。这些网络通常用于采矿业，以无线方式连接工业传感器，如气体监测传感器。在某些情况下，这些系统可以与IEEE 802.11无线网状网络合并。一些网状接入点包含IEEE 802.15.4无线电（例如，ISA100.11a、WirelessHART）来与现场传感器通信，如图14-20所示。一个5GHz的无线电被用来形成网状网络，并将数据回传至地面和控制中心。

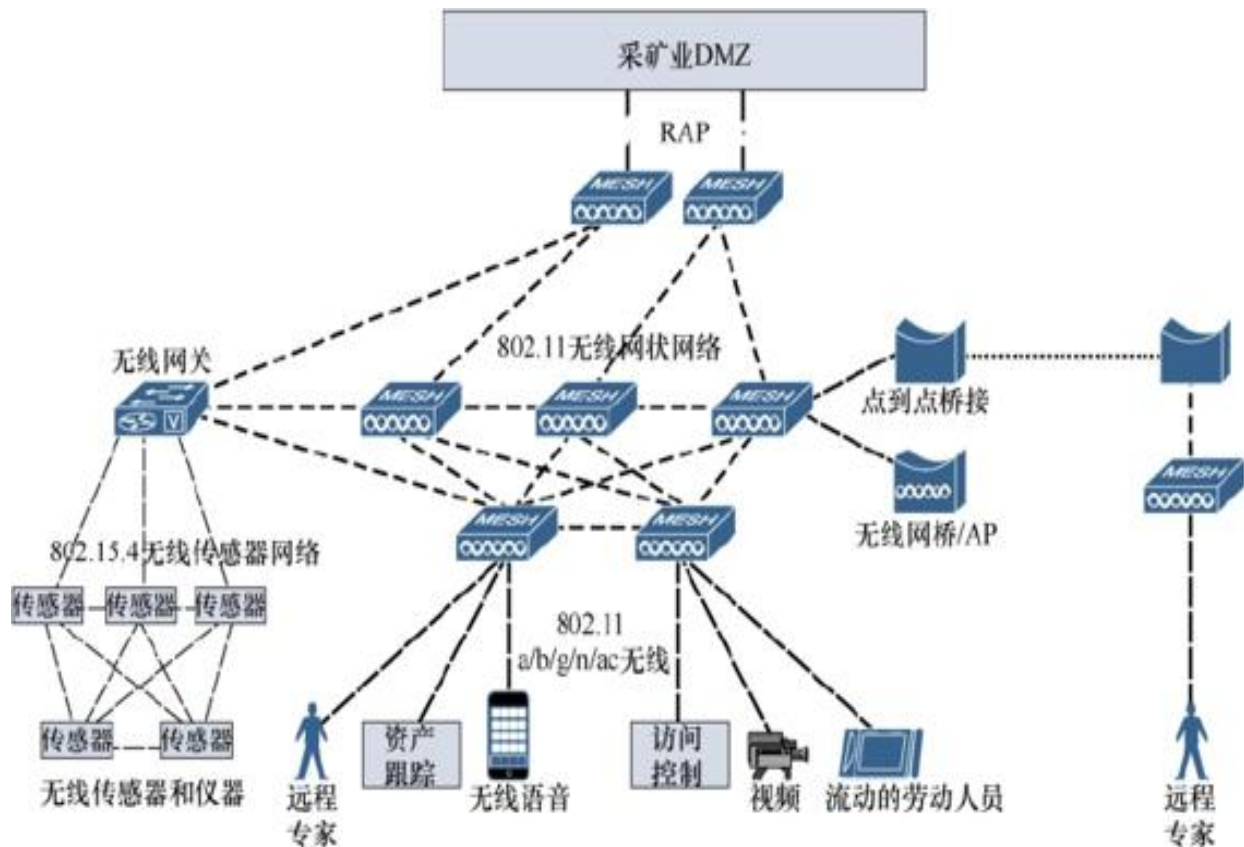


图14-20 整合了IEEE 802.11和IEEE 802.15.4的工业无线解决方案的网络拓扑结构

14.4.6 孤立的矿山网络和连接的矿山网络

图 14-21 显示了一个矿山的无线网络拓扑结构示例。MAP 使用其无线电连接到 RAP。RAP 连接到有线网络。在大多数情况下，无线LAN 控制器负责管理和自动化AP电源和信道分配。

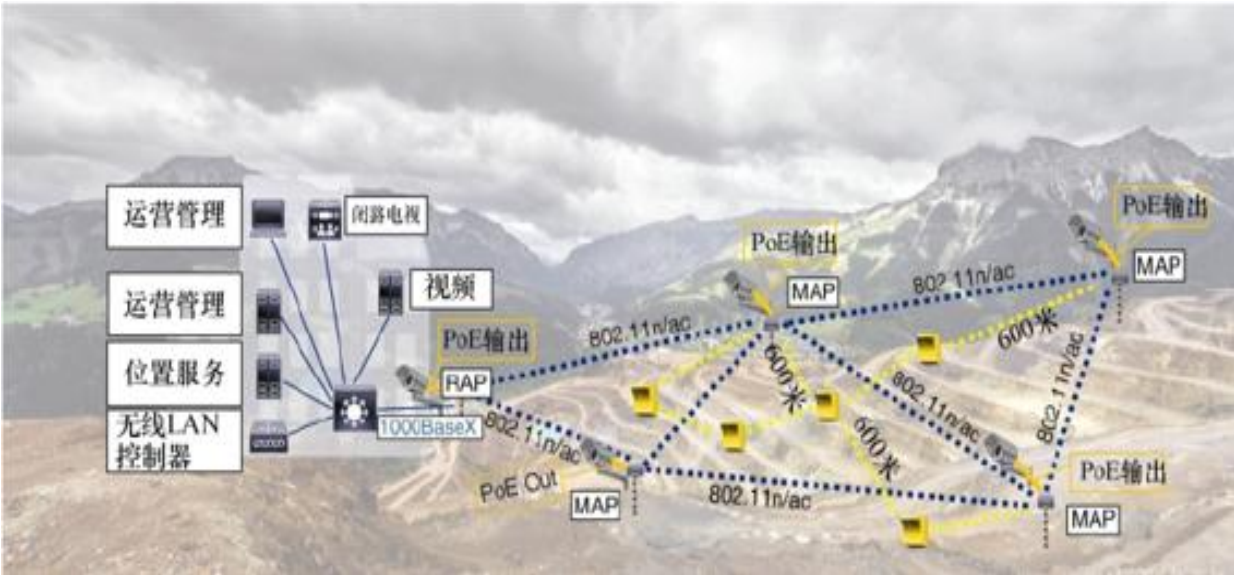


图14-21 简单的矿山拓扑结构，没有连接到外部网络

这个示例拓扑结构很简单，但是包含一些重要的细节。MAP使用PoE输出端口。该端口可以用来连接通过回程发送实时视频的闭路电视摄像机。这些图像可以与人工监控一起使用，也可以输入到计算机系统来分析矿井上的流量模式。这些信息可以用来优化操作。任何其他设备（如传感器和其他协议网关）也可以使用PoE输出端口。

例如，坡度传感器是通常连接到网状网络的设备，它们可以从PoE输出端口供电，也可以有自己的电源。如前所述，坡度传感器可用于预测异常的地形运动。分析软件还可以将这些传感器生成的地形三维视图与矿山测绘软件进行关联，监测采矿效率。这些信息可以用于根据目标矿物的接近度和密度来组织日常作业。

在某些情况下，不同的团队负责操作的各个方面（例如，斜坡监控与RFID和人员位置跟踪）。因此，可能会部署多个WiFi系统，并可能争夺RF信道。WLAN控制器有助于减轻由此产生的干扰。

在图14-21所示的拓扑结构中，操作是在本地进行的，不需要与外部网络连接。大型矿区可能需要连接到矿区外部的运营控制中心。当矿区靠近城市中心时，这种外部连接可以使用WiFi，并与矿区建立点对点连接。或者进行蜂窝连接。远程站点需要卫星连接。如图14-22所示，这种类型的部署允许使用不同的网络基础设施。矿区的网络部署

可能有限，但足以确保正确的运营（例如，位置追踪和通信），而更高级的计算任务（例如，坡度监测、3D制图）则可能在远程控制中心执行。

14.4.7 核心网络连接

虽然一个矿区可能是一个单一的大地理区域，但是不同的团队可能负责网络的不同功能。通常还有不同的控制塔，每个控制塔负责特定区域或特定操作。因此，一个通用的LAN拓扑结构创建了一个模块化的设计，有明确定义的服务块，并由每个相关的团队管理。这种拓扑允许确定性的服务交付。分布层中的关键元素是冗余的，如图14-23所示。

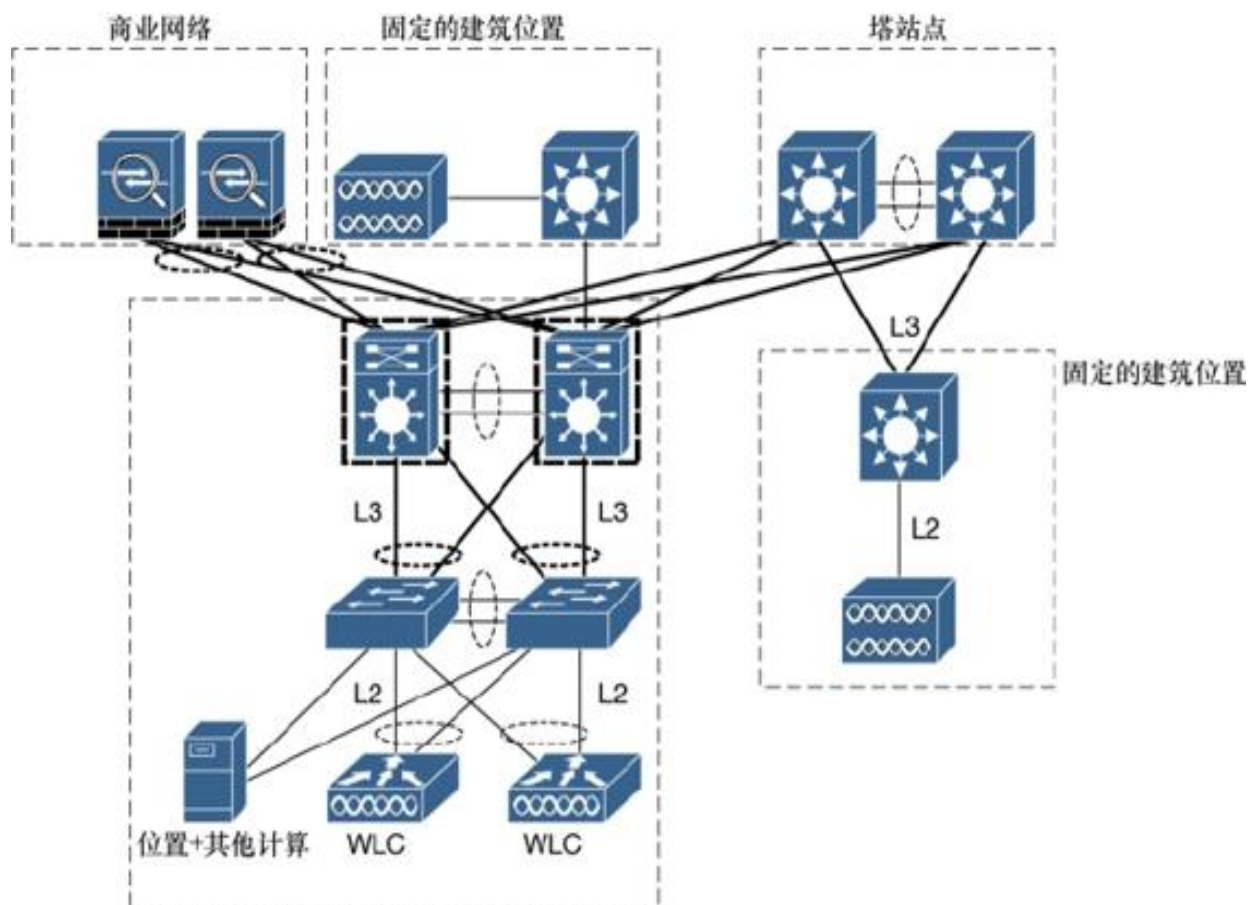


图14-23 常见的矿区核心网络部署

安全性也是一个关键问题。前面几节详细介绍了物理安全性，网络安全性也很重要。在一个竞争非常激烈的市场，任何运营中断和数据盗窃的代价都十分巨大。当网络为模块化网络时，工业防火墙应该安装在模块之间。当网络连接到运营的业务端时，防火墙应该执行周边安全并控制对矿区网络的远程访问。在现场，AAA服务器通常用于控制哪些设备和哪些用户能够访问网络。

