Smart Grid 智能电网, 2013, 3, 141-146
http://dx.doi.org/10.12677/sg.2013.35026 Published Online October 2013 (http://www.hanspub.org/journal/sg.html)

Intelligent Substation Communication Network and Its Security Analysis

Yuanyuan Li, Wei Zong, Lianguang Liu

School of Electrical and Electronic Engineering, North China Electric Power University, Beijing,
Email: 454322886@qq.com

Received: Aug. 2nd, 2013; revised: Aug. 29th, 2013; accepted: Sep. 8th, 2013

Abstract: Intelligent Substation in the power system is an important factor. In order to meet the power system requirements, the system constantly optimizes power communication network structures, including massive introduction of new communications technologies, making electric power communication network more complex than ever. Factors affecting the substation communication safety are increasing. Substation communication network security problems become more complex. In this paper, intelligent substation communication networks based on intelligent substation communication network development process are briefly described, and the advantages and disadvantages of several communication technologies are analyzed and compared. In the end of the article, this paper comprehensive analyzed substation information system threats, present management situation and management system in actual operation.

Keywords: Intelligent Substation; Communication System; Security Analysis

智能变电站通信网络及其安全问题分析

李源源，宗　伟，刘连光

华北电力大学电气与电子工程学院，北京
Email: 454322886@qq.com

收稿日期：2013 年 8 月 2 日；修回日期：2013 年 8 月 29 日；录用日期：2013 年 9 月 8 日

摘　要：智能变电站在电力系统中处于重要地位，为了满足电力系统的要求，电力通信网结构不断地进行优化，大量引进通信领域新技术，使得电力通信网越来越复杂。影响变电站通信安全的因素日益增加，变电站通信网络安全这一问题变的日益复杂。本文以智能变电站的通信网络为基础，对智能变电站通信网络的发展历程进行简要介绍，分析比较几种通信技术的优缺点，针对变电站信息安全面对的威胁以及现阶段管理现状、管理制度等在实际运行中存在的问题进行深入讨论，全面研究分析了变电站面临的信息安全问题。

关键词：智能变电站；通信系统；安全分析

1. 引言

随着经济的发展，在国家建设中电力系统发挥越来越大的作用。智能变电站在电力系统中处于重要地位，智能变电站通信的安全性与可靠性要求也变的越来越高。另外为了满足电力系统的要求，电力通信网结构不断地进行优化，大量引进电信领域新的技术，这使得电力通信网越来越复杂，影响变电站通信安全的因素日益增加[1]。并且由于具有以上几个特点，加上变电站的实际情况各不相同，变电站通信安全这一问题变的日益复杂。

相比其它通信网，智能变电站通信网络安全有以下几个特点：

1) 要求有较高的可靠性、灵活性。电力是人们的生产生活、国民经济的重要基础，保证电力安全稳定供应是电力工作的首要任务。变电站不间断性和运行状态变化具有较大突然性，这要求变电站通信要有较高的可靠性和灵活性[2]。

2) 变电站的传输信息量少，但是信息种类比较复杂、传输实时性强。变电站传输的信号主要有话音信号、保护信号、计算机信息等，信息量一般都不大，但都对实时性有较高的要求。

3) 智能变电站通信的地理范围点多面广。有些变电站地处比较偏远，需要维护通常半径远达上百公里的通信设备。

4) 无人值守站点增多。由于变电站通信点的分散性、业务量少，各个站点都设通信值班不太现实。另外，随着技术的发展，无人值守变电站的比例未来将进一步增大。

2. 智能变电站通信技术

2.1. 智能变电站通信网络的发展

现在，我国智能变电站综合自动化网络使用的主要是总线式结构网络。该结构最初使用 RS-232 总线，后来发展到使用 RS-485 总线。最近几年来，由于新型现场总线 Canbus 和 Lonworks 巨大的灵活可靠性，智能变电站综合自动化通信系统得到了进一步发展。目前，性价比最好的是新型现场 Canbus 总线。

美国电子工业协会在 1969 年推出 RS-232 串口通信标准，这一标准对数据终端和通信设备之间的接口定义为按位串行传输。一般设备近距离传输时，两台具有这一接口的设备可以直接相连，如果需要远距离传输，可以加上一个调解器(图 1)。

