SCADA系统安全：挑战与解决方案

2011年6月 / 白皮书

作者：Metin Ozturk和Philip Aubin

善用其效，尽享其能[SM]

Schneider Electric

全球能效管理专家施耐德电气为世界100多个国家提供整体解决方案，其中在能源与基础设施、工业过程控制、楼宇自动化和数据中心与网络等市场处于世界领先地位，在住宅应用领域也拥有强大的市场能力。致力于为客户提供安全、可靠、高效的能源，施耐德电气2011年的销售额为224亿欧元，拥有超过130,000名员工。施耐德电气助您——善用其效，尽享其能！

施耐德电气在中国

1987年，施耐德电气在天津成立第一家合资工厂梅兰日兰，将断路器技术带到中国，取代传统保险丝，使得中国用户用电安全性大为增强，并为断路器标准的建立作出了卓越的贡献。90年代初，施耐德电气旗下品牌奇胜率先将开关面板带入中国，结束了中国使用灯绳开关的时代。

施耐德电气的高额投资有力地支持了中国的经济建设，并为中国客户提供了先进的产品支持和完善的技术服务，中低压电器、变频器、接触器等工业产品大量运用在中国国内的经济建设中，促进了中国工业化的进程。

目前，施耐德电气在中国共建立了53个办事处，28家工厂，7个物流中心，1个研修学院，3个研发中心，1个实验室，700多家分销商和遍布全国的销售网络。施耐德电气中国目前员工数近28,000人。通过与合作伙伴以及大量经销商的合作，施耐德电气为中国创造了成千上万个就业机会。

施耐德电气 EcoStruxure™ 能效管理平台

凭借其对五大市场的深刻了解、对集团客户的悉心关爱，以及在能效管理领域的丰富经验，施耐德电气从一个优秀的产品和设备供应商逐步成长为整体解决方案提供商。今年，施耐德电气首次集成其在建筑楼宇、IT、安防、电力及工业过程和设备等五大领域的专业技术和经验，将其高质量的产品和解决方案融合在一个统一的架构下，通过标准的界面为各行业客户提供一个开放、透明、节能、高效的EcoStruxure™能效管理平台，为企业客户节省高达30%的投资成本和运营成本。

目录

概要

本白皮书介绍如何提高SCADA系统安全，分析了导致控制系统漏洞增加的因素，并提出新的设计标准来保护关键基础设施，包括对SCADA系统使用加密和身份验证。

SCADA系统安全也是关键基础设施保护工作的一部分

SCADA（Supervisory Control and Data Acquisition）系统，即数据采集与监视控制系统，一般用于地理上的远程监视和控制操作。这些监控系统扮演着整个系统的“幕后角色”，对传感器的测量数据和来自现场的运行数据进行采集、处理、及显示，并将控制命令传递到本地或远程设备。尽管SCADA系统在世界各地被各行各业广泛采用，但是很多人对它的重要性仍然并不清晰。不过，随着越来越多的SCADA系统的计算机漏洞相关信息被公开，这种情况将很快发生变化。

SCADA系统作为监控系统来说，为获取机密信息和中断整个系统正常运行提供了极大的可能性，这也是为什么它受到个别政府、竞争对手、恐怖组织、对公司不满的员工以及其他恶意入侵者“垂青”的原因。

SCADA系统控制着工业和能源领域一些最为关键的基础设施，涵盖石油和天然气管道、核设施、污水处理厂等多个领域。所有这些关键基础设施中任何物理IT资产、网络和服务受到干扰或破坏后将对市民的健康、安全、经济乃至一个国家政府的正常运作造成严重影响。[1] 它的影响可能是时间上的浪费、或者是资源上的消耗，甚至是牺牲生命的惨痛代价。事实上，很多SCADA系统都非常脆弱。因此，所有的SCADA系统用户在设计监控系统时都应该优先考虑系统安全和降低风险这两个方面内容。

1 Myriam Dunn，“关键基础设施：漏洞、威胁、响应”，《安全研究中心的安全政策分析》，2007年6月，第16期，第二卷。一般来说，每个国家对关键基础设施都有自己的定义。更多信息，敬请访问http://www.dhs.gov/files/programs/gc_1189168948944.shtm。

