智能变电站信息安全策略探讨

姚亮[1,2],邹磊[1,2],韩志勇[1,2]
(1. 国电南京自动化股份有限公司,南京 210032; 2. 南京国电南自电网自动化有限公司,南京 211153)

摘 要:智能变电站中报文信息根据网络可分为过程层信息和站控层信息两类。信息安全遵循“安全分区、网络专用、横向隔离、纵向认证”的原则,通过加密、数字签名、虚拟网络、防火墙和入侵检测等技术手段,依靠主动防御和被动防御相结合,建立起信息安全防护的两道防线,增强了信息的可用性、保密性、完整性和不可抵赖性。

关键词:智能变电站;信息安全;主动防御;被动防御
中图分类号:TM 76 **文献标志码**:B **文章编号**:1674 - 1951(2016)12 - 0015 - 03

0 引言

智能变电站作为智能电网“电力流”“信息流”和“业务流”的汇集点,能够实现庞大的电网数据信息采集、传输、分析及处理功能。随着通信技术和网络技术的发展,电力系统通信协议日趋标准化,一方面提高了变电站内设备的互操作性和互换性,另一方面又对变电站的信息可靠性和安全性提出了新的挑战。2015 年圣诞节期间,乌克兰国内多个区域的电网遭遇网络攻击,引发大面积停电,敲响了电网信息可靠性与安全性的警钟。

信息可靠性与安全性是智能电网安全稳定运行的关键要素之一。智能变电站作为智能电网的重要组成部分,其站内二次设备信息可靠性与安全性面临着来自多方面的严峻考验。因此,对智能变电站内部设备以及其与电网内交互信息进行全面、系统的安全防护,利用有效的信息安全防护方法和策略保障信息交互的可靠,消除安全隐患,合理规避潜在风险,是保证智能变电站乃至智能电网安全稳定运行的关键问题之一[1]。

1 变电站信息安全现状

网络通信系统是智能变电站信息传输的基础,站内信息网络具有承载保护、测控、计量、同步相量测量、故障录波等功能。根据应用的不同,站内网络信息包括面向通用对象的变电站事件 GOOSE(Generic Object Oriented Substation Events)、样本值 SV(Sampled Value)、制造报文规范 MMS(Manufacturing Message Specification)和对时信息四类。在线监测和智能辅助控制业务通过站内单独组网或点对点通信方式实现;数据采集与监视控制 SCADA(Supervisory Control And Data Acquisition)等远传类业务由调度数据网、综合数据网向相应功能主站系统传送。过程层设备、间隔层设备和站控层设备采用 IEC 61850 标准实现站内通信。智能变电站通常采用“三层两网”架构,过程层网络中上行信息主要是电流和电压采样值数据的 SV 报文、开关状态量数据的 GOOSE 报文,下行信息为操作控制命令的 GOOSE 报文。站控层网络中上行信息主要是二次设备状态、动作、告警信息的 MMS 报文,下行信息为操作控制命令 GOOSE 报文[2-4]。

过程层网络中 SV 报文和 GOOSE 报文实时性要求很高,数据传输路径跳过了高层协议,从应用层直接映射到数据链路层。站控层网络中 MMS 报文作为变电站内外信息交互的报文,数据传输遵循 TCP/IP 协议,存在不安全因素,如 IP 包明文传输、IP 包没有数据认证等。

2 变电站信息安全相关标准和规范

2.1 国内变电站信息安全规定

2014 年 8 月国家发展和改革委员会审议通过了第 14 号令《电力监控系统安全防护规定》,明确了“安全分区、网络专用、横向隔离、纵向认证”的原则。根据第 14 号令,生产控制区分为控制区(安全Ⅰ区)和非控制区(安全Ⅱ区),管理信息区内部在不影响生产控制区的前提下,根据不同安全要求划分安全区。生产控制区与管理信息区之间设置专用单向安全隔离装置,生产控制区内的控制区和非控制区之间采用防火墙实现逻辑隔离。在生产控制区与广域网的纵向链接处需设置专用纵向加密认证装置或者加密认证网关。电力调度数据网在专用通道上使用独立的网络设备组网,在物理层面上实现与其他数据网及外部公用数据网的安全隔离。

