水电厂电力监控系统安全防护策略浅析

刘 海 波
（四川久隆水电开发有限公司，四川 成都 610041）

摘　要：随着计算机技术和互联网技术的发展，网络信息技术已在电力行业中得到普及；任何事物的发展都具有两面性，信息技术的发展尤为如此，新技术的应用在提升行业发展的同时，也带来不小的负面影响。电力行业作为关系民生的基础工业，必须采取有效的应对措施与策略防范相关网络与信息安全事件的发生，阐述了水电厂监控系统安全防护策略。

关键词：信息安全；计算机网络；安全防护；水电厂
中图分类号：TV7；TV737；TV513　　**文献标识码**：B　　**文章编号**：1001-2184(2018)增 2-0066-02

1　概　述

网络信息技术与电力生产深度融合发展起来的 ICS(Industrial Control System，ICS)工业控制系统，为电力生产提供了精准、实时的现场控制，也为电力营销带来了便捷、高效的策略管理。但工业控制系统越来越多的采用通用的标准协议、硬件和软件，以各种方式与公共网络连接，病毒、木马等威胁正在向 ICS 扩散，导致 ICS 系统安全问题日益突出。2010 年爆发的“震网”病毒事件和 2017 年爆发的“勒索”病毒事件均对工业控制系统进行了攻击，对基础设施进行了不同程度的破坏，充分反映出 ICS 系统安全面临严峻的形势。据权威工业安全事件信息库(RISI)统计，截至 2011 年 10 月，全球已发生 200 余起针对 ICS 的攻击事件，并有大幅度增长的趋势。

我国工控领域的安全可靠性亦问题突出，工控系统的复杂化、IT 化和通用化加剧了安全隐患的发生。比如 2010 年齐鲁石化、2011 年大庆石油炼油厂某控制系统感染 Conficker 病毒而导致 ICS 系统不同程度中断。因此，各行业在进行信息化建设的同时，迫切需要同步建设对 ICS 安全防护的防御体系。

2　电力行业工控信息系统结构

常见的电力 ICS 包括分布式控制系统(DCS)、数据采集与监控系统(SCADA)、可编程逻辑控制区(PLC)、远程测控单元(RTU)等部分。电力行业的 ICS 已发展到第四代 SCADA，普遍采用计算机监控系统，结合现地 PLC 的开放系统。典型的 ICS 包括一个或多个控制回路、传感器、现地 PLC、上位机监控系统、人机交互以及系统对外接口等，其主要网络结构见图 1。

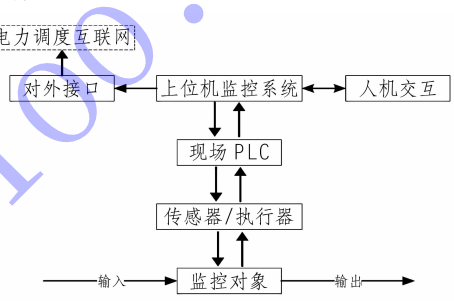

图 1　电力系统 ICS 运行示意图

通常的控制回路由传感器(或变送器)、执行器、现地 PLC 及监控对象组成。其中传感器采集现场工控对象的状态信息并传送给现地 PLC；现地 PLC 对传感器采集的工控对象状态信息(输入变量)进行解析，并根据预定的控制目标产生相应的执行变量发送给执行器；执行器则负责对应的控制操作。

上位机监控系统由负责与现地 PLC 通信的本地主机、负责系统监控运行的服务器、存储系统监控历史记录的数据库及对外通信的网关机组成。

人机交互是操作员或工程师与 SCADA 进行信息交互的接口，操作员或工程师可以通过人机交互界面监控和配置控制对象、控制参数，还可以用于显示系统状态信息和历史信息。

对外接口用于同其他业务系统之间的信息交互。

3　电力行业工控系统面临的安全威胁

收稿日期：2018-03-26

3.1　威胁来源

电力行业工控系统的信息安全问题主要源自外部威胁和自身漏洞。外部威胁有多种来源,包括敌对政府、恐怖主义、恶意入侵、偶然事件、内部人员的恶意行为、自然灾害和设备故障等。自身漏洞包括策略和程序上的漏洞,协议、软硬件和防护软件的缺陷,配置或维护中的漏洞。