控制系统漏洞增加

过去，谈到控制系统的信息安全通常局限于物理攻击。SCADA系统运营商为此找出的辩解理由是，如果控制平台能够充分隔离并且仅限授权人员进入网络的话，那么整个系统就是安全的。在过去由于极少数人掌握着专业技术知识并且数据通讯通道保持隔离，因此控制系统被篡改的风险并不大。

过去的四十多年，SCADA系统一直“躲”在厚重的帷幕后面，信息技术管理员深信通过公司网络或远程访问点无法访问这些系统。然而，现代的SCADA系统已经经过了重大革新。企业用户发现通过将TCP/IP网络连接到他们的SCADA系统可以降低成本，提高访问的便捷性，以及提升效率。因此，将公司网络和因特网集成在一起的这些新一代系统，将面临着诸多的安全挑战。

控制系统漏洞的增加有很多影响因素，包括：

1) 控制系统的联网 - 企业通过将他们的控制系统与企业网络相集成来增加连接性。如果对这两个网络不采取恰当的安全控制，企业安全被破坏的机率大大增加。

2) 不安全的远程连接 - 访问链接，比如用于远程诊断、维护和系统状态检查的拨号调制解调器和无线通讯。如果不使用加密或身份验证机制，所传输信息的完整性将非常容易被攻击。

3) 标准化技术 - 各种组织机构正逐渐转用标准化技术，比如微软的Windows系统，用以降低成本和提升系统的可扩展性与性能。这也导致更多人拥有相关知识和工具来攻击系统，让许多系统在面对攻击时显得不堪一击。

4) 技术信息的可用性 - 潜在的黑客和入侵者很容易就能获得关于基础设施和控制系统的公开信息。关键系统的设计和维护文件以及技术标准在因特网上随处可见，极大地威胁着整个系统的安全性。[2]

我们如此依赖SCADA系统，因此，2001年“911”事件后令政府官员的一项发现不谋而合——恐怖组织通过访问网站获取了数字设备的相关软件和编程指南，这些设备可以用来控制供电、供水、运输和通讯网络。不仅如此，关键基础设施系统的内部控制被证实成为了计算机攻击的目标。比如，在2006年，宾夕法尼亚州哈里斯堡附近的一家滤水厂，其安全系统就受到了黑客攻击。一种能够破坏正常水处理工作的恶意软件从外部被植入到该厂的计算机系统。[3]

2 美国审计总署，“关键基础设施安全控制系统的保护、挑战和成果”，GAO-04-354，2004年3月。

3 Philip Leggiere，“基础设施安全，SCADA系统的安全保障”，HSToday，www.hstoday.us，2008年9月。

2010年6月发现的一种名为‘Stuxnet’的病毒震惊了整个网络安全世界。2010年11月29日，伊朗总统艾哈迈迪-内贾德公开披露，Stuxnet病毒已经使伊朗的提炼浓缩铀计划受阻。该病毒被设计用于破坏核工厂，尤其是将特定公司的配置软件和控制设备作为攻击目标。这种智能蠕虫病毒主要通过USB扩散，也可以通过网络共享和SQL数据库使系统被感染。根据赛门铁克（Symantec）公司的研究报告，该蠕虫病毒搜索的是两家企业生产的特定型号变频器产品。一旦它找到正确配置，就会在数周内逐渐细微修改变频器的速度，最终破坏系统的正常运行，而同时保持各显示读数正常。

Stuxnet病毒自2009年1月起开始感染系统，报告显示世界范围内有超过10万个计算机系统已经被感染。早些时候的攻击数据显示58.85%的感染发生在伊朗，18.22%发生在印度尼西亚，另有8.31%发生在印度。[4] 尽管病毒没有对任何公共设施造成严重破坏，这种高明的恶意软件仍然向我们揭示了SCADA系统在连接性、不安全的远程访问、标准化技术和技术信息易于获取性等方面面临的严峻问题。网络安全是公共设施专家和制造商不能再忽视和回避的一个话题。[5]

4 Jarrad Shearer，“W32.Stuxnet”，赛门铁克（Symantec），www.symantec.com，2010年9月17日。

5 关于控制系统安全计划信息和事故报告相关的更多详情，敬请访问工业控制系统网络应急小组的官方网站(ICS-CERT) www.ics-cert.org。

主动式网络安全是明智的商业决策

确保控制系统的网络安全起初被看作是一项让人望而生畏的任务，因为这需要整个组织机构的共同努力。高层需要认识到并认可一个安全的SCADA系统可以带来诸多好处。这些好处包括，确保系统的正常工作时间、可靠性和可用性。保证网络安全是一项明智的商业决策，因为安全的系统是一个值得信赖的系统，客户的维系和忠诚度都构建在信任的基础上。供应商、系统集成商、IT和控制工程师需要共同承担责任才能完成这一任务。

