

基于发电企业信息管理的安全防护研究

能源互联网被认为是第三次工业革命最重要的标志。发电企业“互联网+”化、智慧化是“互联网+”智慧能源的一个重要组成部分。随着信息技术、网络技术和人工智能的发展，开放标准的普及，管理控制一体化理念的深入，“互联网+”时代发电企业信息安全将面临更大的挑战和威胁。从工控系统安全、大数据安全和工业无线网络安全三个方面着手分析未来智慧电厂中可能存在的问题，并归纳总结了一些具体的应对措施，以保障智慧电厂能够安全可靠运行。

黄综联/浙江浙能兰溪发电有限责任公司

0 引言

在全球新一轮科技革命和产业变革中，互联网、大数据、云计算、人工智能以及其他先进的信息技术与能源产业的融合，正在推动着能源互联网新技术、新模式和新业态的兴起。能源互联网被认为是第三次工业革命最重要的标志^[1-2]。

“互联网+”智慧能源，涵盖两个层面的含义，其一是能源互联网，能源互联网不是简单的信息互联网加上现有的传统能源体系，而是一种互联网与能源生产、传输、存储、消费以及能源市场深度融合的能源产业发展新体系，具有设备智能、多能协同、信息对称、供需分散、系统扁平化和交易开放等主要特征^[3-7]。

其二是智慧能源，表现在发电企业，指的就是智慧电厂。所谓智慧电厂，就是以数字化、信息化、自动化和智能化为基础，通过互联网络或者其他通信设施将生产管理过程中所有的经济指标、环境因素、运行参数、状态信息、故障情况和调整操作指令等数据汇

集，进行针对性的对标、分析和处理，实现集中管控、智能决策、准确控制、自动容错及傻瓜式运行，能够适应智慧能源互联网新体系的发电厂。

发电企业“互联网+”化、智慧化是“互联网+”智慧能源体系发展的一个重要组成部分。但随着信息技术、网络技术和人工智能的发展，开放标准的普及，管理控制一体化理念深入，“互联网+”行动起步，智能设备、工控系统接入范围扩展到企业网、甚至互联网，信息安全将面临更大的挑战和威胁。如何解决“互联网+”时代发电企业的网络与信息安全问题，是需要思考和探索的。

1 发电企业“互联网+”存在的信息安全问题

2005年，在Zotob蠕虫安全事件中，尽管在互联网与企业网、控制网之间部署了防火墙，还是有13个美国汽车厂由于被蠕虫感染而被迫关闭，50 000条生产线工人被迫停止工作，预计经济损失超过1 400 000美元；2010年，伊朗布什尔核电站遭到“震网”病毒攻击，1/5的离心机报废，大大延迟了伊朗的核发展计划；2011年，黑客通过入侵数据采集与监控系统，使美国伊利诺伊州城市供水系统的供水泵遭到破坏；2017年，“永恒之蓝”勒索蠕虫病毒爆发，多个国家遭遇到攻击，包括政府、银行、电力能源企业和机场等重要基础设施被波及，对重要数据造成严重损失^[8]。不难看出，随着智能设备和信息技术应用层



黄综联/高级工程师

关键词/Keywords

“互联网+”·
智慧能源·
信息安全·

面的扩大，互联网连接区域的扩大，互联网连接设备的增加，将带来更多的信息安全问题。

因此，在“互联网+”智慧能源时代，除了关注传统意义的管理信息系统及网络的安全，更要关注与生产管理智能化相关的安全问题，比较典型的有：工控系统安全、工业大数据安全和工业无线网络安全等。

1.1 工控系统的安全问题

随着两化融合的推进，工控网络业务趋于复杂，业务识别、防护压力增大；随着DCS、PLC以及SCADA等工控系统智能化程度的提高，网络数据交互流量增大，行为趋于复杂；随着联网需求的大幅增加，多种互联网接入方式并行存在，工控网络物理边界模糊，安全风险指数增加。

工控系统的现状，是将可用性放在第一位，系统建设过程中基本上没有考虑安全防护的问题。发电企业最多是按国家能源局要求在生产区和管理区中间加了一个物理隔离装置，生产Ⅰ区和Ⅱ区间安装了一个防火墙，去省调和网调的出口安装了一个纵向加密装置，也就是满足了电力监控系统安全防护“安全分区，网络专用，横向隔离，纵向认证”的基本要求，但工控系统内部基本处于无防御状态。随着伊朗核电站被攻击，工控系统的安全才开始引起大家的重视。工控系统主要的信息安全风险如下。