半双工接口的 RS-485 可以在同一时刻一个设备发送信息，另外一个设备接受信息，这可以节省一段信号线，适合于远距离高速传输信息。如果多个智能仪器都配备这一总线，各个设备之间传输信息将非常方便(图 2)。

美国 ECHETON 公司公布的 Lonworks 是一种新型现场总线。其基础思想是把控制系统仿照局域网方式建设，使用网络节点替代局域网的工作站点。在监控现场中安装网络节点，并把网络节点、多种传感器、控制装置连接起来。Lonworks 的通信协议是 Lontalk，这一协议固化在芯片内，可以支持 OSI 参考模型，也可以使简洁的控制信息比较可靠的传输。

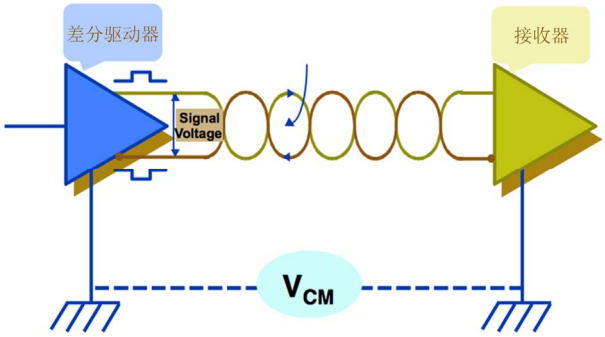

Figure 1. RS-232 bus signal transmission diagram
图 1. RS-232 总线信号传输图

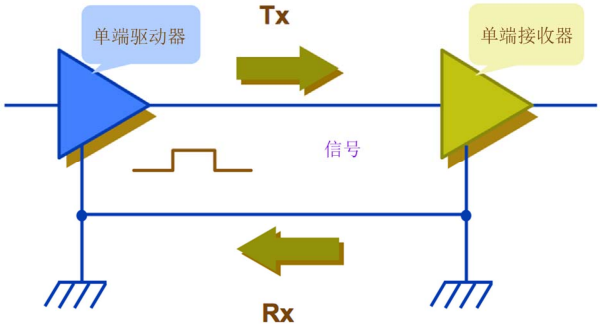

Figure 2. RS-485 bus signal transmission diagram
图 2. RS-485 总线信号传输图

新型现场 Canbus 总线是德国公司最初为汽车控制检测而设计出来的，后来它渐渐地发展到控制中来。Canbus 总线是一种抗干扰性强而且能够见错的新型现场总线。它可以采用光缆、双绞线等各种媒体通信，其设备造价相对低廉，这使得它的应用范围广泛，几乎遍及所有工业领域，电气自动化产业应用的特别多。Canbus 总线的技术特性主要有以下几点：多主方式工作，网络中任一节点可以随时向其余节点传输信息，不分主从，实现非常灵活的传输信息；节点可以划分为不一样的优先级，满足多样实时需要；可以一点对一点、成组全局广播等多种方式互相传输数据。

以上几种总线的优缺点比较如下：

1) RS-232 具有通信距离短，传输速度快的优点，但是在通信网络中，只存在一个主要节点，这就造成了系统的可靠程度比较低，末端节点只有接收到主节点传输过来的命令后，才会依据命令做出反应，导致

在传送重要通信信息时，无法做到高效灵活。

2) Lonworks 的通信协议对系统的综合程度要求比较高，导致系统整体构建费用高，网络的扩展灵活性比较差。

3) Canbus 总线系统结构优于 Lonwork，整体的结构精简，灵活可靠性高，具有很好的扩展性能。

2.2. 智能变电站通信技术

1) 光纤通信技术

目前，随着光纤通信技术已经成熟，光纤通信在电力系统中迅速得到应用，已经发展成为电力通信主要的传输方式。这种通信方式的信息承载体是光波，利用光波在光导纤维中反射，将信号有效地传输到远方。光线通信优点如下：

