

物联网与人工智能应用开发丛书



智能互联汽车的 网络安全技术及应用

Security and Network Applications in
Smart Connected Car

“工业和信息化领域专业技术人才知识更新工程”培训用书

工业和信息化部人才交流中心
恩智浦（中国）管理有限公司 ◎编 著

 中国工信出版集团

 电子工业出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
<http://www.phei.com.cn>

物联网与人工智能应用开发丛书

智能互联汽车的网络 安全技术及应用

工业和信息化部人才交流中心
恩智浦（中国）管理有限公司 编著

电子工业出版社
Publishing House of Electronics Industry
北京·BEIJING

内 容 简 介

本书着重介绍汽车网络互联技术和网络安全技术两大方面，涵盖了对汽车网络互联技术的概念及其面临的安全挑战，介绍了现有的和即将实施的各类汽车网络安全法规，提出了基于纵深防御概念的 4+1 汽车网络安全架构，并结合若干汽车网络安全的应用实例对汽车网络安全技术及应用场景进行进一步的解释和探讨。本书适合汽车网络设计工程师及汽车信息安全相关技术人员阅读参考，同时也适合作为汽车电子相关工程师及交通管理相关技术人员了解汽车网络及网络安全架构的参考书。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有，侵权必究。

图书在版编目 (CIP) 数据

智能互联汽车的网络安全技术及应用/工业和信息化部人才交流中心，恩智浦（中国）管理有限公司编著. —北京：电子工业出版社，2018.12

（物联网与人工智能应用开发丛书）

ISBN 978-7-121-34974-4

I. ①智… II. ①工… ②恩… III. ①汽车—智能通信网—网络安全—研究 IV. ①U463.67

中国版本图书馆 CIP 数据核字（2018）第 198964 号

策划编辑：徐蔷薇

责任编辑：刘小琳 特约编辑：白天明

印 刷：天津千鹤文化传播有限公司

装 订：天津千鹤文化传播有限公司

出版发行：电子工业出版社

北京市海淀区万寿路 173 信箱 邮编：100036

开 本：720×1000 1/16 印张：21.25 字数：320 千字

版 次：2018 年 12 月第 1 版

印 次：2018 年 12 月第 1 次印刷

定 价：79.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888

质量投诉请发邮件至zlts@phei.com.cn，盗版侵权举报请发邮件至dbqq@phei.com.cn。

本书咨询联系方式：（010）88254538，liuxl@phei.com.cn。

物联网与人工智能应用开发丛书

指导委员会

刁石京 工业和信息化部电子信息司司长

丁文武 国家集成电路产业投资基金股份有限公司总裁

王希征 工业和信息化部人才交流中心主任

魏少军 清华大学微电子所所长，中国半导体行业协会副理事长、设计分会理事长

王传臣 电子工业出版社党委书记、社长

郑力 恩智浦半导体全球资深副总裁兼大中华区总裁

物联网与人工智能应用开发丛书

专家委员会

主任：李 宁

委员（按姓氏笔画排序）：

王永文 王自强 王志华 王朋朋 王维锋

邢建平 吕 浩 任 霞 任爱光 杜高明

李金城 何小庆 张 兴 张 悦 张之戈

林国辉 林恩雪 易生海 金宇杰 单光存

赵毅强 耿卫东 董亚峰 董雷宏 粟 涛

傅雄军 曾卫明 廉小亲

《智能互联汽车的网络安全技术及应用》

作 者

吕 浩 陈东华 董 珀
王钰博 罗志昕

物联网与人工智能应用开发丛书

总 策 划：任 霞

秘 书 组：陈 劼 刘庆瑜 徐蔷薇

序 一

中国经济已经由高速增长阶段转向高质量发展阶段，正处在转变发展方式、优化经济结构、转换增长动力的攻关期。习近平总书记在党的十九大报告中明确指出，主动参与和推动经济全球化进程，发展更高层次的开放型经济，不断壮大我国的经济实力和综合国力。