2.2 国际变电站信息安全标准

IEC 62351 电力系统管理及关联的信息交换 -

收稿日期:2016 - 10 - 12;修回日期:2016 - 11 - 02

数据和通信安全主要采取数据加密、数字签名和信息摘录技术，提出了包含 TCP/IP 的通信模型的安全传输层握手协议的改进方法，抵御非法操作攻击系统，保障变电站系统数据通信的保密性、完整性、可用性和不可抵赖性，图 1 为 IEC 62351 与变电站通信协议间的对应关系。

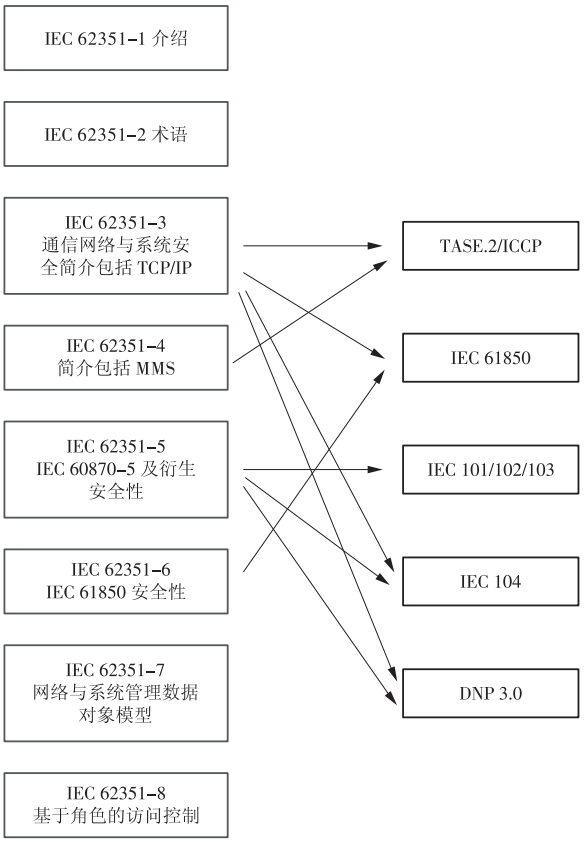

图 1 IEC 62351 与变电站通信协议的对应关系

根据 ISO 7498－2 的三维安全体系结构，结合智能变电站安全需要，对四类安全性能和五类主要安全技术进行关联，见表 1。

表 1 变电站安全需求与机制对应关联

安全机制	安全需求			
	保密性	完整性	可用性	不可抵赖性
加密	●	●	○	○
入侵检测	●	●	●	●
防火墙	●	○	●	○
虚拟网	●	●	●	○
数字签名	○	●	○	●

3 变电站主要信息安全措施

智能变电站系统安全防护重点是强化变电站边界防护，加强内部安全措施，保障变电站安全稳定运行。调控主站端依托智能电网调度控制系统集中监控功能模块实现基于该平台的模型管理、数据传输、网络通信、人机界面、系统管理等服务。通过安全Ⅰ区数据通信网关机将调控主站下发的遥控指令转发给继电保护和安全自动装置，并将继电保护和安全自动装置的状态信息、定值转发回调控主站，同时完成变电站站控层和调度数据网之间通信规约的转换功能，其总体架构如图 2 所示。继电保护和安全自动装置远方操作相关功能部署在安全Ⅰ区，覆盖调控主站、变电站和数据传输通道三部分内容。在主站和变电站配置纵向加密设备，采用调度证书系统签发的设备证书进行调试并按照数据交互需求设定加密隧道及策略，各纵向加密认证设备均应在加密通道运行。变电站内Ⅰ区数据通信网关机采用 IP 地址验证方式进行认证，建立一个 IP 地址白名单列表，只响应 IP 地址白名单列表中装置的 TCP 连接请求；对网关机到继电保护装置之间的控制指令进行安全认证，通过访问控制表 ACL（Access Control List）设置对交换机端口进行 IP 地址和 MAC 地址绑定，每个端口只允许固定 IP 地址和 MAC 地址的链接通过。

