智能电网关键信息安全技术应用研究

智能化已然成为世界电力发展的新趋势。针对智能电网的发展现状和智能电网所面临的威胁，文章研究了目前电力系统中不同关键信息安全技术及其主要机制，并针对不同的安全威胁采取相应的技术手段，确保智能电网的信息安全体系的可控。

引言

随着信息技术的不断发展，全球电力行业发生了巨大的变革，由传统的电力系统朝智能电网发展。智能电网的生产、输送、分配和使用各个环节通过数字化和信息化将电能紧密结合在一起，新一代电力系统通过智能化的控制实现“经济高效、灵活互动、友好开放、清洁环保”。

当前，我国将智能电网作为国家战略发展重要组成部分。信息化、自动化的推进，在为社会带来巨大进步的同时，也使得智能电网所面临的安全威胁与日俱增，现有智能电网的信息安全不容乐观。2000年8月14日，“蠕虫”病毒入侵加拿大安略省的供电系统，病毒通过阻碍恢复正常供电的进程运行，导致了停电事故的发生；2010年7月，伊朗布什尔核电站“震网病毒（Stuxnet）”事件曝光。2011年7月23日，甬温线发生特别重大交通事故。这一切安全事故的发生主要源于对智能电网的信息安全不够重视，没有从本质上认识到智能电网存在的安全威胁。智能电网的开放性和包容性决定了不可避免地存在信息安全隐患，智能电网的安全甚至会关系到一个国家的战略安全。如何应对新形势下智能电网的安全威胁；如何寻求更加先进的安全技术来保护智能电网的安全，已经逐渐成为现今需要考虑的重要问题。面对这些接踵而至的问题，我们需要切实加强智能电网信息安全预防与管理，以最终保障国家经济、人民生命财产和工业生产运行安全。

智能电网安全性分析

智能电网的网络布局

智能电网控制系统主要由发电站自动化系统、变电站自动化系统、配电站自动化系统和数据调度网络构成。如图1所示。

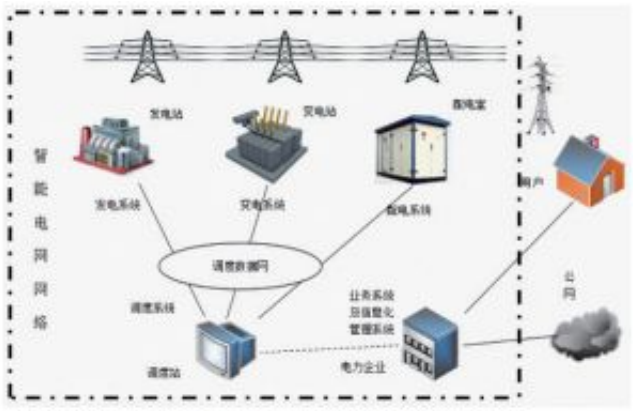

图 1 智能电网网络构成

智能电网网络模块划分为生产控制大区块和信息管理大区块。其中生产控制大区包含发电站自动化系统、变电站自动化系统、配电自动化系统和数据调度网。信息管理大区包含电力企业内部各部门多业务系统。具体的网络结构如图2所示。

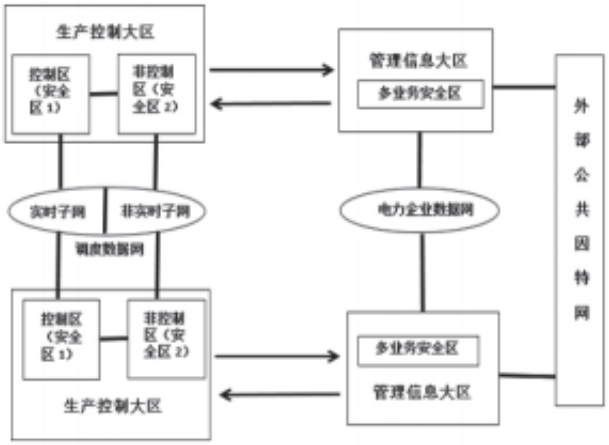

图 2 智能电网网络结构

生产控制大区

发电自动化系统：包含RTU，智能仪表，开关以及用于监控和数据采集的SCADA系统。其主要工作包含运行监视、设备状态监视、远动通信以及厂内AGC等。

变电站自动化系统：其核心是变电站监控系统是由智能化一次设备（电子式互感器、智能化开关等）和网络化二次设备分层（包括过程层、间隔层和站控层）构成。其主要作用是利用智能电气化电气测量系统从电流、电压采集源头实现数字化，从而实现信息集成、网络通信和数据共享。