对于我国的集成电路产业来说，当前正是一个实现产业跨越式发展的重要战略机遇期，前景十分光明，挑战也十分严峻。在政策层面，2014年《国家集成电路产业发展推进纲要》发布，提出到2030年产业链主要环节达到国际先进水平，实现跨越式发展的目标；2015年，国务院提出的中国智能制造发展战略中，将集成电路产业列为重点领域；2016年，国务院颁布《“十三五”国家信息化规划》，提出构建现代信息技术和产业生态体系，推进核心技术超越工程，其中集成电路被放在了首位。在技术层面，目前全球集成电路产业已进入重大调整变革期，中国集成电路技术创新能力和中高端芯片供

给水平正在提升，中国企业设计、封测水平正在加快迈向第一阵营。在应用层面，5G 移动通信、物联网、人工智能等技术逐步成熟，各类智能终端、物联网、汽车电子及工业控制领域的需求将推动集成电路产业的稳步增长，因此集成电路产业将成为这些产品创新发展的战略制高点。

“十三五”期间，中国集成电路产业必将迎来重大发展，特别是加快建设制造强国，加快发展先进制造业，推动互联网、大数据、人工智能和实体经济深度融合等理念的提出，给集成电路产业发展开拓了新的发展空间，使得集成电路产业由技术驱动模式转化为需求和效率优先模式。在这样的大背景下，通过高层次的全球合作来促进我国国内集成电路产业的崛起，将成为我们发展集成电路的一个重要抓手。

在推进集成电路产业发展的过程中，建立创新体系、构建产业竞争力，最终都要落实在人才上。人才培养是集成电路产业发展的一个核心组成部分，我们的政府、企业、科研和出版单位对此都承担着重要的责任和义务。所以我们非常支持工业和信息化部人才交流中心、恩智浦（中国）管理有限公司、电子工业出版社共同组织出版这套“物联网与人工智能应用开发丛书”。这套丛书集中了众多一线工程师和技术人员的集体智慧和经验，并且经过了行业专家、学者的反复论证。我希望广大读者可以将这套丛书作为日常工作中的一套工具书，指导应用开发工作，还能够以这套丛书为基础，从应用角度对我们未来产业的发展进行探索，并与中国的发展特色紧密结合，服务中国集成电路产业的转型升级。



工业和信息化部电子信息司司长

2018 年 1 月

序 二

随着摩尔定律逐步逼近极限，以及云计算、大数据、物联网、人工智能、5G 等新兴应用领域的兴起，其细分领域竞争格局加快重塑，围绕资金、技术、产品、人才等全方位的竞争加剧，当前全球集成电路产业进入了发展的重大转型期和变革期。

自 2014 年《国家集成电路产业发展推进纲要》发布以来，随着“中国制造 2025”“互联网+”和大数据等国家战略的深入推进，国内集成电路市场需求规模进一步扩大，产业发展空间进一步增大，发展环境进一步优化。在市场需求拉动和国家相关政策的支持下，我国集成电路产业继续保持平稳快速、稳中有进的发展态势，产业规模稳步增长，技术水平持续提升，资本运作渐趋活跃，国际合作层次不断提升。

集成电路产业是一个高度全球化的产业，发展集成电路需要强调自主创

新，也要强调开放与国际合作，中国不可能关起门来发展集成电路。

集成电路产业的发展需要知识的不断更新。这一点随着云计算、大数据、物联网、人工智能、5G 等新业务、新平台的不断出现，已经显得越来越重要、越来越迫切。由工业和信息化部人才交流中心、恩智浦（中国）管理有限公司与电子工业出版社共同组织编写的“物联网与人工智能应用开发丛书”，是我们产业开展国际知识交流与合作的一次有益尝试。我们希望看到更多国内外企业持续为我国集成电路产业的人才培养和知识更新提供有效的支撑，通过各方的共同努力，真正实现中国集成电路产业的跨越式发展。



2018年1月

序 三

尽管有些人认为全球集成电路产业已经迈入成熟期，但随着新兴产业的崛起，集成电路技术还将继续演进，并长期扮演核心关键角色。事实上，到现在为止还没有出现集成电路的替代技术。