14.4.8 矿区应用程序的网络设计考虑

用于操作矿区设备的应用程序可能需要解决特定的网络需求。例如，一些采矿调度系统依赖广播消息来进行服务器和客户端设备之间的通信，因此需要将第2层连接从服务器机房扩展到整个矿区的运货卡车和其他重型设备。其他应用程序要求在每台重型设备上使用相同的

私有IP地址方案，因此要求在采矿设备的网关设备上使用NAT。矿区中的网络需要支持各种各样的应用程序和用例，并且必须为适应性和可靠性进行设计。

由于许多矿区的连续作业计划（即每天生产24小时，全年无休），弹性和容错性也是网络设计中非常重要的因素。由于常规性的采矿活动，中间配线架（IDF，或中间配线室）和主配线架（MDF，或中央配线室）之间的回程链路经常会被切断。请记住，矿区是非常动态的地方，物理环境处于不断变化的状态。网络需要适应这种不断的变化，并允许在可能发生物理链路故障时以极快的速度收敛。此外，矿区的电力是动态的，需要考虑暂时的电力损失。关键基础设施应考虑到电力调节、不间断电源和冗余电源等因素。

14.4.9 数据处理

矿区的常规三维建模已成为普遍现象。在露天矿中，边坡监测器由无人机辅助，无人机可以在矿区上空飞行，从不同角度记录图像。这些无人机通常使用光感测距（LIDAR）技术，发送激光脉冲以获得非常精确的三维环境表示。然后将这些表示输入一个操作管理系统，如图14-24所示。在图14-24中，使用3D建模来显示斜坡形状（白线），密度估计值使用色阶表示各种材料类型和密度。该系统可以分析矿区的当前拓扑结构和每个矿堆的大小，并将其与前一天的数据进行比较。这些信息可以与矿物位置和操作的3D地图重叠，从而更好地确定最佳（最安全或最快）的矿物获取方式。其结果是优化了日常作业，这也有助于延长矿山寿命。

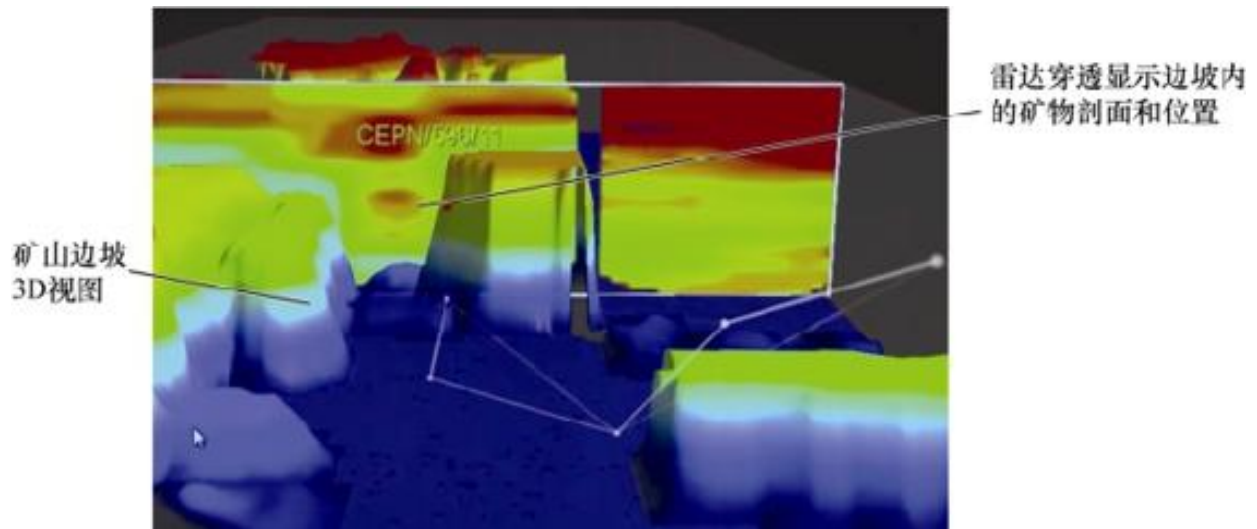


图14-24 无人机获取的图像三维建模与初始矿物图进行对比

拓扑数据也可以反馈给现场车辆。例如，安装在推土机铲刀上的GPS传感器可以引导操作员更准确地定位铲刀，并测量和记录推土机运动产生的新地形。铲斗上的GPS传感器可以记录下每一铲的准确位置。

这些信息可以与矿区的 3D 模型进行比较，从而使操作员能够非常准确地预测将要开采的矿物质数量和类型。这些信息可用于调整生产及其产出以适应市场状况。

14.5 小结

采矿业是全球供应链中极其重要的一部分，它提供了生产各种产品所需的矿物质，从金属、电池、电子元件到我们用来做饭的盐，以及用来发电和取暖的煤。工厂和设备的规模、采矿作业以及进行这些作业所处的环境为物联网的部署带来了非常具体的作业效率、安全和环境挑战。

物联网正在迅速改变矿区的运营方式。物联网使矿区比以往任何时候都能更有效、更安全地运营，为矿业运营公司、企业和消费者提供了切实的成果。通过向系统和矿区运营公司提供关键的实时信息，物联网降低了风险，而在 10 年前，这种风险还被认为是垂直行业的

一个不幸但自然的后果。智能对象可以使过程自动化，使矿物开采更容易，更安全。通过连接到雾或云数据处理应用程序，可以非常准确地测量实时操作，并可以进一步提高采矿设备的寿命和效率。

虽然本章介绍了物联网和采矿业各种各样的主题，但它还远远不够详尽，仅仅是一个浅显的主题介绍。物联网在矿业领域的相关性和价值在与日俱增。

第15章 公共安全

公共安全组织的主要目标是通过更快的响应、改进的运行效率和降低的成本来保证公民、社区和公共空间的安全。随着语音、数据和视频等越来越多的领域对关键通信的需求不断增加，公共安全和应急响应的挑战变得越来越复杂，人们的期望值也越来越高。危机时刻，分秒必争。可能危及生命的情况瞬息万变，必须在几秒钟内做出决定。

尽管物联网是一个相当新的概念，但它已经对公共安全产生了深远的影响，人们对实时信息和态势感知的需求一直存在。物联网是一个可以感知和传输数据的物理对象网络。该技术使用户能够根据智能数据采取行动。当然，在公共安全方面有智能对象，本章将提供一些示例。然而，公共安全的主要关注点是能够快速使用数据。物联网有助于改善人与人之间的沟通。物联网还通过对收集到的数据进行预处理，帮助公共安全机构，使应急响应人员的行动更加有效。

公共安全是一个广泛的领域，包括消防和应急响应人员、执法和安全部队（在公共场所以及特定位置，如学校）、海岸警卫队和国防、海关和边境保护局，以及涉及公众和需要确保安全的许多其他领域。要想涵盖公共安全的所有方面，可能需要一整本书的篇幅。然而，大多数公共安全组织都有类似的需求，并以同样的方式通过改进物联网驱动技术获益。本章重点讨论物联网对公共安全需求典型案例的影响：执法、消防、紧急医疗服务（EMS）和校车。本章包括以下几个部分。

■ **公共安全概述：**本节介绍公共安全相关的不同用例，包括相互作用以实现高效应急响应的不同对象、车辆和服务。

■ **公共安全物联网蓝图：**本节解释任务连续体的概念，列出确保公共安全任务所需的各种要素。

■ 应急响应物联网架构：本节详细介绍各种应急响应车辆（包括指挥中心和移动野战车辆）所需的物联网和通信架构。

■ 物联网公共安全信息处理：本节概述大数据和信息处理如何提高应急响应效率。

■ 校车安全：本节将公共安全应用扩展到校车，展示互联公共车辆如何改善公共服务和安全。

本章的信息可以扩展到其他物联网公共安全用例。

15.1 公共安全概述

公共安全的一个共同主题是需要收集、分析和分发信息，以使个人、工作组、主管和管理人员能够执行各自机构的任务。这些组织依赖于不同群体之间的跨部门协作，通常称为指挥链，以支持公共需求。对于常规和应急响应事件都是如此。无论事件类型如何，公众和机构人员自身的安全取决于通信的可靠性、保密性和完整性。

物联网为连接各机构，增强整个任务环境的态势感知和响应能力，开辟了新的可能性，有助于提供以下服务：

- 实时态势感知；
- 机构内部通信和协作（例如，语音、数据、视频）；
- 数据分析和信息共享；
- 增加社区参与度和利益相关者的外延。

15.1.1 公共安全对象和交换

21世纪的公共安全需要公民、现场人员、执法人员、智能传感器和智能分析系统之间的实时交互。因此，各种物联网解决方案都适用于公共安全案例。智能传感器和警报允许机构捕获数据，并在传感器和数据收集点之间创建回程链路。分析工具处理边缘或云中的数据和事件，并为深入分析和决策提供数据和事件的可视化表示。与公共安全相关的智能对象的新应用每天都会出现，以至于一些作者创造了物联网的新类别，如第一响应者物联网（IoFST）或救生物联网（IoLST）。

本书作者认为，谨慎的做法是简单地使用物联网一词，研究物联网在公共安全方面的应用，同时要认识到这些应用广泛包含下面这3种类型的智能对象。

■ 由第一响应者携带的物体：这些物体可以是专门的传感器，如第一响应者生命体征记录器和发射器，以及收集有关温度、化学品存在情况和任何其他参数信息的环境传感器，这些信息可能有助于第一响应者评估危险，以便立即采取行动或进行事后分析。它们也可以是一般的物体，如随身相机（在本地记录或向中央协调指挥站提供实时数据），甚至是智能手机。从这些对象收集的数据也可以在本地或云端进行处理（例如，枪击触发的警报、图像处理和分析）。

■ 帮助紧急服务呼叫者或受害者的对象：该类别一般包含大量各种各样的医疗设备，从基本的应急按钮（连接到应急反应的呼叫系统）到先进的医疗传感器（例如，健康监测器可以触发警报，并通过手机自动呼叫应急响应人员，提供检测到的问题的详细信息）。

■ 环境中存在的物体：这些是本书其他章节中描述的可能出现在公共环境中的智能物体（详见第12章）。这些传感器通过监测环境（例如，街道摄像头、路灯控制、环境和烟雾传感器、交通位置和密度）来改善公共安全。个人应急响应人员可以访问这些数据，也可以将其用于向应急响应机构提供信息，以提高态势感知或响应效率。

除智能对象外，实时语音和视频还有助于响应方在给定的机构内更快、更可靠地交换信息。人与人之间的交流似乎不是物联网应用。

然而，物联网对公共安全的另一个影响是，人们对收集、存储和处理丰富的实时语音、视频和数据信息，或用于事件后分析的需求日益增加。在边缘收集和处理数据（雾计算）需要物联网解决方案，而将收集和处理的子集实时转发到云端，特别是在数据量超过上行链路能力的位置和情况下更需要物联网。当应急响应人员访问快速连接时，可以将较大或完整的数据集转发到集中存储和处理设施。在这里，仅仅上传所有内容是不够的。可用信息的数量已经非常庞大，物联网正在推动对高级工具和分析（例如，大数据、机器学习）的需求，以确保事件和模式得到识别，从而做出及时、准确的响应。当需要响应时，物联网是公共安全能力的一个组成部分，以协调资源，保护和帮助公众，击退和遏制威胁，并从伤害和破坏中恢复。

一个公共安全机构的成功在很大程度上取决于它与其他机构合作和共享信息的能力。共享信息最普遍的需求是协调外地资源。这种协调可以采取多种形式，包括直接语音、视频和数据通信。物联网发挥着巨大作用，可以自动共享实时位置、分布式和自动化的情况报告和行动计划。在美国，一个众所周知的例子是，公众可以通过拨打911电话向警察、消防和急救中心请求援助。许多911应答系统使用物联网技术，允许操作员采集呼叫者的信息，并将其转发给附近的应答者，并提供呼叫者的实时位置和其他事件信息。高级分析和态势感知工具允许操作员和应答者看到实时情况和先前事件的历史记录。

对于警方的响应，机构需要交换信息，如犯罪历史、个人兴趣报告和生物特征数据，这些信息可以跨许多不同的数据源生成查询。现场工作人员只需轻轻一点，就可以指示现场是否安全，或者工作人员是否需要立即帮助。这些信息可以实时反馈给其他机构。

消防员和紧急救援人员也存在类似的例子，他们共享数据信息（如建筑和施工计划、危险物质特性、医疗历史和处方药信息），并与远程专家和医生进行咨询。所有这些应用都涉及智能对象和标准数据的组合，这些标准数据在系统之间自动处理并相互共享。

另一个例子涉及校车，其中交通主管可以立即查看校车上发生的争吵事件，评估事态，并采取适当的行动，例如向执法人员提供有关

事件的重要背景或实时数据，包括实时视频。

不同的机构还可以从应急响应情景之外的信息共享中获益。例如，许多机构需要访问机动车辆部门或执法机构和犯罪部门的数据，以收集有关驾驶或犯罪记录的信息。许多机构还可能参与收集或提供有关交通、公用事业、学校或任何其他公众感兴趣的信息，如道路危险情况、天气状况、日历事件和时间表，以及电力和水的可用性。