现在，我们已经有许多资源可以帮助关键基础设施的SCADA系统加强它们的安全性。比如，ISA99标准 - 《工业自动化和控制系统安全》就提供了最佳方案、技术报告和相关信息来定义执行和评估电子安全系统的规范。符合这一标准可以改进生产和控制系统的电子安全，帮助识别和减少漏洞，减少机密信息被泄露和系统性能降级的风险。[6]

政府也已经有相关法律法规并且还在不断完善，以便更好地保证关键基础设施行业的安全。在美国，其中对政府政策最具影响力的是非盈利的‘北美电气可靠性公司（NERC）-关键基础设施保护(CIP)’标准，即‘NERC-CIP’。该标准来源于《电气现代化法案》，是《2005年美国能源政策法案》的一部分。在《2005年美国能源政策法案》中，其中一章显示‘NERC-CIP’标准要求所有电厂和电力设施按照3年实施计划开发新的网络安全系统和程序。CIP标准分为8项，覆盖广泛，涉及了从安全管理控制、关键计算机资产、事故报告到恢复方案的所有内容。每项标准都规定了一系列的具体要求。标准包括：

> CIP-002-1:关键网络资产识别
> CIP-003-1:安全管理控制
> CIP-004-1:人员和培训
> CIP-005-1:电子安全边界
> CIP-006-1:关键网络资产的物理安全
> CIP-007-1:系统安全管理
> CIP-008-1:事故报告与响应计划
> CIP-009-1:关键网络资产的恢复计划

美国政府也在寻求国会支持，对不合规行为采取政府处罚。因此SCADA系统网络安全越来越被重视。[7]

6 自动化国际学会，“ISA99，工业自动化和控制系统安全”
http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821

7 Philip Leggiere，“基础设施安全，SCADA系统的安全保障”，HSToday, www.hstoday.us，2008年9月。

加密和身份验证

为了符合CIP-005-1和CIP-007-1标准，加密和身份验证是一个完善的网络安全解决方案非常重要的组成要素。一般来说，SCADA系统安全包含硬件和传输媒体的物理安全以及部署常见的网络安全防护工具，比如密码保护和防病毒软件等。通讯安全措施的执行难度较大，因为现代黑客可以轻易识别机密电话号码，解密私有协议，以及绕过防火墙和网关。加密和身份验证是减少此类网络安全威胁对SCADA系统通讯造成破坏的有效方法。

今天，市场上有两种针对SCADA通讯的公开标准，其目的是利用加密和身份验证确保安全：

- IEEE6189套件 - 也称作AGA 12，并入IEEE 1711，这些标准都是为了保护SCADA设备通讯的安全。
- IEC62351套件 - DNP3通讯的安全身份验证就是基于这一标准。

加密就是信息加工，使这些信息在普通人看来毫无意义。解密就是将加密的信息恢复到之前可阅读状态的过程。

在一个典型的SCADA系统中，信息通过规定的协议格式被送出，比如MODBUS或DNP3。接收到这些信息的人可以解密它们，看到从一个装置传输到另一个装置的信息。在一个加密的SCADA通讯系统中，信息被转换成类似乱码的字节。短信息中加入了额外的随机信息，很难估计出被传输信息的类型或大小。普通人除了能够知道信息被从一个装置传送到另一个装置外几乎无法获得其它细节。加密让侦听和篡改SCADA网络信息更加困难。

和许多物理或电子安全的形式一样，加密需要使用密钥。这种类型的密钥是一串秘密数据，决定了信息如何在装置间被隐秘（加密）传送。保证这一密钥的安全是SCADA系统安全的基本条件。因此，必须要在这里再次重申采取多种不同的安全措施证明是非常有效的。安全的其它层面，比如物理锁、操作规程，将公司网络和SCADA网络隔离都是保护加密密钥乃至整个系统的必要措施。

身份验证是一部分的SCADA系统向另一部分证明自己身份的过程。SCADA装置收到一条关键信息后，比如执行控制操作或对数据做出响应的命令，可以向发出该信息的装置要求进行身份验证。发送信息的装置必须进行身份验证响应。如果收到信息的装置对响应认可，就会执行收到的原始命令。

