智能电网的信息安全及防护措施

——马亚林，韩一鸣，倪倩欣，吕林晖

Contents 目录

研究背景

什么是智能电网？

智能电网就是电网的智能化（智电电力），也被称为“电网2.0”，它是建立在集成的、高速双向通信网络的基础上，通过先进的传感和测量技术、先进的设备技术、先进的控制方法以及先进的决策支持系统技术的应用。

智能电网优势

它的优点是可以更好地管理、节约、监控和使用能源，将能源使用的决定权交给消费者，由他们决定何时、何地以及如何使用。

研究背景

安全性

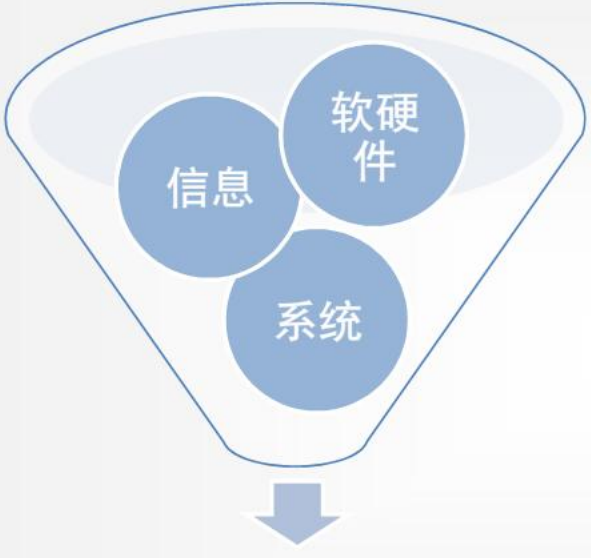
1. 2010年的震网病毒导致伊朗核电站推迟发电。

2.直接暴露在用户面前的终端将有可能被攻击，其中智能电表是用户最常接触，

智能电网信息安全总述

- 智能电网信息资产
- 智能电网信息安全特点
- 智能电力信息网结构

智能电网信息资产



- 信息通信可靠性方面比传统办公网络要求更高。
- 一旦出现故障不仅会带来巨大经济损失，还可能影响人身安全和社会稳定。

智能电网信息安全特点

- 非法用户可能会给电网的安全带来威胁，同时，用户的隐私安全风险也更突出。

智能电力信息网结构

电力网

- 电力网中的节点为电源节点和负荷节点两大类，二者通过输电线进行连接。

信息网

- 信息网络中的节点为两类：一类是信息采集/指令执行节点，负责对控制范围内的负荷和电源的状态信息进行采集和上传，；另一类是信息处理/指令生成节点，负责对采集到的信息进行汇总分析和生成控制指令。

电力网与信息网相互依存

重中之重：
信息网络的安全

1.信息网的安全隐患更多
2.电力网的正常运行对信息网的依赖程度更高
3.信息网的故障更容易造成大范围的停电

智能电网信息安全性的破坏——隐患

1.信息安全防御范围扩大、难度增加。
2.信息交互激增造成网络波动、信息泄露
3.技术更新引入的新型安全问题
4.用户侧安全威胁增大

外在智能电网的安全威胁

1.自然因素。 自然威胁来自于像雷击等不可抗力自然因素引发的威胁，造成电磁干扰，影响信息准确性，甚至损坏设备，从而威胁电力系统安全。

2.人为因素。 人为威胁大致有两种：一种是以工作人员误操作为代表的无意威胁，虽经授权，但对授权数据和资源的使用不合法；另一种是以计算机网络犯罪为代表进行恶意攻击的有意威胁，

智能电网信息安全防护措施

- 物理环境安全
- 应用限制
- 风险管理
- 业务终端安全（数据，接入）

智能电网信息安全防护措施

- 边界安全
- 网络环境安全
- 主机系统安全
- 应用与数据安全

物理环境安全

智能电网的物理安全是指智能电网系统运营所必需的各种硬件设备的安全，主要包括传感设备，网络设备，计算机终端和存储介质等。为了应对物理终端部署在开放区域以及智能电网业务系统向用户侧延伸带来的问题，我们通过以下两方面加强物理安全性。