这些例子表明，物联网智能对象、智能分析和信息共享正在迅速改变公共安全机构的运作方式。

15.1.2 公共安全物联网公私合作

信息共享的合作关系不仅限于公共安全，还包括许多其他政府组织。公共安全实际上是建立在政府机构、非政府组织（NGO）和个人之间的整体关系上的。这种结合通常被称为公私合营。顾名思义，NGO是可以想象到的任何实体，不包括政府机构。非政府组织和个人与公共安全机构相互作用，并依靠公共安全机构在许多不同的环境中为公众提供支持——从街道和高速公路、办公楼和校园、购物中心和当地企业，到公园和娱乐场所。

图15-1所示的公私合作关系是一个生态系统。这意味着合作关系的成功取决于双方的参与。这个生态系统的很大一部分取决于通过信息共享相互联系的能力。在拨打911电话的例子中，信息通过公共和私人合作关系共享。这种共享正在演变为包括公共安全机构、非政府组织和私人组织之间丰富的信息交流。例如，当犯罪发生时，银行、杂货店和购物中心依赖于执法部门的保护和支持，并可能提供对楼层平面图或安全摄像头的实时访问。大型校园或工厂在发生枪击、火灾、疾病、伤亡或化学品泄漏等事件时，依靠消防和EMS来保护非政府组织的人员和财产。在这些事件中，学校或工厂安全团队可能会向应急响应人员发送有关人员位置或设施设备的信息。以校车为例，家长、交通工具和学校管理人员了解每辆校车的位置和乘客情况的功能变得越

来越普遍。另一个不断增长的信息领域是社交媒体，从个人、非政府组织和政府机构收集时事信息的可能性正在无限制地增长。

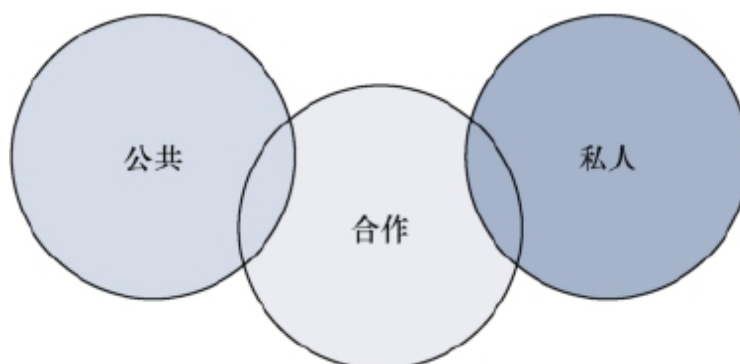


图15-1 公私合作关系

物联网是前面提到的用例的共同主题。一个重要的发现是，这些“物体”不仅仅是传统的传感器，比如光学、声学、压力、流体速度、湿度、温度、接近度、位置、化学和磁性传感器。在公私合作关系中，还有许多其他传感器类型需要考虑。例如，每个拥有智能手机的人都是一个传感器。每个非政府组织及其各种建筑物和业务类型都在通过警报系统、摄像头、烟雾探测器以及其他各种传感器生成有用的信息，甚至政府机构、它们的车辆和工作人员也在通过智能停车计时器、智能路灯、下一代交通系统和联网车辆等方式，为物联网增添数据。随着物联网的发展，信息交换对公共安全和公私合作关系的影响将以指数级扩大。这种不断扩展的合作关系，将催生出许多新的创新和用例，利用新的数据源和传感器类型，并推动更好地存储、分析和共享信息的需求。

15.1.3 公共安全采用的技术和物联网

公共安全历来以技术支持其使命。19世纪后半叶，萨缪尔·莫尔斯、亚历山大·格雷厄姆·贝尔、托马斯·爱迪生和古格里莫·马可尼等发明家发明了莫尔斯电码、电报、电话、无线电以及通过电磁波无线传输和接收信息的新功能。到1870年，美国警察局开始使用电话。到19世纪80年代，电话亭出现在大城市，使公众能够与执法部门

联系。今天，使用电话联系最近的公共安全应答点（PSAP）在美国很常见，而且正在将这种求救方式普及给小学水平的儿童。

除了电话，无线电已成为公共安全不可分割的一部分。在20世纪20年代，这项技术普及后不久，密歇根州底特律市和新泽西州巴约纳市的警察局就开始试验这项技术。到1934年，有194个市政警察系统和58个州警察电台为5000多辆装有无线电设备的汽车提供服务。由于晶体管的发明，这些无线电设备的便携性变得切实可行，公共安全部门继续采用这项技术。到20世纪80年代末，每个警官都拥有一个车载陆地移动无线电设备（LMR）和一个手持移动无线电设备，这已经司空见惯。这些LMR设备几乎总是在政府拥有和运营的私有基础设施上运行，这些基础设施是按照关键任务通信的公共安全等级标准建造的。

20世纪90年代，随着计算机和数据网络的普及，公共安全机构也开始采用这些技术。使用移动数据终端（MDT）或笔记本电脑以及无线数据网络进行通信的能力大大提高了效率和态势感知能力。车载计算机支持诸如计算机辅助调度（CAD）、记录管理系统（RMS）访问、车牌识别（LPR）、车内视频录制和自动车辆定位（AVL）等应用。

这些计算机最初连接到部门的LMR数据系统（如果有的话），速率高达19.2kbit/s。另一种选择是使用商用的蜂窝服务，它们提供1G或2G蜂窝数据。如今，3G和4G蜂窝数据服务已经很普遍，并提供警察、消防、EMS、校车和其他车辆之间的高速数据连接。LMR语音和商用蜂窝电话之间的一个主要区别是，LMR语音是按照关键任务可用性标准构建的，并且是专用的。商用蜂窝服务建立在较低的可用性标准上，并不致力于公共安全。然而，正如本章后面所讨论的，变化正在进行中。

公共安全成为新技术早期采用者的趋势在本章提供的例子中可见一斑。物联网将继续加速这一趋势。例如，在一些国家，机场当局已经将一个人的身份（护照数据）与他们的照片（通过值机柜台的安全摄像头采集）、手提箱的照片联系起来。当一个人在另一个城市着陆时，该数据集将与形状和人脸识别相结合，并在此人接近柜台时显示在海关人员的监视器上。许多执法机构使用无人机监控人群。机载摄

像头具有检测人群密度和异常移动的数据处理能力，以便在需要时根据检测到的异常移动的相对位置向警察发出警报。

15.2 公共安全物联网蓝图

由于技术的迅速采用以及数据源和处理逻辑的多样性，公共服务物联网不能局限于一组严格的用例。因此，公共安全空间中的物联网设计意味着将对象和数据类型分组为可操作的类别。每个用例和每个环境可能有一个独特的架构。在所有这些架构中，公共安全物联网需要一个通用框架。图15-2所示的物联网蓝图为公共安全企事业单位提供了一个框架。这个框架是可扩展的，可用于描述几乎所有公共安全机构（无论大小）的物联网框架。通过使用该蓝图作为指南，我们可以将新的对象、物联网应用程序或需求与整体设计进行关联和调整。

公共安全参考架构

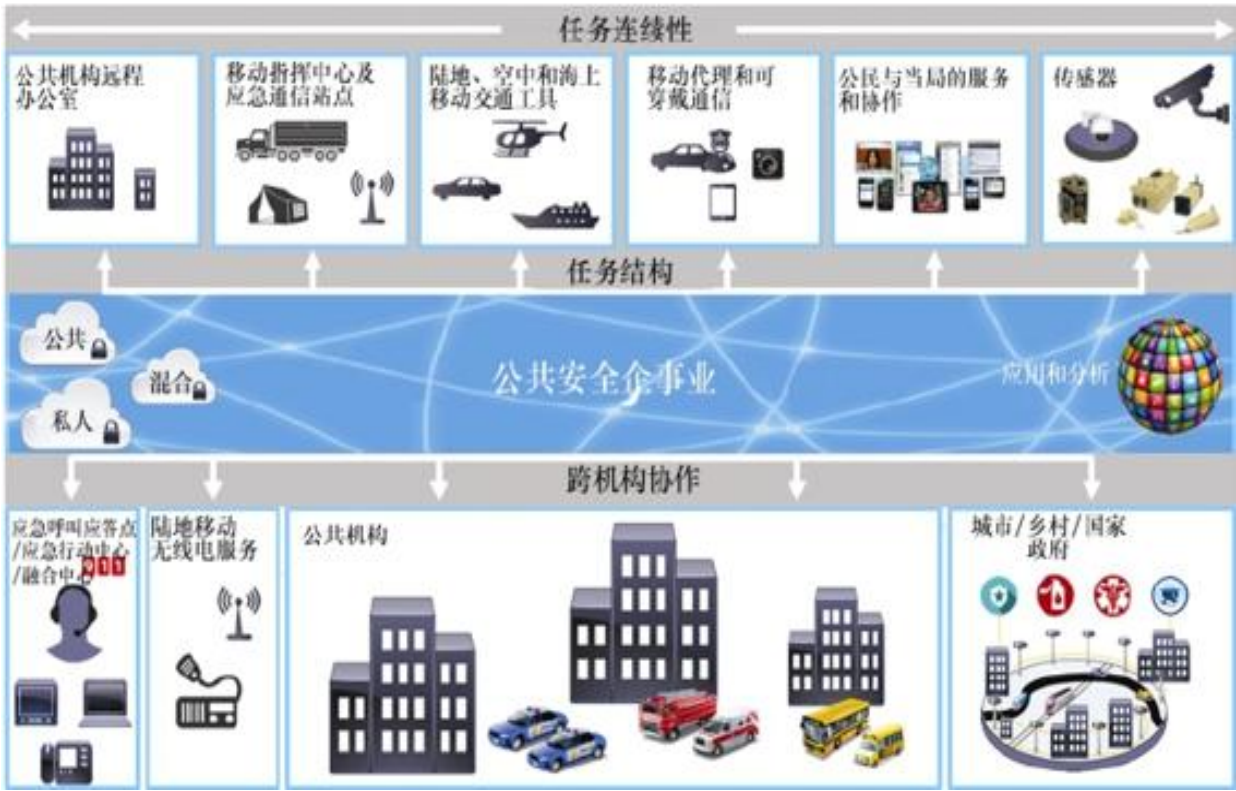


图15-2 公共安全物联网蓝图

15.2.1 任务连续性

在蓝图的顶部，6种类型的通信位置和设备确保了任务的连续性。

■ 远程办公室和固定地点：这些是固定地点，例如警察局、消防局、车厂、学校大楼或支持任务的行政大楼。在这里可以找到路由、交换、统一协作、安全和应用程序等传统网络解决方案。这些网络传输IT和OT数据。

■ 移动指挥中心和应急通信站点：这些是需要部署的临时位置，有时需要快速部署，以便为突发事件指挥、专门小组或公共安全任务中不可或缺的类似功能提供支持。这些站点的IT和OT通信可以由基于套件的或专门设计的车载连接和操作解决方案来支持。这些站点可以在本地处理从外地收集的数据和/或与系统的其余部分交互，以实现集体的态势感知。

■ 陆地、空中和海上移动交通工具：这些移动交通工具平台需要动态连接。这样的例子有支持公共安全使命的汽车、卡车、公共汽车、船只和飞机。这些车辆通常配备多个传感器和智能对象，如摄像头、平板电脑和专用设备。用于这些车辆的技术是为了应对温度、冲击、振动和湿度等变化很大的恶劣环境而设计的。这些位置还特别注意大小、重量和功率（SWaP）要求，这些要求可能受到高度限制。

■ 移动代理和可穿戴通信：这些位置是现场代理本身或其直接环境，通常形成一个个人区域网络（PAN）。这些位置的通信解决方案是手持或可穿戴的解决方案。前面提到的最小化SWaP需求的限制在这里有所增加，以避免给携带设备的个人带来负担。

■ 公民与当局的服务和协作：这是公共安全和公众通过公民与当局的交换进行协作的接口。常见的交换方式是911紧急电话和短信。许多其他的例子已经存在并且正在发生改变，这使得这种交换更加健壮，支持富媒体语音、视频和实时交互。

■ 传感器：为公共安全任务收集信息的设备。这一类别的应用可能性正在扩大。传感器可以是静态的或移动的，可以位于公共安全任务团队外部的环境中，也可以与团队设备集成。其结果是传感器网络能够收集信息，这些信息可以与应用程序、报告和分析相结合，从而驱动态势感知。

15.2.2 任务结构

在公共安全企业中，任务连续体和各种平台通过任务结构（mission fabric）相互连接。任务结构是一个动态和灵活的概念，使固定和移动平台保持连接。它提供了一种统一的无缝方法，使各种人员、过程和事物能够共享一组通用的安全策略并访问应用程序和资源，并且它不受物理层传输的影响。

