

# 引导企业进行工控安全防护能力迭代升级

中国电子信息产业发展研究院副院长 黄子河

为贯彻落实《国务院关于深化制造业与互联网融合发展的指导意见》,保障工业企业工业控制系统信息安全,工业和信息化部于2016年、2017年先后出台了《工业控制系统信息安全防护指南》(以下简称《防护指南》),以及《工业控制系统信息安全事件应急管理工作指南》《工业控制系统信息安全防护能力评估工作管理办法》和《工业控制系统信息安全行动计划》等多个政策性文件,对部分省市区工业和信息化主管部门相关同志和部分专业技术人员进行工业控制系统信息安全培训,并在一些工业企业开展工控系统安全防护能力验证工作,收到良好效果。

## 《防护指南》指导行业制定工作规范

《防护指南》在工业控制系统信息安全工作方面发挥了积极作用。

一是很好地指导了行业制定具有本行业特性的安全防护能力评估工作规范。不同行业的工控系统具有不同的工艺要求、生产流程、网络环境和上下游产业,对于工控系统信息安全工作也有不同的要求。以汽车制造行业为例,该行业涉及冲压、焊接、涂装、总装、机械零部件制造、电子零部件制造等生产环节,其工业控制系统具有智能化程度高、工业机器人应用广、上下游厂商数量多、生产分工细等特点。依据《防护指南》,行业用户可以进一步明确相关信息安全细则,合理控制、规避自身的工控系统安全风险。

二是很好地指导了第三方测评机构开展安全检查工作。第三方评测机构作为专业技术队伍,支撑工信部开展了工业控制系

统信息安全检查工作,摸清了行业企业工业控制系统信息安全现状,发现了安全风险和隐患,提出了整改建议,协助行业企业提升了工业控制系统信息安全防护技术水平,为形成较完善的工业控制系统信息安全检查工作制度奠定了基础。评测机构通过查找典型行业工业控制系统信息安全问题,进一步了解和掌握了我国部分典型行业工业控制系统的信息安全现状,通过分析工业控制系统信息安全整体防护能力和安全防护水平,提出了有效的安全解决方案、对策措施以及下一步工业控制系统信息安全工作重点,为政府部门制定国家工业控制系统信息安全战略规划及政策法规提供了参考依据。

## 《防护指南》提供信息安全指导参考依据

《防护指南》为应对工业互联网、工业APP等工业新常态的信息安全工作提供了

工业控制系统细分领域的信息安全指导参考依据。

一是为在工业互联网背景下的工控安全工作提供指导。工业互联网是支撑智能制造的关键综合信息基础设施,是将机器、人、控制系统与信息系统有效连接的网络信息系统,要求在安全可信的前提下,支撑实现单个机器到生产线、车间、工厂乃至整个工业体系的智能决策和动态优化。《防护指南》要求在工业云平台访问过程中使用身份认证管理,并明确了远程访问过程中的安全加固要求,提升了终端和数据传输过程中的安全防护能力。

二是为工业APP安全防护能力提供了安全指导参考依据。每个工业APP都承载了一定的工业知识和经验,关注于解决特定的工业问题,需要将多个工业APP组成一个有机整体,才能为工业企业提供完整的使用功能和解决方案。而这些可能来自于不同的开发者,也可能来自于工业企业的技术人员,也可能是在其他APP基础上二次开发形成的新APP,因此需要内部建立安全规范和防护体



系。《防护指南》要求建立工业控制系统配置清单,在配置变更前进行严格安全测试,并分离工业控制系统的开发、测试和生产环境,从而保障工业APP在开发过程中的安全属性。

## 依据《防护指南》落实安全保障工作

中国电子信息产业发展研究院依据《防护指南》,落实了多项安全保障工作。一是参照指南要求,建设工控系统通信总线信息安全仿真测试平台,并基于该项目承担了工业控制系统智能化安全云服务平台测试等工作。二是参与编写了《工业控制系统信息安全防护能力评估工作实施细则》《油气管道SCADA信息安全管理办

法》等规范。三是支撑工信部,按照《防护指南》要求,对石化化工、装备制造、汽车制造、能源、航空航天、烟草等重点行业企业进行工业控制系统信息安全检

查。四是在石油石化、电力、轨道交通等大型行业企业开展了油气管道SCADA系统信息安全测评,为油田工业控制系统提供信息安全风险评估服务等数十项控制系统的安全测评服务,通过发现问题并提出整改建议,切实引导工业企业进行工业控制系统信息安全防护能力的迭代升级。《防护指南》在过去三年内一直发挥着积极的作用。通过开展对工业控制系统信息安全自查、抽查工作,协助企业发现安全风险,提升了企业安全意识和防护水平以及专业技术队伍信息安全检查能力。在后续开展工业控制系统信息安全工作时,中国电子信息产业发展研究院将继续支撑工信部开展年度工控信息安全抽查、检查工作,参与《防护指南》相关标准的制修订工作,将《防护指南》的工作思路向各个重点行业推进并落实,进一步为工业控制系统、智能制造、工业互联网、人工智能与工业场景融合等新技术领域的信息安全工作提供信息安全的各项测评、咨询服务。

