多项新技术在智能电网安全性与电网基础设施中的应用

A number of new technology in the smart grid security and the application of the power grid infrastructure

吴康

摘　要：为应对潜在的威胁与攻击，本文将对高级别安全控制和命令及云计算等新技术运用于智能电网嵌入式设备的课题作研讨，并为确保在整个生命周期的智能电网与智能电表的安全性对电力监控系统的与新型电网基础设施的应用作分析说明。

关键词：智能电网，攻击与安全，漏洞与保护，电力监控系统，电网基础设施

Abstract: this paper will be of high level security control and command and new technologies such as cloud computing are used in the smart grid embedded devices for discussion of the topic, and to ensure that in the whole life cycle of the security of smart grid and smart meters on electric power monitoring and control system and analysis of the application of new type of grid infrastructure.

Keywords: smart grid, Attacks and security, Vulnerability and protection, power monitoring system, Grid infrastructure

中图分类号：TN86　　文献标识码：A　　文章编号：1606-7517(2015)04-5-132

全球电力基础设施通常称为“电网”，是一套用于能源生成、传输、转换和分配的互连资产。为提高电网系统的运行效率，当今国内外都致力于智能电网和智能电表的开发与投资，即广泛的部署智能电网基础设施和自动抄表系统(AMR)、自动计量系统(AMI)。然而在这同时，也伴随了输电基础设施的安全性问题，这是何因呐？其一是因为智能电力电网在安全上易受攻击如数据黑客、系统恶意软件等也在逐渐增加。而自动计量设备中易受攻击的地方包括非安全数据总线、串行连接或远程调试端口访问等；其二是电网设计在安全方面相对比较薄弱或忽视，造成传统安全低迷已久和相关厂商缺乏创新实力。

应该说，对智能电网来说，由于电网基础设施容易受到攻击的几率越来越高，则使一个国家稳定的电力供应都处在危险之中，从而使得安全问题的重要性日益增加。也就是说，沒有智能电网的安全就沒有国家电力网的安全，也就沒有国家的安全。由此引发信息化驱动转向网络安全驱动的战略改变。由此其中的智能电网及智能电表的安全问题已成为突出的困扰，即如何在有效使用期限内确保智能能源网关与智能电表等设备中的数据安全与可靠性成为新的挑战，也是厂商与客户迫切需要解决的热点问题。

为应对潜在的威胁与攻击，本文将对高级别安全控制和命令及云计算等新技术运用于智能电网嵌入式设备的课题作研讨，并为确保在整个生命周期的智能电网与智能电表的安全性对电力监控系统的与新型电网基础实施的应用作分析说明。为此先述智能电网与智能电表的攻击类型。

1　智能电网与智能电表的攻击类型与安全架构的构建

1.1 攻击类型

当今智能电网面临的安全隐患有很多种，对智能电网与智能电表的攻击类型大体可分为物理攻击（外部干扰、绕过中线、中线缺失等）、电气攻击（过／欠压、电路探测、ESD 等）与软件和数据攻击（间谍软件插入、网络攻击）。攻击者的目标有二，其一是智能电网数据，以获得自身利益——例如：窃取电费，或隐瞒违禁药物的生产等；其二是对社会构成威胁的活动，包括试图破坏电网运行的活动。这可能是对电网本身的攻击（大区域误报能耗，造成整个电网的资金链紧张）；也可能是对社会的攻击（例如：恐怖

分子袭击），造成电网瘫痪，用户断电。发生断电时，生产和金融损失将无可估量，特别是在极热、极冷气候下，还会对人类的生命安全构成威胁。

根据攻击者希望得到的最终结果，在篡改或攻击具体方式上，黑客采用通过破坏设备就能够实现目标中断设备的运行，并不需要盗取重要安全参数 (CSP) 的简单方式就可达到目的。如今对智能电网的最新调查结果显示，中断设备运行与盗取密钥所带来的破坏后果会更严重或者更糟糕（见图 1 所）。

图 1 中断设备运行与盗取密钥所带来的智能电网遭破坏的示意图

1.2 安全架构的构建与保护措施

1.2.1 高级别安全性的控制和命令的应用

每个系统都有“重要安全参数 (CSP)”的机密，必须保持其完整性，从而才能确保系统完好无缺。在智能电网与智能电表中，这 CSP 是一个密钥，必须在编程到内存时就得到保护。而加密工具对于隐私保护和传输数据、命令的认证非常有效。对此可应用高级别安全性的控制和命令来实现，那用什么高级别安全性的控制和命令呐?