光波的频带比较宽，因此在信号中可以加载的信息量可以很大；

光纤通信依靠光波在光导纤维中的反射来传输信号，光波在反射中的损耗很小，因此可以跨越很大距离进行传输信号；

通信载体之一为光导纤维，体积和重量相比较传统的信号传送方式，可以方便利用现有的电力杆塔进行铺设；

通信传输的两端通过光纤连接，可以很好的实现电气隔离，信号两端的电气量不会产生干扰；

光导纤维的一体性可以实现传输信号的完整性，传输过程中不会有信号的泄漏和外来信号干扰；

光导纤维的防腐性能利于深埋地下，利用年限较长，免于经常性的维护保养；

光纤通信的缺点：光导纤维的强度没有传统信息传输下的金属导体大，相对于金属导体连接，在进行线路分接时，操作难度大，而且由于材质所限，光导纤维需要的弯曲半径比较大。

2) 现场总线信息通信技术

现场总线的传输媒介主要依靠双绞线，是一种用于生产现场的微机测量设备间的底层控制数字通信方式。现场总线具有以下优点：

a) 通信标准的一致性，决定了整体信息通信系统具有良好的开放性：

b) 设备之间兼容性好，即使是不同厂家的设备也能实现相互操作，实现数据的共享：

c) 现场总线能根据现场环境做出调整，具有很好的环境适应性；

现场总线的缺点：现场总线的结构分散程度高，不利于设备的集中维护。

3) 无线通信技术

无限扩频通信：具有建设方便、信息抗干扰性强、投资低的特点。

无线传输电台：利用无线数据传送电台进行远方监测数据的传送。

4) 其他方式的通信技术

利用卫星通信方式，根据全球定位系统来进行通信系统时间的标定。

2.3. 智能变电站网络通信协议

变电站综合自动化系统在基于 IEC61850 标准下有着这些特点：具有状态化的设备检修状态化、分布化的系统分层结构、具有在标准化下的信息系统建模模式、采用网络化这样的通信信息交互模式、具有信息化的采集数据模式、应用信息系统采用集成化的模式、比较紧凑的系统结构、智能化的操作设备方式这些特点[3]。基于 IEC6180 标准的变电站综合自动化系统为一次智能化系统、二次信息化设备的综合[4]。IEC61850 标准的大量应用与不断推广，直接带来了变电站二次设备的越来越高的网络化。和常用的计算机网络不同，对于网络的安全性而言，这也对变电站综合自动化系统的通信网络提出了特定的要求。

IEC61850 标准，即“变电站通信网络和系统”，此标准的最终目标是通过设立标准来达到变电站不同制造厂商的设备能够相互读取与沟通，提高效率，在此基础上，更进一步实现高层次功能的相互操作[5]。IEC61850 标准有这些特性:通信协议集是完全基于现在存在的标准包括有这些通信标准：IEC 通信标准、IEEE 通信标准、ISO 通信标准及 OSI 通信标准。几乎囊括了世界绝大多数设备制造厂商的 SAS，以及设备模型，与此同时对设备模型的扩展方法也重新进行了阐释；对设备模型进行扩展分解，尽可能的对模型的重用功能进行支持；而且也能对设备所支持的其他电气设备进行说明，提供了以后对功能、结构升级的能力；也阐述了通信语法以及语义在电力系统中应用的具体情况；将协议的上层、下层进行分离，上下层可

以映射出不同的协议，因此能够在最大范围内节省成本；标准认为变电站综合自动化系统是整个电力系统控制网络的一个节点。

IEC61850 标准对变电站综合自动化系统的 ASCI 自动化系统的信息交换的方式、信息通信的模型、SCSM 通信服务的映射、变电站 IED 的配置方式这这些方面也进行了详细阐释。由于这四个层面之间有较好的分离性，独立性强，因此变电站综合自动化系统的这四个层面能够有很好的扩展性。

3. 变电站通信网络的安全威胁

智能变电站的安全性，对于网络通信信息而言，有以下几点要求：不可否认的信息、完整的信息、保密性的信息、可用的信息。

1) 不可否认的信息：是指合法用户不能否认自己在网络中的行为。每一项在系统中的操作都留有痕迹、能够记录下具有各种属性的操作，这样做就可以为审查保留有一定时限的信息。一旦有否认的情况发生，将会依照抗否认的机制裁决操作，通过这样的方式，可以最大程度的防止因为由于操作发生是故事，操作者否认该操作，推卸责任。

2) 完整的信息：已经在变电站通信系统中存储或者是正在网络中传输的数据信息不接受以何种方式进行的数据非法删除、数据重发、数据修改，而且能根据标识准确判断是否已经发生了数据不授权的操作。