配电自动化系统：包括馈线自动化和配电管理系统。通过利用配电网数据采集与监视（SCADA）系统、配电地理信息系统（GIS）和需求侧管理(DSM）等技术手段实现配电企业远程以实时方式监视、协调和操作配电设备。

数据调度网：用于传输电网自动化信息、调度指挥指令、继电保护与安全自动装置控制信息的网络，一般采用专网。

信息管理大区

信息管理系统用于对电力企业内部各业务系统，以及电厂、变电站和调度站等处信息系统进行综合管理。

智能电网的特点

与传统电力系统相比，智能电网具有如下特点：

高实时性和连续性

电能的生产，传输，消耗必须同步进行，转化过程非常迅速，作为智能电网的指挥控制系统，必须保证高实时性，保证控制命令实时到达目标设备。同时电能的生产必须具备连续性，否则会造成供电中断。

生产控制区主机应用软件相对单一

为保障数据传输实时性，在生产网络中的主机上禁止安装不必要的应用软件，以减少其他软件对网络带宽的占有，同时还能减少应用软件给网络系统带来的安全威胁。

高度集中性管理、规模庞大、构成复杂

电力生产是高度集中、统一管理，无论多少个发电厂，变电站，供电公司，都要遵从统一的调度。

设备多样性

智能电网是一个复杂而庞大的网络，包含各种各样的光、电磁、温湿度传感器、机械装置、电子电气装置、控制设

备、监控设备和应急设备，而这些设备之间关联极大。

无线网络接入缺乏认证和控制

智能电网中缺少有效的认证和控制机制，控制设备接入无线网络中，会将整个系统暴露在网络中，带来极大的安全隐患。

智能电网威胁分析

安全补丁和杀毒软件缺乏

鉴于业务的特殊性，很难为工业控制信息系统打安全补丁，补丁可能导致正常业务不能进行。同时这些正常业务很容易被杀毒软件识别为病毒程序，工业控制信息系统往往呈现既没有补丁，又没有杀毒软件的裸机状态。

设备生产商可能留有的访问后门

NSS实验室发现德国西门子公司的某些工业控制系统中存在“后门”，据西门子公司解释这些后门是为了便于系统维护和调试，后门通常拥有很大的访问权限，这些后门一旦被利用将对工控系统造成极大地威胁。

电磁屏蔽和间谍程序识别技术缺乏

通过调查，目前我国正在使用的工业控制信息系统大部分核心设备均采用外国品牌，如霍思曼、西门子、施耐德等品牌，这些外国品牌设备当中很可能存在间谍程序，这些程序窃取核心数据通过无线网络发送。而工业控制信息系统缺乏电磁屏蔽，不能阻断间谍程序发送数据，同时也未采用相关设备对间谍程序进行扫描和识别。

工控信息系统硬件和软件的安全缺陷

设备提供商提供的应用授权版本无法做到十全十美，各种后门、漏洞等问题都有可能出现。出于成本的考虑，工业控制系统的组态软件一般与其工控系统是同一家公司的产品，在测试节点问题容易隐藏，且组态软件的不成熟也会为系统带来威胁。