与加密一样，身份验证需要相互通讯的SCADA装置之间有一个共识的密钥。加密使用它的密钥将整个信息转换为加密的数据流，而身份验证请求和响应则使用它们自己的密钥来创建特殊的数字签名。身份验证中使用的算法与加密所使用的算法类似，并且采用了原始SCADA协议中的架构以便获得更高的通讯效率。身份验证可以防止恶意入侵者控制SCADA装置，但是不会阻止他们窃取信息并读取信息内容。

施耐德电气助您保证SCADA系统安全

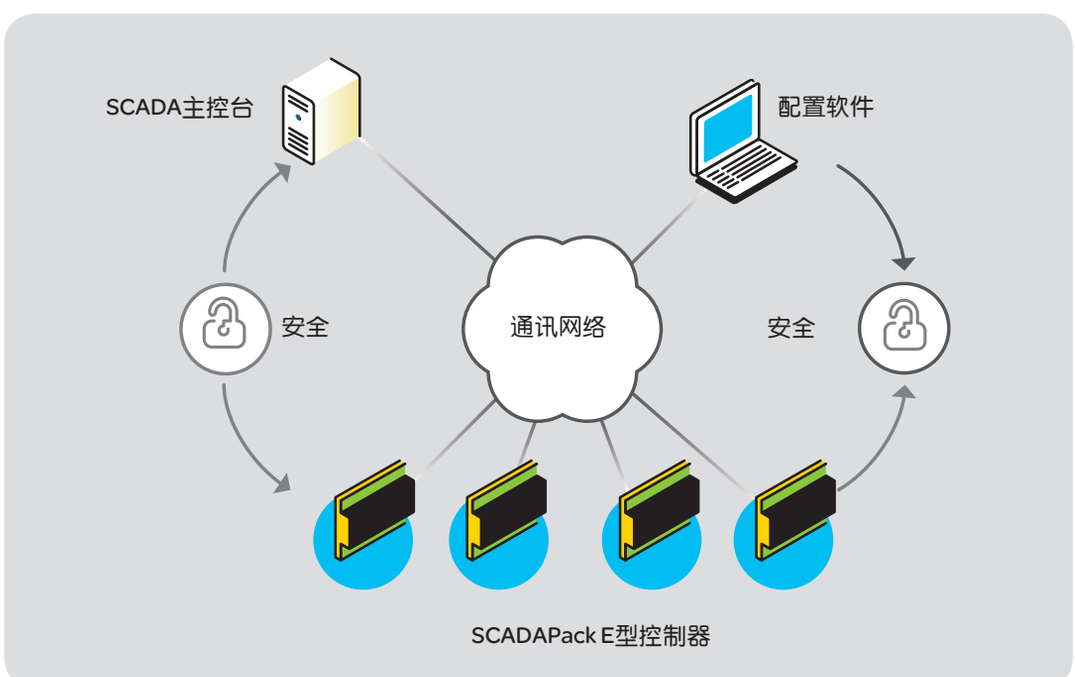
如前文所述，政府正在一些公用事业领域强制要求部署SCADA系统的安全技术，而其它领域则可以自由选择是否部署安全措施。随着控制系统漏洞不断增多，关键基础设施系统被恶意破坏的风险越来越高。SCADA用户应当制定和部署安全方案来满足他们自身的迫切需求。在安全强制命令中，也有多种选择来实现系统安全：身份验证或加密。或两种同时使用。

施耐德电气的SCADAPack E型控制器同时提供IEEE6189信息加密和DNP3安全身份验证两种安全方式。同时，E型控制器现在还能满足最新的DNP3-2009标准。新的用户友好型安全管理软件已经上市，能同时管理DNP3安全身份验证和AGA12加密，可以支持多个分组，因此可以实现系统内多个控制器的安全配置管理操作。

SCADAPack E型控制器管理软件和硬件结合使用能够进一步强化系统安全，它们可以授权配置软件的安装，授权用户以及防止系统被操纵。该项技术弥补了易受攻击的安全缺口——控制器和它们的管理软件间常存在这种缺口。

