ELSEVIER
爱思唯尔

智能电网安全
——下一代电网安全

[美] Tony Flick　Justin Morehouse　著
徐　震　于爱民　刘韧　译
胡红升　主审

Securing The Smart Grid
—— Next Generation Power Grid Security

國防工業出版社
National Defense Industry Press

智能电网安全

——下一代电网安全

[美] Tony Flick　Justin Morehouse　著
徐震　于爱民　刘韧　译
胡红升　主审

ELSEVIER
爱思唯尔

国防工业出版社

著作权合同登记　图字：军-2012-103 号

图书在版编目(CIP)数据

智能电网安全：下一代电网安全/(美)弗里克(Flick，T.)，(美)莫尔豪斯(Morehouse，J.)著；徐震，于爱民，刘韧译．—北京：国防工业出版社，2013.1

书名原文：Securing the smart grid：next generation power grid security

ISBN 978—7—118—08553—2

Ⅰ.①智… Ⅱ.①弗… ②莫… ③徐… ④于… ⑤刘… Ⅲ.①智能控制—电网—电力安全 Ⅳ.①TM727

中国版本图书馆 CIP 数据核字(2013)第 001177 号

※

国防工业出版社出版发行

(北京市海淀区紫竹院南路 23 号　邮政编码 100048)

北京嘉恒彩色印刷有限责任公司

新华书店经售

*

开本 710×1000　1/16　**印张** 16　**字数** 311 千字

2013 年 1 月第 1 版第 1 次印刷　**印数** 1—4000 册　**定价** 58.00 元

(本书如有印装错误，我社负责调换)

国防书店：(010)88540777　发行邮购：(010)88540776

发行传真：(010)88540755　发行业务：(010)88540717

托尼·弗里克的致谢

我想感谢我的父母，是他们将我引入计算机科学领域，从小到大为我买了许多计算机，并且在我通过破解他们新计算机来进行安全实践时没有特别的愤怒。毕竟，我只是效仿父亲为强化吸尘器而做的努力。父亲教会了我许多生活中的事情，并努力工作来为我提供良好的生活环境。从值夜班保证街道安全，到为我所在的队做教练，等某天我成为父亲时，我觉得我最多只能期望做到他的一半。尽管不是传统玩法，在三岁时用父亲搜集的硬币来玩游戏使得我一生的数学课都变得有趣和容易。其他的父母和老师经常问我，我的父母是否用了教学卡片或雇了家教来提升我的数学能力。而我想起的是在我不经意间学习数学基础时，玩卡片游戏的乐趣。母亲，我知道你某天回到家里，听到在玩扑克游戏的三岁的我在喊："打我"时有些担心。但是毕竟，我最终还是拿到了数学学位。

母亲，当你带回家一台显示器只能显示绿色字符的计算机时，你将我引入了计算机世界。和你一起在那台老计算机上玩游戏并学习打字增长了我对电子器件的兴趣，这使得我走进了计算机科学，以致最终的安全领域。我还要感谢你努力的工作来让我过上更好的生活。我知道这是艰辛的，但是我会永远的感谢您在我生命中给我的机会。

我的哥哥马特，谢谢你在本书应用安全部分给我的极大帮助，让我从你那获取想法，并提供本书中许多非常好的想法。我还要感谢你总能从你忙碌的日程中抽出时间来帮助我完成作业、计算机项目，还陪我玩很长时间的电子游戏。

我还要感谢我的姐姐，她耐心地帮我检查我大学的报告并教会我如何专业地写作。尽管在你帮我检查报告时，我在和你未来的老公玩电子游戏，我真的很重视你的评注并且从你温和的编辑笑话中受益匪浅。真希望你能将这本书读给布鲁克和萨曼莎听，在很小的年纪就教授他们安全知识是很好的。

在过去的八个月中，我在周末和每个夜晚把自己锁在办公室或者宾馆房间中来进行本书的写作。我想要感谢在这段时间支持我，允许我为了完成本书而与世隔绝的每个人。我真希望我能偿还那些在我饿的时候给我带来食物，并说服我放松一下去和朋友或所爱的人喝一两杯，那样会对写书有帮助的人的情。

感谢 Syngress 出版社的瑞秋·鲁米里奥蒂斯和马修·凯特给我们撰写本书的机会，并一路上指导我们。克里斯多夫·威尔提索斯，感谢你对本书内容提出的意见和建议。最后，感谢我的合著者——贾斯汀·莫尔豪斯与我一同在晚上和周末来撰写此书。

贾斯汀·莫尔豪斯的致谢

我要感谢我的妻子，我一生的至爱，丽莎，对我整个写书过程的支持、耐心和理解。没有她，就不会有我今天的成就，也不会有今天的我。我感谢我的父母，约翰和苏珊，无论我竭力追求什么他们总是支持我并教会我，只要用心，我能够完成几乎所有的事。

