继电保护设备通信安全的研究

摘要：在数字化和网络化高速发展的今天，电力系统面临着各种网络安全威胁，黑客攻击事件在全球范围内时有发生，继电保护设备的通信安全至关重要。本文将对继电保护设备的通信安全进行分析，同时介绍为保障继电保护设备通信安全所需的配置和管理措施。

关键词：电力系统；通信安全；网络安全；威胁；攻击；防范；

0 引言

电力系统内各种设备通过各类通信协议实现互联，使系统的运营和维护更加便捷，系统运营者足不出户便能快速获取系统运行数据和设备状态等信息。但通信给运营者带来便利的同时也暴露了更大的攻击面，带来了更多的安全风险。继电保护设备作为电力系统关键设备，在保障电力系统安全运营过程中起到了至关重要的作用。保证继电保护设备的通信安全，免受网络攻击，关乎着整个电力系统的安全。

1 电力系统的网络安全威胁

近年来各国电力系统遭黑客攻击的事件频繁发生，远到 2010 年的伊朗核电站震网攻击，2015 年的乌克兰大停电，近到 2019 年以来的相继发生的委内瑞拉停电事件，阿根廷停电事件，纽约停电事件等等。针对电力系统这样的关键基础设施的网络攻击事件，真实而频繁地在全球各地发生着。2019 年，我国暴露在互联网上的工业设备 7325 套，其中电力、石油天然气、医疗健康、煤炭、城市轨道交通等重点行业暴露的联网系统 2249 套，其中存在高危漏洞的联网系统占比约 46.1%，见图 1。电力系统内发现了 653 个安全漏洞，其中有 62 个高危漏洞。这些漏洞一旦被不法分子利用，电力系统设备将处于危险的境地，继电保护设备的保护功能有可能失效，电力系统的安全运行将受到挑战，国家安全和人民的生产生活将受到严重的威胁。因此保证继保设备及电力系统的安全，对保障国泰民安至关重要。

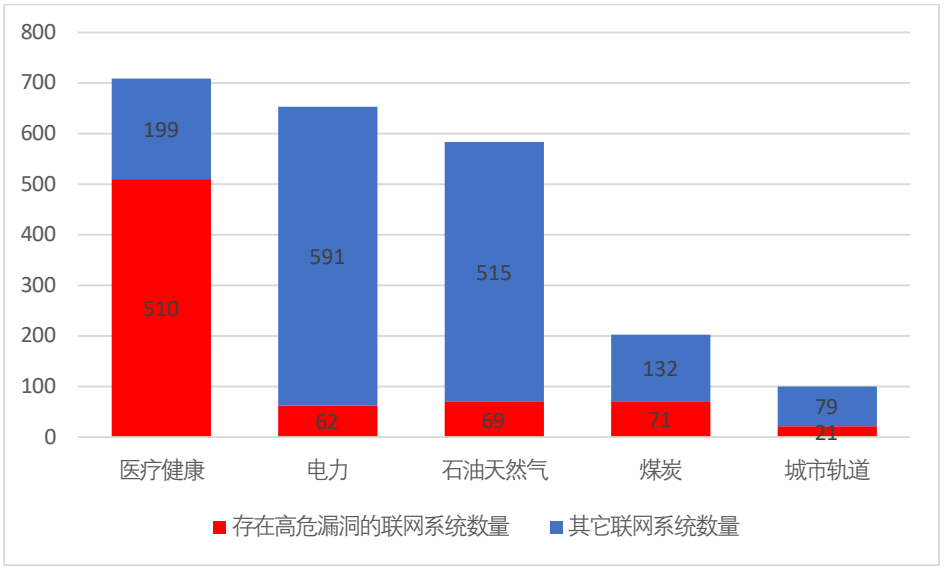

图 1 2019 年我国重点行业联网系统漏洞威胁统计

2 电力系统整体安全框架

电力系统的安全是建立在安全框架基础之上的，见图 2。电力系统通过网络安全设备，如路由器，防火墙，网络隔离设备等，划分为若干区域。并在不同区域部署相应的网络安全防护措施，如防病毒软件，安全审计系统，安全防护系统等，保证各区域的安全稳定运行，从而保证整个电力系统的安全运行。但安全框架下的电力系统也并非无懈可击，随着科技的发展，黑客的攻击手段层出不穷，任何安全漏洞都有可能被利用，设备安全绝不能掉以轻心。