(1) 工控通信协议的风险

工控系统所采用的专用通信协议，大多为了提高效率和可靠性而放弃了协议的安全特性。如应用最多的Modbus协议，仅需要使用一个合法的Modbus地址和合法的功能码即可以建立一个Modbus会话；没有授权和认证的要求，没有基于角色的访问控制机制，任意用户可以执行任意的功能；没有加密功能，数据以明文形式进行传输，可以很容易地劫持、捕获和解析；没有广播抵制功能，容易遭受Dos攻击。

(2) 工控终端及系统不更新的风险

工控专有系统兼容性差、软硬件升级较困难，如需升级可能需要整个系统升级换代，这就

导致了上位机系统版本都偏老。同时，考虑到更新补丁可能会导致工控控制系统软件运行故障，因此上位机的系统基本不更新；同样的考虑，一般也不太可能安装杀毒软件。这样利用系统漏洞就可以轻松地提升权限，执行恶意程序并进行传播和扩散。

(3) 缺少安全审计体系的风险

工控系统对实时性要求很高，因此一般不作安全策略，也不会开启审计功能，而且大部分企业都没有配备日志审计系统和堡垒主机。这样，任何操作都不会被过滤，也不会受到限制，任何程序都能够运行，出现问题就很难查找出原因，找到源头。

(4) 系统管理松懈的风险

大多数企业的工控系统权限管理和控制不严格，没有系统管理员、安全管理员、操作管理员和普通查看者的区分，基本上都是用系统管理员权限的账户进行操作，同时为了操作方便，很多密码都是用户名和密码相同，一串连续或相同数字的弱口令，这样就很容易被猜解和扫描出来，直接对工控系统进行有害操作就可以造成重大的损失。

(5) 没有规范的管理制度的风险

没有完善的管理制度，操作不规范，存在大量的不安全行为：离开控制台的时候不把电脑锁定，而且没有启用屏幕保护及密码恢复功能，如果有外来人员进入，就可以直接对工控机进行操作；随意使用USB设备存取数据，还不是专用安全的USB设备，交叉使用，感染USB病毒的风险极大，系统自带的设备自动播放功能一般也不会关闭，这样USB病毒就可以不知不觉地潜入并运行；工控系统的调试电脑，在生产区与管理区间混用，大大增加了感染病毒的可能。

(6) 核心设备无核心技术风险

工控系统的核心设备严重依赖国外产品和技术，无核心技术，又缺少针对工业控制设备的信息安全检测手段、标准和方法，设备本身要是留有“后门”，将是非常大的隐患。

1.2 工业大数据的安全问题

国务院印发的《促进大数据发展行动纲要》中提到,利用大数据推动信息化和工业化的深度融合,研究推动大数据在研发设计、生产制造、经营管理、市场营销和售后服务等各环节的应用,研发大数据分析应用平台,积极推动制造业网络化和智能化。发电企业大数据是实现智慧电厂最重要的基础之一,主要由电力生产控制数据、各个在线监测系统数据、ERP系统数据和经营系统数据构成。主要应用体现在两个方面:一是提高电力生产控制、分析、诊断检修的智能化水平来提高效率、降低成本;二是以发电企业管理为目的的经营分析和辅助决策,来实现利润最大化。当企业迈入大数据时代,信息安全将面临多重挑战。

(1) 高收益带来更多攻击者

大数据蕴藏着更敏感、更复杂以及更有价值的信息,黑客的一次成功攻击能获得比以往更多的数据量,增加了“攻击收益”,这将引来更多的潜在攻击者。

(2) 攻击方式更多更隐蔽

大数据要求相对开放性的网络,低密度价值分布使得安全防御边界扩大,并且要对复杂多样的数据存储内容作出快速处理,使得网络安全加固策略不能太过于复杂,安全防护系统升级速度很可能跟不上数据量增长的步伐,产生更多的漏洞。大数据以非线性几何式的速度增长,由于数据量庞大,黑客利用大数据将APT攻击代码隐藏在大量数据中,传统的基于特征的安全扫描软件基本上检测不出来。

