电力监控系统网络安全防护体系逐步建立

工业控制系统产业联盟理事长、国家电网公司国家电力调度控制中心原副主任 辛耀中

工业和信息化部发布《工业控制系统信息安全防护指南》（以下简称《指南》）已经三年了，各相关行业认真贯彻落实《指南》要求，取得了长足的进展，工控系统安全水平明显提升。全球网络安全威胁日益严峻，工业控制系统首当其冲，需要认真梳理总结实施情况，明确后续重点努力方向。

认清全球网络战已悄然展开的严峻形势

全球网络安全事件越发频繁，网络安全隐患从软件向硬件延展，我国工控系统网络安全形势不容乐观，引起我国相关行业主管部门高度重视。2002年原国家经贸委发布《电网和电厂计算机监控系统及调度数据网络安全防护规定》，2005年原国家电监会发布《电力二次系统安全防护规定》，2007年公安部联合四部委出台《信息安全等级保护管理办法》，2014年国家发改委发布《电力监控系统安全防护规定》，2016年工信部发布的《工业控制系统信息安全防护指南》提出了11项工控网络安全重要措施，2017年全国人大颁布《中华人民共和国网络安全法》。

在国家相关政策法规的指导下，电力行业用了近20年的时间，逐步建立了比较完善的电力监控系统网络安全防护体系。自《指南》发布以来，电力行业又强化了对生产控制大区的动态实时感知，升级了关键网络安全设施，建立了网络安全专职机构队伍，完善了电力监控系统安全防护体系。根据国家电网外网边界的监测统计，每天遭受的各类恶意网络攻击次数逐年增加，现在平均每天达9000多次，都被安全防护体系有效阻断，保障了电力系统安全稳定运行。

建立重要工控系统网络安全防护体系

工控系统典型特征如下：第一是高可靠性，要求永不停机；第二是强实时性，必须在特定时间内及时完成特定动作；第三是高安全性，首先是业务功能安全，其次是网络信息安全，而且网络信息安全服务于业务功能安全，若影响了可靠性和实时性，相当于自我攻击。

我国电力监控系统网络安全防护体系已经覆盖各级电网调度控制中心上千个、各类变电站和发电厂数万座，经受了多年的实战考验，相关成果形成了国家标准GB/T 36572-2018《电力监控系统安全防护导则》。

根据国家有关部门要求，工业控制系统产业联盟组织编制了《重要工业控制系统网络安全防护导则》（报批稿），用于指导重要行业领域建立其工业控制系统网络安全防护体系。防护体系由安全防护技术（X轴-T）、应急备用措施（Y轴-E）、全面安全管理（Z轴-M）等三维空间坐标和一维时间坐标（时间轴t）构成四维时空立体结构。安全防护技术维度（X）包括基础设施安全、体系结构安全、系统自身安全、安全可信防护等。应急备用措施维度（Y）包括冗余备用、应急响应、多道防线等。安全管理维度（Z）包括全体人员安全管理、全部设备安全管理、全生命周期安全管理，融入安全生产管理体系。时间维度（t）表示随着时间不断发展完善。

结构安全是防护体系的核心框架，采用“安全分区、网络专用、横向隔离、纵向认证”策略，形成栅格状框架结构，防止任何局部故障影响全系统。

工业控制系统的本体安全或内生安全包括四个层面：一是工控系统软件没有恶意隐患，二是操作系统没有恶意后门，三是整机主板上没有恶意芯片，四是处理器芯片内没有恶意指令模块。新开发的工业控制系统应该实现内生安全，但在运的老工控系统，只能强化边界安全，加强安全管理，待升级换代时再实现内生安全。

我国电力行业用了30年时间解决电网控制系统内生安全问题。2009年研制成功“智能电网调度控制系统（D5000）”，将数字证书、安全标签、安全可信等系列安全技术，融入各个控制模块和所有相关环节，实现了核心业务系统的内生安全。D5000系统已在国家电网全部省级以上调控中心及大部分地市级调控中心应用，实现了多级电网调度及与变电站和发电厂的全网协调控制，形成了数万结点的电网调度控制专用云和数亿实时测点的电网控制专用物联网。

防范新技术、新应用带来的网络安全风险

近些年，随着云计算、大数据、物联网等新一代信息技术的快速发展，工业云、工业大数据等新应用发展迅速，工业化和信息化加速融合，工业控制系统变得更加数字化、网络化、智能化。在工业领域应用新技术的过程中，传统网络安全防护措施手段单一、功能分散等缺点逐渐显现，新技术、新应用对工业控制系统带的网络安全风险不容小觑。

