[美] National Institute of Standards and Technology 著
中国电力科学研究院 译

美国国家标准和技术研究院(NIST)
7628号报告

智能电网信息安全指南

第1卷 智能电网信息安全战略
架构和高层要求

中国电力出版社
CHINA ELECTRIC POWER PRESS

[美] National Institute of Standards and Technology 著
中国电力科学研究院 译

美国国家标准和技术研究院(NIST)
7628号报告

智能电网信息安全指南

第1卷 智能电网信息安全战略
架构和高层要求

中国电力出版社
CHINA ELECTRIC POWER PRESS

U.S. Department of Commerce
Gary Locke, Secretary

National Institute of
Standards and Technology
Patrick D. Gallagher, Director

NIST 授权中国电力科学研究院进行中文版翻译，中国电力科学研究院非美国政府官方翻译机构。

北京市版权局著作权合同登记
图字：01-2013-8140 号

图书在版编目（CIP）数据

智能电网信息安全指南：美国国家标准和技术研究院 7628 号报告 / 美国国家标准和技术研究院编；中国电力科学研究院译. —北京：中国电力出版社，2013.1
ISBN 978–7–5123–3884–5

Ⅰ. ①智… Ⅱ. ①美… ②中… Ⅲ. ①智能控制－电力系统－信息安全－国家标准－美国 Ⅳ. ①TM76–65

中国版本图书馆 CIP 数据核字（2013）第 152899 号

中国电力出版社出版、发行
（北京市东城区北京站西街 19 号 100005 http://www.cepp.sgcc.com.cn）
汇鑫印务有限公司印刷
各地新华书店经售
*
2013 年 1 月第一版 2013 年 1 月北京第一次印刷
787 毫米×1092 毫米 16 开本 12.75 印张 307 千字
印数 0001—2000 册 定价 **45.00** 元

致　　谢

本报告由智能电网交流委员会下设的网络安全工作小组（SGIP-CSWG）中的多位成员合作完成，并且由联邦能源监管委员会（FERC）的安娜贝尔·李主持完成该报告的编写过程，其中联邦能源监管委员会的前身为美国国家标准与技术研究院（NIST）。在智能电网交流委员会中，网络安全工作小组（SGIP-CSWG）由原网络安全协调工作小组（CSCTG）演化而来，其现任主席为 NIST 的玛丽安·斯旺森，波音公司的艾伦·格林伯格、思科公司的戴夫·达尔瓦和美国能源部的比尔·亨特曼分任副主席，Neustar 公司的马克·恩斯特龙为书记，NIST 的妲雅·布鲁尔为本报告的主编。网络安全工作小组的成员们拥有广泛的技术专长和知识以满足智能电网中的网络安全需求，并且在过去的一年半时间内取得显著成就。

拥有满足智能电网网络安全需求能力，并承诺参与网络安全工作小组（CSWG）工作的组织数量正在不断增加，网络安全工作小组（CSWG）的成员列表详见本报告的附录 J。此外还要特别感谢 NIST 的智能电网团队，该团队包括 NIST 智能电网办公室和 NIST 的一些实验室。在智能电网交流委员会的政府协调员乔治·阿诺德博士的领导下，NIST 智能电网团队对本报告的顺利完成作出了巨大的贡献。

此外还要感谢波音公司的戴安娜·约翰逊和 NIST 的林茨·列侬对本报告的精心编辑，他们的专业知识、耐心和奉献精神是提升本报告质量的可靠保证。还要感谢博思艾伦咨询公司的维多利亚·YAN 对本报告的倾力相助。

最后，感谢为保证本报告中涉及智能电网安全需求内容文章质量贡献自己时间和知识的所有人。

译 者 序

党的十八届三中全会对全面深化改革做出重大战略部署，将进一步解放和发展我国社会生产力和创造力，也将对能源和电力工业创新发展产生深远影响。当前，随着新能源技术、智能技术、信息技术、网络技术的创新突破，第三次工业革命正在孕育发展。智能电网是承载第三次工业革命的基础平台，对第三次工业革命具有全局性的推动作用。