(3) 存储复杂难管理

大量的数据是非结构性的,这样存储过程就变得很复杂,容易造成数据管理存储混乱,数据完整性难以保证,也容易出现安全问题。

1.3 工业无线网络的安全问题

随着无线网络技术的发展,已经有越来越多的无线设备和应用进入工业自动化领域,实现对网络区域内监测对象和监测环境的实时感知和采

集,并将这些信息进行处理,加以利用。这里主要研究的是无线传感器网络(WSN),作为一种大规模、低成本、低能耗、分布式、节点可移动和拓扑结构高度动态变化的自组织无线网络,已经越来越多地应用到工控网络当中,但该网络同样存在硬件资源有限、电源容量有限、带宽和通信能力有限以及网络规模大但无中心等特点。

(1) 开放网络易非法接入

无线网络是个开放网络,存在非法接入或非法授权接入的风险。

(2) 计算能力弱易被劫持

工业无线传感器网络中节点的存储容量很小、计算能力弱等原因,造成由其构成的网络无法很好地应用传统安全机制,比如高位复杂加密的公钥密码技术,安全风险就更加突出。攻击者一旦接入成功,通过监控数据的传输,就可以对数据进行监听、拦截和修改,还可以将截获的信息重新发给目标节点进行重放攻击。

(3) 网络拥塞易导致资源耗尽

工业无线传感器网络属于多跳无线网络,网络的拥塞和节点对包的处理均可导致网络的延迟,延迟时间过长就会导致通信故障;借助某些特殊工具,向无线网络中传输大量的非法数据覆盖全部无线频段,通过耗尽目标节点的资源令其无法正常采集数据,致使工控系统无法正常使用,影响正常的生产运营。

(4) 节点众多易被物理操纵

无线传感器网络由于节点众多,对每个节点进行到位的保护是比较困难的,这就面临节点容易被攻击者物理操纵,并获取存储在其中的所有信息,从而控制部分网络甚至全部网络的威胁。

2 如何做好发电企业“互联网+”的安全防护工作

从上面的问题可以看出,随着发电企业“互联网+”进程的推进,确实带来了更多安全风险和挑战,做好安全防护工作,将是真正让“互联网+”智慧电厂完全发挥其作用,体现其价值的重要基础和保障。

2.1 工控系统安全防护要点

(1) 防范工控通信协议风险

基于对通信协议与规约的深度解码分析，掌握协议字段和协议命令字，便可以使用工控防火墙对报文进行深度过滤，或者通过网络协议异常性特征识别与监测进行报警提醒，并进行针对性处理。

新建工控系统最好从源头进行控制，在不影响系统实时性、可靠性的前提下，应尽可能采用具有授权、认证和加密机制等安全性较高的通信协议来保障安全传输。

(2) 防范工控终端及系统不更新风险

兼容性问题导致工控终端难以更新换代，可以通过部署主机加固系统来解决，也可以从设备的系统、硬件和应用软件三方面着手防护。

1) 系统方面。一定要关闭不必要的系统服务和端口，比如媒体和设备自动播放功能，比如445、21和80等端口；及时更新可以升级的系统补丁，以防被黑客利用留做后门；部署杀毒防恶意代码软件，最好使用绿色免安装版的，用离线方式及时更新病毒库，定期进行查杀，减少感染病毒的风险。

2) 硬件方面。多余的系统接口必须关闭并贴上封条，做好登记，控制好移动介质和调试设备的接入。确实需要使用移动介质或设备的，最好部署一套安全控制系统，使用安全介质或设备，并保证不能移作他用。有条件的可部署可信计算机平台。

3) 应用软件方面。关键工业控制应用系统的软件升级必须请原厂商或专业技术机构进行安全评估、验证和安装，以减少升级失败导致系统不可用的事件发生。

(3) 防范无审计的风险

针对没有审计功能的问题，建议部署带有检测功能的工业安全审计管理系统，用于实时检测针对工业网络攻击、用户误操作、用户违规操作、非法设备接入以及蠕虫、病毒等恶意软件的传播行为，并做到实时报警，同时详实记录一切网络通信行为，包括指令级的工业控制协议通信记录，为管理系统及工业控制系统的安全分析提

供基础数据。

(4) 防范系统管理松懈的风险

加强系统权限管理，删除系统中多余账户，并根据权限最小化原则配置使用账户；严格实行用户账户口令管理，及时更改产品安装时的预设口令，杜绝弱口令、空口令，强制要求使用复杂密码，开启用户审计策略。