3) 保密性的信息：在通信系统中能够对交换的报文或者操作步骤进行识别，判断信息的合法性，已达到保证重要信息不泄露的目的。

4) 可用的信息：授权操作的合法用户能够在授权范围内控制行为方式与数据流动，比如可以对通信协议进行选择，选择合适的报文始发站来发送信息。

外部网络连接在变电站网络上，这样一来就成为了变电站网络安全所受到的主要威胁[6]。外部网络对于变电站网络所都成的安全威胁只要两者的连接存在，这样的威胁都会存在，不会因为变电站网络与外部网络的组网形式不同而不存在。外部网络构成的威胁存在以下几个方面：

对正常情况下网络中传输的通信过程进行中断破坏，这样也就对远方控制中心和变电站之间或者是变电站网络的通信服务受到外在的非法破坏，这样将会使远方控制中心对变电站的运行工作状态失去有效的监控和控制，与此同时，网络传输数据遭到破坏，远方控制中心对变电站的控制也就失去了联系。

通过伪造网络中的通信信息这样的形式，将不合法的数据，进行外壳伪装后，通过变电站内部的网络，把信息传送到针对的特定智能设备，这种形式的安全威胁从内部网络上对网络中传输的信息造成了很大程度的破坏。

非法访问未授权的信息，要实现这样的途径，主要靠非法冒充“管理员”从而得到正常情况下的管理员权限，这样也就能够对变电站中的一些比较关键的变电站机密信息进行浏览访问，根本上而言，这样的非法操作破坏了网络通信数据保密性，但是同样的是不会给实时通信信息的传输带来很大破坏性，只会对信息的保密性带来一定的影响。

对正常网络中心的信息进行截获，以非法的形式对远方控制中心和变电站传输数据，或者变电站内部网络的数据进行获取操作，以非法的形式占有变电站信息通信网络中的数据。一般来说认为进行信息截获不会给实时通信信息的传输带来很大破坏性，只会对信息的保密性带来一定的影响，可是变电站综合自动化信息通信网络的破坏，首先就是在网络中发生了传输的数据受到外部网络非法截取这种现象，这样的网络信息失窃是信息安全失败关键的一步[7]。由此可见，正常的通信信息避免遭受外部网络的截取也就显得非常重要。

非法更改远方控制中心和变电站之间、变电站网络的通信服务在网络中传输的通信信息，采取的方式是通过非法变更服务命令，改变正常传输的服务信息，变电站无法从远方控制中心得获取合法有效服务命令，这样以来就对变电站的正常运行工作状况造成了破坏[8]。

以非法的形式，从外部网络接入到变电站信息通信系统中，通过发送服务命令的形式，对变电站设备进行非法操作造成事故后却不会对操作做出操作回应，不承认对电力网络的破坏。

从外部网络侵入到变电站内部的网络，在网络的通信端口处发送大量的垃圾数据，阻塞网络，从而造成信息通信网络整体或者局部 IED 设备的瘫痪，对变

电站正常的运行工况造成破坏。

4. 安全威胁产生的机理分析

非法数据在远方控制中心和变电站之间或者在变电站网络中传输对正常网络中的通信服务产生了安全威胁。正常情况下，以报文形式进行网络中服务信息的传递，将服务信息打包成报文进行报文数据下的传输，通过网络媒介，信息传送所送达的 IED 设备，这一个过程可以划分为好几个传输阶段，只有对网络协议进行深入的研究，才能都了解所受到的安全威胁的原因。

通过攻击信息通信网络的网络薄弱点，造成运行中安全事故的发生以及可能带来的事故影响等一系列对通信系统信息安全性带来的不确定影响，这就是信息通信系统网络安全问题。ISO13335 国际标准提出了信息安全风险模型，如图 3。

4.1. 变电站系统安全管理的现状和面临的主要问题

我国电网规模目前已经进入到了大力发展特高压、大机组、大容量电源的时代。智能化水平也越来越高，变电站是电力系统输电和配电过程中电力的集结点，连接不同电压等级的电力网，起着变换电压等级，稳定电网电压的重要作用。