中国已经成为全球最大的集成电路市场，产业布局基本合理，各领域进步明显。2016年，中国集成电路产业出现了三个里程碑式事件：第一，中国集成电路产业第一次实现制造、设计、封测三个领域的销售规模均超过1000亿元，改变了多年来总是封测领头、设计和制造跟随的局面；第二，设计业超过封测业成为集成电路产业最大的组成部分，这是中国集成电路产业向好发展的重要信号；第三，中国集成电路制造业增速首次超过设计业和封测业，增速最快。随着中国经济的增长，中国集成电路产业的发展也将继续保持良好态势。未来，中国将保持世界电子产品生产大国的地位，对集成电路的需求还会维持在高位。与此同时，我们也必须认识到，国内集成电路的自给率不高，

在很长一段时间内对外依存度仍会停留在较高水平。

我们要充分利用当前物联网、人工智能、大数据、云计算加速发展的契机，实现我国集成电路产业的跨越式发展，一是要对自己的发展有清醒的认识；二是要保持足够的定力，不忘初心、下定决心；三是要紧紧围绕产品，以产品为中心，高端通用芯片必须面向主战场。

产业要发展，人才是决定性因素。目前，我国集成电路产业的人才情况不容乐观，人才缺口很大，人才数量和质量均需要大幅度提升。与市场、资本相比，人才的缺失是中国集成电路产业面临的最大变量。人才的成长来自知识的更新和经验的积累。我国一直强调产学研结合、全价值链推动产业发展，加强企业、研究机构、学校之间的交流合作，对于集成电路产业的人才培养和知识更新有非常正面的促进作用。由工业和信息化部人才交流中心、恩智浦（中国）管理有限公司与电子工业出版社共同组织编写的这套“物联网与人工智能应用开发丛书”，内容涉及安全应用与微控制器固件开发、电机控制与 USB 技术应用、车联网与电动汽车电池管理系统、汽车控制技术应用等物联网与人工智能应用开发的多个方面，对于专业技术人员的实际工作具有很强的指导价值。我对参与丛书编写的专家、学者和工程师们表示感谢，并衷心希望能够有越来越多的国际优秀企业参与到我国集成电路产业发展的大潮中来，实现全球技术与经验和中国市场需求的融合，支持我国产业的长期可持续发展。

魏少军 教授

清华大学微电子所所长

2018 年 1 月

序 四

千里之行 始于足下

人工智能与物联网、大数据的完美结合，正在成为未来十年新一轮科技与产业革命的主旋律。随之而来的各个行业对计算、控制、连接、存储及安全功能的强劲需求，也再次把半导体集成电路产业推向了全球经济的风口浪尖。

历次产业革命所带来的冲击往往是颠覆性的改变。当我们正为目不暇接的电子信息技术创新的风起云涌而喝彩，为庞大的产业资金在政府和金融机构的热推下，正以前所未有的规模和速度投入集成电路行业而惊叹的同时，不少业界有识之士已经敏锐地意识到，构成并驱动即将到来的智能化社会的每个电子系统、功能模块、底层软件乃至检测技术都面临着巨大的量变与质变。毫无疑问，一个以集成电路和相应软件为核心的电子信息系统的深入而全面的更新换代浪潮正在向我们涌来。

如此的产业巨变不仅引发了人工智能在不远的将来是否会取代人类工作的思考，更加现实而且紧迫的问题在于，我们每个人的知识结构和理解能力能否跟得上这一轮技术革新的发展步伐？内容及架构更新相对缓慢的传统教材，以及漫无边际的网络资料，是否足以为我们及时勾勒出物联网与人工智能应用的重点要素？在如今仅凭独到的商业模式和免费获取的流量，就可以瞬间增加企业市值的 IT 盛宴里，我们的工程师们需要静下心来思考在哪些方面练好基本功，才能在未来翻天覆地般的技术变革时代立于不败之地。

带着这些问题，我们在政府和国内众多知名院校的热心支持与合作下，精心选题，推敲琢磨，策划了这一套以物联网与人工智能的开发实践为主线，以集成电路核心器件及相应软件开发的最新应用为基础的科技系列丛书，以期对在人工智能新时代所面对的一些重要技术课题提出抛砖引玉式的线索和思路。