云计算技术的实质是“硬件面向集群、软件面向服务”。面向全社会的公共业务可以采用公用云，而工业控制业务必须基于专用云，实现业务隔离，确保其安全性。目前，我国电力行业已经建立了电网调度控制专用云，仅地市级及以上调度控制中心的计算节点就达数万个，物理分布在数百个调控中心，并与其他“云”物理隔离。

保障电力领域的工业大数据安全，就是要构建涵盖数据采集、传输、存储、处理、交换和销毁等全生命周期的工业大数据安全防护体系，特别针对电流传感器和电压传感器采集的实时数据，要按照数据采集最小化、使用授权最小化、分级分类保护、受控审批等原则，建立相应的数据防护体系，确保关键数据不被篡改、核心技术不被窃取、生产业务不被中断。

物联网技术的应用，是实现电力生产传感互联的基础，在物联网环境下保障工业控制系统安全，必须实行工控专用物联网的物理隔离。目前，我国电力行业已经建立了电网控制专用物联网，数亿个传感器与电网控制专用数据网连接，必须确保专用物联网与其他物联网的隔离，减少数据交互带来的网络安全风险。

总之，在实现工业控制业务与新一代信息技术深度融合的同时，必须保障工业控制业务更安全可靠、更经济高效、更绿色环保、更方便友好。

工业控制系统是冶金、石油/石化、电力、核电、轨道交通、水处理、公共卫生等重点领域的核心中枢，是国家关键信息基础设施的重要组成部分。工业控制系统信息安全（以下简称“工控安全”）是实施制造强国和网络强国战略的重要保障，是关系到国家安全、经济发展和社会稳定的关键因素。

安全防护应贯穿工控系统全生命周期

中控科技集团创始人 褚健

近年来，随着“两化融合”走向深入，工业数字化、网络化、智能化快速发展，大量工业系统和生产设备与工业互联网连接。以往由物理环境的封闭性和专用性所带来的安全性将不复存在，关系到国计民生的诸多重要工业领域成为网络攻击的主要目标，针对能源、交通、制造业等重要领域的网络攻击事件频发。

工控安全要求对系统核心部件有效保护

2016年10月17日，工业和信息化部为保障工业企业工业控制系统信息安全，制定了《工业控制系统信息安全防护指南》（以下简称《指南》）。《指南》坚持“安全是发展的前提，发展是安全的保障”，以近年来我国工业控制系统面临的安全问题为出发点，注重防护要求的可执行性，从管理、技术两方面明确了工业企业工控安全防护要求。

中控科技集团在《指南》发布后，针对“两化”融合之后日益复杂的工业信息安全风险，通过对相关国际、国内标准的研究，并结合自身丰富的工程实践经验，提出了“内建安全、纵深防御、全生命周期管理”综合工控系统深度安全防护体系，突破安全隔离、内核自主可控等关键技术，从内在机理上逐步规避信息安全风险。经过实践，中控工控信息安全整体解决方案及产品在各种大型项目中进行应用，并取得了良好的效果。

《指南》发布前，工控安全防护聚焦于工控系统的边界防护，事实证明这种单一的防护模式无法完全保障工控系统的安全运行。在《指南》发布后，工控安全技术向多元化发展，基于纵深防御、适用于工控现场环境的解决方案被普遍提出。同时，越来越多的工控安全厂商认识到，工控安全不同于传统的信息安全，其要求是对工控系统核心部件——控制设备的有效保护，这要求工控安全防护必须覆盖工控系统的所有部件，并紧密结合生产工艺和操作流程，贯穿工控系统的全生命周期。

亟须加快构建新型工控安全防护体系

基于《指南》三年的实践，工控安全防护取得了诸多成绩和进步，但现有的工控安全防护体系仍难以保证所有工控系统的安全运行，亟须加快构建更专业的新型工控安全防护体系，有效维护工业信息安全，为制造强国和网络强国顺利实施提供坚实保障，为此提出五点建议。

第一，要加强顶层设计，整合资源，统一标准。工控系统网络安全问题不能一概而论，作为国家层面要明确对工控系统网络安全进行分类。

第二，工控系统要逐渐实现自主、安全可控。自主可控的同时，也不能忽视安全。为了实现工控系统核心部件——控制设备安全，工控系统厂商需研究适合工控环境的安全防护技术并融合到控制系统内，研制具备内生安全的控制系统，通过内生安全加固提升控制系统自身的防攻击防护能力。

