电力监控系统网络安全防护

张怡迪[1] 姚亮[2] 张玉琼[3] 王品卓[4]
国网河南省电力公司洛阳供电公司

[摘 要]在互联网与信息技术日益普及的背景下，电力监控系统近年来常常受到网络攻击，采取有效措施将网络安全防范能力增强，现已成为电力监控系统急需解决的问题。工业控制系统主要包括集散控制系统（DCS）、数据采集与监视控制系统（SCADA）和可编程控制器（PLC）等，已广泛应用于国内重大的基础设施中，在工厂运行中发挥着巨大的作用。本文主要对电力监控系统网络安全防护做论述，详情如下。

[关键词]电力监控系统；网络安全防护
【DOI】10.12252/j.issn.2096-6288.2021.12.024

引言

随着信息时代的来临，人民的生活和生产都会产生大量的数据信息，尤其是对于企业生产而言，如果无法保障信息安全。将会造成严重的不良后果。电力监控系统包含电能生产、传输和使用等过程，可避免数据丢失，保障数据安全运行，为电力系统安全运行提供保障，也为电力工业的发展提供重要支持。电力监测系统是一种集视觉、红外和声音传感器于一体，可以对电力设备的热缺陷、断电状态和异常现象进行监测的系统。电力系统的安全保护仍是电力企业关注的重点问题，为解决现有电力监控系统涉密检测不及时、不准确的问题，采用云计算访问控制技术来提升检测正确率和检测效率。

1.电力监控系统安全现状

电力监控系统工控安全的脆弱性是指工控系统在防护措施中和在缺少防护措施时系统所具有的弱点，而工控系统内部的脆弱性问题是导致系统易受攻击的主要因素，脆弱性问题的根源可概括为以下几个方面：（1）网络结构：无法保证外网接入安全，保证对主机和应用系统资源的合法使用和用户身份的合法性。通常电厂会在DCS系统网络和外部网络之间设立一个DMZ区，使连接尽可能最小化。（2）区域边界：现场控制层与监控层之间存在安全威胁互侵。缺乏边界保护，容易受到信息网络和相邻系统的安全影响。（3）通信网络：按照《国家电网公司关于加快推进电力监控系统网络安全管理平台建设的通知》的要求，在电力生产系统I区和II区中部署网络安全监测装置，对电气网中的服务器、工作站网络设备安全防护等监测进行数据采集和分析，但未对发电监控系统进行监控，无法及时发现网络中的各种违规以及入侵攻击行为，无法溯源入侵的未知设备、非法应用和软件。（4）终端设备：生产控制系统和生产监控系统的操作终端大部分采用Linux和Windows系列的操作系统，为保证过程控制系统的相对独立性，同时考虑到系统的稳定运行，通常现场工程师、操作员等在系统开车后不会安装任何补丁，部分终端同时安装多种防病毒软件，上位机专用编程组态监控软件与传统杀毒软件不兼容、无严格的U盘等移动介质管控、终端登录无身份认证措施、应用软件存在使用默认密码和用户口令粘贴于显眼位置现象、外部设备管理采取封条方式、未部署安全技术措施，终端设备存在被攻击的可能。（5）通讯协议：工业协议为了满足相应的数据实时性和周期性，往往缺乏有效的用户安全认证、数据传输的加密解密等基本信息安全手段。协议的相关信息又能通过公开渠道获取，攻击者很有可能利用协议的漏洞对工控网络发起攻击。企业的安全网和非安全网的自动控制协议都是基于通用的服务器、操作系统和数据库系统运行于TCP/IP协议之上，TCP/IP协议的诞生主要解决网络间的通信问题，而不是立足于安全，随着TCP/IP的发展，很多方面都被一些不法分子所利用，暴露出TCP/IP中的不少安全问题。（6）控制系统：在系统维修或升级检测过程中，第三方人员的远程维护可能会导致相关生产数据的信息泄密，对运维过程中的误操作事件缺乏证据支撑。