变电站信息安全防护旨在保护变电站站内信息和站与调度传输信息的保密性、完整性、可用性和不可抵赖性，目前主要采用加密技术、数字签名技术、防火墙技术、虚拟网络技术和入侵检测技术等[5－7]。

3.1 加密技术

加密技术是按照特定的规则将传输的数据转换为乱序，一般有链路加密、节点加密和端到端加密三种形式。变电站加密的信息主要有遥控信息、遥调信息、保护装置和其他安全自动装置的整定信息等直接关系电网安全运行的信息。

3.2 数字签名技术

数字签名类似传统纸上的笔迹或印章，采用了两种互补的算法，一种用于签名，另一种用于验证，包括密码生成算法、标记算法和验证算法。智能变电站过程层包含 GOOSE 和 SV 两类信息，过程网络数据的传输需要严格保证实时性和安全性。GOOSE 和 SV 若采用加密或其他安全方法会使原始数据增加很多字节数，既增加了报文处理时间，也延迟了传输速度，采用数字签名技术则可兼顾过程层信息的安全性和实时性。

3.3 防火墙技术

防火墙是介于两个网络之间的安全系统，根据设定的规则，控制信息流向和进出网络的报文。对变电站系统进行分区，各区之间使用防火墙进行网络隔离，对变电站业务实施重点防护，这将大大增强整个系统的安全性。