智能电网关键信息安全技术

针对智能电网所面临的威胁，对于不同区域应采用不同的防护手段和防护技术对智能电网进行保护。防护框架如图3所示。

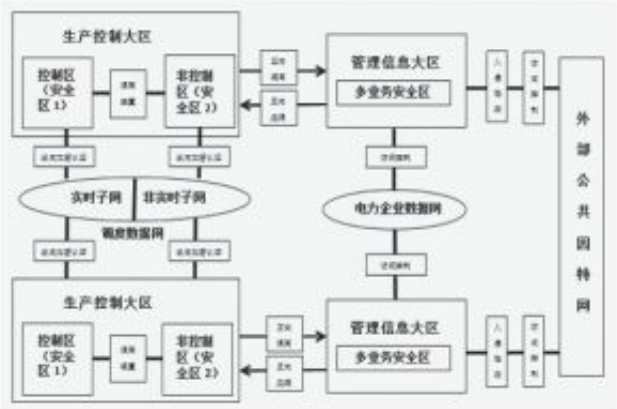

图3 智能电网安全防护模型

本文介绍了常用的七种技术手段，确保智能电网的信息安全体系的可控、能控、在控。针对不同的区域、不同的环境应采取不同的安全技术。

访问控制技术

访问控制是指对主体访问客体的权限或能力的限制，以及限制进入物理区域（出入控制）和限制使用计算机系统和计算机存储数据的过程（存取控制）。其基本目标是防止非法用户进入系统和对系统资源的非法使用。根据访问控制策略的不同，访问控制机制可分为三种访问控制模型：

自主访问控制（DAC）

自主访问控制用户可以按照自己的意愿对系统进行修改和操作，来决定哪些用户可以访问他们的资源，也被称为随意访问控制。

自主访问控制的优点是表述直观，易于理解，但存在着明显的不足之处，首先，在访问控制需要消耗大量的时间，效率底下。其次，自主访问控制对资源管理比较分散，易产生安全漏洞，不适用于安全级别较高的系统中。另外，自主访问控制不能对系统中的信息流进行保护，信息容易泄露。

强制访问控制（MAC）

强制访问控制是指系统强制主体服从访问控制政策，通过无法逃避的访问限制来防止各种直接或间接的攻击。

强制访问控制对于信息系统的保密性极强，但是因其极强的安全性要求，主要应用于军事系统中，对其他系统来说，强制访问过于严格，使得用户难以管理系统数据。

基于属性的访问控制（ABAC）

基于属性的访问控制主要是基于任何与访问安全相关的实体属性进行授权决策。

基于属性的访问控制优点是能够增强访问控制系统的灵活性和可扩展性，具有强大的表达能力。基于属性的访问控制在多个领域、多个部门不同安全之间的数据访问管理中应用十分广泛。与传统的访问控制技术（包括MAC、DAC）相比具有一定的优势，如表1所示。

表 1 DAC、MAC 与 ABAC 三者的比较

属性	DAC	MAC	ABAC
安全性	弱	强	强
实现难易度	易	易	难
授权管理	复杂	复杂	容易
应用领域	广泛应用于商用系统	较窄，主要为军用	广泛

智能电网是一个结构庞大且构成复杂的信息系统，根据不同工作内容划分多个安全区域，针对不同安全级别敏感区域应采取合理、有效的访问控制。基于属性的访问控制技术，应用场景通常为按照管理者安全策略能够根据不同访问主体（用户、应用程序或进程）分配允许访问的资源，并为其设置访问权限和权限的有效期。基于属性的访问控制技术能够有效地控制外部对智能电网内部敏感信息的窃取；能够减少非法用户和程序对智能电网信息系统的破坏。

身份认证技术

身份认证是一种利用物理技术、密码技术等手段判别消息发送方或资源使用方身份的真实性的验证技术。在信息传递过程中利用身份认证可以确保访问系统资源或利用系统处理设备的用户是合法的、通过对已授权的用户进行身份认证可以实现访问控制的有效实施，避免非授权用户或者黑客伪造身份非法获取资源或者恶意篡改数据。

目前，认证的实现主要有物理特征、密码技术和物理特征与密码技术结合使用三种形式。

其中物理特征的认证典型方式有实物认证（例如个人身份证、驾照、工作证等）和特征认证（例如个人指纹信息、面部信息和瞳孔信息等）；密码技术包括利用传统的用户名密码，数字证书等；物理特征与密码技术结合使用认证较为典型是移动终端认证。