■ 安全策略很重要，并且可能根据每个平台的物理或逻辑环境而有所不同。例如，在一个固定的站点，这些位置的物理安全性应该得到很好的定义，并且应该减少未经授权的物理访问和暴露的风险。在整个任务系统中，安全政策的要求不断变化。在图15-2中，外部影响和访问从左到右显著增加。这是因为平台是在社区内运行的，在某些情况下是完全无人值守的（例如远程传感器）。

■ 对应用程序和资源的访问也应在整个系统中实现无缝连接，使得在任务中的任何地方的人员都能履行其职责。这种能力可能会随着带宽和网络可用性的变化而变化，但它不应该排除或阻止通过语音、视频和数据应用程序进行统一和连续协作的能力。

■ 任何物理层传输都应与任务结构兼容，以确保无论任务必须在何处运行，都能实现连接。这意味着可以支持任何现代有线或无线技术：以太网、串行、SONET和DWDM光纤、MPLS、WiFi、商用或专用蜂窝网络、点对点和多点微波、移动自组网和卫星。

任务结构是将任务连续体连接到公共安全企业的互连网络。任务结构必须提供与位置特征（固定或移动平台）无关的无缝集成。任务

结构还确保对云中的资源的访问是统一的，并且与云类型（公共、私有或混合）无关。在这些配置中，应用程序对最终用户的可访问性应该相同。同样，数据收集、报告和分析等工具应该在公共安全企业中扩展。例如，一个消防安全官员团队应该具备与团队协作并共享关键信息的能力，无论他们在固定的基础设施现场、事故指挥所、机动响应车辆中还是步行。同样，当这个团队与传感器或公众交互时，通信能力应该被视为所有元素的无缝连接，并在整个结构中一致地提供适当的安全和策略实施手段。

15.2.3 跨机构协作

图15-2的上半部分与内部机构和公民与当局的合作有关。蓝图的下半部分涉及机构间的互动。这与前面提到的公私合作关系的概念是一致的。许多国家有各种各样的公共安全机构，例如PSAP（公共安全应答点，用于响应应急呼叫），EOC（应急行动中心，一个或多个机构在这里开会以协调应对突发事件）、融合中心（通常是情报中心，收集、分析和传播信息到当地机构）和LMR（陆地移动无线服务，用于管理一个或多个本地机构之间的关键任务的语音通信）。这些公共安全基础设施的关键要素是公共和私人组织之间协调和协作的共同点。在许多情况下，这些组织的工作人员可以由公务员（警察、消防人员、急救人员）和具有其他专业技能的第三方人员共同承担。为协作提供可靠的互联意味着将及时、准确和有意义的信息进行交换，以更精确和更有效地指导现场人员。

关于公共安全机构之间的信息共享和协作存在一个普遍的误区。在许多情况下，共享信息的困难可能是技术的限制，但这些限制往往与每个机构的任务 and 政策的多样性有关。例如，在2001年9月11日的恐怖袭击之后，有消息称无线电的互操作性问题是导致第一响应者伤亡的潜在因素。警察单位不能通过无线电与消防单位直接通信，救护车不能通过无线电与警察单位直接通信，等等。虽然技术可以改进，使急救人员能够更好地沟通，但一个未被关注的事实是，警察、消防人员和紧急救援人员的工作方式不同，使用的工作语言也不同。每个组织都接受了不同的培训，因此他们的技术、战术和程序都大不相同。

事件后的初步报告表明，如果这些机构能够直接通信，就可能挽救生命。事实上，后来的报告表明情况正好相反。将100名警察和100名消防员连接到同一个语音频道只会妨碍他们的整体表现，因为他们不会使用相同的会话协议。一个更好的模型可能是为中级主管和事件指挥人员提供一套强大的工具，用于语音和视频协作、资产位置跟踪和态势感知，他们可以使用多个操作协议，并提供更好的跨部门协调工作。随着物联网解决方案在公共安全领域变得越来越普遍，它们需要进行调整，特别是在现有的对话协议、操作方法和战术程序方面，以弥补各机构的任务。

关于公共安全如何变化的另一个值得注意的情况与移动交通工具有关。大多数公共安全机构认为车辆是办公场所的延伸。然而，随着时间的推移，这些车辆系统和功能已经得到了不同程度的实施。与拥有共享基础设施和服务设备的远程办公室不同，每个系统都像远程接入客户端那样运行，导致了车辆技术的差异，并增加了安全风险。例如，现在大多数警车中，支持CAD/ RMS的笔记本电脑可能有一个蜂窝调制解调器。车载摄像头可能也有WiFi无线电设备和蜂窝调制解调器。LPR系统可能有一个WiFi无线电设备。AVL跟踪系统可以通过笔记本电脑或车载LMR工作，也可以是独立的，并且有自己的蜂窝网络连接。其结果是运营成本以及集中统一管理和保护这些系统的难度成倍增加。这种情况不仅发生在警车上，也存在于消防车、急救车和校车上。聚合的框架和架构可以降低运营成本，增加所有系统的可用性和冗余，并支持一致的安全实践。

这一公共安全物联网蓝图可以应用于各种机构及其各种运营模式。通过参考蓝图，有助于确保每个单独的解决方案和架构适用于更大的模型。这种包容性将促进解决方案间和架构间的通信和信息共享。

要了解每一个可能的公共安全机构和部署模式，则需要多个章节来介绍。而本章的其余部分将重点介绍几个关键的例子：警察、消防员、EMS和使用物联网解决方案的学校。相同的逻辑和构造可以扩展到许多其他公共安全机构环境和用例中。

15.3 应急响应物联网架构

警察、消防员和紧急医疗服务是截然不同的组织。然而，从物联网的角度来看，它们有共同的需求。物联网使应急响应人员能够更迅速地履行其使命：保护生命、财产和证据。物联网还有助于保护应急响应供应商。应急响应人员（警察、消防员和急救人员）在非常特殊的环境中工作。与大多数其他行业的工作人员不同，应急响应人员在不可预知的环境中工作。他们在保护公众的同时，可能会招致个人风险。他们也知道自已不能独立工作，必须与其他救援人员、指挥系统和公众合作，才能成功地履行职责。本章的应急响应解决方案着眼于各种可用的物联网能力，以支持公共机构的使命。

本书其他章节中讨论的大多数物联网架构都是以垂直方式组织的，从街道层面到核心的应用程序。应急响应物联网架构的情况略有不同，因为它是围绕移动或静态指挥或应急中心组织的。这些中心需要建立与现场人员的下行通信，并从各种传感器收集数据（直接来自传感器、来自雾计算系统，或者来自云应用程序）。因此，连接性是这种拓扑结构的首要关注点，它驱动着与指挥中心互连的各种元素的体系结构。

图 15-3 显示了各种可能的应急响应移动平台，以及它们如何通过移动服务门户连接到云。在这种环境中存在3种常见的移动平台：移动代理、移动指挥中心和移动车辆。



图15-3 应急响应任务组组织架构

15.3.1 移动指挥中心

移动指挥中心是固定办公场所的延伸。在紧急情况下，如炸弹威胁、火灾或自然灾害，移动指挥中心作为一个通信中心，可以用来进行战略会议和其他战术行动。它被部署在应急机构所在地附近或现场，以帮助评估紧急情况，并促进与当地利益相关者的实际互动。因此，移动指挥中心的需求与静态办公室的需求相同。

图 15-4 显示了一个典型的移动指挥中心架构。它的目的是提供一个移动办公环境，类似于机构的固定办公地点的环境。主要的区别是指挥中心可以完全独立于企业进行操作，也可以是功能齐全的远程办公室。大多数移动指挥中心在两种可能的状态下运行。在第一种状态下，它们移动到感兴趣的区域，在移动过程中通信系统的功能会受到限制。一旦到达现场，它们会进行一个简短的设置过程，包括激活

通信系统、部署带有天线和传感器的天线，以及扩展隔间，以增加内部工作空间。此时指挥中心处于第二种状态，并完全投入运行。当任务完成后，这个过程被逆转，以允许车辆移动。这种操作方法被称为“暂停通信”，因为车辆在开始工作之前必须停止移动。

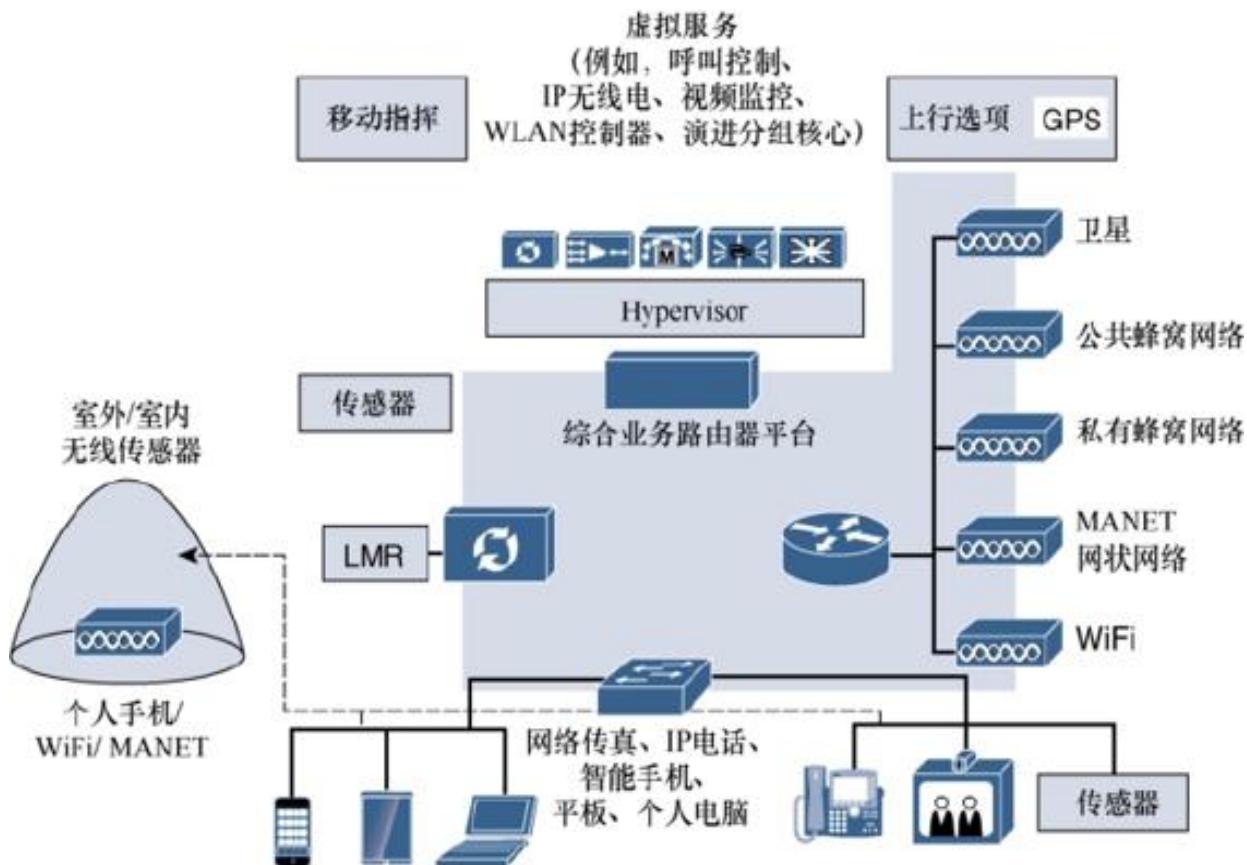


图15-4 移动指挥中心

1. 网络及安全服务

移动指挥中心通常有足够的空间来支持传统的IT设备，包括19英寸的机架安装空间。这使得可以使用路由、交换、无线控制、安全和计算服务的许多标准产品。指挥中心与标准远程办公室的不同之处在于，它与云的所有连接通常都是无线的。

移动车辆架构基于这样一个概念：任何上行链路技术都应该是到达企业云的有用工具。这意味着几乎任何有线或无线技术都是可以接

受的。例如，可以从本地互联网连接源提供有线以太网连接。如图 15-4 所示，有许多可用的无线选项。这些可以通过策略进行配置，以支持各种配置，例如主动/备用和主动/主动负载共享。从一种链接技术到另一种链接技术的自动故障转移能力是该架构的固有特性，应该在所选的解决方案中强制实现。应该选择 IP 服务水平协议（IP SLA）、链路跟踪、双向转发检测（BFD）和路由协议等工具，这些工具能够实时识别条件并更改当前操作配置，以确保始终在线上行，同时根据任务需求优化并平衡带宽和成本。主动/主动负载共享也可以通过多种方式实现，例如使用基于策略的路由（PBR）、性能路由（PfR）和网关负载平衡协议（GLBP）。这可以形成一组灵活的工具，允许在高度可扩展的模型中使用几乎任何无线或有线上行链路路径的组合。