未来的智能电网，是网架坚强、广泛互联、高度智能、开放互动的能源互联网。随需接入、广泛互联的信息通信网络，种类繁多、高度智能的供电设施和用电终端，智能电网中用户与电网、能源供应商的广泛互动都为智能电网的安全防护和安全管理带来全新的挑战。

美国国家标准和技术研究院（NIST）发布的 7628 号报告《智能电网信息安全指南》共分 3 卷，详细分析了智能电网的逻辑结构和信息安全需求，提出了智能电网信息安全防护的策略和构架，并重点分析了智能电网用户隐私保护等核心问题，对我国智能电网的信息安全防护工作具有重要的借鉴意义。

本书是该报告的第 1 卷，主要由高昆仑、徐志博、郑晓昆、李凌、赵婷、梁潇、徐兴坤、李焕、王宇飞、赵保华、树娟等进行翻译整理。本书翻译参考了大量资料，并得到多位同行的支持和帮助，在此表示感谢。

译 者

2012 年 12 月

计算机系统技术报告

美国国家标准和技术研究院（National Institute of Standards and Technology，NIST）的信息技术实验室（Information Technology Laboratory, ITL）通过为美国测量和标准基础设施提供技术领导来推动美国经济和社会发展。ITL 的开发内容包括测试技术、测试方法、参考数据、概念实施论证及技术分析报告，从而促进信息技术的发展并提高其成效。ITL 的责任包括开发管理、行政、技术及物理标准和指南，它为联邦计算机系统中的非涉密敏感信息提供了低成本、高效率的安全和隐私权保护。本跨部门报告讨论了 ITL 在计算机安全领域的研究、指导和外包工作，以及其与工业界、政府和学术机构的合作活动。

为了能够充分描述实验进程或概念，本报告可能会引用某些商业实体、设备或材料的名称。这种引用并不意味美国国家标准和技术研究所提出的建议或做出的认可，以及这些实体、设备或材料本身就一定是最佳选择。

执 行 摘 要

美国的电力基础设施正面临一次重大转型。这个从家庭和公司客户延伸到以石油为燃料的电厂和风力发电场的庞大基础设施升级工程，已经成为美国相关工作的核心，最终将提高能源的使用效率、可靠性和安全性，从而过渡到使用可再生能源、降低温室气体排放和建立一种确保未来繁荣的可持续经济模式。智能电网的这些优势以及其他可预见优势正在成为世界各国努力追求的目标。

推动美国日益老化的电网转型，使之成为一种具备双向信息通信、设备控制和电力配送能力的先进数字化基础设施，需要用很长时间循序渐进地进行。与这些发展以及政府和私营部门的投资支持相呼应，关键的启动活动也必须完成。其中的首要任务是制定出行之有效的战略，以保护智能电网相关数据的隐私，确保即将作为未来电力基础设施性能和可用性核心的计算和通信网络的安全。将信息技术融入电网，是建设智能电网和实现其优势的根本，但是这些联网技术同时会增加复杂性，并带来新的相互依赖性和脆弱性。在向智能电网转型的初期，首先必须设计并执行相应的方法，一方面要确保这些技术能够安全使用，另一方面又能让隐私得到保护。

由 3 卷组成的《智能电网信息安全指南》报告介绍了一个分析框架，它可供机构在综合考虑智能电网相关特点、风险和脆弱性的基础上，根据自身特殊情况制定有效的信息安全战略。智能电网领域拥有众多利益相关者，从电网公司到能源管理服务供应商，再到电动车和充电站设备制造商，种类繁多；这一领域的机构可将本报告介绍的方法和提供的支持性信息作为指南，用以评价风险、识别和落实相关安全要求。这种方法体现了我们对电网的认识，电网正在从一个相对封闭的系统转变成一种高度互联的复杂环境。随着技术不断发展以及电网安全面临威胁的成倍增加和日趋多样化，每个机构的信息安全要求也应不断进化。