首先应明确当今有哪些加密技术呐？ DEC 密码 / 算法、对称数据块密码，3DES 密码 / 算法、对称数据块密码，AES 密码 / 算法、对称数据块密码、密钥长度为 128–256 位，RSA 密码 / 算法、非对称数据流密码，SHA–1 / SHA–2 密码 / 算法、散列密码等等。

从上所知，AES 对称密钥密码系统适用于批量数据，但安全级别不高。非对称密钥密码系统如椭圆曲线数字签名算法 (ECDSA)，适用于加密远程断开 / 连接实时电价更改等控制 / 命令。这就确保了控制电网设备的命令是高度真实性。而基于椭圆曲线加密技术 (ECC) 的密钥交换可提供高级别的安全性，则 Zigbee@ 等无线网络可采用 ECC 提供数字证书，以交换智能电网生态系统内 ZigBee 节点 / 设备之间的信息。几乎所有安全协议要求一项或多项加密技术来加密数据。而 128 位 AES 密码广泛应用于智能电表应用并用于单个电表与电表数据采集设备之间的通信。由于数据已被加密，因此可以防止被窃取。

1.2.2 安全架构的构建

根据上述高级别安全性的控制和命令可设计出如图 2 所示的智能电网与智能电表的的安全架构。

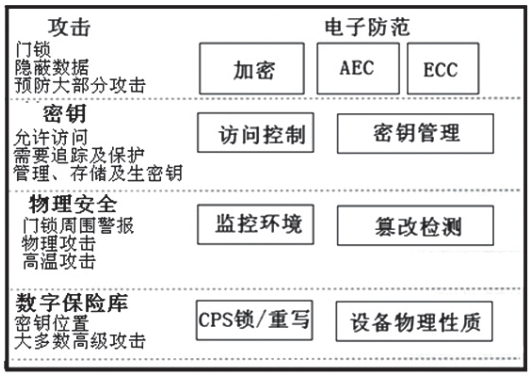

图 2 智能电网与智能电表的的安全架构

图 2 这样的安全系统考虑了电子系统面临的所有攻击途径。首先是数据本身。数据就像保险库里的钱。保护数据的第一步就是要搭建“保险库大门”，采用加密技术来隐藏数据。这样可以保护数据免受 99% 潜在攻击者的攻击。攻击者的第二种途径是试图获取保险库的密码组合（或加密方案的密钥）。

1.2.3 智能电网与智能电表的的保护措施

由智能电网与智能电表的的安全架构可拓展出具体保护措施：其一是，着重于密钥保护，以采用芯片级硬件和防攻击多重保护措施，对新的配置、固件更新和指令进行加密和签名，以验证数据来源的可靠性；其二是，可靠通信，通信双方可通过密钥对通信线路上的数据进行加密、解密、签名或验证，这是由于从嵌入式传感器到控制系统的数据加密非常关键，用于加密的密钥保护也更加重要，一旦密钥被窃取，整个网络也就不再安全；其三是，使用新的存储技术扩大可靠性和安全性。对于图 1 中因中断设备运行与盗取密钥所带来的设备严重破破坏，则 Sentry 安全模块是最佳选择，因为存储 CSP 的理想存储器是在器件之中，这存储器可与模块内（或电表内）可用于篡改检测所必需的传感器直接相连。它的优点并不仅限于低功率监控，而且是通过采用最新的非易失性 RAM(NVRAM) 存储器技术，

这类模块从几个新的方向扩展了数据保持和分析能力。为使电网变得更为智能和可靠，必须不断地监控和分析大量运行数据；其四是，对于电网或智能电表，必须用互联网协议安全性(IPSec)、传输层安全(TLS)及安全外壳(SSH)等协议取代非安全协议。这是因为电网中的各方使用的数据交换协议有多种，包括了全球信息技术领域广泛使用传输控制协议(TCP)/互联网协议(lP)、超文本传输协议(HTTP)和文件传输协议(FTP)等，但由于传输的数据很容易被黑客窃取，所以这些数据不十分安全且容易遭受攻击。

2 应对漏洞与安全威胁的挑战与新一代威胁感知系统应用

2.1 漏洞与安全威胁依然存在

值得提醒的是上述智能电网与智能电表的的安全架构及保护措施中还可能有漏洞与威胁的存在。其原因：一是，因加密的作用在于防止被保护数据在传输或存储过程中被解密或伪造，但往往有误区，即认为依赖调频方式则复杂的RF或电力载波通信可完全保证数据的安全性。其实不然，此类保护往往很容易被漏洞与威胁所攻破。况且由于电网已经互联，多数已知的漏洞都与通讯媒介和通讯协议有关。二是，在有足够资源和时间的前提下，一些人可以编写出一个类似功能的程序，在程序中植入获取密钥数据或篡改账单的病毒。即使挂网的电表都具备一定的保护措施，仍然能够发现一些容易遭受攻击的环节（如生产环节），为攻击者侵入IP和生产流程提供了机会，造成巨大损失。