使用一个或多个无线上行链路的决定通常是基于本地可靠性、成本、性能和可用性做出的。卫星和 4G 蜂窝网络是最常用的选择。然而，卫星连接可能很昂贵，还可能导致 600 毫秒或更大的往返延迟。当可用时，蜂窝网络通常比卫星网络更受欢迎，因为同等带宽的成本和延迟更低。在大多数城市环境及其附近地区，4G LTE 蜂窝服务是可用的，可以以合理的价格提供良好的性能，1~30Mbit/s 带宽对应的往返延迟为 30~80ms。

一些公共安全机构正在使用一种称为 MANET（移动自组织网络）的独特无线技术。MANET 无线技术能够自己形成对等网络。当两个或两个以上的 MANET 无线网络可以互相连接时，它们可以建立一个高速的第二层链路。这些无线网络也允许支持中间节点跳数的节点形成网状网络。这意味着如果两个节点相距太远，但是有一个或多个中间节点可用时，这些节点可以一起工作，动态地形成多跳的端到端连接。MANET 是自我形成和自我修复的。它们的范围是灵活的，因为它们可以改变频率以适应范围和链路条件（30MHz~5GHz）。一些节点可以通过快速连接（例如，WiFi 或以太网）连接到 Internet，并与其他远程节点共享连接。MANET 无线技术在军事和政府的使用案例中越来越受欢迎，每台无线设备的价格下降到公共安全领域能够采用该技术的程度。因此，图 15-4 中的架构显示了用于上行链路和客户端访问应用程序的 MANET 无线技术。

在公共安全领域，私有蜂窝网络服务是一个不断发展的概念。许多国家正在采取重大举措，部署使用4G LTE技术的国家公共安全宽带网络。这些网络在一个专用频段中运行，与传统的服务提供商系统相分离。无论公共商用蜂窝服务的状况如何，私有蜂窝网络能确保公共安全机构能够进行通信。在图 15-4 所示的架构中，移动指挥中心可以作为客户端访问私有蜂窝系统，并将该服务用作上行链路。

作为公共安全事业的一部分，移动指挥中心必须提供与机构远程办公室类似的安全通信和数据隐私支持。由于移动指挥中心使用与远程办公室类似的设备，因此可以在两端实现相同的安全策略和功能。在这种情况下，可以从两个方面考虑安全性：物理安全性和网络安全性。物理安全可以通过访问控制、警报和视频监视系统来解决，就像在机构的远程办公室一样。各种物理安全解决方案提供了标准的物理访问读卡器和门执行器，如图 15-5 所示。物理访问控制还可以包括各种资产控制标记、身份管理解决方案和警报面板。IP摄像头非常适合于从车辆周围收集视频流，记录内容以供查看和回放，并将视频分发给事故区域的人员。

移动指挥中心的网络安全应符合或高于机构远程办公室使用的政策和程序。在移动指挥中心架构中，路由器是车辆与外界连接的共同集成点。因此，路由器必须提供高级安全服务（例如，高级加密、防火墙服务、威胁保护、VPN），以便在通过无线上行链路连接到企业时保护数据。它还可能需要保护本地Internet访问连接。

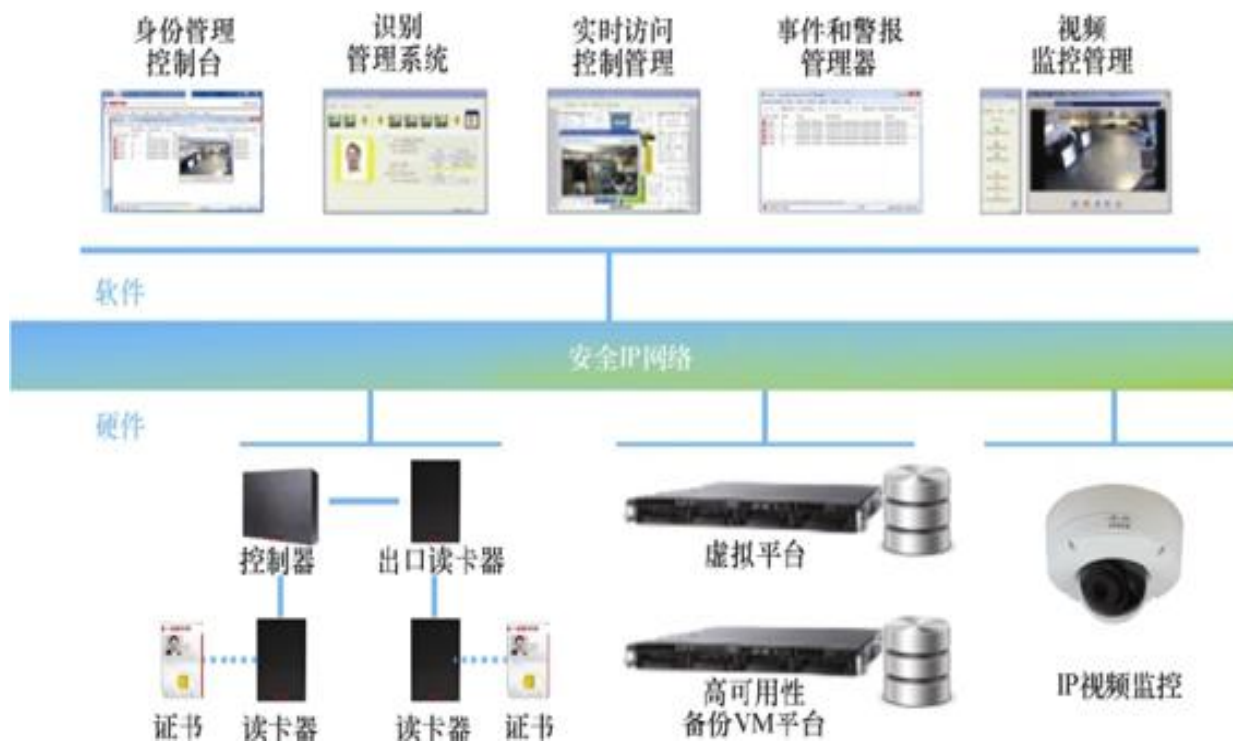


图15-5 访问控制与视频监控集成

保护开放的以太网端口和无线访问是移动指挥中心的一个重要考虑因素。在移动平台中，这一点尤其重要，因为公共安全机构之外的人员可以接触到IT基础设施。图15-6提供了一个用例。移动指挥中心不具有与固定办公室相同的物理安全保护。在指挥中心范围内的任何个人都可以探测到WiFi网络，并试图窃听、劫持或中断通信。常见的部署模型使用基于WLAN控制器的架构，其中AP位于指挥中心，而WLAN控制器位于静态办公室。AP通过WAN上行链路连接到WLAN控制器。用户身份验证通过中央WLAN控制器和RADIUS服务器进行。命令中心交换机上的任何端口也受到802.1x身份验证的保护。如果无法验证访问请求，则本地交换机或WiFi接入点上的策略可以完全阻止访问或限制访问，直到能够提供身份验证为止。这种方法确保对有线和无线连接的访问进行统一管理，并基于对车辆的物理访问来缓解威胁。



图15-6 WiFi通信架构

虽然车辆上的接入点配置为提供本地服务，但集中式管理方法提供了更高的安全性和一致性（中心团队管理所有部署的无线系统，而本地团队专注于任务）。这确保了公共安全企业中有一组通用的安全策略和访问设计。如果移动指挥中心的WiFi基础设施与固定办公环境中的WiFi基础设施相同，还可以减少终端用户的培训需求。

移动指挥中心可以在事故中为授权机构人员和其他人员提供支持。很多时候，当指挥车出现在事故现场时，它可以为其他合作机构和公众提供协助，特别是那些需要上网的人。利用前面讨论的解决方案，可以使用来宾网络向外部机构人员和公众提供有线和无线连接。这些连接可以直接指向本地Internet连接，也可以通过广域上行链路连接到企业云进行处理。两种配置都可以应用Web过滤、病毒扫描和类似服务等安全特性。

WAN 链路是此类部署中的一个常见瓶颈。3 个关键特性对于成功运行至关重要，特别是在使用卫星服务的情况下。

■ 延迟：众所周知，通过卫星使用IP应用程序的问题是，当网络的往返延迟超过500ms时，网络流中的TCP窗口大小将缩小，以适应网络延迟。不幸的是，即使是单个卫星跳转也会带来至少550~600ms的往返延迟。大多数卫星调制解调器提供商都试图通过实现性能增强代理（Performance Enhancement Proxy, PEP）或类似的服务来解决这

个问题，以便动态地检查和改变网络流中的TCP窗口大小。如果PEP不可用，任何卫星连接的可用带宽都会被大量闲置，并将最终用户的性能限制在非常低的水平。当PEP可用时，性能会得到极大的改善。

■ 加密：为了满足安全需求，路由器通常被配置为在网络流量到达卫星调制解调器之前对其进行加密。这可以防止调制解调器中的PEP服务看到TCP流量。在这种情况下，可以在路由器后面安装本地服务，通过WAN链路提供PEP功能和压缩，如图15-7所示。

■ 设备或虚拟机：本地PEP服务可以是独立的设备、虚拟机或嵌入到路由器中的模块。这种方法可以极大地提高WAN上行链路的性能，使链路利用率接近100%，并可以实现较高的压缩比（100:1）。

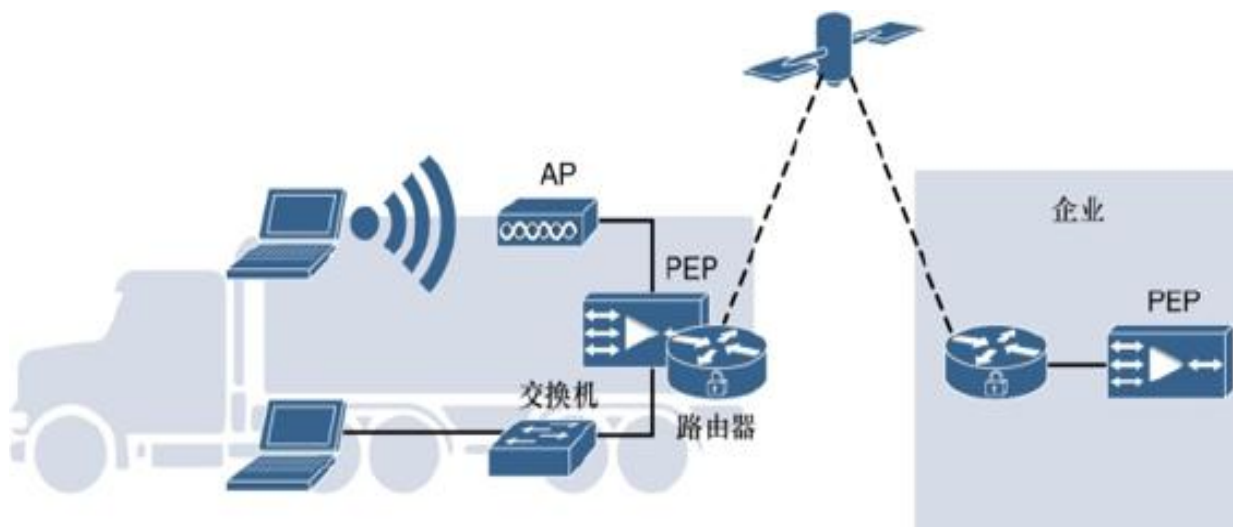


图15-7 WiFi与卫星通信架构

2. 计算和应用服务

移动指挥中心需要灵活，能够支持任务的动态特性。计算和应用服务需要与企业与事件区域资源进行交互和无缝地协同工作。在企业云不可用时，这些服务还需要自给自足，移动指挥中心是在事故中一个机构的指挥结构的唯一可用表示。这些被称为从属和独立的运营模式。为了同时支持有依赖性和独立的运营，移动指挥中心应该具有本地计算能力，能够承载虚拟机和应用程序。托管应用程序可以通过专

用服务器或通过路由器中的嵌入式功能实现，这两种方式都是为支持应用程序虚拟化而设计的。

移动指挥中心的效能在很大程度上取决于其IT和OT能力。语音、视频会议和数据共享的传统IT功能为指挥中心提供了基础。特定于OT的应用程序，如CAD、RMS、COP、车队管理，以及在此基础上添加的类似工具，为公共安全添加了处理用例。

