“十三五”国家重点图书规划项目

网络法律话语经典译丛

丛书总主编：程乐　王春晖　时建中　张延川

智能电网安全

［美］桑杰·戈埃尔　［美］洪源

［比］瓦格利斯·帕帕康斯坦丁努　［比］达里乌斯·克洛扎　著

程乐　刘樊　刘曙元　裴佳敏/译

SMART GRID
SECURITY

Sanjay Goel　Yuan Hong

Vagelis Papakonstantinou　Dariusz Kloza

中国民主法制出版社

全国百佳图书出版单位

“网络法律话语经典译丛”编委会名单

时建中(中国政法大学)
石文昌(中国人民大学)
司春磊(山西法商研究中心)
孙钰岫(浙江大学)
万学忠(法制网)
王　欣(浙江大学)
王春晖(南京邮电大学)
王文华(北京外国语大学)
王学高(中国电信集团有限公司)
谢永江(北京邮电大学)
杨　巧(西北政法大学)
叶　宁(浙江警察学院)
张吉豫(中国人民大学)
张建文(西南政法大学)
张延川(中国通信学会)
张子健(重庆交通大学)

前　言

不可逆转的趋势已经开始了：全球日趋智能。目前重新考虑将各类科技转化成集智能、感知与通信于一体的互联网设备。此番重新考虑是因为有很多不错的理由加持。正如以往所见，此类转化有诸多好处。现如今的技术发展以高密度、高同步性和高效率的技术为主要特征，不易出现人为错误，可以提供更多的功能且整体上利润更为丰厚。总之，很多利益相关者争相设计此类技术及开发相关商品市场。

但是一般而言，技术尤其是信息技术，会产生风险和负面影响。现有范式是将我们以前的“愚蠢”技术“智能化”，旧技术的风险与新技术的功能及风险相互对抗并渗透。该融合质疑了很多最初的设想并以新颖的方式开创关于安全性和保密性的概念。尽管在机电安全概念的语境下，许多如传统技术中的物理损耗等风险是可控的。但当芯片与操作规则替代了单纯的开关与阀门，以及当网络逐渐渗透之时，这些风险即有可能改头换面（以不同的形式与规模）重新出现。某种程度上，智能汽车和智能工厂可能更加高效与透明，但是它将对外来者更加开放，更易于接受，并且更倾向于出现不必要的复杂开发，因为任何类型的信息技术总是会增加巨大的复杂性，而且它肯定需要更多的注意力、更多维护和更多的专业知识。另外，还会出现全新的风险，例如，仅仅是驾驶汽车或房屋供暖而产生的隐私问题，因为“智能”技术产生数据——这在一定程度上会成为与人们相关的信息。

相应地，新旧技术的全新融合需要远见与智慧。实际上现在要求这些可能为时过晚了。很久以前，工程师和工业部门便已开始尝试这些范式，并且现在正开始快速地生产与销售因新旧技术相融合而产生的产品。在停顿和重新思考上已经花费了太多的金钱和努力。顺便提及，这是技术研究中非常经典的问题。只要技术还处于发展初期，其实际影响和使用模型就无法准确预测，其风险以及负面影响也难以查明。技术研究人员仅能猜测和假设，这反过来使其大部分努力一直处在象牙塔里。只有技术达到成熟的

第一阶段，以及使用模型真正实施时，才能作出更加精确、正确和相关的假设。然而，已经花费太多金钱，并且太多实施中的范式已经返回到起草委员会，然后重新开始研究一些基本问题。在那时，建立了技术与经济上的路径依赖。当然，这些可以改革。有一句名言“你无法停止进展”在此不太准确。由于很多原因，进展一般是不会停止的。但是，任何特定的进展总是可以被塑造和引导的，如果进展的好处与风险几乎不一致——尤其是在进展尚未完全确立的情况下，甚至可以重新考虑和完全撤回进展。