2.电力监控系统网络安全防护

2.1云计算访问控制的电力监控涉密自检模型

电力监控系统主要通过技术服务和数据服务来实现功能，为提高系统各模块之间的有效连接性，降低耦合度，采用层次结构设计系统，电力监控系统可分为数据层、业务层和应用层3层。数据层主要负责系统数据的采集，并通过中间件向应用层及业务层传输相关数据，为系统运行提供数据支持。业务层主要包括数据库检测和系统服务两部分，在系统中承担数据处理及事物的逻辑处理等任务。应用层包括控制中心及云计算访问控制模块等，是一个人机交互端口，主要负责与用户进行连接，满足用户需求。中间件具有屏蔽不同结构层差异的功能，可帮助系统顺利完成数据和网络通信。系统各模块为安全管理、监控管理等子系统提供服务，子系统根据自身需求与该系统相互连接，完成数据处理和资源共享，从而实现系统的电力监控任务。为保证电力监控系统中涉密信息的安全，提高系统可信度和安全度，设计一种系统涉密自检模型。电力监控系统涉密自检主要以控制中心为主，通过连接数据库涉密检测模块与云计算访问控制模块实现系统功能。本系统在业务层还设置了数据库涉密检测模块，如在系统中发现涉密信息，会自动反馈给控制中心，完成电力监控系统涉密信息自检。云计算访问控制与控制中心相连接，当用户主体访问或操作系统资源时，通过所连接的控制中心可自动判断访问资源是否为涉密信息，从而决定是否阻止用户访问，完成涉密信息自检和保护。控制中心是电力监控系统运行的总指挥，会定时扫描数据模块以及服务模块，对数据库检测模块和云计算访问控制模块反馈信息进行再判断，采用数据匹配方法进一步识别涉密敏感数据，进而阻止用户访问，实现系统安全管理。

2.2加强计算环境安全建设

计算环境安全主要体现在恶意代码防护、入侵检测、系统漏洞、安全审计、外设管理、剩余信息保护几个层次。基于工业控制系统本身的安全特点，可以采用白名单技术，

保证软件和应用程序正常运行，对其进行充分的代码审计、安全监测和分析，结合完整性检查方法，当发现程序被修改后，会阻止该程序的运行，从而阻止病毒的扩散；实时监控USB端口、网络端口状况，提供自定义外设管理，严格控制非授权外设接入，提供完备的操作日志，当泄密事故发生后，可以从操作日志中追溯到泄密文件、设备、日期等关键信息，从而为事后问责提供有力依据。此外，工控安全事件的发生，或多或少都利用了工业控制系统的“漏洞”，进而攻陷了整个工业控制系统。通过部署工控漏洞扫描系统，在工业控制系统受到攻击之前为客户提供专业、有效的漏洞分析和修补建议，防患于未然。

2.3基于云计算的电力设备智能监测系统

融合云计算技术的监测系统架构。按功能划分，该架构可分为底层和云端两部分；底层主要由传感器、电机驱动器和通信模块等物理设备构成的分布式巡检智能体；云端包括三种云服务模式：基础设施即服务（IaaS）、平台即服务（PaaS）和软件即服务（SaaS）。按层级划分，系统分为物理层、控制层、信息共享层、API接口及应用层；其中物理层属于底层，由众多物理设备或基础设施构成；控制层、信息共享层、API接口及应用层属于云端，主要完成信息通信、共享、计算及展示等。系统中分配给某个分布式巡检智能体的虚拟机（VM）对应于服务模式IaaS。该系统还为相关智能体二次应用开发提供了平台，即为PaaS类。应用软件将通过SaaS模式共享给不同的用户。在云端，VM是动态分配的，一旦智能体连接到云中，就会根据存储服务器中存储的相关数据创建相应的VM，这些数据主要包括系统配置数据、算法和历史数据等。用户可以通过应用层的用户界面与系统进行交互。当一个任务包含大量的计算部分时，智能体VMs会请求并行计算集群中的计算节点协调完成任务。系统在工作过程中，分布式智能体或信息采集单元监测的对象会随着任务要求的变化而变化，如仪表监控时主要采集表盘信息，电力线巡检时主要采集电力线信息，为此通过自适应学习模块建立目标特征库，同时将监测任务的对象特征及相关识别算法都存储在云中。当智能体或信息采集单元将图像发送到云端，根据云端命令采用基于视觉注意的目标检测算法进行目标检测，从而提高图像匹配的效率。此外，系统利用多核、PC集群和GPUs计算等并行计算技术，将云端的数据按需共享给多个分布式智能体。