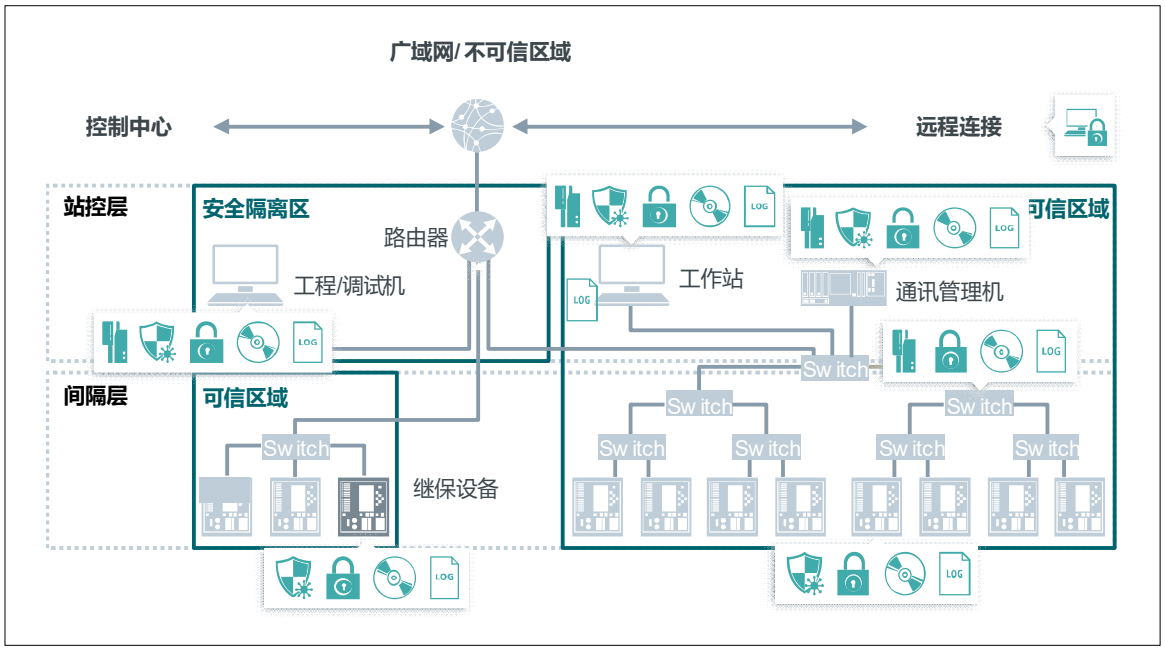

图 2 电力系统整体安全框架

3 继电保护设备的通信安全

继电保护设备是电力系统的重要组成部分，对于保障电力系统安全、可靠运行发挥着极为重要的作用，继电保护设备的通信安全直接关系着该设备乃至整个系统的安全。目前继电保护设备通信方面的安全漏洞和威胁主要包括：敏感信息明文传输带来的信息泄露，非授权用户的非法控制和拒绝服务攻击等。针对这些安全漏洞和威胁，继电保护设备可通过对敏感信息和通信报文加密、认证身份、提高通信性能等方式来保证设备的安全、可靠运行。

3.1 敏感信息和通信报文加密。继电保护设备的敏感信息包括用户名，密码，控制命令以及保护配置等。攻击者可以通过窃听网络报文，窃取明文传输的敏感信息，并通过报文回放或伪造报文等方式伪造或篡改控制命令，修改保护配置，导致继电保护设备据动或误动，从而达到破坏电力系统正常运行的不法目的。继电保护设备可以通过对敏感信息进行加密，并对网络传输的报

文进行加密，来保证传输过程的安全和敏感信息的保护，防范敏感信息的泄露，攻击者即使侵入了电力系统内也不能窃取任何敏感信息。

3.2 身份认证机制。继电保护设备一般采用标准通信协议实现与主站或后台的通信，如 IEC-61850，IEC60870-5-104 等。不同厂家的设备和后台，只要采用了标准的通信协议，便可建立通信连接，实现数据传输和远程控制功能，这大大提高了电力系统的互联性。但同时也大大降低了网络攻击的难度，攻击者一旦进入电力系统局域网内，便可以通过电力协议软件对继电保护设备发送非法控制命令。继电保护设备可以通过应用层和传输层身份认证机制，来保证的安全，继电保护设备和后台在建立通信连接时需验证对端证书，只有持有合法证书的后台才能与 继电保护设备建立连接，不能提供合法证书的连接请求将被继电保护设备拒绝。此证书由运营者认可的机构签发，运营者妥善存储。攻击者无法获取合法证书，将无法连接继电保护设备，不能对对继电保护设备实施非法控制。继保设备可根据国际标准 IEC62351 或我国国标 GB/Z 25320 系列标准，实现电力通信协议的加密和通讯双方的身份认证。我国在 2019 年发布的《信息安全技术 网络安全等级保护基本要求》标准中，对三级及以上的保护对象有明确的通信加密和通信双方身份认证的要求。

3.3 通信性能满足业务高峰期需要。攻击者通过制造网络风暴、高频的重复请求、发送畸形报文等方式，对继电保护设备进行 DOS 攻击，使继电保护设备无法提供正常保护功能、逻辑错误甚至系统崩溃，从而破坏电力系统安全运营。继电保护设备的通信能力需满足电力系统业务高峰期的需要，当继电保护设备的网络负载过高时，继电保护设备的保护功能应不受影响，网络负载恢复正常后，继电保护设备应恢复正常通信。对高频的重复请求，继电保护设备应当根据电力系统应用，合理拒绝。对各类异常或畸形报文，继电保护设备应能正确处理或丢弃，保证通信正常运行。

4 继电保护设备的安全配置和管理

保证继电保护设备的通信安全，除了要具备通信安全相关的功能和性能外，还需要对其进行合理的配置和管理。

- 保证机电保护设备的物理访问安全，使继电保护设备免受物理破坏和非法操作。
- 关闭继电保护设备所有不必要的网络端口和服务，把暴露给攻击者的攻击面和可能性降到最低。
- 选用适当的网络设备，如防火墙，隔离设备等，对电力系统内的设备进行合理的分区和隔离。
- 继电保护设备应对重要网络通信事件进行记录并保存，并根据需要提供报警。
- 即时安装安全升级补丁，确保继电保护设备免受对已知安全漏洞的攻击。
- 在电力系统内部署适当的防病毒软件、配置合理的应用程序白名单或软件签名，确保系统免受恶意软件的攻击。

5 结束语

继电保护设备的通信安全对保证电力系统安全运行至关重要，继电保护设备供应商应当不断紧跟科技发展步伐，研发和生产更安全、高性能的继电保护设备。运营商和系统集成商应当制定更安全的解决方案，实施更有效的安全防护策略。各方共同努力方能建立更坚强的电力系统。

参考文献

[1]. 国家计算机网络应急技术处理协调中心， 2019 年我国互联网网络安全态势综述，2020： 40-41