幸运的是，智能技术相对而言依然年轻，并且可以从“设计乐观”的角度来看待。当然，智能技术具有危险、风险和难度，因为两类高度复杂的技术相互融合，涌现出很多不同的方案。但是，智能技术仍然是可塑的甚至是机遇。创新的任何全新开始也是这次将事情做到更好的机会。信息技术在其安全性上极其糟糕，无法防御破坏和间谍活动，监视和操纵，因此在安全和保障问题更加严峻的环境中进行改革，可以促使其回归一些基本问题上并更加努力。

该努力的前提是透彻理解、明确构建问题及其根源所在。他们在技术、经济、法律和社会层面必须具有可理解性，因此才可以创造选择和机会并推荐实施。为此，“智能化”的整个过程仍然需要更多著作，尤其是交叉学科的作品，将技术与人类世界相结合，并思考智能世界可能存在的现实问题。

智能电网（又称智能电源）是第一个通过互联网信息技术改革的大型技术领域。现已在应用和实施中，并就其过程和监管、技术和风险等方面进行评估。

该书作者们为阐明这一全新领域作出了卓越而杰出的工作，并阐释了该领域的风险与好处、条件与机遇、因果关系以及知名专家学者。由于作者们的出色工作，该书可以作为优秀指南——真实的简报——不仅仅是介绍智能电网，还有整个新兴的智能世界及其核心话题。

ESMT Berlin, January 2015

Dr. Sandro Gaycken

目　录

CONTENTS

第一章
实施智能电网所面临的安全挑战

摘　要:智能电网架构将物理电网和通信网络合并为单一的单片网络。这会造成几个众所周知的安全隐患(Li et al. in IEEE Trans Smart Grid 3:1540—1551,2012[1],McDaniel and McLaughlin in IEEE Secur Priv 7:75,77,2009[2],Bisoi and Dash 2011[3])。然而,智能电网面临来自信息物理接口的未知威胁,如果可以操纵物理设备来破坏通信基础设施,网络威胁便可以驱动物理设备,反之亦然。智能电网的运营和安全所面临的最普遍的威胁来自物理破坏基础设施、数据中毒、拒绝服务式攻击、恶意软件和入侵。消费者所面临的最普遍的威胁在于违反数据隐私以及恶意控制个人设备与电器。本章将阐述智能电网架构以及智能电网容易遭受的物理威胁。

第一节　智能电网架构

一、引言

智能电网是指在传统电网上覆盖通信网络而形成的电网。通信网络和电网彼此关联:通信网络依靠电网获取数据,而电网依靠通信网络进行活动运营。电网的作用在于提供无处不在的通信能力,从传感器和电表收集数据并原地处理,以及提供相关信息以支持多样性活动,例如,确保电网稳定,检测并解决异常现象,预测负荷,促进需求响应。这一切均需要完成,同时要保护消费者的隐私,保护关键运营数据不被敌对国家窃取,并确保数据的完整性以满足业务和运营需求。出于将不同的通信媒体整合到单个的单片网络的需要,为多个应用程序提供有保障的延迟和带宽的需求,以及必要时

确保数据的隐私和安全等原因，这并不是易于应付的挑战。

电网通常分为输电、配电和最后一英里。输电是指将高压电流远距离输送到分电站。配电是指将分电站的低电压数据传输到本地变压器。最后一英里是指将本地变压器与用户连接起来，这也是公用事业公司和用户互动的地方，以支持实时管理能源的生产、分配、使用和效率。随着智能电网技术的整合，传统网络正在进入家庭和企业。与电网相似，通信网络可以分为广域网（WAN）、城域网（MAN）、场域网（FAN）和家域网（HAN），如图 1.1 所示。