第三，重要工控系统必须部署工控网络安全防护系统。重要工控系统部署的工控网络安全防护系统应具备以下特点：针对内置预埋代码，切断危害，进行应急处置；在安全区域、系统出口，加强预警防范；以不影响生产和生产安全为前提，注意数据保护和操作保护；对系统重要性识别、系统资产识别、系统脆弱性识别、系统威胁识别及系统风险识别等维度进行安全防护；采用软件防护、边界维护、PLC嵌入式代码防护、控制异常监测与阻断等措施进行立体防护；对工控系统进行无扰动实时在线修复，并启动安全应急系统，实现数字化、网络化、智能化环境中工业企业的工控网络安全。

第四，尽快建设针对行业建设工控系统网络安全测试床。国家、企业应加快建设其所在领域行业的工控系统网络测试床，以测促评，以评促用，测试控制设备自身的安全性；检验安全产品的功能、可用性、安全性、可靠性及对工控系统是否有影响等；模拟工控安全攻击行为，建设威胁库，增强工控系统及其安全产品的主动防御能力。

第五，要加强工控网络安全人才队伍建设，完善或制定工控网络安全产品标准体系。工控系统网络安全攻防技术研究攻防兼顾，以攻促防。人才队伍不仅要懂工业控制系统的各类技术，还要懂使用工业控制系统的具体对象的工艺、设备技术，只有这样才能做到定点攻击或精确防护。

另外，由于工业控制系统运行连续性、操作周期性、功能实时确定性和现场环境易燃、易爆、有毒、强腐蚀、强电磁干扰的工程特征，面对日益复杂的纵深渗透、动态协同的集团化攻击，仅依靠传统信息安全技术体系已无法有效应对，亟须在攻防地位严重不对称、存在大量被利用的漏洞或后门的现实环境中，建立覆盖设计、建设、验收、运维和退役等全生命周期安全防护技术体系，突破信息物理空间深度融合场景下的工控安全防护难题，完善或制定工控网络安全产品标准体系。

夯实工控安全防护基础 助力制造业高质量发展

（上接第1版）扎实推进《指南》落实工作，在全国范围内分区域、分阶段开展《指南》宣贯培训，累计培训各地工信主管部门和重点领域工业企业工控安全负责人1200余人，促进企业安全意识大幅提升。支持江苏、浙江、四川、广东等8个省市开展技术专题培训，帮助各地建立工控安全专业技术队伍。

二是抓好落实，贯彻《指南》防护要求。引导产学研用依据《指南》防护要点，开展联合攻关和集成应用，研发具备安全功能的工业控制系统产品，促进内生安全水平提升。在冶金、石化、电力等重点行业，形成了一批安全解决方案。落实企业主体责任，以较低成本实现防护能力跃升，消减了自身面临的主要安全风险。

三是提升能力，建设技术支撑服务体系。加强工控安全技术保障能力建设，围绕落实《指南》要求，初步形成了产品检测、态势监测、风险处置和事件响应能力。加快工控安全标准体系建设，推动《指南》配套国家标准、行业标准、团体标准制修订，增强标准供给能力，近三年，推动发布工控安全国家标准13项。

《指南》发布以来，在工业和信息化部指导下，产学研用各方围绕落实《指南》开展了一系列工作，加快推动工控安全防护从理论研究进入概念普及和实践阶段，初步形成了政策指导、标准支撑、技术创新、产业协同的良好工作局面，工控安全综合防护水平显著提升，为守好制造业高质量发展的安全大门奠定了坚实基础。

三、加强政策标准引领，护航高质量发展迈上新台阶

目前通过落实《指南》，我国工控安全工作取得了阶段性成效，但同时也面临着不少困难和挑战。例如，部分企业落实工控安全防护主体责任还不到位；地方主管部门仍然缺乏有效的管理手段和支撑力量；科研机构尚未建立完善的技术支撑服务能力等。面对新形势、新问题，我们必须以习近平新时代中国特色社会主义思想为指导，牢固树立总体国家安全观，坚持安全和发展同步推进，以工控安全防护贯标为突破口，充分发挥《指南》及配套标准的规范和引领作用，推动安全防护步入实践深耕的新阶段，助力制造业迈入高质量发展的快车道。

第一，贯标推进机构要组织技术力量加快重点标准研制发布，扎实推进重点地区贯标培训深度行活动，进而在全国范围推动贯标工作。搭建公共服务平台，为企业提供自对标、自诊断服务，逐步形成贯标长效推进机制。