IT语音和视频通话服务的本地控制是协作的核心。它允许移动指挥中心在与企业云连接或不连接的情况下进行操作。当指挥中心可以访问企业云时，网络语音、视频通话等服务可以保证安全，降低运营成本。在独立模式下，指挥中心和语音服务提供商之间可以直接通过互联网连接建立VoIP语音服务。只要指挥中心至少有一条上行链路能够接入互联网，就可以建立语音服务。这种方法可以是直接向内和向外拨号的主要方法，也可以是备份方法。使用适应性强的解决方案提供了许多灵活的功能。例如，工作人员可以使用指挥中心的一个开放工作区，登录到桌面上的电话，然后开始使用自己的电话号码拨打和接收电话。在这种情况下，桌面电话使用扩展移动性来为最终用户提供适当的个性，允许用户在任何位置都可以被联系到。用户可以在完成后注销手机，以便下一个用户使用。通过个人通信客户端应用程序还可以提供来自计算机、智能手机和平板电脑的即时消息、状态信息以及语音和视频拨号。在运营环境中，办公空间和对物理电话或视频终端的访问可能是有限的，拥有这样一个灵活的通信工具可以增加人员的可用性，并降低事故的复杂性。

按键通话语音是公共安全机构的一种常用语音。移动指挥中心依赖对其LMR系统的访问来有效地与现场人员进行交互。一种基本方法是在指挥中心安装便携式手持或传统车载移动无线电。这可以在每一张办公桌上进行，也可以在带有扬声器和麦克风的遥控头的橱柜中完成。这种方法很常见，但是存在一些问题。在繁忙的环境中，让许多扬声器发出刺耳的声音会增加噪声，分散注意力，降低运营效率。此外，决定在每个办公桌上安装哪种无线电设备也很有挑战性，因为每个办公桌位置的功能角色可能会由于任务的不同而发生变化。安装过多的LMR设备或安装错误的类型可能是一个昂贵和浪费的错误。使用高

级的无线电控制系统（见图15-8）集中管理指挥中心的无线电，并动态地将访问权分配给用户，是一种可扩展、灵活的方法。它允许任何用户通过安装在Android或Apple智能手机或平板电脑上的移动客户端访问车内的任何无线电设备。这种系统还可以通过到企业的IP连接与现有的无线电基础设施集成。这一点很重要，因为它可以最小化系统所需的无线电数量。它还可以增加指挥中心的可访问性，包括该机构和任何其他合作机构可用的任何当地公共安全资源。



图15-8 IP广播示例

IT电话会议、视频会议、Web和白板协作是当今大多数人（包括公共安全人员）用于协作的工具。提供这种服务的软件解决方案在移动指挥中心很常见。

公共安全机构特定的OT应用程序也可以通过移动指挥中心托管和/或访问。这些CAD、RMS、LMR调度、PSAP呼叫管理和EOC管理工具可以在部署期间使用。这些车辆中开始出现的另一个应用程序称为通用操作界面（COP），如图15-9所示。与CAD工具不同，COP旨在用于显示各种资产的实时战术操作，如人员、车辆、无人机和传感器。大多数COP工具与诸如视频源之类的富媒体集成，可以引导COP的其他用户查看感兴趣的内容。COP还支持触屏感应，可以在地图、图像甚至视频显示器上徒手绘制或使用多边形。例如，队长可以使用COP来指挥野战部队朝目标前进。COP工具的一个重要特征是，任务中的每个人都可以看到一个共同的画面；以前的态势感知工具只允许主管或指挥官看到整个画面。在移动指挥中心中拥有这种灵活性可以允许平台根据事件承担各种角色，例如PSAP恢复解决方案、事件指挥所、联合作战和协调中心或特别任务组任务。



图15-9 智能手机上的通用操作界面（COP）

15.3.2 移动交通工具——陆、空、海

公共安全移动交通工具架构如图15-10所示，描述了用于公共安全的各种移动平台。这种架构类似于前一节中的移动指挥中心，但是有几个重要的区别。最重要的区别是，移动指挥中心架构以车辆暂停或停车时进行通信为基础。移动指挥中心还可以通过企业网络和云服务自主运行。陆、空、海三种移动交通工具架构是为移动通信而设计的，同时也是公共安全企业的延伸；因此，它通常依赖于应用程序等企业服务。这些平台不使用有线上行链路通信。当交通工具在陆地、空中和水上行驶时，它们依靠无线上行链路和点对点连接。

另一个重要的区别是移动工具的物理和环境特性。实际上，这些工具内部的物联网解决方案必须是独立的，或至少提供最小的设备占用空间。这些工具是为执行任务而设计的。例如，消防车或EMS车辆有许多专用设备部件。分配给通信、传感器或数据处理单元的空间必须尽可能小。在环境方面，这些交通工具在高温和低温下运行，经历冲击和振动，并暴露在潮湿、潮湿和灰尘中。虽然通用设备可以用于这些交通工具，但环境条件会大大缩短电子设备的寿命。一些专用交通工具，如飞机或船舶，可能需要设备经过适航性认证或在恶劣条件下使用。为了解决物理和环境要求的问题，公共安全机构定义了车载设备的尺寸、重量和功率（SWaP）规范。它们还需要工业级、公共安全级或军事级的强化。

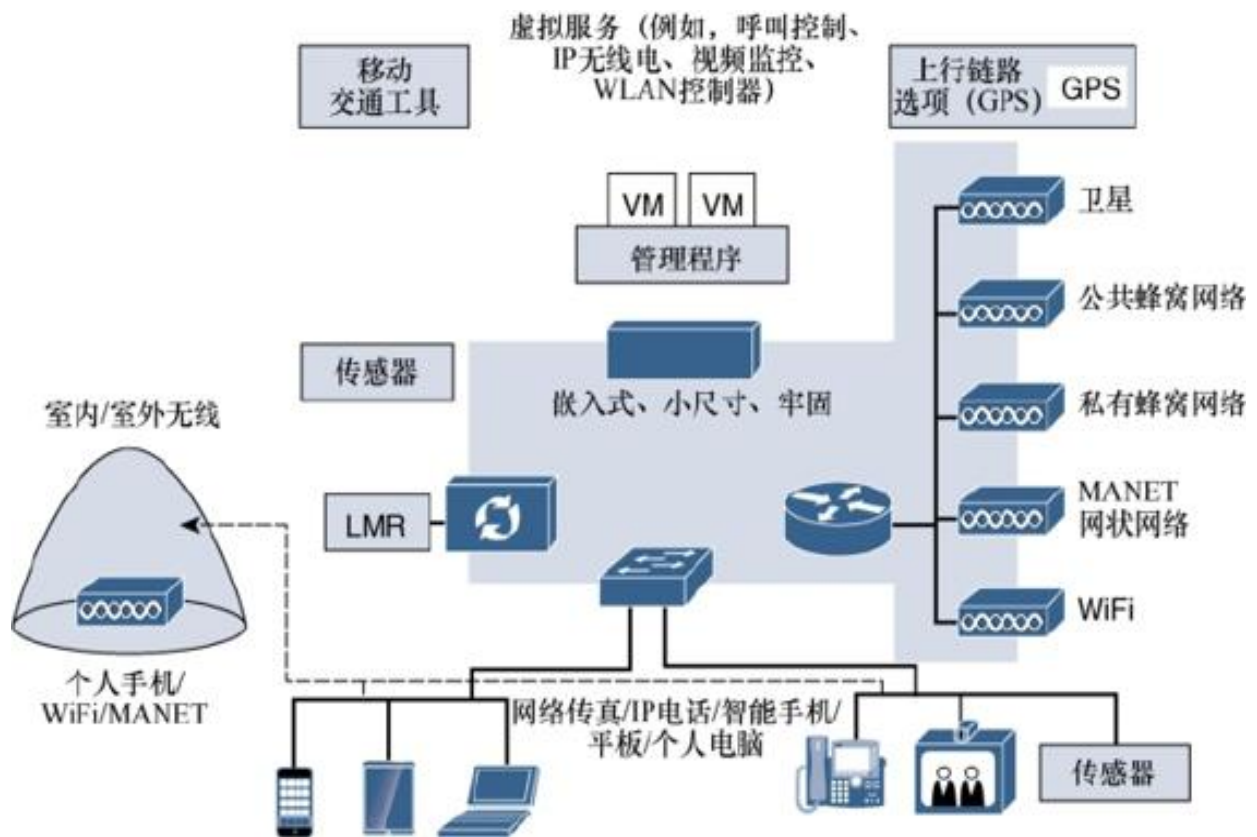


图15-10 陆地、空中和海上移动交通工具

1. 网络及安全服务

陆地、空中和海上交通工具需要能够满足SwaP和强化规模的路由、交换、无线、安全和计算能力。这种网络设备允许扩展工作温度范围，并且许多设备都无须内部冷却风扇即可运行。该设备必须设计成在直流电源上运行，且有较大的上下限范围。它需要更高的耐湿性，而且一些设备也需要加固以抵抗冲击和振动。它还要小巧，有时可以直接集成到交通工具上。

这些交通工具对上行链路无线电灵活性和多样性的需求与移动指挥中心相同。然而，携带许多无线电或大型天线（如卫星天线）的方案可能不切实际。此限制将上行链路集中于一组更受限制的通信媒体。交通工具的大小、用途和部署模型（包括射程和部署环境）通常决定了上行技术的选择。

交通工具本身可以通过DSRC等技术连接到周围的物联网架构（DSRC在第13章中有详细介绍）。该技术使交通工具能够获得特权访问，并交换有关旅行路径或其他车辆的信息。例如，传感器越来越多地安装在铁路交叉口的位置。当火车在交叉路口之间运行时，交通数据可以通过LTE传输到OBU。可以利用多个物联网系统来实现这一目标。列车可以与中央控制系统（LTE、卫星或轨道沿线的有线网络）实时通信。然后可以（使用API）将这些信息导出到云中的应急导航数据库。然后，根据每个应急车辆的行驶路径，将这些信息的相关部分推送到各个应急车辆上。与此同时，火车可以向铁路道口传感器发出信号。这些传感器可以将这些信息传递给正在接近的车辆（DSRC或其他）。对于紧急服务车辆，其结果是车载导航系统可以考虑应急车辆的速度和铁路道口的可用性，从而在必要时动态地改变车辆的路线，避免在封闭的铁路道口浪费时间。

同样地，急救车可以通过较低的ISM频率（例如433MHz）或DSRC与智能交通灯进行通信，以确保在前往紧急地点的途中总是绿灯。这种控制通常是分散的（车辆在接近交通灯时直接与其进行通信；指挥中心不需要协调灯光）。当车辆在路上时，总部团队可能能够访问到从紧急情况现场周围获得的数据，如本章前面所述。然后，当车辆接近紧急情况的位置时，将这些数据的子集输入车辆计算系统。因此，反应小组可以获得与任务有关的有用数据，例如建筑物的楼层数、楼层平面图、住户人数、附近消防栓的位置、该地点或附近地点的犯罪记录、附近环境传感器的数据（例如，是否存在烟雾、有害气体）。在应急响应过程中，智能对象可以提高响应的效率。例如，当使用EMS车辆时，平板电脑用于输入基本诊断信息，帮助接收医院准备好合适的设备和团队。

对这些交通工具来说，物理安全也是一个挑战。如果车辆或船只足够大，可能需要使用移动指挥中心等物理安全解决方案。否则，物理安全可能仅限于汽车后备箱或设备锁。这些交通工具的视频监控取决于交通工具的类型及其职责。例如，警车通常都配备了行车记录仪，许多警车都在拘留区部署摄像头和麦克风。车载录像机对车辆结构有特殊要求，以避免通过4G蜂窝网络等计量服务上传本地录制的视频。大多数机构倾向于在车辆接近警察局或类似设施的WiFi接入点时

上传视频。这意味着车载路由器必须具备应用感知功能，只有在WiFi可用时才允许上传视频。

移动交通工具的网络安全特性与移动指挥中心的网络安全特性基本相同，例如健壮的AES 256位加密、有状态防火墙检查和VPN。高级的威胁保护服务可能会受到较小的路由平台性能的限制。在需要考虑威胁保护的情况下，在车辆中添加计算资源可能是最好的方法。

上行链路压缩和优化对于使用受限的无线上行链路（如蜂窝网络和卫星服务）的移动交通工具至关重要。然而，大多数陆地车辆不使用卫星作为上行链路，除非它们经常在蜂窝网络覆盖范围之外运行。飞机和一些大型的或长距离航行的海上船舶通常会用到卫星通信。

2. 计算和应用服务

与移动指挥中心相比，陆地、空中和海上交通工具有不同的计算和应用服务需求。移动交通工具更侧重于执行特定的、通常是短期的任务。任务的主要部分是与企业协作，这意味着需要共享通信和应用程序。不过，有时人们的注意力会转移到某个特定事件上。在这种情况下，可以理解为协作减少，应用程序受制于事件区域内的可用性。其结果是，大多数移动交通工具只在本地携带很少的应用程序集（主要是客户端功能），并且依赖于企业或命令中心来承载应用程序。这种逻辑的一个典型例子就是一键通语音服务。