感谢里纳尔迪·雷朋、杰夫·洛萨皮奥以及麦克·沃尔克发掘了我的能力，告诉我，我不仅可以做一名顾问，还可以将我的激情变为事业。感谢史蒂夫·邓克尔提醒我在事业上我可以更加有所成就。感谢贝克斯、赖安、梅丽莎和乔尔对我一直以来的支持和理解。

感谢瑞秋·鲁米里奥蒂斯、马修·凯特和克里斯多夫·威尔提索斯的支持以及在编写此书时你们提供给我的想法。感谢马特·弗里克、杰夫·耶斯处莫科斯、里奇·罗伯特森和肖恩·莫耶给我打来的电话并回复我的邮件。最后，感谢我的合作者，托尼·弗里克，在这几个月中和我并肩奋斗来使本书得以出版。

序

迎接智能电网新时代

曾几何时，电力作为现代文明繁荣社会的基础支撑，发挥了十分重要的作用，电力技术也作为第二次技术革命带领人类进入了现代化大工业时代，成为工业时代的显著标志。那么人类的下一个时代——信息时代的标志是什么呢？无疑是信息技术及其广泛应用。工业时代的电力技术经历了从单台机组、单用户时代向集约化、现代化大电厂、大电网的转变；信息时代的信息技术也正在从单机、单应用向互联网、物联网、云计算等方向转变，二者是何其之像！与工业时代相比，信息时代的一个显著特征就是智能化，社会的各个要素均具备一定的逻辑推理和自动处理能力，具备一定的互联和沟通能力，而不再是被动的、简单的重复执行一套动作。于是我们的社会将成为智能化社会，政府将成为智慧政府，企业成为智慧企业，交通将向智能交通转变，医疗将向智能医疗转变，电网将向智能电网转变，城市将向智能城市转变，地球将向智慧地球转变。美国未来学家杰里米·里夫金提出的第三次工业革命的新模式，就强调了从工业时代向信息时代转变的必由之路，即将互联网与可再生能源相结合，从而达到绿色、可持续、低碳发展的新型工业化之路。

关于智能电网，各国均有不同的理解角度和侧重点。欧洲侧重于用户的便捷性、分布式电源和可再生能源接入的高效性。美国更注重供电可靠性和电能质量提高、国家能源安全、应对气候变化和环境保护等。而中国则更加系统和全面，从发电、输电、变电、配电、用电、调度的电力系统全环节提高电网的智能化程度，建设

运营一个坚强、安全、可靠、稳定、灵活的电网，为社会提供清洁、可靠、透明的电力，应对资源环境问题带来的挑战，适应发电多样化的发展要求，满足多元化用电服务的需求。中国国家电网公司在电网智能化“十二五”规划中，将发展目标定为“到2015年，形成坚强智能电网运行控制和双向互动服务体系，智能电网效益初步显现，国家电网智能化程度达到国际先进水平。”尽管各国家的侧重点不同，但是大家公认智能电网具有信息化、自动化和互动化的特征，即电网是高度自动化的，与用户高度的互动，可对各环节的信息进行采集、传输、处理、加工和反馈。为实现电网的智能化，需要从各个方面对现行电网进行改造。在发电方面，包括有新能源和分布式发电技术、储能技术以及电厂与电网的互动交易技术等。在输电方面，包括有设备监测技术、状态检修技术、数字化勘测技术等。在变电方面，包括有智能变电站、可视化运行、变电巡检等技术。在配电方面，包括有电能质量检测、配网自动化技术等。在用电方面，包括有用电信息采集、需求侧管理、节能技术、市场分析、电动汽车服务网络运营管理等技术。在电网调度方面，包括有电网实时监测与预警、电网综合分析与评估等技术。这一切俱需要信息通信网络的支撑和信息技术的广泛深入的应用和融合。

信息技术的广泛应用具有双刃剑效应。电网越是智能，信息技术的应用越广泛，信息安全的问题就越突出。由于电网的高度智能，电网的各基础设施将通过信息网络逐步连接起来，电网设备的运行状态将被实时采集和集中存储起来，用户的互动性又使得用户通过互联网可对电网运行数据进行必要的了解和处理，这一切均可能对电网安全造成威胁。电网不可能与互联网完全隔绝，电网运行状态和设备信息有可能被读取，因此信息安全是智能电网不可逾越的一道屏障。2010年9月爆发的“震网（Stuxnet）”病毒席卷了全球工业界，感染了全球超过45000个网络，直接攻击了伊朗核电站并造成损害，也给部分国家的电力部门带来了威胁和破坏。2012年5月爆发的“超级火焰”病毒危害性更大，更为智能，攻击了中东多个国家。这些均为智能电网信息安全敲响了警钟。智能电网既要保证电网的安全、可靠、稳定运行，又要防止各种对电网的不良企图得逞，面对现实或潜在的智能电网安全威胁，各国政府纷纷成立专门研究机构，就相关问题和观点进行充分讨论，信息安全工作者肩负着重要的职责。