第二，地方工信主管部门要以贯标为工作抓手，充分调动区域内优势资源，建设地方贯标支撑队伍，引导工业企业积极参与贯标、实施贯标，扎实推进《指南》和配套标准落地落实。

第三，工业企业要切实落实安全防护的主体责任，积极参与贯标工作，将工控安全贯标纳入企业信息化发展战略，建立更加有效的安全管理制度和技术防护体系，探索形成安全防护样板工程。

第四，工业控制系统厂商和工控安全厂商要增强协同攻关和集成应用，研发具备安全功能的工业控制系统产品，配合贯标形成可操作、可复制的成套解决方案，助力工业企业提升安全防护水平。

虚拟技术加速赋能

（上接第1版）“5G急救车运用了5G、NB-IoT、eMTC等新一代宽带无线移动通信技术，及居民健康码、物联网手环、高清影像设备、远程心电监护、医用AR眼镜等设备，将院前急救、院内救治、院后康复等环节联系起来，形成闭环的全链条。”黄潇介绍说。

AR赋能各行各业

除了5G通信，记者在本次展览会上看到众多科技龙头企业发力VR/AR领域。HTC的展台让很多观众驻足观看，记者在展台上看到了HTC最新推出的VIVE Cosmos虚拟现实头戴式显示设备。HTC中国区总裁汪丛青向记者表示，该设备的最大特点是在完善虚拟现实与现实场景结合的同时，能够快速转换虚拟世界与现实世界。

“VIVE Cosmos虚拟现实头戴式显示设备应用了当前最先进的人工智能计算机图像识别技术，头显上6颗摄像头对周围环境进行识别扫描，可精准实现头部位置追踪及双手交互识别，让用户在虚拟世界中进行双手自然交互，体现身临其境的感觉。”HTC中国区产品总监袁野向记者表示。

微软的最新产品Hololens同样亮相了本次展览。微软高级产品营销经理刘拉雅向记者表示，微软的这款最新产品将打破VR眼镜的“线的束缚”。“传统的VR眼镜都会携带一个小尾巴，受众在体验时难免会受到束缚。所以我们进行了创新——Hololens One将线拿掉，打造成一体机，让用户随时随地享受VR。”刘拉雅说。

在联想的展台，记者看到了行业在中医药领域的大胆创新。利用VR的虚拟能力，联想可以把不同身高的体能特征传递至电脑端，将热敏灸与增强现实（AR）、人工智能（AI）及协作机器人等技术结合，致力打造国内首个智能热敏灸诊疗平台。“这款产品我们在这次VR产业大会正式推出。下一阶段将继续优化产品设计，进入临床验证后，将彻底完善解决热敏灸医疗资源不足问题，从而推动热敏灸向全国乃至全球推广。”联想新视界PR主管唐榕蔓对记者说。

AR产品已融入各行各业。在圆周率的展台，见到了VR技术在直播领域的最新发展。圆周率市场总监李兴宇带记者体验了VR直播神器——Pilot Era。作为一台专业级智能8K全景相机，Pilot Era实时实现视频拼接技术，完成展览会场的AR直播。

展会国际化程度高

在2019VR/AR产品与应用展览会上，记者深刻感受到展会的国际影响力。据官方数据，本次展会上除了美国的两家知名企业（微软和Fingsoft）参展外，德国Dronoss、波兰Sensory等国家的企业也参加了展览，韩国组织了25家企业参展。在去年只有美国、日本和韩国组团参展的基础上，新增了5个国家的相关企业。

今年展会参展企业数量相比去年增加了30%，吸引了HTC、微软、联想、华为、故宫博物院、中科院、中国电信、中国移动、中国联通等VR行业的优秀企业参展。

在展会同期的2019世界VR产业大会产业对接会上，不少参展企业收获颇丰。南昌VR产业大力开展招商，通过广泛深入的对接洽谈，与企业达成发展共识。据记者现场了解，在本次对接会上，共签约项目104个，其中战略合作框架协议8个、投资合作项目96个，投资合作项目签约总金额652.56亿元。

社长：卢山 社址：北京市海淀区紫竹院路66号赛迪大厦18层 邮编：100048 每周二、五出版 周二8版 周五8版 零售4.50元 全年定价420元（包含手机客户端） 广告部：010-88558848/8808 发行部：010-88558777 京昌工商广登字第20170004号 经济日报印刷厂印刷