2009 年 11 月，NIST 成立了一个公共私营合作实体——智能电网互操作性专家组（Smart Grid Interoperability Panel，SGIP）[1]，作为专家组成员达成的共识，SGIP 所属信息安全工作组（Cyber Security Working Group, CSWG）推出了初版《智能电网信息安全指南》。如今，CSWG 的成员已超过 475 名，分别来自私营部门（包括生产厂家和服务供应商）、制造商、标准制定组织、学术界、监管部门和联邦机构，还有一部分成员来自其他国家。

---

[1] 读者可登录 http://collaborate.nist.gov/twik-sggrid/pub/SmartGrid/CMEWG/Whatis_SGIP_final.pdf 查阅简短介绍这个机构的文章：Smart Grid Interoperability Panel: A New, Open Forum for Standards Collaboration。

本报告是 NIST 于 2010 年 1 月 19 日出版的《NIST 智能电网互操作性标准框架和路线图 1.0》（NIST SP 1108）❶的姊妹篇。这份框架和路线图报告描述了智能电网的高层概念参考模型，识别了适用于（或可能适用于）当前正在开发之中的可互用智能电网的标准，指出了一系列与标准相关的亟待优先解决的差距和问题。信息安全已被认为是一个贯穿各个领域的关键问题，为智能电网应用制定的所有标准都必须认真对待。鉴于信息安全对智能电网性能和可用性有着超出一切的重要性，本报告对初版的《NIST 框和路线图》深入拓展，提供了相关技术背景和附加的详细信息，可帮助机构在风险管理工作中安全实施智能电网技术。框架文件的出台，仅仅是持续展开的标准制定和协调融合进程的第一步。这个进程最终会推出数以百计的通信协议、标准接口以及会被广泛接受和采用的其他技术规范，而这些恰恰是建设一个具备双向通信和控制能力的先进、安全电网所不可缺少的。《智能电网信息安全指南》延伸了框架文件中有关信息安全的讨论。随着框架文件不断更新及扩大至测试、认证和总体架构开发等问题，同时还有更多标准被确定下来，CSWG 将继续提供更多的指南。

本报告是 2009 年 3 月启动的公开征求意见进程的产物，在这个进程中召开的研讨会和每周电话会议全都对所有利益相关方开放。3 卷草案至少都经过一轮正式公开的评议，有些部分甚至经过了两轮评议，这两轮公开评议都通过《联邦公报》发出了通知。❷

构成指南的这 3 卷文件主要面向负责智能电网系统以及构成其子系统的硬件和软件组件的信息安全事务的人员和机构。鉴于电力基础设施在美国经济中广泛且日益提升的重要性，这些人员和机构构成了一个庞大而多样化的群体，包括能源信息和管理服务供应商、设备制造商、电网公司、系统运营商、监管部门、研究人员和网络专家。除此之外，在编纂指南的过程中，还把含电网公司和其他公司的电力部门、信息技术业和电信部门这三个因新兴智能电网提供的机会而凝聚在一起的工业行业作为考虑问题的主要对象。

在执行摘要之后，报告的第 1 卷描述了分析方法，其中包括用来识别高层安全要求的风险评估流程。第 1 卷还介绍了所有逻辑接口架构都必须依照的高层架构，用于识别和定义 7 个智能电网域内或贯穿所有 7 个智能电网域的接口类别。随后描述的是针对 22 个逻辑接口类别中每类逻辑接口提出的高层安全要求。第一卷最后讨论了涉及智能电网系统和设备的密码和密钥管理技术问题。

第 2 卷以个人住宅内的隐私问题为重点，描述并讨论了各个相关主题，例如，不断发展的智能电网技术以及有关个人、个人群体及其在处所和电动汽车内行为的新信息类型，以及这些新信息类型是否含有迄今尚未经过法律检验的隐私风险和挑战等。此外，第 2 卷还根据被广泛接受的隐私原则为参与智能电网的实体提出了建议，其中包括建议实体编制隐私用例，用以跟踪含个人信息的数据流动，以化解和抑制智能电网业务流程中存在的常见

---

❶ 国家标准和技术研究所国家智能电网互操作性协调办公室，*NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0 (NIST SP 1108)*, Jan. 2010。读者可登录 http://nist.gov/smartgrid 下载报告全文。

❷ 1) *Federal Register*: October 9, 2009 (Volume 74, Number 195) [Notices], pp: 52183-52184; 2) *Federal Register:* April 13, 2010 (Volume 75, Number 70) [Notices], pp: 18819-18823.

