电力系统通信技术中的信息安全及应用

张金宸

国网陕西西咸新区供电公司　陕西　西咸新区　712000

[摘　要]近年来电力建设加快了自身发展的速度，通信信息安全对电力系统的安全可靠运行影响重大，进而影响电网安全，因此对电力系统通信技术中的信息安全有了更高的要求。鉴于此，本文将对电力系统通信技术中的信息安全及应用进行简要的探讨。

[关键词]电力系统；通信技术；信息安全

【DOI】10.12252/j.issn.2096-627X.2021.10.306

1 电力通信的特点

1.1灵活度强可靠性高

电力工作的核心就是保证电力系统的正常运转，电力通信系统有着极高的可靠性，它能对突发情况及时地做出应对，这也是电力系统的灵活性。

1.2具有实时性

电力通信系统的信息传送量较少，但它的信息传播是多种途径的，它是具有较强的实时性的。

1.3具有紧急备用手段

比如：电力系统出现意外发生故障导致电厂的电力设备、网络通信、电力监测信号等系统出现问题，电力通信系统可以对突发问题的出现进行风险抵御。当遇到自然灾害时，同样可以利用紧急备用手段。

1.4系统网络复杂

电力通信系统具有很多复杂的接口与不同通信系统进行连接，连接过程十分复杂，这种复杂的通信模式也在工作的过程中带来了不便。

1.5电力通信点分散

电力通信除电力总局外其他区域的发电厂，电力所同样属于电力通信中的一部分。变电站本身是建立在偏远地区的与维护场所距离较远，因此对维修的进行带来了很大麻烦。

2 常见的电力通信技术

2.1电力线载波

电力线载波通信是利用电力系统现有的高压线路（35kV及以上）、中压线路（10kV）或低压线路（380/220V）作为介质进行信息传输的通信方式。这种通信方式具有投资少、施工期短、设备简单、通信安全、实时性好等多种好处，因此在电力系统调度通信、配网自动化数据传输等方面得到广泛地使用。

2.2微波中继通信

微波中继通信是指使用特定波长的电磁波实现远距离通信的手段，它不需要借用任何固态介质，但为了增加通信距离，必须在通信两端构建多个中继站，从而实现电磁波的转接，微波中继通信利用率频率较高的有微波频带宽、中继传输方式、天线增益高、外界干扰小、通信灵活性大、投资见效快等优点。近年来，5G作为现阶段移动通信的代表，与大数据、AI技术紧密结合后开启了全新的万物互联时代，对传统电力系统通信技术提出更高的要求，需要转变原有作业方式与运营方式，突破微波中继通信地束缚，以此满足5G网络20Gbit/s峰值速率的需求，实现应用场景的多样化。

2.3光纤通信技术

光纤通信技术大规模投入使用已经有数十年时间，该技术也历经几代变革，它利用光波作为通信手段，用光纤传送信息，具有很强的通信能力，而且能够实现高质量的通信，且具有抗电磁干扰能力强、传输容量大、频带宽、传输衰耗小等优点，它一问世便在电力部门得到应用并迅速发展。

3 提升信息安全的措施

3.1明确划分好网络安全区域

网络安全区域划分主要是从网络信息的基本性能、承载对象以及网络安全对象的角度出发，将网络信息分成多个逻辑子网，通过此种方式，在同一个逻辑子网络中，可以使用相应的安全访问手段，不仅可以实现对边界控制，同时还能够加强对不同逻辑子网访问的监督管理工作。利用此种方式，可以达到以下目的：第一，通过将复杂的信息系统安全问题，转变成为一些小区域的安全问题，可以降低系统安全隐患。第二，充分发挥安全域划分技术，可以更好地理顺网络，做好地信息指导系统的规划、设计以及联网验收等工作。第三，确定安全区域的保护重点，利用有限的信息设备，充分保护系统信息资产，确保设备的有效性。第四，优化信息安全的运行管理工作，科学合理地规划安全审计设备，为信息检查和审核提供良好的依据。

3.2采用虚拟专网（VPN）技术

虚拟专网是指采用隧道技术以及加密、身份认证等方法，在公共网络上搭建专用的虚拟网络，使数据通过安全的“加密隧道”在公共网络中传输。虚拟专网虽然属于临时链接，但是其具备较高的安全性以及访问控制功能，可以对数据进行加密，也可以阻止入侵者访问网络，大大提升网络的安全性。有效应用虚拟专网技术还可使用户和企业通过公共的互联网络，连接到远程服务器和网络，或作用于多个企业之间，同时保护通信的安全。

3.3通过数字证书执行相关操作

安全系统的设计需要使用一个计算机化的证书服务器，配置证书发件人，以便其他用户可以向证书发件人申请证书确定。进入系统进行某一特定操作的用户需要严格的加密认证，才能操作一个重要的服务器或访问数据，安全系统首先核实用户的身份，并核查用户是否是通过签发人签发证书的用户，然后用户的相关操作请求被发送到服务器，并通过用户证书发送给用户。在用私人钥匙签署证书之后，服务器还核查签字证书，确认证书是合法的，从证书中撤销公用钥匙，核证用户证书的签字，并在用户身份确定之后，才可访问该网页进行相关的操作。

3.4实现数字签名认证

为加强电力网络系统平台的安全，需要在数字证书用户身份认证技术的基础上，对电子文件数据进行数字签名，这将在一定程度上确保信息的完整性，并确认数据的真实性，防止数据受到否定和伪造。首先，发送方用HASH函数从明文文件中生成一个数字[摘　要]，用自己的私钥对这个数字[摘要]进行加密形成发送方的数字签名；选择一个对称密钥对文件加密，然后发送到接收方，最后将该数字签名作为附件和报文密文一起传输给接收方；再用接收方的公钥加密对称密钥，并通过网络将加密后的对称密钥传输到接收方。最后通过数据[摘　要]的比较对数据签名进行验证。通过此种方式，可以保障验证签署工作的有效性，一旦系统确定签名有效，则可以自动从签名者的证书中找到公钥，从而去验证被HASH函数作用的数据内容，如果内容匹配，最终返回验证成功值。

4 结束语

随着信息科学和技术的迅速发展，各种通信技术的应用得到广泛传播，信息技术在电力企业的应用大大促进了电力系统运营方面的工作，但也给“电网”与“通信网”的联合运作带来诸多潜在的风险。信息安全正在逐渐成为电力公司面临的一个重要问题，严重制约着业务发展和电力正常供应。因此，加强电力系统中的信息安全保障对企业发展有着积极的贡献。

参考文献

[1]李白.研究光纤通信技术在电力系统调度自动化中的应用[J].城市建设理论研究：电子版，2020（11）：6.

[2]黄繁.研究光纤通信技术在电力系统调度自动化中的应用[J].建材与装饰，2020（9）：218-219.