车载移动和手持便携LMR设备一直是公共安全通信的主要方式。这些设备使用通信基础设施进行远距离通信。基础设施包括基站、互联和中央交换功能，这与企业云模型提供的功能非常相似。急救人员也以点对点的方式进行本地通信，称为视距、对讲或单工模式。这种通信独立于更大的通信基础设施。然而，基础设施支持与更广泛的机构进行协作。在一个事件中，大多数机构训练他们的人员在单工模式下工作，或者至少在战术谈话组中工作。这种模式的主要好处是效率高。对讲模式消除了对基础设施的任何依赖，并将范围限制为紧急场景附近可用的媒介。该模型将通信重点放在事件区域活动上，避免了

广域基础设施资源的紧张（广域基础设施资源在LMR系统中总是受到约束）。这种模式还避免了通过本地对话来分散机构中其他成员的注意力。虽然仍然可以与该机构进行联系，但仅限于特定要求。物联网改变了一键通公共安全语音环境。在21世纪的前十年中，一键通语音和IP相结合，提供了基于IP的广播（RoIP）。无线网络的可用性促使公共安全采用RoIP。一个关键的影响因素是商业4G LTE服务的覆盖范围和可用性不断增加，这些服务现如今更多地在地地铁、城市甚至农村地区提供高密度的覆盖。私有专用蜂窝网络程序，如FirstNet，也在不断发展，为公共安全提供关键任务级别的蜂窝网络。RoIP的应用程序也在不断发展，扩展到软客户端和寻呼业务。

在RoIP和FirstNet等网络完全取代LMR之前，必须克服各种限制。与物联网相关的一个问题是，需要为移动通信提供依赖和独立的操作模式。负责LTE和未来蜂窝技术的标准组织“第三代合作伙伴计划”（3GPP）正在研究一种解决方案，使蜂窝智能手机和类似设备能够以独立于基础设施的模式（即“对讲模式”）运行。其他问题包括电池寿命、信号和应用程序交互。

诸如语音和视频会议、即时消息、在线状态和Web协作等协作工具需要访问企业云，以便在事件区域之外进行协作。如果应用程序托管在企业云中，没有可行的上行链路连接，协作是不可能的。这种情况类似于广域一键通语音的LMR基础结构模式。

公共安全专用工具，如CAD、RMS和COP，是移动交通工具的一个重要讨论领域，因为它们满足了该机构的特定任务需求。CAD和RMS从20世纪90年代开始出现，有助于管理工作流程和现场人员。它们还允许现场代理运行查询和报告。这些应用程序是基于客户端/服务器的，这意味着它们能够访问车辆中有限的计算能力，并且依赖于上行链路连接和企业云来访问应用程序和数据存储库。为了避免连接减慢或间断的问题，传统的CAD和RMS应用程序需要使用会话持久性软件来维护应用程序连接。该软件还提供VPN服务来保护应用程序。下一代CAD和RMS应用程序是为移动工作人员设计的；它们不存在会话持久性问题，并且支持嵌入式安全性，以最小化对VPN软件的依赖。

COP是用于公共安全的下一代应用程序，它提供了对事故区域环境的实时视图。它可以在客户端/服务器模式下工作，其中一个或多个服务器从网络周围的客户端收集多播事件，并将其分发给所有其他客户端。它还可以在事件区域模式下运行，在这种情况下它是独立于大型企业的。后一种情况可能是有限的网络连接的结果，也可能是为了控制协作和信息共享的范围而设计的。这种事故区域模式很好地映射到移动交通工具架构。回想一下，交通工具可以使用各种上行链路和点对点MANET无线网络。这种设计允许路由器动态管理链路，并允许COP在客户端/服务器或对等模式下工作。

车辆平台内嵌入的计算资源根据应用程序的需求来调整大小。许多车辆平台应用程序通常运行在笔记本电脑、智能手机、平板电脑或类似的客户端计算设备上。在一些新的部署模型中，客户端计算机的性能有限，只提供远程键盘、视频和鼠标（KVM）功能或轻量级虚拟桌面功能。这种方法限制了客户端计算机的配置和管理负担，并将处理过程转移到企业云。

一段时间以来，车内视频管理已经可供公共安全和其他车队车辆来使用。在许多情况下，这些解决方案独立于车辆上的其他设备。通过在车载平台中嵌入视频管理系统，该系统可以作为整个企业的一部分进行集中管理和操作。远程信息技术是这种集成概念的另一个例子；它提供了通过企业来监视和控制车辆的能力。用例之一是连接到车辆的机载诊断（OBD）接口。OBD接口可用于所有现代车辆。利用OBD接口可以收集和报告车辆的运行特性，包括确定维护需求、驾驶模式和制动状态。车辆系统（例如门锁）也可以远程控制。应急灯、警报器、武器柜和车辆的其他功能也可以进行监测。在过去，传感器事件和通过OBD接口监控的事件被实时传输回企业。在覆盖率低的地区，信息可能会延迟或丢失。如今，车辆平台包括雾计算代理和运行在车辆内部的轻量级微服务。雾代理可以收集、存储、处理和合成数据，然后将原始数据或合成数据传输回企业。还可以与事件区域对等点共享数据。当车辆处于覆盖不良的区域时，雾代理尤其有用。代理可以检测网络条件并保存数据，直至连接恢复。

物联网为公共安全和应急响应提供了许多有用和重要的好处。移动指挥中心和陆、空、海移动交通工具平台建立在一个共同的参考设计基础上。影响这些平台的因素与它们的操作、物理需求和环境需求相关。操作需求有助于确定可用的功能级别。功能的变化取决于车辆是否连接到企业网络或从企业网络断开，以及响应者是在广域还是在事故区域中工作。物理需求涉及设备的交换空间，以及设备与车辆的集成。环境需求用于确定加固的操作阈值。由于这些解决方案适用于特定的公共安全机构，因此需要考虑网络、安全、计算和应用服务选项，以满足每个机构的特定需求。

15.4 物联网公共安全信息处理

物联网是一个可以感知和传输数据的物理对象网络。处理这些数据是物联网的关键部分，详见第7章。在公共安全方面，特定的智能对象有助于加速应急响应。例如，烟雾探测器和火灾报警器是众所周知的对象。通过物联网，这些物体可以连接到互联网，并向最近的消防部门发出警报。同样，这些传感器可以互相通信。如果邻近的房屋或建筑物失火，这种通信方式可以通过特定的声音或铃声模式触发火灾警报，从而采取主动措施。

在学校、大学和犯罪敏感的社区，通常会部署枪炮探测器。这些传感器处理声音，以搜索特定的枪声模式。如果检测到这种模式，警报将通过有线或无线通信链路自动发送到最近的警察局。事件检测时间的缩短会同时导致总体响应时间的缩短。

视频处理在公共安全领域的应用越来越普遍。新的机器学习算法提高了人脸识别的成功率，处理犯罪现场的图像已经成为一个常见的物联网应用。实时视频通常也被用来在多种紧急情况下提供远程专家协助，包括涉及事故、特定危险材料和自动人群运动模式分析的紧急情况。视频还被用于与紧急情况无关的公共安全案例，以提高效率并减少与交通相关的风险。例如，视频传讯和远程出庭的应用已经成为

普遍现象，这降低了运输罪犯的成本和风险。远程语言翻译也可以帮助急救人员与讲不同语言的市民进行交流。

大数据也被用于公共安全。例如，可以对犯罪数据进行详细分析，以提供犯罪可能性的预测。大数据系统无法预测未来。然而，这些工具可以分析过去的犯罪特征并绘制犯罪行为模式，从而推断未来犯罪活动的可能性。图15-11显示了一个示例。

警察部队可以利用这些信息在正确的地点部署适当数量的警察，以防止犯罪发生。

许多其他公共安全机构也采用了同样的逻辑。例如，消防部门使用机器学习来交叉分析数据和预测火灾。信息可以包括明显的元素，如火灾历史或建筑材料。在火灾发生前，可以采取主动措施避免火灾。



图15-11 预测犯罪审计报告

15.5 校车安全

公共安全不仅限于应急服务，还包括涉及公众及其安全的任何领域。今天，物联网正被应用于校车，为交通主管、家长、校长和学生提供新的能力和洞见。架构的很大一部分直接关系到学生的安全。此外，校车现在能为车上的学生提供网络连接和完成家庭作业的服务。从本质上说，校车成为了校园网络的延伸。图15-12显示了该架构和所提供服务的示意图。

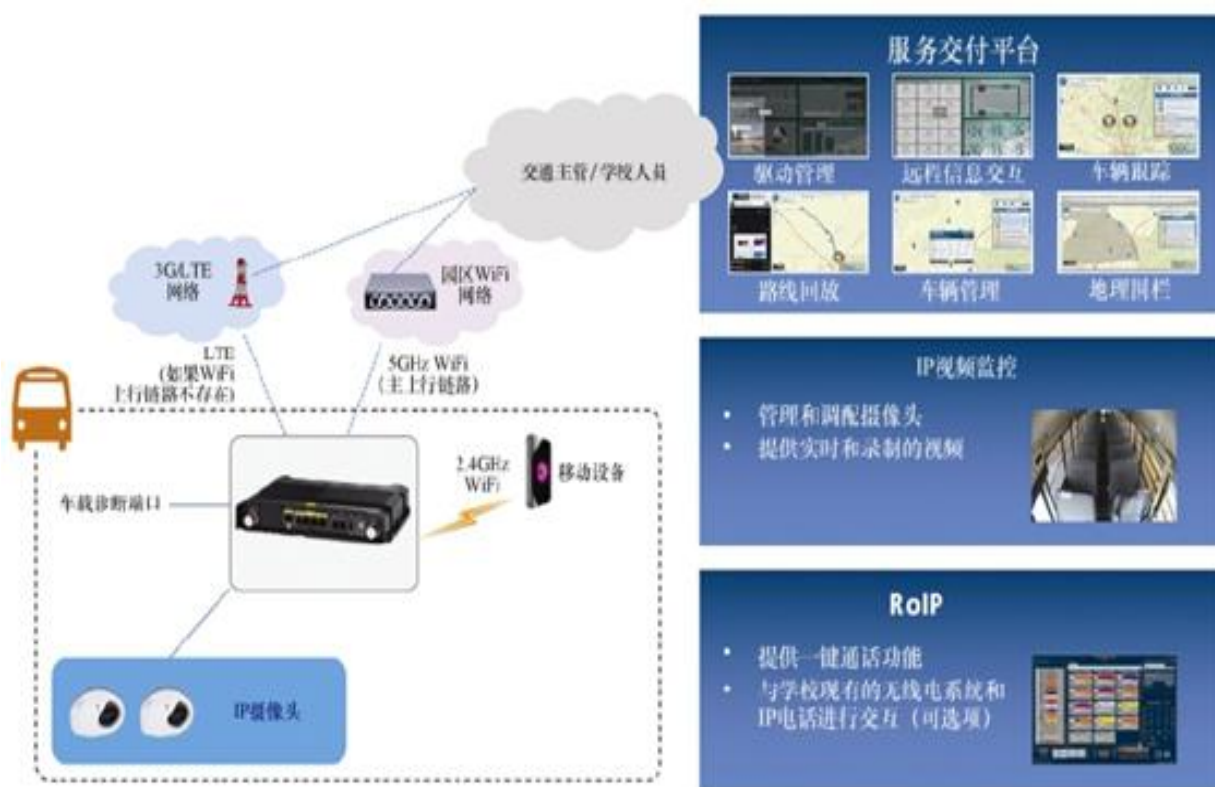


图15-12 校车安全通信架构

15.5.1 校车位置及学生上下车情况

家长和学校工作人员每天面临的一个大问题是需要知道校车的位置，以及学生是否在校车上。有可能成为一个更大的问题的是，在学区分布广泛的地理区域，有一个巴士站，学生必须换乘巴士。学校交

通主管通常要等到所有的学生都清点完毕，所有的公共汽车都返回到车场后才算结束工作。在很多情况下，如果学生没有按时回家，家长会打电话给交通部门找学生。没有物联网的帮助，交通部门的工作人员只能通过电话或无线电设备来确定学生是否在车上。在许多情况下，校车司机可能不知道确切的情况（也许是一个不认识所有学生的替补司机）。很有可能某学生当天没有上车（可能是留在学校进行课外学习或活动），或者可能是学生下车到一个朋友家去了。在物联网的帮助下，交通主管可以实时了解一辆巴士的确切位置、学生在车上的位置以及学生上下车的位置。现在，当父母打电话找他们的孩子时，交通主管可以准确回答，“你的孩子下午 3:30 在史密斯琼斯街的拐角处下车”。或者，也许交通主管会回答，“你的孩子今天没有上车”。

只要知道公共汽车的位置就可以对交通主管部门大有帮助。当学校的巴士离学校很远时，该功能特别有用。在发生与安全相关的事故时，运输主管可以准确知道将应急响应人员派往何处。交通主管部门还可以大致了解校车到达给定位置（可能是校车停放场地）的时间，并且如果校车已经超出了预先定义的边界，则可以发出警报（这就是所谓的地理围栏）。

