

新一代智能变电站网络通信安全体系架构研究

为满足智能电网和“三集五大”体系建设要求，以掌握现状为基础，以需求分析为引领，以关键技术研究为突破口，围绕新一代智能变电站网络通信面临的安全威胁和安全防护部署策略，定制设计原则，从站内通信网络、站外通信网络，网络系统安全、网络信息安全，网络技术安全、网络管理安全等层级和维度建立一整套新一代智能变电站网络通信安全体系架构，从而指导变电站通信网络安全系统的部署，提高变电站通信网络的系统安全性和信息安全水平。

尉钺/国网山西省电力公司

0 引言

以新一代智能变电站为代表的智能电网建设促进了电力系统电力流、信息流、业务流的高度融合，随着国内外、行业内外信息网络安全形势的日趋严峻，有必要结合新一代智能变电站新技术、新设备、新业务的应用，全面梳理变电站网络通信安全应用现状和存在的问题，深入研究变电站通信安全技术及应用范围，建立一整套科学、系统的网络通信安全体系架构。

国家电网公司发布国家电网调[2011]168号文《关于加强配电网自动化系统安全防护工作的通知》中对配电网自动化系统安全防护要求进行了补充规定，对系统主站与子站及终端的通信方式、控制命令认证方法，采取了指定的加密算法，并分别对子站终端、纵向通信、主站和横向边界的安全防护提出了新的技术要求。方案的一个重要措施就是采用非对称加密算法进行公钥签名，对配电传输规约的完整性进行保护。现阶段新

一代变电站站外远传系统采用了横向隔离、纵向加密认证的安全防护技术，但在站端尚未建立完整的系统安全防护平台，本文提出的站内安全防护系统方案对变电站信息网络的建设提出了更新、更高、更为全面的要求。

1 新一代智能变电站网络通信安全防护需求分析

2012年初，国网公司提出建设新一代智能变电站，公司选取了北京、天津等6座110 kV、220 kV电压等级新一代智能变电站进行建设试点工程，解决电网发展现实的迫切需求。新一代智能变电站提出了“运行安全可靠”、“系统高度集成”、“支撑调控一体”的建设目标，应用智能化高压设备、集成化二次装置，采用层次化保护控制、一体化网络与业务系统等技术，充分考虑对新能源、分布式电源、智能配用电的吸纳与接入，新一代变电站成为智能电网最为重要的基础运行参量采集点、管控执行点。

(1) 智能电网新型业务的接入，为变电站网络通信安全带来新的隐患

新一代智能变电站进一步强化了变电站作为智能电网体系中信息支撑点的作用和地位，变电站需要满足和应对智能电网发、输、配、用等环节系的对接，分布式电源、输电线路在线监测、配电自动化、用电信息采集等新的系统与业务不断接入智能变电站。智能电网新型业务的接入不但对变电站通信网络的技术架构、流量带宽提出了新的要



尉钺/高级工程师

关键词/Keywords

新一代智能变电站 ·
通信 ·
安全 ·
架构 ·

求，同时，由于其中相当一部分业务点处于一种开放的物理环境中，不可避免的增加了信息网络外部攻击源，提高了网络通信安全应对难度，因此有必要对新的安全隐患点进行整理分析，提高新形势下变电站网络通信安全防护水平。

(2) 智能变电站新设备、新业务的应用，对现有网络安全架构造成影响

集成化、智能化是新一代智能变电站重要的技术特征，传感器、智能组件与一次设备集成，一次设备之间、二次设备之间的集成，使得智能高压设备、多功能二次装置不断应用在新一代智能变电站中，同时，作为提升变电站应用功能的站域保护控制、一体化业务系统等新技术和系统在也得到应用，变电站信息网络由传统的“三层两网”向“一体化网络”逐步演进，变电站内各种信息共享水平大大提高，网络结构和信息流量流向的变化对信息网络产生很大影响，无论是网络的系统安全，还是网络的信息安全都面临新的挑战，有必要结合智能变电站内出现的新信息流特点对网络通信安全策略进行认真的梳理、研究。