在智能电网中身份认证技术被广泛用于各安全区，例如在配电系统中，在配电网主站、子站、终端之间的通信会利用身份认证以确信主站、子站发送的配电指令是有效的；在电厂发电自动化系统中上位机与下位机之间的通信也需要

进行身份鉴别。

防火墙技术

防火墙是一种对网络间信息传递和数据访问进行访问控制的安全设备，可以对网络之间传送的数据包和连接方式根据一定的安全策略进行检查，审查网络之间的通信是否被允许。防火墙能够有效地实现数据访问和数据传输，从而达到保护私有网络的信息不受外部非法用户的访问以及过滤不良信息的目的。

防护墙按照系统管理员事先配置好的安全策略，过滤内部与外部间的所有数据，仅允许符合安全策略的数据流通过。其主要功能有包过滤、充当代理服务器、状态包检测以及网络地址转换。随着技术的发展，目前一部分防火墙还具有反病毒功能。

防火墙在智能电网中的应用有：

（1）区域划分：电力企业网络系统一般被分为不同的区域，至少应包含内部、外部和DMZ三个分区。内部区域是指企业内部区域（包括管理区和生产区）视为信任区。外部区域通常是指公网（Inter网）由于存在各种未知的威胁是不被信任的区域，需要防火墙加以监控。DMZ区即非军事化区是电力企业对外提供服务的区域，防火墙将DMZ区和内网相隔离，保障内部网络安全，同时对外能正常服务。

（2）访问控制策略制定：依据区域的重要性设置不同的安全策略实现区域的访问控制。

入侵检测技术

入侵检测是通过对某网络的状态和系统使用情况进行监控，检测用户对系统的访问是否越权以及记录非法用户对系统的入侵行为等方法为系统内部提供安全保障。在智能电网的生产网络中利用入侵检测系统用于分析生产网络中数据，对系统网络进行监控、实时跟踪探测、及时响应，防范各种入侵行为。

智能电网中智能电表成为攻击者攻击的重要方向，通过破解智能电表密码，可以篡改存储数据，中断网络中的数据通信，修改计量报文。通过篡改电表数据（用电需求和链路d的状态)引起系统震荡，并最终造成断电。如果引入入侵检测技术，检测电表或集中器中传感器的状态、内存的通信数据，针对入侵行为能够有效的检测智能电表中的入侵行为并发出告警。同时，入侵检测技术提升系统管理员的安全防护能力，完善智能电网信息安全结构的完整性。

漏洞挖掘技术

漏洞挖掘是一种针对系统或网络的安全测试技术，通过对系统的软硬件进行模拟渗透以及对数据的分析发现系统漏洞。针对智能电网系统（包括软件、硬件以及操作系统）和网络的脆弱性，分析其面临的安全威胁，率先检测出系统漏洞，完成对智能电网控制系统的优化升级。在智能电网中利用漏洞挖掘技术及时发掘系统存在的安全隐患，设置有效的安全策略，并及时改进安全控制手段对保障智能电网系统安全运行具有十分重要的意义。

隔离交换技术

防火墙技术可以实现部分隔离效果。但是，网络安全隔离交换设备的安全性能要比防火墙强很多。网络安全隔离交换技术主要是切断内部网络和外部网络的直接联系，从而实现阻断不同网络间的数据交换。网络安全隔离与信息交换技术主要作用，一是用于保护内部网络的服务器，避免内部数据库和操作系统免受外网病毒的侵袭；其二可以有效避免内部网络访问外部网络时出现的有意的或无意的信息泄露。通过建立数据交换平台满足数据交换业务需求，系统框架如图4所示。