由于智能电网属新兴事物，智能电网信息安全也会出现新的威胁和情况，系统

了解发达国家在该领域的工作对我国智能电网信息安全防护体系建设极有裨益。本书的引进，可谓恰逢其时。本书主要对智能电网的优点和安全脆弱性相关内容进行阐述。通过对智能电网环境下各个实体进行深入分析，对各实体在机密性、完整性和可达性方面存在的安全问题以及如何保证上述安全特性进行了论述，对当前美国智能电网安全标准规范进行了介绍，对公用事业公司如何构建成熟的安全防护体系进行了论述，对于第三方合作、移动应用、社交网络、智能电表等内容的信息安全管控进行了详细讨论。同时给出了智能电网消费者、设备供应商以及公用事业公司如何进行控制从而最大化降低智能电网安全风险的方法，阐述了在智能电网安全方面美国联邦政府、地方政府、国营及私营电力公司的重要作用。通过本书，用户能够更为深刻的理解在智能电网部署时存在的安全威胁、安全攻击，从而为有效避免这些问题的发生做好防范措施。

该书作者长期从事智能电网和信息安全研究工作，书中内容立足于美国智能电网实际，对我国智能电网建设也将起到很好的借鉴作用，与其他从传统信息安全技术角度对智能电网安全进行阐述的书籍相比，本书针对性更强，对于从事智能电网信息安全研究和建设工作具有更强的指导作用。

虽然在智能电网建设中要解决和克服的问题很多，但我们有充分的理由相信，我们在建设过程中一定能够解决各环节存在的问题，一个安全、可靠、灵活的智能电网将会给人类带来更新的体验、更便捷的生活，为人类信息时代带来更美好的未来。

王继业

电力行业信息标准化委员会主任委员

中国电机工程会学会信息化专委会副主任委员

国家电网公司信息通信部副主任

译者序

第二次工业革命以来，电力得到了广泛应用，电力的发、输、配、用技术在电力、电气工作者的持续努力下走向成熟，电力网络也逐步发展成为人类社会生产、生活的核心基础设施。然而，现代电网正面临着能源浪费、可靠性低、可再生能源支持少等一系列重大挑战，亟待构建更为智能化的电力网络以应对上述挑战。谈到智能化，很自然就与信息通信技术紧密关联起来。在智能电网的背景下，信息通信技术被系统化地应用于电力的发、输、配、用各个环节。这里电网与信息通信并非简单的叠加，而是深度的有机融合，以构建更为可靠、经济、环保的未来电力网络。

信息通信技术与电网的深度融合也意味着智能电网成为网络空间的重要组成部分。作为陆、海、空、天之外的第五维空间，网络空间得到了各发达国家的高度重视。目前，活跃于网络空间的攻击者已经不仅仅是单打独斗的黑客，有组织的专业级组织，乃至国家力量都已浮出水面。近年来的“震网”、“火焰”病毒的案例昭示着这些网络空间的新兴攻击力量逐渐成为主流。因此，来自网络空间中的安全问题已成为智能电网面临的重大现实挑战。

电力企业的信息安全防御思想目前还停留在边界防护的阶段，并假定隔离的生产网络自身是安全的。“震网”病毒对伊朗核电站造成的巨大破坏可视作对上述假定的颠覆。因此，电力信息安全的管理和实践必须采用全新的指导思想，以构筑全新的智能电网信息安全体系，相关工作需要大批兼具电力和信息安全专业知识的人才。而遍观市场现有书籍，能够综合阐述智能电网和安全技术，以支撑智能电网安全专业技术人才培养的书籍可谓少之又少。

本书的出版可谓恰逢其时，它对智能电网的优点和安全脆弱性相关内容进行

了系统性的阐述。通过对智能电网环境下各个实体进行深入分析，对各个实体在机密性、完整性和可用性方面存在的安全问题以及如何保证上述安全特性进行了论述。通过本书，读者能够更为深刻地理解在智能电网部署时存在的安全威胁、安全攻击，从而为有效避免这些问题的发生提供支持。此外，本书还给出了智能电网消费者、设备供应商以及公用事业公司如何进行控制从而最大化降低智能电网安全风险的方法。虽然，本书是在美国“智能电网”背景下讲述安全技术，但他山之石可以攻玉，它对我国智能电网安全体系构建也将起到重要的借鉴作用。

在此，感谢国防工业出版社让我们有机会引进这本智能电网安全方面的重要书籍。同时，是牛旭东编辑的细致耐心工作，让这本书的翻译、审校和出版工作能够有序的进行。在本书的翻译过程中，汪丹、张妍两位博士和杨溢学、周启惠、敖赢戈三位硕士生都做出了重要贡献，在此对他们的辛勤工作致敬。

译　者

2012 年 12 月

目　录