(3) 与主站系统信息交互需求提升，对网络信息安全提出新的要求

公司“大运行”、“大检修”、“大营销”业务纵向贯穿的管理模式要求新一代智能变电站信息一体化、功能集成化，支撑电力流、信息流、业务流的高度融合。“大运行”体系应满足调度运行业务一体化需求，为实现变电站设备监控统一管理，应与电力调度系统全景全息共享；“大检修”体系应满足设备状态可视化需求，为检修管理提供最佳的决策依据；“大营销”体系要求变电站实现变电站计量信息与营销服务系统的准确交互。可以看出，“五大”体系对智能变电站与主站系统间信息交互的实时性、可靠性、安全性提出了更高的要求，对变电站网络通信安全架构进行研究对保障电网安全稳定运行具有重要意义。

2 新一代智能变电站网络通信安全体系架构设计原则

新一代智能变电站以结构布局合理、系统高

度集成、技术装备先进、经济节能环保、支撑调控一体化为技术特征，遵循“功能集约、信息集成、设备智能、设计优化”的建设原则，以高度可靠的智能设备为基础，以协调互动的测控技术为支撑，以高效便捷的运维模式为保障，实现全站信息数字化、通信平台网络化、信息共享标准化、应用功能互动化，满足高可靠、高智能、易施工、便扩展、轻维护的建设、运行与检修要求，全面支撑调控一体，助力电网发展方式转变。

(1) 高可靠性原则

由于电力生产的连续性和重要性，站内通信网络的可靠性是第一位的，通信网络的生存性能要远高于一般通信网络，应避免个别装置损坏导致站内通信中断：① 站内通信网络必须具备最长的运行时间、最少的故障时间；② 站内通信网络必须具备故障弱化的特性，单点故障不会影响整个网络的正常工作，且网络要具有一定的容错能力；③ 站内通信网络必须能够通过软硬件进行便捷维护，且对系统的正常工作影响最小；④ 在不影响网络正常工作的条件下，可最大程度地动态改变网络结构；⑤ 站内通信网络必须具备抵御服务拒绝和非法入侵的能力；⑥ 在变电站的强电磁干扰环境中，网络必须具备较强的抗电磁干扰能力；⑦ 站内通信网络必须具备故障监测、故障自恢复和数据校验等功能。

(2) 高度集成性原则

新一代智能变电站遵循整体设计的原则。从结构上分析，新一代智能变电站由站控层、间隔层、过程层三层结构组成，并将三层设备连接到站控层网络上。站控层网络又细分为核心层网络和接入层网络，其对应的设备通过“一体化网络平台”汇聚应用层多种业务，实现结构的高度集成；在设备方面，实现了一次/二次设备高度集成，提高设备集成度与智能化水平。

(3) 智能化和网络化原则

各种光纤传感器替代了变电站内传统的磁式电流电压互感器，直接对外提供数字式光纤以太网接口；站内采用具备高智能化的变压器、断路器等设备，并在一次设备上内嵌智能终端用以实现信号转换与状态监测，实现智能化和数字化的

要求。新一代变电站中的二次设备还具备对外光纤网络通信接口，与传统变电站通信方式采用电缆为媒介不同，智能变电站二次信号传输是基于光纤方式实现的。

(4) 高实时性原则

变电站内传输的安稳保护信号实时性要求高，虽然数据流量并不大，但一旦出现电网故障就要传送大量的继保数据，要求数据能在站内通信网络上快速传送。为保证变电站稳定运行，通信网络实时性能必须达到IEC 61850标准对报文传输性能的要求，以输电间隔为例：极快速报文不超过 3 ms、快速报文不超过 20 ms、中速报文不超过100 ms、低速报文不超过500 ms。