隐私风险；并告诉智能电网内的隐私风险教育客户和其他相关个人，可以采取什么行动来抑制这些风险。

第 3 卷汇编了用来帮助机构制定高层安全要求的支持性分析和参考文献，以及前两卷采用过的其他工具和文献资料。其中收入了 CSWG 工作组定义的脆弱性类别，论述了在制定指南的过程中实施的自下而上的安全分析。第 3 卷还单辟一章专门论述了研究与开发主题，意在示范性地展示信息安全的变化方向——在智能电网持续发展、技术上日趋先进的背景下，信息安全将使智能电网在可靠性和安全性方面达到更高水平。此外，第 3 卷还概括性地介绍了 CSWG 开发的流程，专门用来评价 NIST 为支持智能电网互操作性而识别的各项标准能否满足本报告提出的高层安全要求。

除了执行摘要所介绍的内容，我们期望读者通过阅读本报告的全文能够对电网及其网络安全知识拥有全面了解。

报告内容

- 第 1 卷——智能电网信息安全战略、架构和高层要求
  - 第 1 章——信息安全战略：包括有关智能电网的背景信息、确保电网可靠性和具体信息保密性的信息安全的重要性，还讨论了智能电网信息安全战略和战略规定的具体任务。
  - 第 2 章——智能电网的逻辑架构和接口：包括一个高层框图，以复合高层图的形式展示了智能电网每个域中的行为者，同时还收入了智能电网的总体逻辑参考模型，涵盖了智能电网的所有主要域。本章还收入了 22 个逻辑接口类别中每类逻辑接口的逻辑接口图。该逻辑架构着重展示了智能电网的短期愿景（1～3 年）。
  - 第 3 章——高层安全要求：为第 2 章收入的 22 个逻辑接口类别中的每一类规定了智能电网高层安全要求。
  - 第 4 章——密码和密钥管理：识别了涵盖智能电网内所有系统和设备及潜在备选方案的密码和密钥管理技术问题。
  - 附录 A——信息安全文件的相互关系。
  - 附录 B——满足高层安全要求的安全技术和服务用例。
- 第 2 卷——隐私和智能电网
  - 第 5 章——隐私和智能电网：收入了对智能电网的隐私影响评估，其中还讨论了抑制风险的因素。该章还识别了智能电网新能力带来的潜在隐私问题。
  - 附录 C——州法律——智能电网和供电。
  - 附录 D——隐私用例。
  - 附录 E——与隐私相关的定义。
- 第 3 卷——支持性分析和参考文献
  - 第 6 章——脆弱性类别：收入了智能电网潜在的脆弱性的类别。每个脆弱性都划分到具体类别之中。

- 第 7 章——智能电网自下而上安全分析：识别了智能电网存在的大量具体安全问题。目前，这些安全问题还没有专门的解决方案。
- 第 8 章——智能电网信息安全的研究与开发主题：收入的研发主题旨在识别哪些方面的技术水平没有达到智能电网预期功能、可靠性和可扩展性要求。
- 第 9 章——标准审阅综述：概括性介绍了对照本报告所述高层安全要求评价相关标准的进程。
- 第 10 章——电力系统安全要求关键用例：列举了在智能电网安全要求方面具有架构性重要意义的关键用例。
- 附录 F——智能电网的逻辑架构和接口
- 附录 G——接口类别分析矩阵表
- 附录 H——高层要求对应表
- 附录 I——术语和缩略语
- 附录 J——SGIP-CSWG 成员名单

目　　录

第 1 章

信 息 安 全 战 略

随着智能电网投入实施，信息技术（information technology，IT）和电信基础设施越来越成为确保电力部门可靠性和安全性的关键，因此，IT 和电信基础设施中系统和信息的安全，也必须得到不断发展中的电力部门的高度重视。安全的概念必须扎根于从设计到实施，经维护再到销毁的整个系统开发生命周期的所有阶段。