# 以标准服务带动市场 助力工控安全防护

中国电子技术标准化研究院  
副院长 杨建军

在工业互联网蓬勃发展的大时代背景下,工业控制系统中大量应用网络通信技术已成为现代工业的典型特征之一,但同时也为黑客提供了更加便利的入侵渠道,工控领域的信息安全问题日益凸显。为应对不断增长的工控安全风险,工业和信息化部于2016年10月正式印发了《工业控制系统信息安全防护指南》(以下简称《指南》),为工业企业、安全服务企业、地方主管部门围绕工业控制系统开展安全防护工作指明了正确方向。

## 积极科学引导 重点示范先行

《指南》发布以来,在工业和信息化部指导下,包括中国电子技术标准化研究院在内的部属技术支撑机构,每年根据产业发展状况、企业信息化水平、安全态势焦点等情况,选取具有典型代表性的重点工业企业开展工控安全检查评估专项工作,为工业企业“问诊把脉”,全面分析安全威胁现状,找准安全问题短板,开具堵漏补缺的整改“药方”,对企业乃至产业的整体工控安全防护水平提升具有重大促进作用。

三年来,工控安全检查评估专项已覆盖石油石化、煤化工、钢铁有色、汽车制造、能源电力、机械装备、电子制造等重要行业领域。同时,《指南》还带动了部分省市主管部门主动设立地方专项,对生产自动化、信息化程度较高的工业龙头企业实施跟踪服务式评估检查,工控安全隐患得以逐一排查,工控漏洞风险得到有效控制,降低了发生大规模工控安全事故的可能性,也使企业能够对自身工控安全状况做到心中有数。工控安全做得比较到位的部分企业还被评为示范单位,在行业内推广分享经验。

三年来,通过这种“政府搭台、机构主导、企业唱戏”的工控安全防护工作模式,工控安全的理念已在业界深入人心,大部分工业企业建立了科学的安全意识观,明确了要将“工控安全与

生产业务两手一起抓”作为长期发展指导思想,并能够从技术和管理双重维度部署安全防护工作,为重要工业控制系统的安全运行奠定了坚实基础。

## 深化落实“放管服” 以标准助力防护

今年6月,国务院召开的全国深化“放管服”改革优化营商环境电视电话会议对深化“放管服”改革作出部署,李克强总理强调要以习近平新时代中国特色社会主义思想为指导,认真贯彻党中央、国务院决策部署,推动“放管服”改革和优化营商环境取得更大成效。深入领会会议精神,从理论和实践结合上理解把握“放管服”改革的内涵、作用和走向,对我们持续推进工控安全防护工作有着重要意义。

国家统计局数据显示,截至2018年年底,全国规模以上工业企业共有37.8万家,平均每省超1.2万家,有的沿海发达省份甚至超过3万家。要在全 国范围内全面铺开工控安全防护工作,仅靠各级主管部门设立专项来推动显然是远远不够的,迫切需要转变工作思路和模式,充分依托市场化服务的力量来调动各参与方的主观积极性,彻底贯彻“网络安全全国一盘棋”的指导思想,在整体上提升和强化工控安全防护能力,而这也是与当前“放管服”改革目标方向相一致的。

围绕工业控制系统的信息安全标准化需求,中国电子技术标准化研究院研制了较为完善的标准体系,并持续推进国家标准立项和发布工作。截至2019年9月,全国信息安全标准化技术委员会(TC260)已发布相关国家标准13项,内容涵盖了工控设备安全、工控网络安全、安全分级、安全管理、风险评估、安全防护产品等方方面面,对工业企业、设备生产商、系统集成商、安全企业都具有重大指导意义。当前,我们正加速推动国标《信息安全技术 工业控制系统安全防护能力建设实施规范》研制、宣贯和发布工作,以便进一步完善和配合《指南》内容要求,同时通过全国范围的持续贯标培

训,加速培育一批专业化的标准服务队伍,扩充市场服务供给能力,形成国家级、地方级、行业级多样化的服务机构组织,以标准服务带动市场,助力工控安全防护。

## 对标核查防患于未然 齐头并进踏上新征程

为更快更好地落实工控安全防护工作新思路,在工信部软科的指导下,部属技术支撑机构正在开展或计划开展一系列配套工作:一是在全国选取了6省市作为先期试点,开展贯标培训深度行活动,以标准内容为核心,重点针对工控系统面临的安全威胁、常用的防护手段、典型安全事件、优秀实施案例等内容进行宣贯,为工业企业持续提供标准培训服务,扩大标准的影响力;二是依托中国电子工业标准化技术协会,成立工业控制系统信息安全防护能力推进分会,集结工控行业相关骨干企业,孵化和培育一批对标审核服务机构,构建对标服务供给能力;三是鼓励工业企业主动对标核查,无论是自对标还是采购对标服务,都能够使得企业对自身的工控安全防护状况有清醒的认识,并且制定可行的改进方案和实施目标,将安全风险降低到可控水平,持续有效保护工控资产。通过以上工作,在全国范围内开展贯标,构建起全国工控安全防护工作内生式发展的良好态势。