(5) 防范无规范制度的风险

建立全面的标准化管理体系，不断完善工控系统规划、设计、建设、运维、管理和应急处置等制度，加强监督、规范操作，明确安全责任，并落实执行。关注并学习国家及行业最新的法律法规和标准制度，及时修订各类标准及管理制度。

(6) 防范核心设备的风险

慎重选择核心设备，尤其是工业控制系统设备，允许的情况下优先选择国产设备。在供货合同中明确供应商应承担的信息安全责任和义务，签署保密协议。信息安全管理人员要密切关注产品是否发现新漏洞，并及时进行干预。

利用技术手段降低可能存在的设备“后门”对工控系统的影响，构建工控系统安全运行的“白环境”。建立网络设备、控制设备和计算机设备等所有联网设备的白名单，非白名单设备无法进入；建立并启用应用程序白名单，只允许预先经认可的应用程序才能执行；建立数据存取、指令执行白名单，只允许符合特定规则的数据操作，只允许符合工艺规则的指令运行。

2.2 工业大数据安全防护要点

(1) 增加攻击的难度和成本

存储数据加密，并分离密钥和加密数据，防止存储中的数据被窃取后直接被利用，同时做好密钥的生命周期管理，以防止密钥泄露造成的损失；传输过程也必须使用加密通道，防止流量被嗅探和篡改。另外，大数据一定要分散存储，这样任何一个存储单元被攻破，都不可能拿到全部数据；确立有限管理边界，加强重点保护，增加特征标识建设内容，增强对数据资源的管理和控制，遵循网络防护和数据自主预防措施并重原则，构建一体

化的数据安全管理体系。这样就增加了黑客的攻击难度和成本，可以让不少黑客知难而退。

(2) 搭建大数据智能防御平台

防范大数据时代的攻击，尤其是APT攻击，同样要借助大数据处理技术，针对APT安全攻击潜伏时间长、攻击数据分散、攻击路径不确定和隐蔽性高等特点，采用具备实时检测、建模和关联分析能力的全流量审计及安全态势感知平台，实现智能防御。

(3) 保证数据有备无患高质量

做好系统备份工作，异地大带宽双链路或多链路备份，数据库采用热备容灾配置模式，通过敏感信息集中管控和数据管理产品，保证数据的完整性及高质量。

2.3 工业无线网络安全防护要点

(1) 给开放的网络加上锁

部署网络准入控制系统，严格控制无线设备接入，做到实体认证，MAC地址控制，“违规不入网、入网必合规”，非法接入时提供预警功能；网络拓扑图和资产清单要详细，并及时更新，定期对接入网络的设备情况进行检查，做到实物与清单一一对应。这样就可以有效阻止非法接入点的接入。

(2) 设计新型加密认证方案防窃取和重放攻击

为了防止无线传感器网络发生信息泄露、信息篡改等事件，最好设计出一个灵活而强健的加密方案，容易部署且能摆脱传感节点处理能力有限的限制，最好还能保证当部分节点被控制后不会破坏整个网络的安全性；针对攻击者利用网络监听或者其他方式盗取认证凭据发起重放攻击，可以通过设置合适的时间戳、事先协商好一个消息序列号以及生成一次性随机数等方式来防范。

(3) 多种方式减轻网络压力防止资源耗尽

无线传感器的网络拥塞导致资源耗尽其实就是一种Dos攻击。防御此类Dos攻击没有一种固定的方法，它随着攻击方法的不同而不同。利用跳频和扩频技术减轻网络拥塞，利用恰当的认证可以防止在无线网络中插入无用信息、限制网络发

送速度及节点设置，诸如自动抛弃多余数据请求或对过度频繁的请求不予理睬的策略，这些措施可以有效地防止资源被耗尽。

(4) 监测、伪装及定位三位一体防范物理操纵

由于无线传感节点容易被物理操纵的事实，就要采用更精密的保护措施。最好有完善的物理损害感知机制，根据其失去连接时间、设备控制方式变化和其他一些敏感信号的变化，来判断是否遭受物理侵犯，及时采取干预措施，如销毁数据、断开节点以及进行安全处理等，来保护网络中其他节点免受安全威胁；也可以采取隐藏和伪装的方法，减少节点被发现的可能；另外，还可以部署智能人员定位系统，记录人员的活动轨迹，结合视频联动功能及时发现未授权人员在生产区的活动。