信息安全不仅必须涉及恶意攻击，如心怀不满的员工、工业间谍和恐怖分子发动的攻击，而且还必须涉及因用户错误、设备故障和自然灾害引起的对信息基础设施的无意破坏。脆弱性会使攻击者成功渗透网络、访问控制软件、篡改负载条件，进而以无法预计的方式造成电网瘫痪。消除潜在脆弱性的必要性，已在包括 NIST❶、国土安全部（Department of Homeland Security, DHS）❷、能源部（Department of Energy, DOE）❸和联邦能源监管委员会（Federal Energy Regulatory Commission, FERC）❹在内的联邦政府机构达成共识。

电网面临的其他风险还包括：

- 电网不断增加的复杂性带来脆弱性，使电网越来越多地暴露在潜在攻击者和无意误操作之下。
- 相互连接的网络带来各个网络共有的脆弱性。
- 引发通信中断和造成恶意软、硬件或被破解硬件的脆弱性事件日益增多，导致拒绝服务攻击（deny of service, DoS）或其他恶意攻击频发。
- 可供潜在攻击者恶意利用的入口点和路径越来越多。
- 相互连接的系统令私有信息暴露激增，加大了数据聚合的风险。
- 越来越多的新技术投入使用带来新的脆弱性。
- 需收集数据的大幅增加带来破坏数据保密性的潜在可能性，其中包括对客户隐私的侵犯。

随着电力部门逐渐向智能电网转型，IT 和电信部门将被越来越深地直接牵涉进来，这些部门制定有消除脆弱性的信息安全标准和识别系统已知脆弱性的评价方案。而在智能电网基础设施环境中，不但存在着与 IT 和电信部门相同的脆弱性，而且还因智能电网复杂程度高、

---

❶ NIST 信息技术实验室主任 Cita M. Furlani 为美国众议院国土安全小组委员会就新涌现的威胁、信息安全和科学技术等问题作证，2009 年 3 月 24 日。

❷ 国土安全部国家保护和方案局国家信息安全处控制系统安全计划主任 Sean P. McGurk 为美国众议院国土安全小组委员会就新涌现的威胁、信息安全和科学技术等问题所做的记录声明，2009 年 3 月 24 日。

❸ 美国能源部电力输送和能源可靠性办公室：Smart Grid investment Grant Program, Funding Opportunity: DE-FOA-0000058, Electricity Delivery and Energy Reliability Research, Development and Analysis，2009 年 6 月 25 日。

❹ 联邦能源监管委员会，Smart Grid Policy, 128 FERC ¶ 61,060 [Docket No. PL09-4-000]，2009 年 7 月 16 日。

利益相关者数量庞大和操作要求时间高度敏感而额外存在不同于 IT 和电信部门的脆弱性。

从最广义的角度上说，电力工业的信息安全涵盖了涉及自动化和通信的所有问题；而自动化和通信不仅影响着电力系统的运行，同时还影响着管理电力系统的电网公司和支持客户群的业务流程的正常运转。长期以来，电力行业一直把工作的重点放在提高电力系统可靠性的设备实施上。直到最近，业界才普遍认识到通信设备和 IT 设备是保证电力系统可靠性的重要组件，并且已有越来越多的这种部门成为维系电力系统可靠性的关键。例如，2003 年 8 月 14 日发生的加州大面积停电事件，控制系统的通信延迟是原因之一。除了最初是电力设备出了问题外，接踵发生连锁性事故，其主要原因是应该在正确时间发送给正确人员的消息发送错误造成。而且，当时并没有任何恐怖分子或互联网黑客对 IT 基础设施发动攻击。造成 IT 基础设施故障的原因是无意事件——误操作、关键时刻缺乏警报，设计不当。由此可见，对于无意间造成的破坏必须给予足够的重视，必须采用一种全方位防救灾害的方法。2009 年 3 月，信息安全协调任务组（Cyber Security Coordination Task Group, CSCTG）在 NIST 的领导下建立，制定《智能电网信息安全指南》的工作自此开始着手进行。现今，CSCTG 有来自私营部门（包括生产厂家和服务供应商）、制造商、标准制定组织、学术界、监管部门和联邦机构的 475 名以上成员。任务组于 2010 年 1 月划归 SGIP 领导，更名为信息安全工作组（SGIP-CSWG，简称 CSWG）。