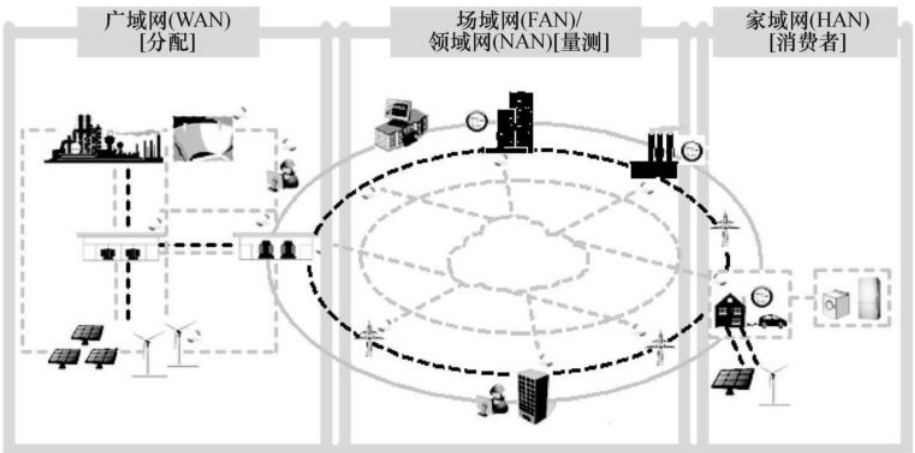

图 1.1　智能电网的演变过程

传输网络相关的主要目标是提供态势感知能力，其中需要跨越大型地理网络进行监测和控制电网的技术。这将包括纳入监测电网状态的同步相量，以确保其同步并支持监控与数据采集（SCADA）系统。该层面的任何疏忽都将对整个电网造成深远的后果，包括大规模停电。因此，WAN 需要提供高带宽（600kbps—1500kbps）、低延迟（20ms—200ms）以及高可靠性（超过 99.999%）。无线技术可能无法满足此种可靠性，并将主要依赖于光纤或其他有线技术。在配电层面，目标是能够监测配电网络的故障和其他异常情况，并能够整合微型发电源。这将提出带宽（10kbps—100kbps）和延迟（从 10ms 到 15s）以及可靠性超过 99% 的可变要求。

关键要求是在停电期间处理来自多个源头的峰值数据。这些网络通常密集且遍布整个城市，需要不同技术的组合，包括无线电、电力线载波（PLC）和高级计量架构（AMI）。最后一英里将负责用户的计量信息以及提供需求

响应能力。这要求供应商的互操作性能够支持用户家中不同类型的设备。冗余、容差和安全对于该网络而言都是至关重要的。HAN 需要在短距离内能够将来自多个设备的极高数据速率穿透墙壁。通信信道应该能处理来自多个设备的一系列干扰，并且能够可靠地运行。为了美观与方便，HAN 很有可能是无线的。

二、通信技术

目前，大部分电力系统基础设施综合使用多种技术，包括专用电缆、微波、电力线通信和光纤技术。以专用光纤通信取代一切现有的基础设施会导致成本过高。因此，基础设施将由无线电、光纤、电力线载波和传统电缆或以太网组成。

实施的最诱人的一项技术将是 PLC，因为电力基础设施已经将所有层级的整个电网连接在一起。该技术自 1920 年以来一直在开发，最初是用于通过远程站之间的高压线进行语音和数据通信，最近则用于控制负荷和自动抄表。早期技术是以低于 3kHz 的频率运行，从而可以远距离传输 60bps 的低数据速率。1992 年，欧洲电工标准化委员会（CENELEC）制定的标准中规定了四个频带中所使用的频谱：电力公司为 3kHz—95kHz；一般应用为 95kHz—125kHz，家庭网络为 125kHz—140kHz，安全应用为 140kHz—148.5kHz。在 WAN 层面的创新是在位于传输塔顶部的地线中使用光纤以防雷击。世界上大多数电网系统都使用装入光纤的地线。这些通信信道可以在很远的距离内有效运行，损耗最小并且可靠性高。更新安装的传输线中的这些光纤有助于部署智能电网，而无须任何额外的通信容量。虽然此种基础设施支持智能电网的需求，但驱动目前通信的 TCP/IP 协议无法提供发电厂（包括核电）、控制设备、变电站以及最终配电网之间通信所需的必备安全。

无线媒体将成为智能电网通信基础设施的重要组成部分，主要是由于其便利性与可接入性，特别是在计量和家庭网络领域。通信可以远距离通过中继段（电线杆）进行传输。有几种不同的技术可以使用，包括微波、WiMax、MESH、LTE、Cellular、WLAN 和 Zigbee。微波是一种高容量的点对点无线传输，为无线电接入网和 WAN 在内的电信业务提供基础。它可以应用于 SCADA、AMI 和需求响应等应用。作为 GSM 和 CDMA 的替代品，WiMax 是大型区域内具有成本效益的信道宽带接入技术。它可以适用于 AMI、SCADA、需求响应、流动员工和视频监控。网状网络是通过使用以网状拓扑