(5) 合理性原则

新一代智能变电站通信网安全体系设计从公司变电站通信网建设的基本情况入手，以“减少改造、重点防护”的宗旨降低通信网安全防护带来的成本代价，仅对电力通信网关键防护区域和范围实施必要的技术措施。新一代智能变电站通信网安全体系设计将具有较强的实用性和可操作性，为网省公司通信专业人员的设计、建设、操作和管理工作提供依据。

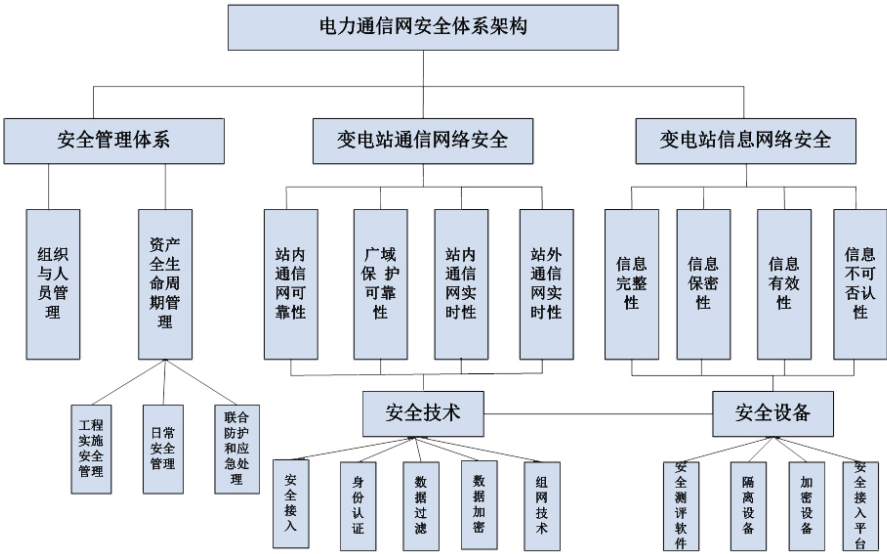
3 新一代智能变电站网络通信安全体系架构方案

图1为新一代智能变电站通信网络安全防护体

系基本模型。

变电站通信网络安全体系基本模型由三模块组成，分别为安全管理体系、通信网络安全体系、信息网络安全体系。变电站通信系统主要分为站内通信及站外通信，而系统的可靠性及实时性是通信网络安全最主要的两大考核指标，因此本文以这两大内容研究为基础，将架构中通信部分分为四小块，分别为站内及站外的可靠性和实时性的研究。另一方面变电站信息网络主要是指数据传输的可用性、保密性、完整性和不可抵赖性。实现这些性能的方法有逻辑技术和物理硬件来支撑，如身份认证技术、安全接入技术和数据过滤技术等。在间隔层中交换机里可以采用IEEE 802.1X安全接入控制技术，在间隔层也可以增加加密认证网关，网关中采用SHA-1哈希散列算法或MD5信息摘要算法进行数据加密，能够保证变电站运行信息的完整性；在控制层中，数据过滤技术可以监控数据流量包，提取有用传输信息，提高传输效率；主站平台上，为了防止恶意的内部人员攻击，采用身份认证技术鉴别进入人员的合法性，通过输入用户口令来保证计算机的使用安全。

除了安全技术以外，安全管理部分是不可或缺的。安全管理主要由人员管理及设备资产管理组成，由具体的安全管理规范作为支撑。



新一代变电站通信信息安全面临的威胁大致分为自然威胁和人为威胁。自然威胁主要来自于雷击造成的IED元件损坏、高压设备对IED电磁辐射和电磁干扰、计算机网络和IED等各种设备自然老化等原因，这些都会影响数据的准确性，甚至直接损坏新一代变电站数据存储的载体，直接威胁到变电站计算机网络系统安全。人为威胁主要指通过网络攻击而暴露出来的漏洞，使得数据的完整性、可靠性、保密性、可用性和可控性无法保证，造成IED装置的误动、上传数据紊乱、整定参数的错误等电力系统安全稳定运行遭受破坏的行为，最终导致严重的经济损失和社会影响。