15.5.2 司机的行为报告

具有位置和远程信息的另一个优点是可以监控校车司机的行为。例如，如果校车司机超过了安全速度，可以向交通主管发出警报。此警报可以实时发生，也可以记录在数据库中。在一次调度中，一位忧心忡忡的家长打电话给学校，报告说几天前他曾跟在一辆运行的校车后面，而那辆校车当时的车速很快。学校工作人员回顾了校车路线的整个行车记录，发现校车确实开得太快了。此外，学校工作人员还可以查看校车上的历史录像，以确定校车上是否存在某种分散注意力的因素，从而解释车辆超速的原因。

图15-13显示了驱动行为报告的另一个示例。这种类型的报告是用于确定某个司机是否在公交车站为寄宿学生安全就坐而提供了足够时

间，或者某个司机消耗的燃油与里程不合理，原因是在一条路线上花费了过多的空转时间。这类报告可以促进更安全的驾驶并节约成本。

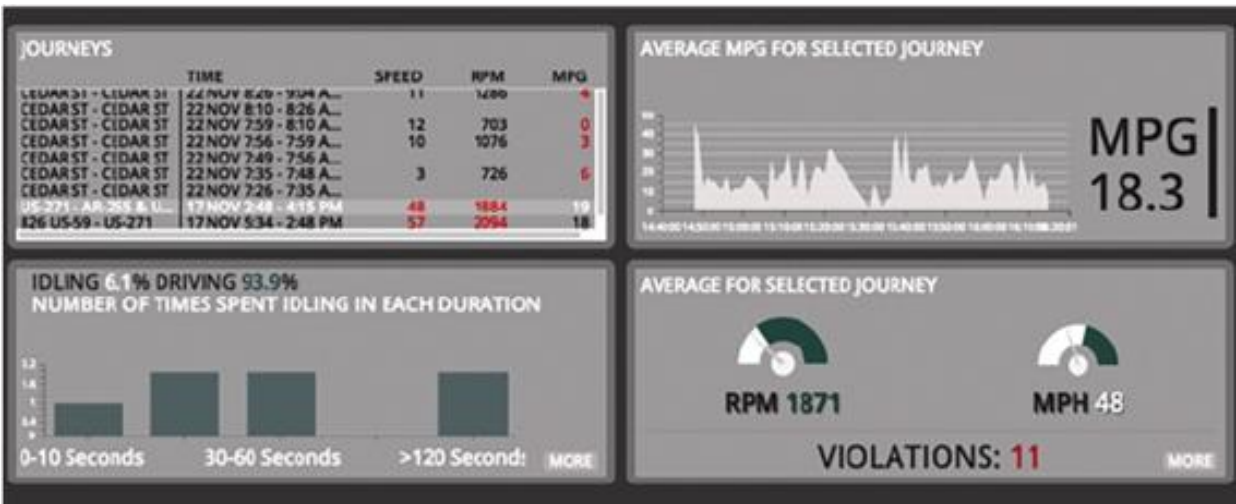


图15-13 校车司机行为报告

15.5.3 诊断报告

在许多情况下，早在任何明显的症状出现之前，OBD端口就报告了一个问题。通过从校车收集这些数据，可以自动地提醒维护人员可能出现的问题，而无须亲自前往校车处对其进行检查。

15.5.4 视频监控

校车安全解决方案最广泛使用的一个功能是视频监控。视频监控可以用来监控学生在校车上的安全，也可以用来记录发生事故时校车外的情况，以防发生事故或司机非法超车。一个常见的案例是，一位家长打电话给学校，报告她的孩子在校车上目睹了欺凌、打架行为。学校工作人员可以观看当天的录像来确定到底发生了什么。学校工作人员也可以实时观看视频。因此，如果校车司机向交通主管报告学生们在公交车上打架，交通主管可以查看现场视频并确定适当的行动方案（例如，请求急救人员支持）。图15-14和图15-15显示了查看实时视频和录制视频的示例。



图15-14 公交车摄像头的实时显示

许多国家/地区不允许司机对停驶的校车超车，因为孩子们可能会在校车周围走来走去或横穿马路，而没有仔细注意可能发生的交通状况。例如，2014年，北卡罗来纳州发现每天约有3000名司机对停驶的校车超车。这对学生造成了明显的安全隐患。由于识别和起诉罪犯非常困难，因此很难产生有效的威慑力。例如，2014年，尽管每天发生数千次违法事件，但在北卡罗来纳州，全年只有1300起案件开庭审理，其中只有29%的司机被判有罪。改善这种状况的一种方法是安装一个外部摄像头（或多个摄像头）来捕捉超车行为。这样就可向执法人员提供拍摄违规车辆识别特征的视频剪辑。校车的速度、转向灯和刹车应用数据也可以叠加在视频上，用于事故调查。在常见的部署中，用于捕捉车牌号码的高清视频需要较大的带宽进行传输，因此视频被存储在本地的校车摄像头上，当校车回到停车场时通过WiFi上传。

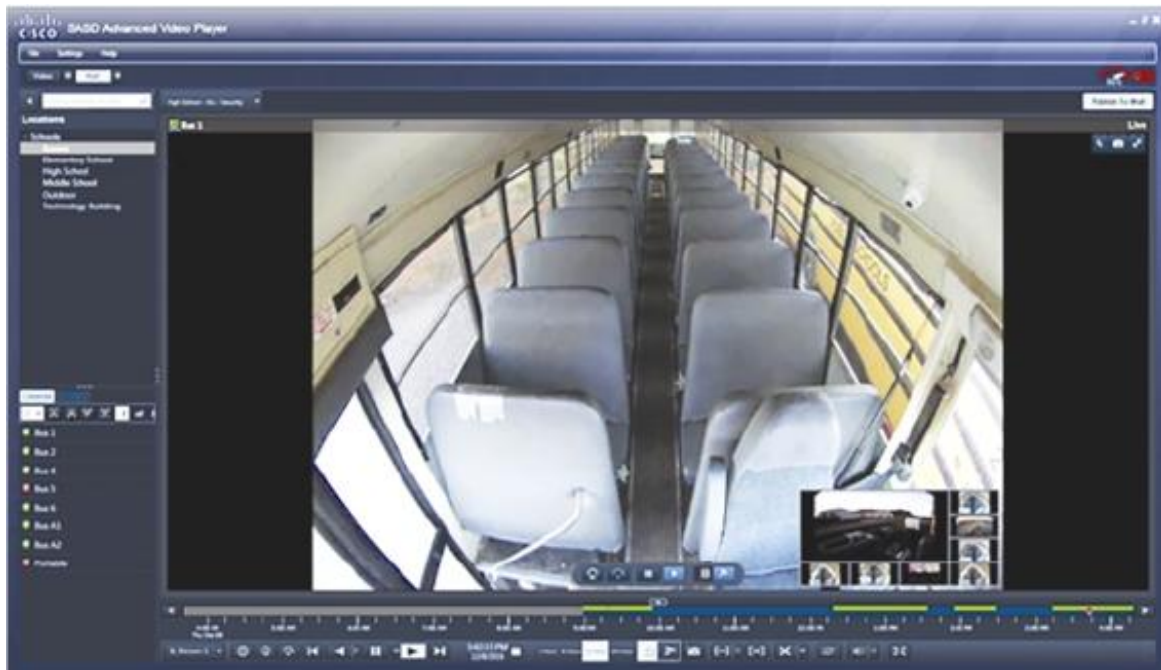


图15-15 查看历史视频

15.5.5 学生WiFi

有些学生每天坐公共汽车的时间超过两个小时，这本来是宝贵的学习时间。校车可以提供WiFi连接供学生在校车上完成作业。所有学生的WiFi流量返回学校网络，在该网络中可以应用学校系统的互联网接入和过滤策略。接入点部署在校车上，小型路由器将查询转发给蜂窝数据连接。在某些情况下，小型计算和存储系统可以缓存经常访问的资源，如学校网站和教师作业页面。

15.5.6 一键通通信

学校工作人员和校车司机之间的语音通信正在成为一种常见的用例。软移动客户端允许智能手机执行一键通语音通信。在校车应用程序中，学校可以向校车司机提供智能手机或平板设备，也可以要求校车司机在个人设备上安装应用程序。在这两种情况下，设备都连接到校车上的WiFi网络，从而避免使用智能手机设备上的蜂窝数据网络。

15.5.7 校车安全网络架构

图15-16显示了互联校车网络架构的高级示意图。该示意图将前面几节中讨论的用例和服务映射到实际部署中。

在该架构中，所有服务都托管在数据/运营中心中。校车停车场的WiFi网络是使用加固的户外AP建立的。管理学校传统WiFi网络的无线LAN控制器也可以管理这些AP。

从校车到数据/运营中心的数据通过5GHz WiFi传输（如果可用的话）。如果没有WiFi，数据通过商业运营商的蜂窝网络进行加密传输。

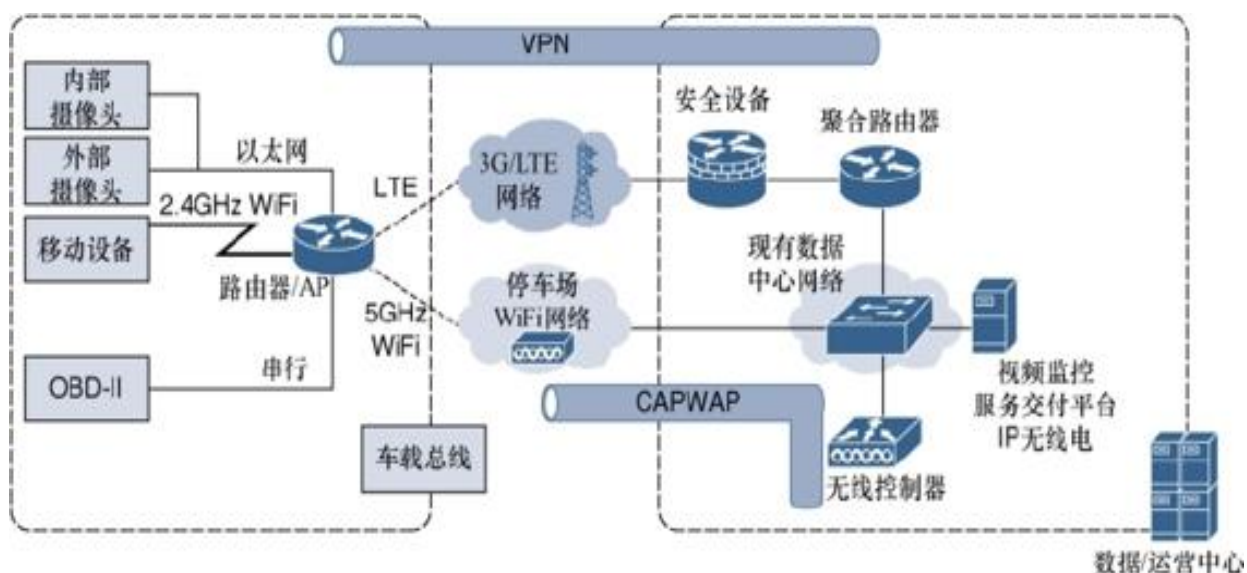


图15-16 互联校车的网络架构

在校车上，路由器处理所有的边缘网络连接功能，以及雾计算功能。它在车上提供2.4GHz的WiFi（作为AP），并允许使用5GHz频段连接到校车停车场的WiFi作为工作组网桥（WGB）。该路由器还提供蜂窝网络连接，包括用于连接摄像头和其他设备的以太网端口。路由器还通过校车和运营中心之间的蜂窝网络进行数据加密。

校车内外摄像头将视频流传输到位于数据/运营中心的媒体服务器。在一些部署中，视频并不总是通过LTE传输，而是存储在本地的摄

像头中，然后在校车返回停车场后通过WiFi传输。

来自校车的诊断数据由校车的车载诊断端口提供。在路由器内部运行一个小型软件客户端来解释数据并将相关信息发送到数据/运营中心的服务器。

15.6 小结

虽然公共安全涉及的物联网的范围非常广泛，但从急救人员、消防员、警察到校车，几乎所有的用例都有一个共同的主线。在所有情况下，数据从传感器收集，通过安全网络传输、处理分析、可视化，并实时（或接近实时）共享。一个常见的需求是能够在本地处理数据并定义需要在现场响应小组的成员之间共享数据的区域。同时，部分数据还需要转发到中央指挥中心，以促进不同应急服务之间的整体交互。语音和视频协作是在应急响应人员之间实现丰富通信和信息共享的核心工具。它们提高了参与方的态势感知能力，有助于更快、更协调、更安全地做出反应。

与此同时，多个传感器正在提高感知和响应效率。与紧急救援人员携带的传感器、嵌入到车辆内或集成到周围环境中的传感器进行交互，增强了紧急救援人员的意识，并允许反应小组能够更大规模地应对突发事件，同时通过控制红绿灯缩短其响应时间，通过访问紧急区域环境传感器来收集更快更好的信息，并通过支持在人群中识别出机器学习运动模式来更快地做出反应。