结构排列的无线节点网络而创建的，通常用于为最后一英里提供宽带接入。它可以覆盖或替换铜线 DSL 或提供冗余的通信通道。它可以用于远程监控、需求响应、AMI 和分布自动化。存在的问题是由于路由器之间的跳跃而导致的延迟；然而，通过添加额外的节点并允许在网络中构建冗余使它很容易扩展。LTE 是移动通信的下一代网络，可提供高频谱效率和低延迟。它可以用于所有使用网状网络的应用；然而，LTE 技术并非现成的并且安装成本高。蜂窝网络通常用于大多数用户的应用程序，包括移动电话、互联网连接、语音和视频聊天以及发送短信。智能电网中，蜂窝网络可以用于员工协调、AMI 等。主要优势在于其已经被广泛部署，实施智能电网举措所需要的资金成本最低。WLAN 已经广泛用于室内连接，并且可以轻松用于家庭区域网，并将智能电表与内部可视化设备相连接。Zigbee 是专门针对智能电网而制定的标准，针对包括智能电表、智能照明和电器在内的家庭网络应用。

三、传感器与设备

虽然通信基础设施推动了智能电网的发展，但是真正的益处将来自网络上的传感器和设备。智能电表将安装在网络的每个节点上，这有助于通过双向计量实现双向电力交换，并允许电力公司精确控制用户电器的用电情况。电表还将允许用户远程访问家中的电器，并为其提供详细的使用数据。此外，它还将为商业实体提供监控、诊断和维修设备的权限。智能电网也将最大限度地减少电网上的人为数据收集。

直到最近，电力公司员工已经人工收集了运营数据包括计量电量、识别损坏设备和故障。智能电网基础设施将允许远程控制和自动化几项运营活动，包括监控由电线、变电站、变压器、交换机等组成的分布式基础设施。网络上的每个设备将由传感器来收集数据（电压、相位、温度等）。该数据将通过电网的双向通信系统接力传送到控制中心。电网的关键需求之一是提高稳定性，这需要在整个网络中安装同步相量设备以进行数据收集。同步相量将实时测量来自整个电网的电量，用于几个关键应用，包括动态响应估计、电网同步和故障识别。这些设备由全球定位系统（GPS）卫星同步时钟、同步相量测量单元（PMU）、相量数据集中器和分析软件组成。

智能电网的另一个关键元素在于电网的自我修复能力，可以自动修复缺陷或隔离故障，从而最大限度地保障用户正常用电。为了在电网中开发自我修复能力，每个开关都需要处理器，并且断路器和机电开关需要用固态

电子电路来替代。电网中将添加自动重合闸装置，从而允许因诸如掉落的树枝和大风等事件而导致的暂时性瞬时故障进行自我纠正。为了管理和分析数据，需要结合分布式分析处理能力以及电网的存储能力。最后，保护电网需要通过外围防御和增强对网络入侵和攻击的可见性，我们将进一步讨论这一点。

结语

智能电网需要整个国家全面连接的大型通信基础设施。基于地域分散的基础设施元素，通信将需要由多种通信媒介混合组成。起初，至少在分配网络中，通信为其他服务所共享。然而，随着时间的变化，通信网络可能变得更加专用，因为通信基础设施专门用于智能电网。电网基础设施同样需要传感器来检测和诊断整个电网，并且将现有的机电开关升级为电子开关，以增强自我修正能力。智能电网取得成功的关键因素将在于强大的安全机制，不仅能防止入侵还能确保用户的隐私和数据的完整性。