2.4 其他通用的安全防护要点

(1) 人员安全意识管理

信息安全严重依赖于人为因素，即使最为严格的安全防护措施也可以被人轻易破坏，不管是有意还是无意的。安全意识薄弱会给工业控制系统带来致命的危险，通过社会工程学进行的定向钓鱼攻击，很可能使重要岗位人员沦为外部威胁入侵的跳板。因此，加强思想教育，做好《网络安全法》等法律法规的宣贯，让企业员工树立正确的安全观、价值观和世界观，是非常必要的。一旦出现问题，必须让其承担相应的责任，这样才会起到有效的警示作用。

(2) 应急管理

制定安全处置应急预案，明确应急流程和临机处置权限，落实应急技术支撑队伍。不定期进行网络与信息安全重大突发事件应急演练，提高处理应急事件的能力，学习如何更好地控制和消除信息安全突发事件带来的危害和影响，做好预防工作。

3 结束语

“互联网+”时代，发电企业信息安全管理面临越来越多、越来越高科技以及越来越智能化的挑战，必须建立一套全面的纵深防御体系，

以等级保护为基础,深入信息系统的整个生命周期,“自下而上”逐步推进安全防护策略,提升设备级、系统级和管理级的安全防护能力,实现一体化的安全防护,从而真正起到保障企业信息安全的作用。

参考文献

- [1] 尹松.发电管控发展与智慧电厂[C].智慧电厂践行论坛,2016.
- [2] 汪国良.电力企业大数据集成技术与安全[C].电力安全与信息技术研讨会,2015.
- [3] 中国软件评测中心.工业控制系统安全认识和思考[C].工业控制系统信息安全峰会,2016.
- [4] 杜成龙.探究无线网络安全问题[J].网络安全技

术与应用,2016(5):72-73.

- [5] 魏旻,王平,王泉.工业无线控制网络安全方法的研究与实现[J].仪器仪表学报,2009,30(4):679-684.
- [6] 周晓媛,王东树.大数据时代下的网络安全问题分析[J].网络安全技术与应用,2016(5):50.
- [7] 刘凯俊,钱秀槟,刘海峰,等.首都城市关键基础设施工业控制系统安全保障探索[J].网络安全技术与应用,2016(5):81-86.
- [8] 杜伟奇,王平,王浩.工业控制系统中安全威胁分析与策略[J].重庆邮电大学学报:自然科学版,2005,17(5):594-598.

(收稿日期:2018-06-08) **EA**

(上接第64页)

4 结束语

小电阻接地系统继电保护整定计算中,接地变压器过电流保护、零序保护与馈线保护在时间和定值上应进行配合,时间上应该馈线首先动作,然后是接地变压器、主变压器出口开关和主变压器各侧开关等。依据现有规程整定所得接地变压器速动段和馈线零序Ⅰ段的时限,会出现二者相同或者后者比前者大的情况,此时,若馈线上发生单相接地故障,流过接地变压器的故障电流达到接地变压器速断定值,接地变压器会越级动作,造成事故扩大,故需考虑接地变压器速动段和馈线零序Ⅰ段在定值上保证选择性要求。另外,对于有条件的现场,可以考虑采取对接地变压器电流速断保护加装方向元件的措施来保证选择性。本文在现有规程基础上给出了整定建议,经工程实践验证方法可行。

参考文献

- [1] GB/T 14285—2006 继电保护和安全自动装置技术规程[S].北京:中国电力出版社,2006.
- [2] DL/T 584—2007 3~110 kV电网继电保护装置运行

整定规程[S].北京:中国电力出版社,2007.

- [3] 水利电力部西北电力设计院编.电力工程电气设计手册(电气一次部分)[M].北京:中国电力出版社,1989.
- [4] Edson R Detjen, Kanu R Shah. Grounding transformer applications and associated protection schemes[J]. IEEE Transactions on Industry Applications, 1992, 28(4): 788-796.
- [5] Shen M, Ingratta L, Roberts G. Grounding transformer application, modeling, and simulation[C]. Power and Energy Society General Meeting-conversion and Delivery of Electrical Energy in the 21st Century, 2008: 1-8.
- [6] Peter E Sutherland. Application of transformer ground differential protection relays[J]. IEEE Transactions on Industry Applications, 2000, 36(1): 16-21.
- [7] Oka K, Yoshinaga J, Koizumi S, et al. Study of neutral grounding for 22kV distribution system[J]. IEEE/PES Transmission and Distribution Conference and Exhibition, 2002, 3(3): 2143-2148.

(收稿日期:2018-03-06) **EA**