2.2 基于云计算的新一代威胁感知系统应用是最佳对策

针对漏洞与安全威胁的挑战，应有以下二种对策。对于上述第一种漏洞与安全威胁原因的对策，那就是从IT安全性入手。对此可应用支持端到端的通信数据加密方案，如：数据集中器、监控器和数据采集器系统(SCADA)等。因为需要确保“空中”传输数据的安全性；对于上述第二种漏洞与安全威胁原因的对策是，则应用基于云计算的新一代威胁感知系统。新一代威胁感知系统是面向下一代未知威胁的垂直类精确检测产品，通过动态行为检测、静态模式匹配、半动态行为分析、大数据分析等多项技术实现对APT攻击与0day漏洞可利用攻击的精确检测与全过程回溯。

其新一代威胁感知系统功能可对威胁作检测。即，它可对未知威胁与已知威胁进行检测。所谓未知威胁，包括0daY漏洞对传统安全产品（如IDS、IPS、UTM）无能为力的未知漏洞、攻击具有出色的精确检测效果并也对传统终端杀毒软件、防毒墙无能为力的未知木马、未知病毒、未知恶意代码、特种木马具有出色的精确检测效果。而所谓已知威胁，指已知漏洞（已知系统漏洞、应用漏洞进行攻击的行为）与已知恶意代码（已知木马、蠕虫、病毒等恶意代码）的访问行为具有全面、快速的检测能力。

同时，新一代威胁感知系统亦可通过与终端安全管理系统或移动终端安全管理系统联动，对APT的攻击可从发现到阻断分级并构建出纵深防御体系。那末什么是智能电网终端安全管理系统呐？终端安全管理系统是面向智能电网、金融、制造业等大型企事业单位推出的以安全防御为核心、以运维管控为重点、以可视化管理为支撑、以可靠服务为保障的全方位终端安全解决方案。为用户构建能够有效抵御已知病毒、0daY漏洞、未知恶意代码和APT攻击的新一代终端安全防御体系。其架构为见图3所示。

从图3万可看出智能电网终端安全管理系统可终端安全防御，及时发现定位出未知威胁并全面查杀已知或未知

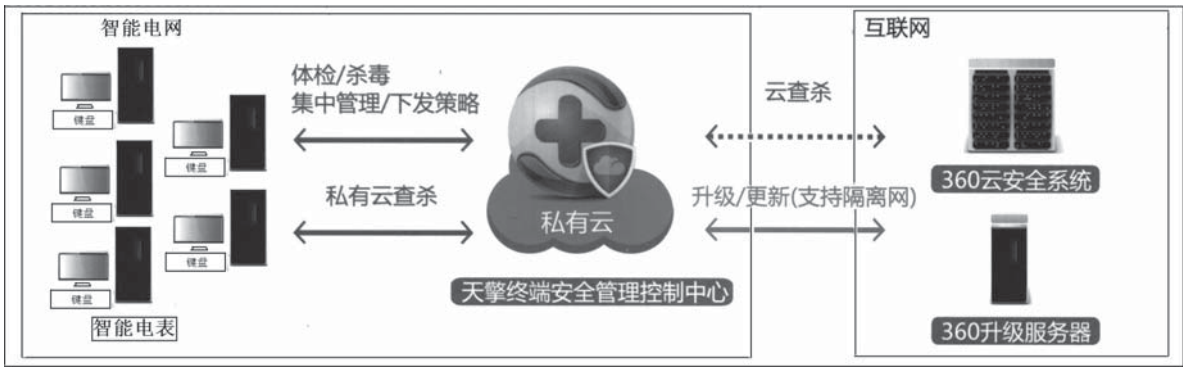

图3 智能电网终端安全管理系统架构图

病毒恶意代码，以彻底解决病毒木马威胁，作全网漏洞修复；网络安全管理，包括终端软件准入控制，保证软件合规安装运行，软件使用安全，可对无线热点、手机、光驱、打印机、USB 等相关设备作准入控制，消除智能电表接入安全无隐患。