本文基于IEC 61850标准变电站三层两网的架构及IEC 62351变电站的安全规约，构建新一代智能变电站通信网络安全体系架构，如图2所示。

横向部署，在“三层两网”基础网络架构基础上，综合考虑不同层通信业务传输特征及层内设备性能，采用针对性的安全加密及防护手段保障变电站通信网络的安全传输。如在过程层和间隔层中，接入交换机和核心交换机使用IEEE 802.1X认证安全接入技术，可以提高系统接入安全性，IEEE 802.1X准入控制技术可以定义不同VLAN之间的切换，在核心层上定义不同的访问控制列表，以允许不同的VLAN用户访问所需的网络资源。接入设备通过客户端设备代理软件获取接入网络的客户端设备的设备身份和安全信息，并将这些信息发送给安全策略服务器，通知网络控制设备采用不同的访问控制口令，动态地切换交换机端口VLAN，从而获取内部网络资源；变电站内常用的网络报文记录分析仪就是基于内容的数据过滤技术，仪器主要用来监听相关网络安全事

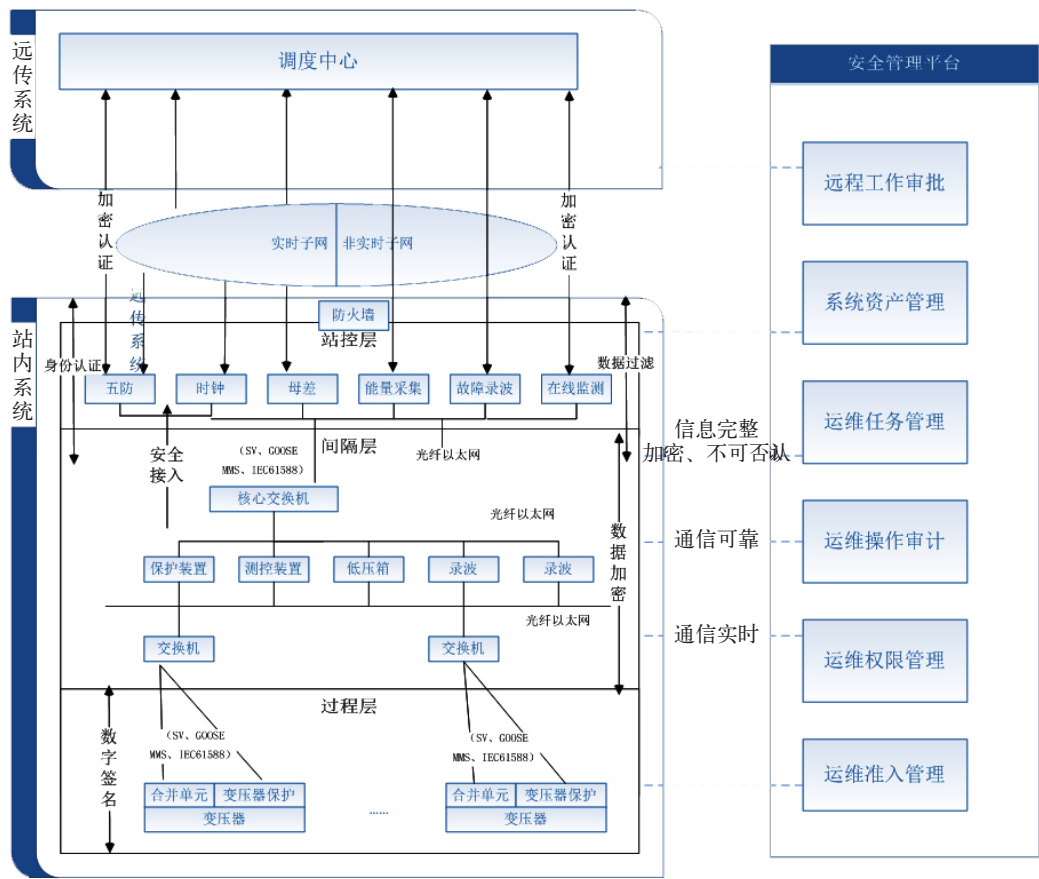


图2 新一代变电站通信网络安全体系部署图

件，如网络风暴、流量异常、异常APPID告警、SCD配置不符及异常IP告警等。在智能变电站调试完成后，网络内的流量基本处于稳定状态，流量处于一个可预测的范围之内。而相对于网络风暴，报文具有重复的特性，流量异常告警是对网络风暴告警的补充，流量异常告警可以检查持续变化的报文。利用数据过滤技术之一的向量机算法，网分装置可以对监听端口的流量设定一个上限和下限，如监听到的流量不符合设定的上下限值后，装置会给出流量异常告警。

纵向部署，网络架构分为安全管理平台和站内站外通信安全防护平台。安全管理平台按照安全管理规范对站内站外设备资产、人员、运维工作票、权限等系统操作管理，贯穿整个变电站全生命周期管理。指定专人负责管理本单位所辖变电站的公共安全设施，明确各业务系统专责人的安全管理责任；加强重要变电站设备全生命周期的安全管理，系统上线前由国家或电力行业认可的测评机构开展源代码安全检测，审查系统中可能存在的后门和隐蔽信道；变电站安全防护实施方案严格经过本企业上级专业主管部门、信息安全主管部门以及相应电力调度机构的审核，方案实施完成后应当由上述机构验收。