配置有远程终端的这种可编程逻辑控制器，专门用于净水和污水应用的遥测与远程控制SCADA系统。E型控制器的核心是提升整个系统的可视性和安全性，它还能保持数据无漏洞，即使通讯线路出故障，也能保证终端用户不用担心他们计费应用或关键操作的系统数据的完整性。

在2011年，我们将看到公用事业领域采取更具前瞻性的加密和身份验证技术来保护它们的SCADA基础设施，以符合相关标准，避免因安全漏洞被处罚款或受到名誉损失。



施耐德电气(中国)有限公司

施耐德电气(中国)有限公司	北京市朝阳区望京东路6号施耐德电气大厦	邮编：100102	电话：(010) 84346699	传真：(010) 84501130
上海分公司	上海市普陀区云岭东路89号长风国际大厦 5-14楼	邮编：200062	电话：(021) 60656699	传真：(021) 60656688
张江办事处	上海市浦东新区龙东大道3000号9号楼	邮编：201203	电话：(021) 61598888	
广州分公司	广州市珠江新城临江大道3号发展中心大厦25层	邮编：510623	电话：(020) 85185188	传真：(020) 85185190
武汉分公司	武汉市汉口建设大道568号新世界国贸大厦I座37层01、02、03、05单元	邮编：430022	电话：(027) 68850668	传真：(027) 68850488
天津办事处	天津市河西区围堤道125号天信大厦22层2205-07室	邮编：300074	电话：(022) 28408408	传真：(022) 28408410
天津分公司	天津市河东区十一经路78号万隆太平洋大厦1401-1404室	邮编：300171	电话：(022) 84180888	传真：(022) 84180222
济南办事处	山东省济南市顺河街176号齐鲁银行大厦31层	邮编：250001	电话：(0531) 8167 8100	传真：(0531) 86121628
青岛办事处	青岛崂山区秦岭路18号青岛国展财富中心二号楼四层414室	邮编：266061	电话：(0532) 85793001	传真：(0532) 85793002
石家庄办事处	石家庄市中山东路303号世贸广场酒店办公楼12层1201室	邮编：050011	电话：(0311) 86698713	传真：(0311) 86698723
沈阳办事处	沈阳市沈河区青年大街219号华新国际大厦8层F/G/H/I座	邮编：110016	电话：(024) 23964339	传真：(024) 23964296
哈尔滨办事处	哈尔滨市南岗区红军街15号奥威斯发展大厦21层J座	邮编：150001	电话：(0451) 53009797	传真：(0451) 53009640
长春办事处	长春解放大路 2677号长春光大银行大厦1211-12室	邮编：130061	电话：(0431) 88400302/03	传真：(0431) 88400301
大连办事处	大连沙河口区五一路267号17号楼201-1室	邮编：116023	电话：(0411) 84769100	传真：(0411) 84769511
西安办事处	陕西省西安市高新区科技二路72号西岳阁201室	邮编：710075	电话：(029) 65692599	传真：(029) 65692555
太原办事处	太原市府西街268号力鸿大厦B区1003室	邮编：030002	电话：(0351) 4937186	传真：(0351) 4937029
乌鲁木齐办事处	乌鲁木齐市新华北路165号广汇中天广场21层TUVW号	邮编：830001	电话：(0991) 6766838	传真：(0991) 6766830
南京办事处	南京市中山路268号汇杰广场2001-2005室	邮编：210008	电话：(025) 83198399	传真：(025) 83198321
苏州办事处	苏州市工业园区苏华路2号国际大厦1711-1712室	邮编：215021	电话：(0512) 68622550	传真：(0512) 68622620
无锡办事处	无锡市太湖广场永和路28号无锡工商综合大楼17层	邮编：214021	电话：(0510) 81009780/61/62	传真：(0510) 81009760
南通办事处	江苏省南通市工农路111号华辰大厦A座1103室	邮编：226000	电话：(0513) 85228138	传真：(0513) 85228134
常州办事处	常州市局前街2号常州椿庭楼宾馆1216室	邮编：213000	电话：(0519) 88130710	传真：(0519) 88130711
合肥办事处	合肥市长江东路1104号古井假日酒店913房间	邮编：230011	电话：(0551) 4291993	传真：(0551) 2206956
杭州办事处	杭州市滨江区江南大道588号恒鑫大厦10楼	邮编：310053	电话：(0571) 89825800	传真：(0571) 89825801
南昌办事处	江西省南昌市红谷滩赣江北大道1号中航广场1001-1002室	邮编：330008	电话：(0791) 2075750	传真：(0791) 2075751