信息安全在一个完整周密的进程中得到高度重视，必将形成一整套高层信息安全要求。而这些要求正如本章下文将要详细阐明的，将在本报告有关信息安全战略的章节定义的高层风险评价进程中被不断开发（或在现有标准/指南的基础上扩展）。信息安全要求是所有优先行动计划的关键组成部分，2010 年 1 月出版的《NIST 智能电网框架和路线图 1.0》（NIST SP 1108）详细说明了这些优先行动计划。❶

该框架文件描述了智能电网高层参考模型，可识别出当前支持智能电网开发的 75 个现行标准，指出了 15 个急需通过出台新标准和要求或修订现行标准和要求来优先解决的（不仅涉及信息安全的）差距和协调问题，并提出了交由指定标准制定组织弥补这些差距的紧迫行动计划，同时还阐明了建立智能电网信息安全要求和标准的战略。这个框架文件的出台仅仅是一个持续展开的标准制定和协调融合进程的第一步，这个进程最终会推出数以百计的通信协议、标准接口以及会被广泛接受和采用的其他技术规范，而这些，恰恰是建设一个具备双向通信和控制能力的先进和安全电网所不可缺少的。《智能电网信息安全指南》延伸了框架文件中有关信息安全的讨论。随着框架文件的不断更新，将扩大至涉及测试、认证和总体架构开发等问题，同时随着有更多标准的确定，CSWG 将继续提供更多的指南。

本报告是供从事智能电网技术研究、设计、开发和实施工作的机构使用的一个工具，报告收入的信息安全战略、风险评价流程和安全要求适用于整个智能电网系统。

信息安全风险是机构在实施和维护智能电网系统时无法回避的问题。因此，机构应该把本报告用作一个指南，借以在系统设计、实施和维护等各个阶段评估智能电网系统的总体信息风险。机构确定的智能电网风险抑制战略必须能够适应信息风险环境的不断变化，目的是利用机构和系统层面采用的风险评价方法来识别和抑制智能电网系统的信息风险，包括系统内具体组件的信息风险。这种方法如果与系统层面的架构融为一体，将使机构得到一种既能

❶ 参见：http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf。

确保安全，又能满足电网可靠性要求的智能电网解决方案。

本报告所含信息是对机构提供的指南，NIST 没有在指导意见中规定任何具体解决方案，各机构必须为确保智能电网的安全开发出适合自身情况的信息安全保护手段，其中包括风险评价方法。

1.1 信息安全和电力部门

下述立法和美国能源部 DOE 的《能源部门计划》阐明了信息安全在确保智能电网有效运行中扮演的关键角色：

2007 年《能源独立性和安全法案》（P.L. 110-140）第 1301 款指出：

支持国家输电配电系统实现现代化是美国的一项国策，唯有如此，方可保持电力基础设施的可靠性和安全性，满足未来不断增长的需求以及实现作为智能电网特征的以下两点要求：

（1）增加使用数字信息和控制技术，提高电网的可靠性、安全性和有效性。

（2）在全面实现信息安全的基础上动态优化电网运行和资源。

智能电网的信息安全既支持电网的可靠性，也支持被传输信息的保密性（和隐私）。

DOE 的《能源部门特定计划》[1]指出：“构想了一种极富适应性的强健能源基础设施，其中业务和服务连续性可通过安全可靠的信息共享、行之有效的风险管理方案、协调一致的响应能力及业界与政府之间所有层面相互信任的公共和私营合作伙伴关系来保持。”