3.2　威胁入口

从图 1 中可以看出,对电力工控系统具有威胁的入口包含在各个信息流转的环节之中,纵向的连接缺陷和系统交互接口、横向系统之间的信息交互接口以及人机交互接口。除了接入系统的直接威胁外,工控系统的通用协议缺陷亦成为威胁的重要漏洞。

3.3　原因分析

(1)我国现行的电力 ICS 的设计基于优先确保系统的高可用性和业务的连续性,而对安全性普遍考虑不足,缺乏足够强度的认证、加密、授权等防御和数据通信保密措施,通信协议存在造成远程攻击、越权执行的漏洞。

(2)国外的工控设备占据 ICS 的主导地位,如 PLC、卫星导航芯片,存在一定的安全风险。

(3)缺乏足够的安全管理制度和技术,操作人员安全意识不足,社会工程学相关的定向钓鱼攻击可能使重要岗位的人员成为外部威胁的入侵跳板。

4　电力行业工控系统的安全防护

4.1　安全防护策略模型

为了保障工控系统安全可靠地运行,我们可以从管理、操作、技术等方面进行控制,建立较为完整的安全架构。目前应用较广的是基于安全策略的安全防护框架 P2DR2,其模型见图 2。

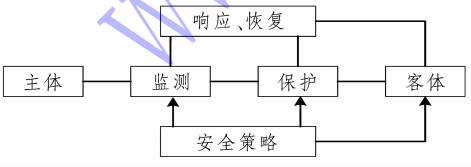

图 2　P2DR2 安全模型示意图

该模型通过时间计算对防护能力进行考量,计算方式为:

$$Pt > Dt + Rt \qquad (1)$$

式中　Pt 为防护时间;Dt 为检测话费时间;Rt 为防护体系将系统恢复到正常状态的响应时间。

当针对保护的安全目标满足数学公式(1)时,视为达到安全防护目标。当 $Pt=0$,假设 Et 为系统暴露给入侵者的时间,则有:$Et = Dt + Rt$。

从该安全模型示意图及公式中可以看出,该安全模型着重对系统安全检测、响应和恢复,强调对系统的防护能力。

对于管理控制方面,依据 P2DR2 模型建立基于安全策略的防护、检测、响应、恢复联动机制;操作控制方面主要从人员安全、物理和环境安全、意外防范、配置管理、维护、事件响应、意识和培训等方面进行规避;技术控制主要用于 ICS 的安全措施,主要通过身份识别认证、访问控制、审计和通信数据的保护构建系统自身的安全防护体系。

4.2　安全技术措施

安全技术措施包含深层防御架构策略(纵深区域防护和横向边界防御),通过部署防火墙、逻辑分离控制网络、网络物理隔离(除防火墙外其他任何设备不能配置成双宿主机)、入侵检测、反病毒等安全措施并做好单点故障预防,采用安全审计、功能冗余和主机故障容错策略予以实现。

4.3　安全管理措施

根据国家和行业的相关规定,制定相应的管理制度,强化并落实安全防护责任;开展信息安全教育培训,提高全员的安全意识,消除内部人员带来的安全威胁;及时对系统及相关软件进行漏洞修复,及时更新杀毒软件及防火墙的病毒特征库,提升系统抵御外部攻击的能力。

5　结　语

安全是相对的。电力系统中的安全风险与隐患将长期伴随着行业的发展,任何一个安全防御方案都不可能一次性解决所有的安全问题,其终有被攻破的时候。工控系统的安全防护是长期不断探索的过程,只有依靠足够长的防护时间,通过较小的检测和响应时间来达到电力系统安全稳定运行的目的。安全防护不是静态的,新的安全防护系统也会被攻破,同时,更缜密的安全防护体系将不断出现。只有通过采用先进的管理和技术手段,跟踪最新的防御体系和防护技术,才能最大程度地保障电力工控系统的安全可控运行。

作者简介:

刘海波(1983-),男,四川广安人,工程师,学士,从事水电站信息与通信技术工作.

(责任编辑:李燕辉)