本套丛书的准备工作得到了工业和信息化部电子信息司刁石京司长，国家集成电路产业投资基金股份有限公司丁文武总裁，清华大学微电子所所长魏少军教授，工业和信息化部人才交流中心王希征主任、李宁副主任，电子工业出版社党委书记、社长王传臣的肯定与支持，恩智浦半导体公司的任霞女士、张伊雯女士、陈劼女士，以及恩智浦半导体各个产品技术部门的技术专家们为丛书的编写组织工作付出了大量的心血，电子工业出版社的董亚峰先生、徐蔷薇女士为丛书的编辑出版做了精心的规划。著书育人，功在后世，借此机会向他们表示衷心的感谢。

未来已来，新一代产业革命的大趋势把我们推上了又一程充满精彩和想象空间的科技之旅。在憧憬人工智能和物联网即将给整个人类社会带来的无限机遇和美好前景的同时，打好基础，不忘初心，用知识充实并走好脚下的每一步，又何尝不是一个主动迎接未来的良好途径？

郑力

写于 2018 年拉斯维加斯 CES 科技展会

前 言

汽车产业的创新越来越依赖于相关电子器件的创新，而站在迅速发展的汽车产业前沿的汽车电子产业的发展创新，使汽车从简单的交通工具演变成个性化的智能互联移动终端。V2X 通信、远程信息处理、中央网关和多标准数字广播接收等车载装置的使用，以及车辆门禁无线技术、近场通信（NFC）、先进驾驶辅助系统（ADAS）等先进技术的引入也大大推动了汽车智能化方面的发展创新。

所有这些电子装置的使用和电子技术的引入为驾驶员带来巨大的便利，提高了驾驶的舒适性、便捷性、安全性和效率，但是车辆的无线接口需要将这些“互联汽车”的车载系统与外部网络（如互联网）连接起来，通过支持新的功能和服务，加强客户体验，这种连接功能也让“互联汽车”容易遭到黑客攻击。事实上，早在多年前，有几项研究就已经对黑客攻击汽车的可能性提出过警告，而最近的研究表明，黑客其实能实现对车辆的远程控制。与

此同时，现今汽车和卡车中的技术系统和数据极易遭到盗用、黑客攻击及当今任何技术系统所面临的同类入侵。

因此，业界迫切需要采取措施使“互联汽车”得到安全保护，以确保所有车载系统发挥正确的功能，并保护用户隐私。这意味着车载电子设备的设计需要实现“范式转变”。过去一直非常强调汽车的安全性，比如刹车在任何情况下都要起作用，随着车载电子设备和软件数量的增加，未来将会同样重视安全性，但将会需要额外的车载信息安全功能以保护车辆免受黑客攻击。

随着人工智能（AI）在移动互联终端中的大量实施和推广，该技术也逐步开始在汽车上应用，比如各种基于云端 AI 的语音和手势识别技术在车载娱乐系统中的应用。

然而，在汽车对安全性严格要求的同时，车主也对本地数据隐私提出了要求（不希望将所有信息上传），AI 的应用需要向汽车终端迁移。例如，具备人工智能引擎的本地处理平台，可实现高效高速的数据融合、目标识别和路径规划。

本书是“物联网与人工智能应用开发丛书”中的一本，主要关注智能“互联汽车”的网络技术应用及信息安全，通过对汽车互联技术的需求与技术分析，提出相应的网络安全解决方案和建议。

由于篇幅和知识所限，本书主要基于车载的硬件加密技术进行梳理和讲解，务求能让读者对于汽车网络安全的需求和实施策略，与标准相关的基本网络安全技术、流程有初步的认识，同时对智能“互联汽车”的网络和安全技术发展方向有所涉及。

本书重点分析了基于纵深防御概念的针对智能“互联汽车”的 4+1 汽车网络安全架构，帮助读者从架构的层面理解汽车网络安全的各种需求和分工，