1.2 范围和定义

为了确保形成统一的认识，本报告收入了《国家基础设施保护计划》有关信息基础设施的以下定义：

信息基础设施：包括电子信息和通信系统及服务，以及这些系统和服务包含的信息。信息和通信系统及服务由处理、保存和传输信息的所有硬件和软件或所有这些元素的任何组合组成。处理涉及对信息的创建、访问、修改和销毁，保存涉及纸质、磁质、电子和其他所有类型介质，传输涉及共享和散布信息。举例来说，计算机系统、控制系统（如 SCADA）、网络（如互联网）和网络服务（如受控安全服务），都是信息基础设施的组成部分。

传统的 IT 信息安全概念侧重于以被要求的手段保护领域电子信息通信系统的保密性、完整性和可用性，然而，对于电力系统与 IT 通信系统融合为一体的许多领域来说，唯有适当应用信息安全概念，才能确保智能电网的可靠性和客户信息的隐私安然无恙。智能电网的信息安全必须考虑电力及信息系统技术、IT 进程以及电力系统的运行和监控等诸多因素的平衡。把一个领域中的做法原封不动搬到另一个领域使用，很有可能造成可靠性下降。

长期以来，电力行业一直把工作的重点放在提高电力系统可靠性的设备实施上。直到最近，业界才普遍认识到，通信和 IT 设备可以用来支持电力系统的可靠性。然而，现在已有越来越多的这种部门成为维系电力系统可靠性的关键。安全性和可靠性在电力系统中有着至高

[1] 美国能源部，*Energy, Critical Infrastructure and Key Resources, Sector-Specific Plan as input to the National Infrastructure Protection Plan*，2007 年 5 月。

无上的重要性。在这些系统中执行的任何信息安全措施都不得妨碍电力系统的安全和可靠运行。

本报告旨在向相关机构（如电网公司、监管部门、电力设备制造商和供应商、零售服务供应商以及电力和金融市场交易者）提供有关智能电网信息安全的指南。报告的依据是 CSWG 当前对以下情况的了解：

- 智能电网和信息安全。
- 相关技术及其在电力系统中的使用。
- 这些技术运行的风险环境。

本报告从背景信息的角度介绍了可以用来为智能电网挑选和修改适用安全要求的分析流程。这个流程包含了在为智能电网挑选和修改安全要求时采用的自上而下法和自下而上法。自下而上法侧重于识别脆弱性的类别，如缓冲区溢出和协议错误等；自上而下法侧重于定义智能电网系统的组件/域以及这些组件/域之间的逻辑接口。为了降低复杂性，对逻辑接口进行了分类。对于基于交互的逻辑接口类别，其安全需求指定在内部组件与域之间。以高级量测体系（Advanced Metering Infrastructure, AMI）为例，电表对数据收集者的认证、隐私保密性保护和固件更新的完整性等即为其安全需求的一部分内容。

最后需要说明的是，本报告注重的是智能电网的运行而非企业的运行。不过，机构在设计、开发和部署智能电网信息系统时，应该从基础设施、技术、支持和运行等多个方面充分考虑企业的当前情况。

1.3 智能电网信息安全战略

CSWG 在编纂本报告的过程中采用的智能电网总体信息安全战略探究了各域特有的要求和通用要求，提出了一种旨在确保解决方案可在基础设施不同部分之间互用的抑制风险方法。信息安全战略涉及预防、检测、响应和恢复 4 个方面，这一总体战略也可能适用其他复杂的基础设施。

信息安全战略的实施，要求为智能电网定义和执行一个总体信息安全风险评价流程。所谓风险，是指取决于发生概率和相关影响的事故、事件或变故造成有害结果的潜在可能性。这类风险是机构风险的组成部分，包括许多类型，例如投资风险、预算风险、方案管理风险、法律责任风险、安全风险、库存风险以及来自信息系统的风险。智能电网风险评价流程基于私营和公共部门开发的现行风险评价方法，包括识别资产、脆弱性、威胁和规定影响级，以形成对智能电网及其域和子域（如家庭和公司）面临的风险的评价。由于智能电网包含了来自 IT、电信和电力部门的系统，风险评价流程适用于与智能电网互动的所有 3 个部门。本报告所含信息是对机构提供的指南，NIST 没有在指导意见中规定任何具体解决方案，各机构必须为确保智能电网的安全开发出适合自身情况的信息安全保护手段，其中包括风险评价方法。