3.4 虚拟网络技术

为满足不同应用之间的信息隔离，变电站站内

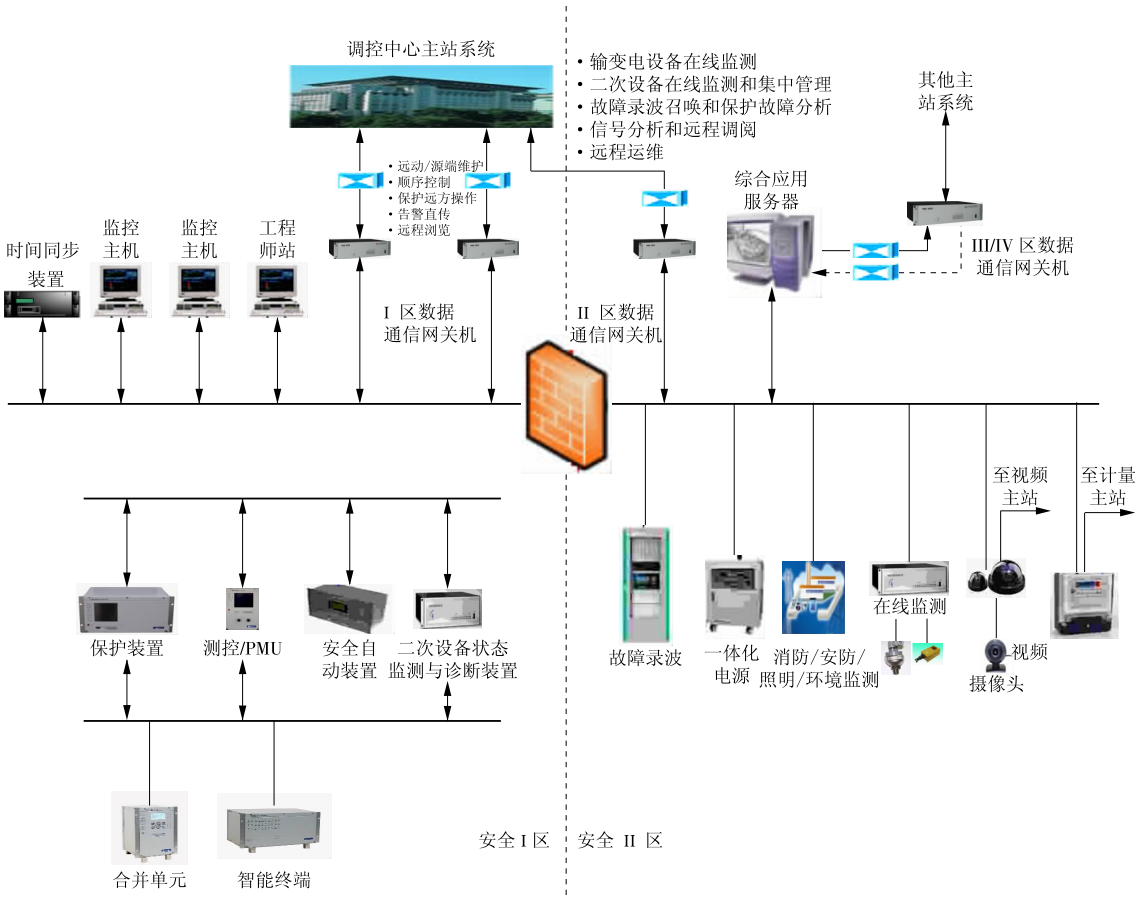

图 2　变电站安全分区系统架构

采用虚拟局域网 VLAN(Virtual Local Area Network)技术。

VLAN 将设备划分成不同的广播域,实现虚拟工作组的数据交换。GOOSE 信息传输实现设备间信息交互,通过在交换机上设置基于端口的 VLAN,不同业务的数据流限定在不同的 VLAN 中,不仅防止黑客攻击,更可控制流量,减少设备投资,简化网络管理并提高网络的安全性。

3.5　入侵检测技术

入侵检测是检测网络中违反安全策略行为,包括系统外部的入侵和内部用户的非授权操作。变电站网络入侵检测先收集系统、网络、数据及用户活动的状态和行为,再通过模式匹配、统计分析和完整性分析来实现数据分析,根据记录分析结果检测是否入侵,入侵则发出告警通知,对攻击源实施控制,保护被攻击对象。

4　变电站信息安全体系建设

4.1　安全体系模型

如图 3 所示,"WPDRRC"信息安全模型在传统 PDRR(防护 Protection,检测 Detection,响应 Reaction,恢复 Recovery)信息安全体系模型增加了预警(Waring)、反击(Counterattack)两个环节,以人员为核心、策略为纽带、技术为保证,体现信息系统安全系统的预警能力、保护能力、检测能力、响应能力、恢复能力和反击能力,针对不同的安全威胁,采用不同的安全措施,对受保护对象进行多层次保护。

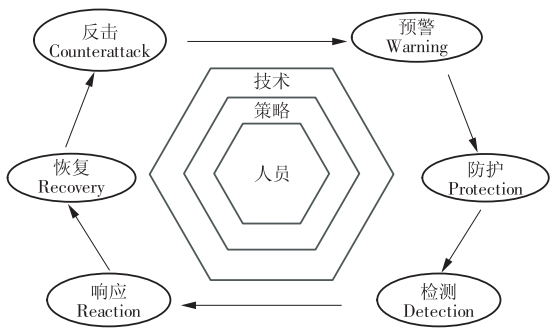

图 3　WPDRRC 信息安全模型

4.2　被动防御和主动防御

防护是一种被动防御,系统受到入侵后,根据入侵特征,将特征添加至防御策略库,防御受到再次入侵,但防御永远落在入侵之后。检测则是一种主动防御,系统根据状态判断,发现入侵行为则报警,并自动采取防护措施。

系统受到攻击时,可以通过漏洞扫描和入侵检测发现和阻断入侵行为,断开网络或关闭特定的服务、追踪入侵源、记录入侵痕迹,并(下转第 24 页)