变电站的作用决定了它的安全管理运行有着重要意义。在目前值班员参与变电站的管理过程中，工作主要可以分为以下截然不同的两大类工作：一种是要求工作人员要具备专业性强的专业操作技能，如相关电气设备的手动合闸、倒闸等操作。另外一种是相对专业技术要求不是很高，但是相对繁琐的工作，如设备的日常维护保养等工作，但是一旦这类工作处理得不好，也容易造成变电站不能安全稳定运行。

4.2. 变电站运行管理制度问题

当前，随着技术的发展，越来越多的变电站转变成智能变电站，相应的安全管理模式也发生了变化。原先分散在各个变电站的变电站运行维护任务，如变电站的控制操作，视频监控等工作任务，开始集中到了远端枢纽变电站或远方控制中心进行集中控制。目前，智能变电站中的值班工作主要有以下两部分内容：

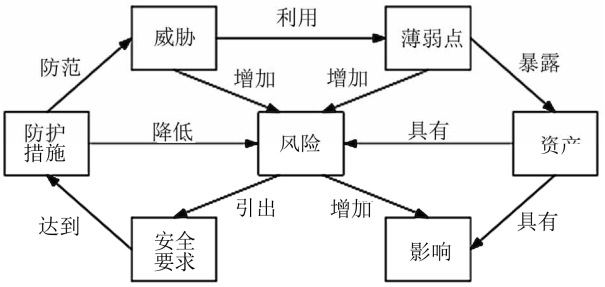

Figure 3. Safety risk model based on ISO13335
图 3. ISO13335 标准下安全风险模型

1) 进行变电站电气设备、通信设备的监控，数据记录工作，这部分工作由运行值班员远程操作就能实现；

2) 变电站巡视，对电气设备进行维护，做好设备的安全防护措施，以及发生事故后能快速消除故障，这部分工作由变电站操作班来实现[9]。

当前，智能变电站运行管理模式有了新的变化，根据以往变电站运行调度的制度和经验，考虑远方监控中心等因素，应当进一步完善变电站的运行管理制度。对于值班人员，对变电站的关键设备，电气一次设备、二次设备、变电站通信设备进行专人操作维护，做好操作日志记录，各项文档手续应当记录清楚，按照操作票严格执行操作[10]。值得注意的是要建立强有力的变电站通信系统来保证远方信息交流的畅通，在操作异常时能及时上报远方控制中心，依据指令做出反应。

5. 结论

智能变电站实际运行维护中，信息系统的薄弱点将通信信息暴露给了安全威胁，网络安全威胁利用掌握的薄弱点信息，通过攻击网络薄弱点，给通信系统信息安全性带来不确定影响，这样就给系统的安全带来了风险影响。这就是当前智能变电站信息通信系统网络面临的主要安全问题。通过进一步的风险影响分析，对整个变电站系统专用网络进行安全升级改造，通过采取针对性的系统威胁防范措施，可以达到智能变电站通信系统的安全。

参考文献 (References)

[1] 刘振亚. 智能电网知识读本[M]. 北京: 中国电力出版社, 2010.

[2] 杨文征. 数字化变电站信息安全及网络可靠性研究[D]. 浙江大学电气工程学院, 2007.
[3] 吴在军, 胡敏强. 基于IEC61850标准的变电站自动化系统研究[J]. 电网技术, 2003, 10(10): 61-65.
[4] ITU-T Recommendation X.509 [ISO/IEC 9594-8: Information Technology-Open Systems Interconnection, The Directory: Public-Key and Attribute Certificate Frameworks, 2001.
[5] IEC Std 61850-1, Communication networks and systems in substations—Part 1: thentication. ACM Transaction on Computer Systems, 1990, 25(3): 1-13.
[6] 冯登国. 国内外信息安全研究现状及其发展趋势[J]. 网络安全技术与应用, 2001, 1(1): 8-13.
[7] ISO/IEC-2008. ISO/IEC TR 13335: Guidelines for the management of IT security.
[8] 董玉格, 金海, 赵振. 攻击与防护网络安全与实用防护技术[M]. 北京: 人民邮电出版社, 2002.
[9] 严剑生. 变电运行中的安全问题与应对方法[J]. 中国高新技术企业, 2008, 24: 198.
[10] 胡炎, 董名垂, 韩英铎. 电力工业信息安全的思考[J]. 电力系统自动化, 2002, 26(7): 1-4.