3 如何保证智能电网设备生命周期的安全性

随着对能源的需求的不断加快，政府与电力生产商、经销商及设备供应正合作改变传统电网基础设施，以增加智能、通信和分散控制等数字化和信息化技术确保实现智能电网设备生命周期的安全性。应该说，电力线通信技术提升了大量智能电网应用（包括智能电量计、照明、太阳能、电动汽车充电、智能设备、家庭自动化、智能楼宇控制和网络）的智能性和可靠性。而电力监控系统与保护继电器、断路器等电网基础设施的应用是保证智能电网设备生命周期的安全性的重要举措。值此将从应用角度对其架构与应用特征作分析说明。

3.1 电力监控系统的应用

电力监控系统是电力系统数字化和信息化的产物，是智能电网的基本组成部分，建设安全可靠的电力监控系统对智能电网的发展有重要的作用。电力监控系统主要用于电力系统、工矿企业、科研设施、医院、智能建筑等诸多领域的供配电系统中，以实现对电压、电流、功率、功率因数、频率和电能等电力参数的实时监测和显示，并能根据监测结果对相关设备进行控制，提高供配电系统的可靠性和安全性。智能测控仪表是电力监控系统的前端元件，其主要作用是高精度的测量所有常用电力参数，并具有数据通信和远程控制功能，以实现与电力监控系统之间的信息交换。

3.1.1 电力监控系统的基本架构

电力监控系统是以现代电子技术、计算机技术、网络通信技术和测控技术为基础，通过对供配电系统中的高压开关柜、低压开关柜、电力变压器、测控仪表等设备的工作状态进行监控，实现供配电系统的集中监控管理和分散数据采集。监控系统主要由现场监控层、网络通信层和系统管理层构成，其系统结构如图 4 所示。

从图 4 可知电力监控系统的结构由现场监控层、网络通信层及系统管理层构成。其现场监控层是电力监控系统中的最底层，位于变配电系统现场，主要包括各种测控仪表、智能断路器、微机保护装置、温湿度控制器和现场监控装置等。现场监控层的主要作用是采集变配电系统现场的电压、电流、功率、功率因数、开关状态等信息，并将采集到的信息通过网络通信层传递给系统管理层。同时，现场监控层也可以作为执行单元，通过网络通信层接收系统管理层发出的各类指令。现场监控层中的设备或装置应相对独立，可以不依赖于监控网络而独立运行；网络通信层是电力监控系统中的中间层，负责与现场监控层中的设备或装置进行数据通信，收集各类设备或装置的数据或状态信息，进行处理后集中打包传送给系统管理层，同时负责接收系统管理层发送的各类指令，并转发给现场监控层。网络通信层通常由现场总线通信网络和以太网通信网络构成；系统管理层是电力监控系统中的最高层，位于监控室内，主要由电力监控管理计算机及其外围设备、网络设备等构成。系统管理层负责对整个变配电系统进行监控，其主要作用是解析网络通信层上传的数据包，对数据进行管理和分析，并根据系统运行的状态，向现场监控层中的设备或装置发送指令，执行相关操作。

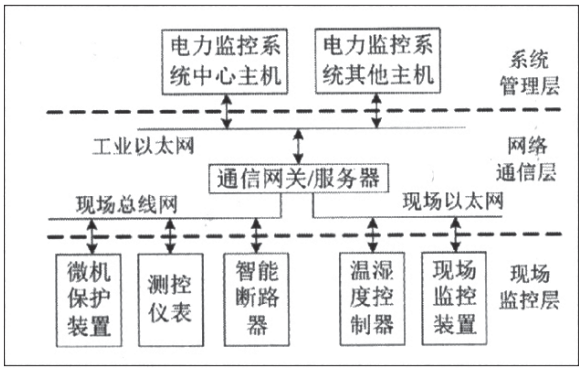

图 4 电力监控系统的结构示意图

3.1.2 基于微处理器的智能测控仪表构建方案

智能测控仪表位于电力监控系统中的现场监控层，用于完成电力参数的数据采集与传输，并执行由监控主机下发的操作指令。其智能测控仪表的基本结构由输入模块、数据处理模块和输出模块三部分构成，其结构框图如图 5 所示。

输入模块主要包括互感器接口电路，开关量输入接口电路，主要用于采集交流电压信号、交流电流信号、频率信号以及负荷开关位置、低压断路器位置、熔断器熔断状态等状态信号。数据处理模块主要由微处理器、测量芯片、