第二节　智能电网的安全问题和威胁

智能电网有望从根本上将以公用事业公司为中心的集中式电网改变为以消费者为中心的分散式电网，在此消费者能够充分了解情况并积极参与能源生产和消耗的过程。智能电网还能带来更多可见性，有助于更好地监测和控制电网以确保稳定性并降低大规模停电的概率。无处不在的通信网络将所有用户、公用事业公司以及生产者连接成单片网络，可推动实现该功能。然而，这一切都需要付出代价，即增加了受到网络攻击的风险。威胁来自不同的行为主体，包括恐怖分子、民族国家、犯罪分子以及不满的雇员。此外，还需要保护消费者隐私，因为通过精确传输用户数据可以泄露消费者隐私。如果没有足够的安全性，电网中的通信网络可能成为债务而非资产。智能电网已经遭受了无数次的攻击且面临多种安全威胁，我们将在本节讨论其中一些安全问题和威胁。

一、电网攻击事件

由于针对性的网络攻击或者网络异常的意外结果导致如上所述的 SCA-

DA 系统故障[4]，已经有几个文件证明对电网的影响。2003 年 1 月，Slammer 蠕虫侵袭了俄亥俄州橡树港的戴维斯贝塞核电站的计算机网络，造成安全监控系统和工厂处理计算机瘫痪了几个小时。2003 年 8 月，第一能源公司 FirstEnergy 报警处理器的故障导致无法监测电网，并且多种传输线路因为各种原因而跳闸，连锁故障导致东北发电厂瘫痪并且造成停电时间延长。2006 年 8 月，阿拉巴马州布朗渡口核电站的循环泵因为控制系统网络的流量过多而瘫痪。对 2009 年事件的调查显示，黑客通过侵入智能电表以及改变电耗读数窃取电量。在电力批量提供商处也检测到网络钓鱼事件，并且检测到的恶意软件样本表明这是有针对性和复杂的入侵。

以上提及的网络攻击引起了关注，关于民族国家参与这些攻击已经有所影射。还有一些攻击属于信息战役和宣传的范畴，例如，在与俄罗斯闹矛盾期间，针对爱沙尼亚和格鲁吉亚的网络袭击。Stuxnet 震网病毒袭击是攻击国家重要基础设施的首次重大网络战，目的是削弱伊朗的核浓缩设施。Stuxnet 震网病毒是一种利用多个零日漏洞的蠕虫病毒，利用被盗的数字证书来控制西门子公司 S7 PLC 微控制器上的 WinCC SCADA 应用程序[5]。Stuxnet 震网病毒的有效负载是通过使用核试验员的被感染的 U 盘进行传播。恶意软件不仅能提高用于浓缩铀的离心机的转速，而且还显示离心机运行正常。这是其他国家重要基础设施首次遭受的重大战略攻击，此次事件推动了各国进行军备竞赛以研制该武器作为威慑和反击的战略选择。

已有侦察和探测重要基础设施的一些数据[5]。“夜龙”攻击行动的目标是探测美国能源公司（石油、天然气以及石油化学产品）的工业控制系统。这些攻击结合了 Windows 平台上的远程管理工具中的社会工程和漏洞，从而闯入网络中的关键计算机并收集专有信息，包括涉及油气田勘探和商业谈判的文档以及 SCADA 系统的细节。布达佩斯的研究人员发现了另一个名为 Duqu（毒区）病毒的计算机恶意软件，它由一系列工具和服务组成，包括按键记录器、内核驱动程序和注入工具。该病毒在制造工业控制系统的公司计算机上被发现。有人猜测，Stuxnet 病毒编写者使用恶意软件来收集开发 Stuxnet 的信息。针对控制系统的更为复杂的恶意软件是 Flame 工具包，其中包括软件后门、特洛伊木马以及允许其在网络和可移动媒体上传播的复本和传播机制。Flame 是搜集情报的恶意软件，可以通过命令和控制服务器来嗅探流量、截取屏幕、录制音频对话、捕获击键和传输文件。

对智能电网的攻击可能发生在多个层面，包括传输、分配和家庭网络。

这些攻击可能包括基于协议的攻击、路由攻击、侵入式攻击、恶意软件攻击和拒绝服务式攻击。攻击媒介多种多样，包括社会工程、随机网络扫描、内部恶意活动以及破坏通信基础设施。