2.4基于信息智能联盟的电力监控实时数据交互

在电力系统中，控制终端与前端执行设备之间频繁进行数据交互，包括指令的下达、状态信息的上传等。随着电力系统结构的复杂化，以及对实时数据要求的严格化，传统的数据交互由于存在数据迟报、交互性差等问题，已经无法满足新的管理要求，探究和使用一种处理效率更高、响应速度更快的数据交互模式势在必行。智能体联盟可以对系统内海量异构信息进行快速处理、智能分析，将其应用到电力监控系统中，有助于进一步提高实时数据的交互能力，进而很好地满足全时段、全方位、全过程的监控需要。在这一背景下探究基于信息智能联盟的电力监控实时数据交互应用技术具有重要的现实意义。当电力系统中有实时消息事件发生后，所有消息事件均需要在接收智能体的Message映射表中进行注册。然后接收智能体会根据映射表中各条消息的类型、范围、时间等进行排序。这样就能保证优先级较高的消息事件最先发送到消息触发器中。接收到消息事件后，消息触发器动作，将该消息发送至监控终端。按照顺序依次发送消息事件，有效避免了轮询信息时产生的额外开销，对减轻通信负载、提高通信效率有积极帮助。除了智能体与前端执行设备进行通信外，多个智能体之间也会相互通信。这种设计方式的好处在于分担了单台智能体的信息处理压力，有助于提高电力监控系统的稳定性与可靠性。

2.5内生安全关键技术

设备作为一个物理单元，内生安全比较容易理解，其实作为系统同样可以构建内生安全能力。系统是多个设备通过连接和协作建立起来的业务逻辑集合，也存在物理上和逻辑上的边界。系统的内源性主要体现为系统边界内的设备单元、网络结构，以及网络空间内的通信交互和资源访问，则系统内生安全的重点也就是在网络结构的安全设计、通信交互的身份认证和保密传输、资源访问的安全性控制、过程行为审计等，其设计思路上和设备内生安全是一致的。

2.5.1可信免疫

可信免疫是一种运算同时进行安全防护的新计算模式，以密码为基因抗体实施身份识别、状态度量、保密存储等功能，及时识别“自己”和“非己”成分，从而破坏与排斥进入机体的有害物质，相当于为设备培育了免疫能力。一个可信计算系统由信任根、可信硬件平台、可信操作系统和可信应用组成。

2.5.2拟态防御

拟态防御是通过构建一种动态变化的多重并行协同架构，从源头上将安全基因植根到网络信息系统之中，建立起具有内生效应的免疫体系，从而有效解决利用未知漏洞、未知后门的未知攻击的防御难问题。

结语

网络安全现有基于威胁特征感知的精确防御，在机理上属于“后天获得性免疫”，这种被动防御机制本身实际上已经成为网络空间日益明显的脆弱性。因此我们用主动性思维对网络空间尤其是关键基础设施领域的安全防护思路进行研究和探索，将内源性安全技术和安全设计融入关键设备和系统中去，构建内生安全能力，并作为系统安全防护整体解决方案的有力补充，为有效提高安全防护效果提供积极的借鉴和参考。

参考文献

[1]郑雪娜，陶家元，王瑞雪，等. 基于智能可视化管理的变电站智能监控系统设计[J]. 现代电子技术，2020，43（16）：30-33.

[2]王勇，韩少晓，尚力，等. 智能变电站监控系统新型体系架构研究与实践[J]. 电力系统保护与控制，2019，47（8）：145-151.

[3]李娜，姜志，王军，等. 基于FasterR－CNN的仪表识别方法[J]. 液晶与显示，2020，35（12）：1291-1298.