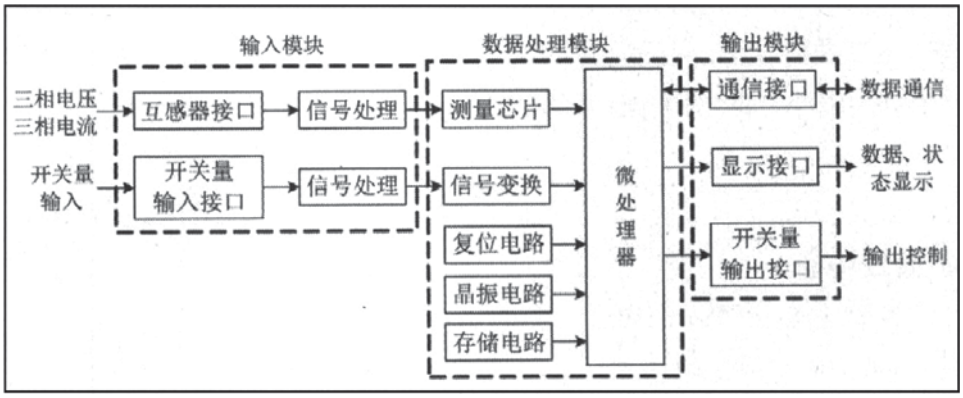

图 5 智能测控仪表的的构建方案框图

数据存储器、晶振电路和复位电路等构成，主要起输入信号采集，电气量计算、逻辑控制、故障信息处理等作用。输出模块主要由通信接口、开关量输出接口和显示接口等构成，主要起数据通信、输出控制、数据和状态显示等作用。

3.1.3 应用

经测试该智能测控仪表的电压、电流、频率和功率因数的测量误差可达 0.2%，有功功率和无功功率的的测量误差可为 0.5%，可比较好地满足了电力监控系统对测量的要求。

3.2 新型保护继电器在电网基础设施中的应用

保护继电器在从发电到输配电等电网基础设施的各个环节上很常见。它们能够让运营商在不同的点监视和控制电网。保护继电器的两大主要功能是测量和保护。在现代保护继电器中，通信也是解决方案的必要组成部分，能够让运营商远程监视和运行电网基础设施。

保护继电器通常可实现局部智能，即让断路器自行打开或关闭。保护继电器的基本目标是在出现故障的情况下保护电网（下流线路）。保护继电器通过监视特定电网线路的电流和电压来实现上述目的。断路器位于线路上。保护继电器的输入通常是来自线路传感器的电流和电压，以及来自电网网络中其他相关设备的任何通信。输出包括向断路器发送的信号（打开或关闭）以及与电网网络的通信。当保护继电器检测到故障时，它会命令断路器将经检测发生故障的线路置为开路，从而为保护继电器下游线路的一切提供保护。

保护继电器以多种方式监视电流和电压。无论是电压还是电流，都可对其同时设定不同的阈值。例如，可将一个阈值设为高限值，另一个设为低限值（超出该值的时间需要达到一固定时长）。因此无论在哪种情况下，一旦触发了所设阈值，保护继电器就会启动断路器。这些不同的阈值由处理器监控。处理器可能还会处理谐波分析和其他此类与电源相关的计算，从而更好地了解电力线状态。如 TI 的 MSP430 和 AM335x 系列处理器是处理各种此类应用的适当处理器的典范。通常当高压线路与电子产品连接时，数字隔离器或模拟隔离器会用于隔离数据路径。如今的保护继电器不仅会通过 RS485/232 处理传统通信，还会处理基于以太网的通信。

4 拓展智能电网的安全性新趋势

确保智能电网的安全性除上述电网基础设施外，现已开发出低频窄带 PLC 技术闻世，它可确保数据完整性同时降低功耗和系统成本，适合各种应用（如智能计量和控制应用）。其低频窄带 PLC 技术发展蓝图提供了适用于从公用变电站到整个家庭局域网络等智能电网各个阶段的解决方案。而针对实现 PLC 和射频连接的系统的数据集中器应用方案是一典例。在此作一简介说明。

其数据集中器应用自动计量系统 (AMI) 中的重要节点，其中 AMI 与若干公用事业仪表和中央公用事业服务器相连，可实现仪表与公用事业服务器之间的数据通信。 基础设施中若干点上的数据集中器会从可控数量的仪表中安全地聚合数据，并发送至公用事业服务器。而通信模式很大程度上取决于电力基础设施，而且可以是有线或无线通信。有线通信包括电力线通信 (PLC)，无线通信主要包括低功耗射频（IEEE 802.15.4g 协议）通信，在某些情况下还包括现有的移动电话媒介。集中器向公用事业服务器的通信可通过以太网、GSM、GPRS、WiMAX 或电信网络实现。