二、安全问题

智能电网由传感器、监视器、设备网络以及用于数据收集和分析的计算机组成。所有这些都容易受到网络攻击。分析人员发现了与智能电网[7]相关的计算机安全系统所面临的五大挑战，其中包括大量敏感的用户信息、分布式控制设备、缺乏物理保护、行业标准薄弱以及大量依赖电网的利益相关方。与其他典型电力系统一样，智能电网的安全问题具有机密性、完整性和可用性。机密性需要保护消费者和运营数据；为了确保电网的稳定性，在计量和计费的消费者层面以及运营层面都要求完整性；可用性意味着无论系统状态如何，电源都会继续由用户传输和接收。

智能电网面临着与所有复杂计算机网络都相同的安全挑战，因此需要确保网络的周界防范和可视可信。根本问题在于，鉴于整个网络规模较大且相互连接，蠕虫和病毒可能会迅速传播。而且，由于网络的分散性，有大量易受攻击的目标。另外，SCADA 系统的安全性设计不足。例如，西门子公司仍然使用硬编码密码来访问控制系统[8]，这些系统一旦遭到破坏就会导致大规模的安全漏洞。管理密码通常进行了预编码，并且从未改变原始设置。可通过如下几种方式进入网络的入口点，包括从被感染的设备渗透、基于网络的入侵、使供应链受损以及恶意内部员工。

除了第三方[9-14]专门攻击和入侵之外，智能电网仍面临几个威胁，包括通过窃取数据侵犯隐私、盗电、扰乱服务、物理性损坏设备、拒绝服务以及市场欺诈。侵入智能电表、无线通信或窃取公用事业公司服务器的数据可以获得详细的用户消费计量信息[9]。该信息对于公用事业公司的计费、需求响应和负荷预测是必要的。然而，相同的信息可以揭示个体的生活方式。每个电器具有独特的用电署名，可以从显示用户从事活动的总体使用模式中提取，包括计算机办公、看电视、洗澡和烹饪等活动。雇主、营销人员、保险公司以及犯罪分子可以将这些信息用于不同的目的。营销公司可以将该信息用于有针对性的营销或引入非竞争性定价。犯罪分子可以利用这些信息来判断用户的日常工作或家庭情况，例如，在房屋里没有人或者仅有一个人时进行盗窃或其他犯罪。通过篡改电表或在破坏加密密钥后改变信息来

更改电表读数时，可能会发生窃电[9]。

三、安全威胁对智能电网的影响

通信中的细小破坏（约5%）可以造成重大延迟问题，导致操作性能大幅下降[15]。已经为智能电网中的通信技术定义了若干指标，包括分组递交率（#递送/#预期）、平均端到端延迟和平均数据包跃点数（中间节点数）、成功的断开请求比率（#断开请求已发送/#断开请求已发布）[15]。需要定义并保证这些指标的极限值，以确保电网的无缝接入。除通信延迟问题外，关键问题是从传感器收集的数据可能会被破坏。有一些机制可以检测到基于其他传感器数值的数据损坏。然而，攻击者可以使用足够多的传感器处理数据，以致数据损坏难以察觉[16]。这种攻击不是随机而是相互协调的，不可能按顺序来避免检测。为了攻击成功，黑客需要知道控制中心使用的测量检测和分析技术。

智能电网广泛依赖于广域监测系统（WAM），并根据GPS定位对网络中分布式传感器的数值进行空间分析[17]。测量设备可能伪造GPS定位，导致基于伪造数据而产生错误的控制决策，其结果根据攻击的广度可能会由轻微至严重。可以通过制造干扰来伪造GPS数据，使GPS接收器丢失信号，然后使用提供虚假信息的较高相关峰来创建错误信号。虚假数据可以阻止控制者接收故障信号或者提供错误的故障定位，延迟电源线的检修和恢复。电压尖峰可能被伪装，并且可能会产生错误的电压尖峰，导致控制者产生错误的纠正措施，造成电网不稳定。可以伪造干扰的坐标以防止三角测量并延迟故障位置的识别。由于消息定时在智能电网中至关重要，因此攻击者可以使用合法手段来延迟消息并导致拒绝服务或引发故障。攻击者可以用虚假数据冲击数据流并严重降低性能[18]。