福州办事处	福州市仓山区建新镇闽江大道169号水乡温泉住宅区二期29号楼101单元	邮编：350000	电话：(0591) 87114853	传真：(0591) 87112046
洛阳办事处	洛阳市涧西区凯旋西路88号华阳广场国际大饭店609室	邮编：471003	电话：(0379) 65588678	传真：(0379) 65588679
厦门办事处	厦门市思明区厦禾路189号银行中心2502-03 B室	邮编：361003	电话：(0592) 2386700	传真：(0592) 2386701
宁波办事处	宁波市江东北路1号宁波中信国际大酒店833室	邮编：315040	电话：(0574) 87706806	传真：(0574) 87717043
温州办事处	温州市车站大道高联大厦写字楼9层B2号	邮编：325000	电话：(0577) 86072225	传真：(0577) 86072228
成都办事处	成都市科华北路62号力宝大厦22楼1、2、3、5单元	邮编：610041	电话：(028) 66853777	传真：(028) 66853778
重庆办事处	重庆市渝中区邹容路68号重庆大都会商厦12楼1211-12室	邮编：400010	电话：(023) 63839700	传真：(023) 63839707
佛山办事处	佛山市祖庙路33号百花广场26层2622-2623室	邮编：528000	电话：(0757) 83990312/0029/1312	传真：(0757) 83992619
昆明办事处	昆明市三市街6号柏联广场A座10楼07-08单元	邮编：650021	电话：(0871) 3647550	传真：(0871) 3647552
长沙办事处	长沙市劳动西路215号湖南佳程酒店14层01, 10, 11室	邮编：410011	电话：(0731) 85112588	传真：(0731) 85159730
郑州办事处	郑州市金水路115号中州皇冠假日酒店C座西翼2层	邮编：450003	电话：(0371) 6593 9211	传真：(0371) 6593 9213
泰州办事处	江苏省泰州市青年南路39号会宾楼永泰酒店8512房间	邮编：225300	电话：(0523) 86397849	传真：(0523) 86397847
中山办事处	中山市东区兴政路1号中环广场3座1103室	邮编：528403	电话：(0760) 88235979	传真：(0760) 88235979
鞍山办事处	鞍山市铁东区南胜利路21号万科写字楼2009室	邮编：114001	电话：(0412) 5575511/5522	传真：(0412) 5573311
烟台办事处	烟台市南大街9号金都大厦2516室	邮编：264001	电话：(0535) 3393899	传真：(0535) 3393998
扬中办事处	扬中市前进北路52号扬中宾馆2018号房间	邮编：212000	电话：(0511) 88398528	传真：(0511) 88398538
南宁办事处	南宁市青秀区民族大道111号广西发展大厦10层	邮编：530000	电话：(0771) 5519761/9762	传真：(0771) 5519760
东莞办事处	东莞市南城区体育路2号鸿禧中心A406单元	邮编：523009	电话：(0769) 22413010	传真：(0769) 22413160
深圳办事处	深圳市罗湖区深南东路5047号深圳发展银行大厦17层H-I室	邮编：518001	电话：(0755) 25841022	传真：(0755) 82080250
贵阳办事处	贵阳市中华南路49号贵航大厦1204室	邮编：550002	电话：(0851) 5887006	传真：(0851) 5887009
海口办事处	海南省海口市文华路18号海南文华大酒店第六层 607室	邮编：570105	电话：(0898) 68597287	传真：(0898) 68597295
施耐德(香港)有限公司	香港鲗鱼涌英皇道979号太古坊和域大厦13楼东翼		电话：(00852) 25650621	传真：(00852) 28111029
施耐德电气大学中国学习与发展学院	北京市朝阳区望京东路6号施耐德电气大厦	邮编：100102	电话：(010) 84346699	传真：(010) 84501130

客户关爱中心热线：**400 810 1315**

施耐德电气中国
Schneider Electric China
www.schneider-electric.cn

北京市朝阳区望京东路6号
施耐德电气大厦
邮编: 100102
电话: (010) 8434 6699
传真: (010) 8450 1130

Schneider Electric Building, No. 6,
East WangJing Rd., Chaoyang District
Beijing 100102 P.R.C.
Tel: (010) 8434 6699
Fax: (010) 8450 1130

本手册采用生态纸印刷

2012.11