1.首先是建立一定的物理安全防护和接入控制措施，保护部署于开放环境的设备，尤其是涉及关键业务信息的物理设备，以防止信息泄露和人为破坏。

2.其次是设计并实施针对火灾、水灾、地震、爆炸等灾害的物理保护措施。

Strong&SmartGrid
智能电网 接通未来

应用限制

保障智能电网系统中的网络、服务器、工作站和终端仅为电力生产业务专用，严格限制智能电力控制系统处理、存放和传输的信息类型，严格限制电力生产测控网络中承载的业务和网络的数据连接类型，严格限制服务器和工作站上其他应用程序的安装和个人数据的存放，严格限制允许访问的智能电网系统的应用。

Strong&SmartGrid
智能电网 接通未来

风险管理

从可靠性和业务逻辑性角度考虑，智能电网系统在上线运行以后一般禁止配置更改，而且很少进行设备更新，因化,此部分信息安全防护与加固工作必须在系统上线前完成，具体工作包括在系统设计与采购阶段实行安全功能或设备的集成，在系统上线前有专业的信息安全技术队伍对软硬件的安全性进行评测和加固，并开展常态化的智能电网信息安全风险评估工作。

业务终端安全（数据，接入）

在业务终端中使用的信息安全技术有两方面作用，确保存储在终端内部的数据安全以及控制终端的接入。具体实施时，需要根据终端的类型、应用环境以及通信方式选取适当的安全防护技术。

1）终端数据的安全

采用最小安装原则装配终端的操作系统，对系统和应用进行必要的加固；安装第三方安全工具增强终端安全性；采用加密措施对存储在终端的重要数据进行加密处理，加强终端数据防护。

2）终端接入控制

采用认证、加密、访问控制等技术措施实现终端安全接入以及数据的远程安全传输。终端需进行身份认证后方允许接入网络。需要终端利用公用通信网络与主站进行数据传输时，应采用应用开发，或启用软件自身的加密配置，或通过SSL、IPSEC等方式实现加密。重要数据采用数字签名技术保证通信的完整性。

边界安全

建立清晰的智能电网安全防护边界，并对经由边界的会话过程进行严格的监控、审计和管理，禁止边界以外的网络访问被保护区域的数据，严格控制边界出口数据流量边界访问控制设备缺省应拒绝所有网络连接，一旦防护设备失效则默认为网络连接中断，防止信息泄露和非法接入，严格控制交叉使用移动存储介质和便携式计算机。

网络环境安全

网络环境安全面向智能电网提供网络支撑平台以及配套的所有设备设施，具体包括网络中提供连接的路由、交换设备及各种安全设备、网络基础服务设施，网络拓扑结构图等等。智能电网的通信网使用安全隔离装置或物理隔离的方式划分安全大区，同时充分利用防火墙、虚拟专用网，采用加密、安全隔离、入侵检测以及网络防杀病毒等技术保障网络安全。

Strong&SmartGrid
智能电网 接通未来

主机系统安全　应用与数据安全

主机系统保护

主机系统安全即服务器安全，技术适用对象包括业务应用服务器、网络服务器、WEB服务器、文件与通信服务器等。一般采用身份鉴别、访问控制、安全审计、入侵防范等技术对主机操作系统、数据库系统进行安全防护。

应用与数据安全

智能电网应用与数据安全的防护对象包括应用系统本身、用户接口、系统间（域间）和系统内（域内）数据接口。具体采用的安全技术包括双向强身份认证、访问控制、安全审计、数据加密、数据完整性保护技术、数据备份、异地容灾以及云存储等等。

Strong&SmartGrid
智能电网 接通未来

Thank You !

东南大学电气工程学院