结语

无处不在的通信技术是智能电网的必备条件，但是它同样为黑客使用相同网络访问电网元件提供了机会。物理性通信基础设施以及基于包括入侵、拒绝服务式攻击、恶意软件和社会工程等在内的传统威胁的网络逻辑运算还面临着安全威胁。此外，疏忽大意、设备故障以及自然灾害也会带来威胁。个别行为主体包括不满的员工、竞争对手、恐怖分子、民族国家以及犯罪分子，他们都会构成威胁。整个智能电网是由数据驱动的，数据用于关键

操作包括资源管理、负荷预测、错误纠正以及故障隔离。机密性、完整性和可用性在智能电网的数据安全方面均非常重要。无数次数据病毒攻击通过无端的纠正措施或缺乏必要的纠正措施来破坏电网的稳定，而这二者均会导致连锁故障。缺乏可用性将导致网络失去可视性，这对电网又是危险的。简而言之，确保电网的安全性对其取得成功至关重要。

第三节　确保智能电网安全

电网是在地域上和逻辑上分布的极其复杂的系统。智能电网通过通信基础设施来连接分散的组件，并且通过广泛的数据采集和分析来管理电网，以此获取实时的运营智能。此种运营上的智能为电网带来几个好处，包括改善负荷预测、通过需求响应降低尖峰负荷、更好地利用可再生微能源、自动检测和隔离故障以及某些情况下自我纠正。另外，贯穿整个电网的通信基础设施为攻击者接近整个电网提供了机会。因此，智能电网必须拥有强大的安全性能。

智能电网将用户、发电厂、公用事业公司、变电站、网络监督机构和组件相互连接，其中组件包括保护继电器、断路器、SCADA 系统以及家用电器。智能电网分为三个不同的部分，即输电、配电和家庭局域网。传统电网中，通信基础设施在配电网络中的主要作用是监测变电站。然而，通信网络已全面延伸到拥有智能电网的家庭和个人电器。这同样意味着有一个更大的网络需要保护。传统意义上，大量配电体系已成为网络安全的主要焦点，因为其影响最大。配电网络故障有可能引发大规模连锁故障。然而，随着智能电网的发展，攻击智能电表也会造成很大影响，因为攻击通过网络迅速传播，从而导致巨大灾难性故障。电网[19]中存在几个弱点，包括架构、互操作性、通信协议、接口、HAN、用户门户和硬件。

当今部分问题是在电网的分散地点采集和分析的大量数据成为黑客进行数据操纵攻击的目标。大部分数据来自同步相量，它从电网中提供状态信息，包括确保电网稳定所需的电压和电流。基础设施的数据以及软件组件成为亟待解决的大块漏洞。一些传统漏洞来自软件的校验检查，包括跨站脚本、命令注入和缓冲区溢出[20]。其他一些漏洞包括对访问控制、优待和许可的管理不善，缺乏适当认证和管理访问凭证，缺少完整性检查。其

他问题包括系统配置不当、延迟补丁管理、缺乏安全审计、日志监控不足、硬件和网络设备配置不当，以及最终缺乏对管理员在安全实践方面的培训。

很多遗留设备是几十年前制造的，且没有内置网络安全。但是，当设备在过渡期间逐渐被替换时，会形成大型漏洞。在过去，电网基础设施的安全范式是“不公开即安全”，也就是说，如果存在的漏洞是未知的，它就会受到保护。我们都知道，在互联网不断扫描网络漏洞点的情况下，事实并非如此。而且，随着 SCADA 系统的软件日益标准化，有可能通过网络进行大规模攻击，致使大规模故障和毁坏。有必要实施迁移计划、全面测试和电网敏捷监控以确保遗留系统不对智能电网构成网络安全威胁。