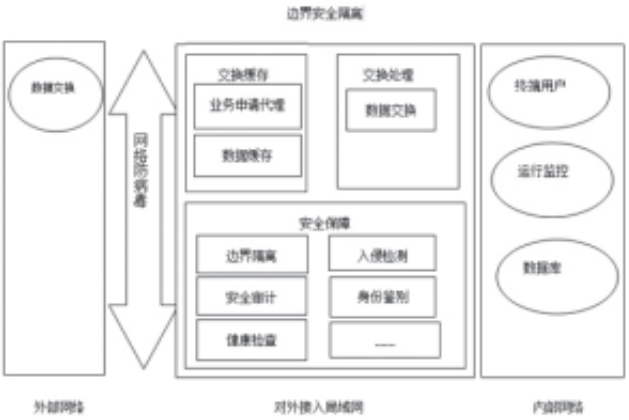

图 4 网络安全隔离与信息交换技术的系统模型

智能电网的信息安全隔离体系架构也不例外，它应当满足智能电网各类业务数据在信息内外网之间进行安全交互的一些基本要求。

安全态势感知和预测技术

目前，应用最广泛的态势感知理论模型框架是由Endsley在1995年提出来的，Endsley模型将态势感知分为3个阶段：态势要素获取，态势理解，态势预测。简单定义为“在一定的时空间条件下，对环境因素的获取、理解以及对未来状态的预测”。态势感知过程可由图5所示的三阶段模型直观的表述出来。

图 5 ENDSLEY 模型三阶段

在智能电网中应用态势感知技术，能够实现智能电网信息系统运行的智能防控，通过在配电网实施实时的态势感知，快速准确地判断出系统安全状态，为运行控制人员提供一个较为准确的配电网运行趋势；利用态势感知系统具有自适应能力和自学习能力，实时跟踪配电网运行状态，实现电网运行态势的智能化告警在事件发生之前进行预测，并准确地发现潜在的运行风险，帮助管理员提高对智能电网运行的控制力。

智能电网关键信息安全技术应用

信息安全技术在智能电网中的实际应用如图6所示。图6展示了火力发电网生产控制大区中，信息安全技术的相关应用。调度中心的调度命令通过工业防火墙或者隔离交换机到达生产控制区的服务器。服务器、操作员站、工程师站以及历史站上部署身份认证、访问控制和入侵检测技术，对人员操作、通信访问以及外部入侵进行监控防护。从操作员站、工程师站等上位机发出的指令通过工业防火墙到达具体的DCS系统等下位机，执行操作。而这些指令需要使用加密技术（如加密机）进行加密处理。信息调度区与生产控制区之间的工业防火墙连接管理交换机，操作员站、工程师站等上位机连接监测审计平台，然后接入管理交换机，最后接入安全监管平台由安全监管平台进行统一的安全监管。生产控制大区的边界为服务器与DCS系统，将其接入态势感知系统，对物理环境安全和信息环境安全进行态势感知，预防安全事故的发生。使用漏洞扫描工具对相关操作系统以及应用软件进行漏洞挖掘，发现潜在漏洞，及时修补。

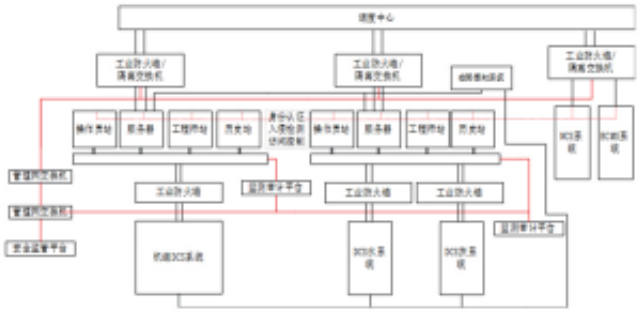

图 6 火力发电网生产控制大区中信息安全技术的相关应用

展望

为了确保智能电网可靠安全，只有设置多道安全防线，提高系统的入侵检测能力、事件反应能力和快速恢复能力，从技术上实施系统的安全防护，形成全方位的网络安全技术防护体系，使得智能电网信息安全走向纵深防御阶段，有效应对在动态、复杂和多变的电力信息网络环境下实现智能电网业务应用安全防护。

作者>>>

封亚辉，江苏出入境检验检疫局工业产品检测中心主任，研究员，研究方向为信息安全认证管理。

王彩学，中国网络安全审查技术与认证中心工程师，研究方向为信息安全。

戴东情，江苏出入境检验检疫局工业产品检测中心工程师，研究方向为信息安全认证。

原文地址：http://www.china-nengyuan.com/tech/131033.html