建立变电站安全管理制度，主要包括：门禁管理、人员管理、权限管理、访问控制管理、安全防护系统的维护管理、常规设备及各系统的维护管理、恶意代码的防护管理、审计管理、数据及系统的备份管理、用户口令密钥及数字证书的管理、培训管理等管理制度，对关键安全设备、服务器的日志进行统一管理，及时发现安全管理体系中存在的安全隐患和异常访问行为；建立健全变电站安全的联合防护和应急机制。由上级机构负责对变电站安全防护的监管，电力调度机构负责统一指挥变电站安全应急处理。当出现出现安全事件，尤其是遭到黑客、恶意代码攻击和其他人为破坏时，

应当立即向其上级电力机构报告，同时按应急处理预案采取安全应急措施。相应电力调度机构应当立即组织采取紧急联合防护措施，以防止事件扩大。同时注意保护现场，以便进行调查取证和分析。事件发生单位及相应机构应当及时将事件情况向相关监管部门和信息安全主管部门报告。

4 结束语

- 1) 分析了新一代智能变电站信息网络安全面临的威胁与挑战，为建立新形势下智能变电站信息网络安全体系架构奠定基础。
- 2) 提出了智能变电站信息网络安全防护体系架构及部署方式，站在顶层设计的高度指导未来智能变电站信息网络安全建设。

参考文献

[1] Hoga C, Skare P. IEC 61850 projects in Germany and Switzerland[C].Transmission and Distribution Conferece and Exhibition, 2005/2006 IEEE PES, 2006 IEEE:390-393.

[2] 高会生, 靳玮玮. 基于OPNET的变电站端对端通信实时性仿真研究[J]. 继电器, 2006, 34(19): 33-37.

[3] 周静, 雷煜卿, 张睿訥, 等. 基于 IEC 62351-6 的电力控制系统通信安全防护探讨[C]. 2012年电力通信管理暨智能电网通信技术论坛论文集, 2012.

[4] 沈宏涛, 李瑞芳. 变电站自动化通信系统仿真[J]. 电力自动化设备, 2007, 27(6): 114-11.

作者简介

尉镡（1975-），男，高级工程师，主要研究方向为电力自动化。

（收稿日期：2015-12-10） EA

（编辑：鞠佳）