续表

	项目	自由度 df	方差 SS	均方差 MS	F 检验	显著性 F	
方差分析	回归分析	5	129758.3	25951.67	407.2882	1.21484E-72	
	残差	118	7518.745	63.71818			
	总计	123	137277.1				
因子系数	项目	回归系数	标准误差	t Stat	*P* 值	下限 95%	上限 95%
	常数项 c	-905.836	229.947700	-3.939310	0.000139	-1361.194586	-450.4765
	因子 t(温度测值)	-0.089720	0.153451	-0.584680	0.559876	-0.393595232	0.2141545
	因子 X_1(#1 传感器测值)	0.130363	0.083810	1.555462	0.122514	-0.035603411	0.2963302
	因子 X_2(#2 传感器测值)	-0.203340	0.052631	-3.863610	0.000183	-0.307567919	-0.0991220
	因子 X_4(#4 传感器测值)	1.111740	0.079413	13.999440	7.74E-27	0.954480432	1.2689998
	因子 X_5(#5 传感器测值)	0.091307	0.009689	9.423479	4.65E-16	0.072119745	0.1104948

3 结论

在弹性变形下,锚索测力计内置的各支传感器的输出值是近似同步增大或者减小的,即使在偏心受力状态下,各支传感器的输出值在偏心两侧仍然表现出同步增大或者减小的规律,各传感器的输出值与参与计算的总输出值的平均值存在一定的相关性。

在综合考虑影响锚索测力计测值变化的情况下,不需要修正仪器自身参数,可采用多元回归的方法进行数据的修正,得到一个合理的实际测值范围,其结果精度很好,但本数学模型的长期稳定性仍是一个需要继续研究的问题。

参考文献:

[1]汪志福. 弦式锚索测力计仪器系数修正方法探讨[J]. 水电自动化与大坝监测,2005,29(3):60-63.

[2]徐闽,张平. 弦式锚索测力计仪器系数修正方法研究[J]. 中国科技信息,2014(2):32-33.

[3]周启,李刚,王秘学. 弦式锚索测力计数据缺陷修正方法探讨[J]. 大坝与安全,2006(6):44-47.

(本文责编:刘芳)

作者简介:

侯光强(1986—),男,贵州遵义人,助理工程师,从事水电站水工建筑物维护方面的工作(E-mail:331809469@qq.com)。

(上接第17页)与安全网关互动,自动完善防御策略,阻挡再次入侵,形成主动、被动防御体系的联动[8-9]。

5 结束语

变电站大量应用网络技术传输信息,其安全性和可靠性愈显突出。制定信息安全防御的策略是一个系统性的问题,仅凭借单一的防御手段不能有效解决问题。采用主动防御和被动防御相结合的网络安全方案,可以为信息安全构筑双重防线,建立起一个立体的防护体系。

参考文献:

[1]莫峻,谭建成. 基于 IEC 61850 的变电站网络安全分析[J]. 电力系统通信,2009,30(4):12-16.

[2]高吉普,徐长宝,胡炎. 智能变电站二次系统安全性定量评价方法的研究[J]. 电器与能效管理技术,2014(7):47-51,67.

[3]徐东伟,陈惠,陈志源,等. 智能变电站网络安全策略分析与研究[J]. 电力安全技术,2016,18(4):1-4.

[4]侯伟宏. 数字化变电站系统的可靠性与安全性研究[D]. 上海:上海交通大学,2010.

[5]高春雷,耿群锋,陈亮. 变电站通信网络安全分析与实现[J]. 江苏电机工程,2008,27(6):27-29.

[6]严童,谢吉华,温立超,等. 智能变电站 TCP/IP 通信网络的安全解决方案[J]. 电气自动化,2013,35(5):44-45,60.

[7]钟伟杰. 试论网络安全访问的规划与建设[J]. 信息安全与技术,2011,2(6):6-8.

[8]盛兆勇. IEC 61850 安全性分析及解决方案研究[D]. 青岛:中国海洋大学,2013.

[9]李彬,温蜜,齐钰. 智能电网 AMI 系统中一种新型密钥管理方案[J]. 计算机应用与软件,2016,33(1):321-325.

(本文责编:刘炳锋)

作者简介:

姚亮(1979—),男,江苏南京人,高级工程师,从事智能变电站二次设备技术研究和应用开发工作(E-mail:liang-yao@sac-china.com)。

邹磊(1982—),男,吉林长春人,工程师,从事智能变电站二次设备技术研究和应用开发工作。

韩志勇(1988—),男,吉林敦化人,工程师,从事智能变电站二次设备技术研究和应用开发工作。