智能电网开发风险评价方法时使用的文件如下：

- SP 800-39《信息系统风险管理：机构视角》（草案），NIST，2008 年 4 月。
- SP 800-30《信息技术系统风险管理指南》，NIST，2002 年 7 月。
- 联邦信息处理标准（Federal Information Processing Standard, FIPS）200《联邦信息和信息系统最低安全要求》，NIST，2006 年 3 月。

● FIPS 199《联邦信息和信息系统安全分类标准》，NIST，2004 年 2 月。

●《电力部门安全指南：脆弱性和风险管理》，北美电力可靠性委员会（North American Electric Reliability Corporation, NERC），2002 年。

●《国家基础设施保护计划：共同加强保护和提高适应性》，国土安全部，2009 年。

● IT、电信和能源部门具体计划，2007 年首次发表，后逐年更新。

● ANSI/ISA-99.00.01—2007，《工业自动化和控制系统的安全：概念、术语和模型》，国际自动化协会（ISA），2007 年。

● ANSI/ISA-99.02.01—2009，《工业自动化和控制系统的安全：制定一项工业自动化和控制系统安全方案》，ISA，2009 年 1 月。

智能电网信息安全战略的下一步是挑选和（按需要）修改安全要求。这个步骤使用的文件见后述的任务 3。本报告收入的安全要求和支持分析，可供智能电网的战略制定者、设计者、实施者和运行者（如电网公司、设备制造商、监管部门等）在实施风险评价以及智能电网安全生命周期其他任务的过程中参考。这些信息可作为基本指南供各种机构评价风险和挑选适宜安全要求之用。NIST 没有在本文的指导意见中就信息安全问题规定任何具体解决方案。

实施智能电网功能的机构必须面对复杂多样的信息安全问题。本报告收入了一种用以评价信息安全问题以及挑选和修改信息安全要求的方法。这种方法体现了我们对电网正在从一个相对封闭的系统转变成一种高度互联的复杂环境（复合式系统）的认识。随着技术和系统不断变化以及攻击者所用技术手段不断变化，每个机构执行的信息安全要求也应不断进化。

智能电网信息安全战略内的各项任务由 CSWG 的参与者执行。下面将描述在实施信息安全战略的过程中已经落实或即将落实的各项任务，其中包括每项任务的成果。由于本报告编纂时间有限，以下所列任务是在充分考虑了负责具体任务的各小组间互动的基础上平行执行的。

图 1-1 示出了智能电网信息安全战略定义的由 CSWG 负责执行的各项任务。

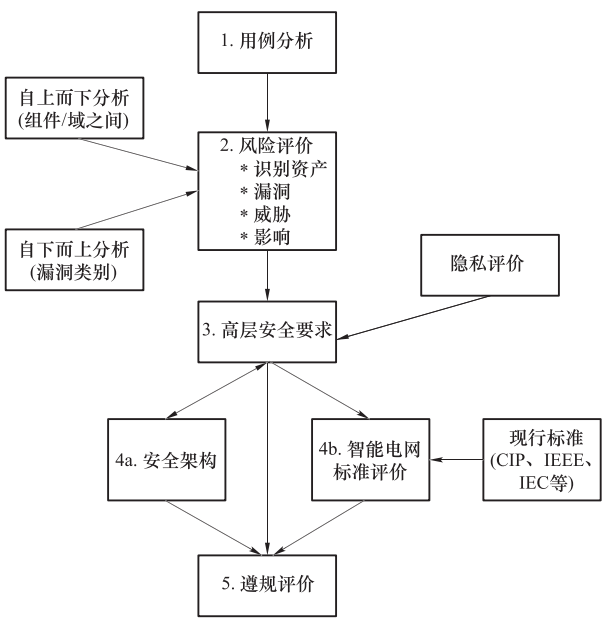

图 1-1　智能电网信息安全战略的各项任务