一、标准与架构

智能电网家电的标准仍在不断发展，因此，针对不同设备创建了不同的安全控制，从而防止测试和评估过程的标准化。数个团队正积极致力于创建标准，包括智能电网互操作性小组（SGiP）、网络安全工作小组（前身是 NIST 美国国家标准技术研究所的网络安全协调工作组），以及智能电网建筑理事会（GWAC）。智能电网的安全要求可归为数据安全（访问控制、数据认证、存储、备份、恢复以及密码协议）、管理安全（风险分析、安全策略以及培训）以及基础设施安全（风险和设备配置、边界安全以及个人密钥交换）[21]。此外，有必要开发过程，以便为网络进行广泛的数据记录和分析获得可见性。需要通过通信基础设施与系统来实现安全，包括 SCADA 系统（DNP3、GOOSE、IEC 61850、IEC 60870-5）、WAN、陆地移动无线电设备（LMR）、WLAN 和 WiMax。

智能电网的大部分通信将被加密，需要在网格中使用公钥基础设施[22]。并且，通信基础设施需要整合安全，包括适当的网络拓扑设计，安全的路由协议、安全的信息转化、端到端加密、安全传播、抵抗拒绝服务攻击（例如，产能过剩、快速检测以及应对措施）。这同样需要数据包验证和不良数据检测。

智能电网通信网络有可供选择的多种搭建架构，例如：包括 HAN、邻域网（NANs）和 WAN 以及网状区域网络（因其可提供多种冗余路径，而被推荐使用）的三层网络架构（关于此架构的研究请见本章参考文献）。这一架构主要侧重于防止拒绝服务攻击以及信号中断。又如，利用分层的方法实现

智能电网的安全，从低层次的技术执行到高层次的战略方向，即物理、网络、主机、数据、应用程序、商业过程和企业组织。

二、传感器与设备

个人智能电表需要防止篡改、数据泄露以及侵犯。黑客可以在用户端访问，非法侵入 AMI 电表以及终端设备间的无线通信，或者非法入侵 AMI 电表至当地集中器之间的无线通信。入侵式攻击可以允许通过终端访问公用事业公司的通信网络。已经针对其保护提出了一些建议，其中一项建议是仅针对用电量的变化限制传播。但是，黑客可以从传播的能量使用变化中重构相应文件。已经有人建议将人工欺骗数据包纳入数据流，以致能量使用情况看似正常而非主人不在场。欺骗数据包可以通过用电量或历史模板[1]的泊松分布随机产生。在传播层面，侵犯和攻击的缓冲区溢出类型需要检测。大部分通信网络开放连接以等待合成器/认可信号的响应，有时候只要 75 秒。攻击者可以按照欺骗合成器要求溢出缓冲区，造成网络拥堵。数据包信息可以使用贝叶斯数据分析以检测攻击[24]。运用传输数据和之前数据库的融合中心可以用来确定是否有恶意数据通过[25]。对每个节点进行独立分析，从而防止分布式攻击。

大部分安全模型通过将其与一系列已知的安全状态进行对比，从而来评估系统的当前状态是否有效。暴露分析图可以用于识别用户和数据流。此处，图表上的每个节点有以下至高点：安全机制、系统权限、信息对象以及失信用户；边缘是通向其他节点的路径。这可用于检查欺骗、篡改、否认、信息暴露或泄露、拒绝服务以及权限升级[26]。分层的皮特里网已经用于建模多种攻击[27]。攻击树无法跟踪协同攻击，多步的皮特里网局限于跟踪三个攻击者。分层的皮特里网不限攻击的数量，并且可以用于多种攻击包括窃取、干扰或通信中断，未经授权的数据访问，服务窃取和拒绝服务。分层模型以小组为单位建立，以至当地专家在各自领域映射威胁途径与结果，区域专家采取本地模式，将皮特里网映射到网络，并创建层级结构和区域层次结构，用对应点组合成单一整体的超级皮特里网。

物理状态的安全对于保持电网的稳定至关重要。从同步相量以及其他状态分析设备中收集的数据需要用来分析恶意变更造成的破坏。以安全为导向的物理状态评估体系[28]试图通过利用电网的网络组件与物理组件之间的相互关系来实现该做法。它利用 bot 病毒主机和网络入侵检测系统的警