放眼整个世界工业领域,自动化、智能化、网联化是工业控制系统的大势所趋,工控安全已经是不得不考虑的关键影响因素,越是重要的工控系统越需要加固安全。委内瑞拉水电站遭受攻击引发大规模断电、挪威铝业集团工业控制系统危机导致生产停滞,这些案例不断警示着我们:工控安全是一项长期斗争,要切实且全面抓好防护工作。我国是工业大国,更是工业控制系统应用大国,要不留死角地落实好工控安全防护任务,我们的工作模式就需要与时俱进的转变。相信在“放管服”改革思想指导下,充分宣传、引导、利用标准化服务这一有力武器能够实现既定目标,推动工控安全防护全面迈入“齐头并进”的新征程。

# 为提升工控安全防护能力 提供专业服务

工业和信息化部电子第五研究所  
副所长 王勇

随着信息化和工业化深度融合,工业控制系统从单机走向互联、从封闭走向开放、从自动化走向智能化,为实现制造业数字化转型,不断提升制造业数字化、网络化、智能化发展水平,为推动我国制造业高质量发展提供了重要支撑。在显著提高生产力的同时,工业控制系统也面临着日益严峻的信息安全威胁。工业和信息化部于2016年10月印发了《工业控制系统信息安全防护指南》(以下简称《指南》),并组织编制了《工业控制系统信息安全防护建设实施规范》(以下简称《实施规范》)标准,指导企业提升安全防护水平,为我国制造业高质量发展保驾护航。工业和信息化部电子第五研究所(以下简称五所)持续开展贯标和评估服务,帮助各行业企业落实《指南》相关要求。

## 建立有效体系 形成规范化安全保障

工控安全防护能力贯标是在落实《指南》要求的基础上,形成对《指南》的有效补充。从工控安全防护设计、建设、运维全生命周期出发,帮助企业按照标准有关要求建立有效的工控安全管理和技术防护体系,形成规范化、体系化的安全保障,对推动两化深度融合、保障制造业高质量发展具有重要意义。

一是统一思想,提高认识。要充分认识开展工控安全防护贯标既是国家安全体系总体部署的要求,也是企业持续健康发展的基础。企业高层务必高度重视,统一思想,提高认识。全员参与,提升全员贯标意识,做到贯标工作人人有责,推行贯标人人尽责。

二是通力协作,加强沟通。工控安全防护能力贯标既涉及技术层面的物理与环境安全、数据安全防护、监测预警与态势感知等内容,也涉及管理层面的安全规划与机构建设、人员管理及培训、访问控制与审计等内容,要做到全面贯彻落实标准内容,必须做到技术部门和管理部门通力协作、生产部门和IT部门充分沟通。

三是梳理对标,有的放矢。在实施贯标工作前,企业必须充分梳理自身的需求,找到与标准之间的差距,在贯标过程中才能做到有的放矢,切实开展和落实纠正措施、预防措施等改进机制。在贯标完成后,通过不断检查和持续改进,确保各项措施得到正确的执行,才能保证贯标工作取得实实在在的效果。

四是借助力量,增强合作。企业在面对一个新的标准体系时,难免会遇到标准理解不深入的问题,

此时,可以借助政府行业指导经验、科研院所研究能力、技术服务提供商技术能力等专业机构力量,加强政产学研合作,加大与科研院所和技术服务提供商的对接,在其专业指导下开展贯标工作。

## 提升防护能力 构建良性发展格局

面对复杂多变的网络安全新形势,应当坚定不移地坚持以习近平新时代中国特色社会主义思想为指导,以工业企业安全防护能力提升为主线,调动政产学研各方资源,加强顶层设计、培育产业环境,加快推进工控安全保障体系建设,形成政策引导、标准支撑、产业创新的良性发展格局。

一是应用方示范,引领贯标工作扎实落地实施。各行业、各地区相关主管部门需加大工控安全贯标指导力度,结合本行业、本地区特点,推动工控安全防护能力本质贯标。通过培育工控安全防护典型成功案例,切实发挥示范带动作用,引领工控安全工作高质量落地落实。

二是需求侧牵引,切实提升工控防护本质安全。工业企业在开展本质贯标的过程中,加强工业控制系统及相关产品的安全性评价和筛选,从本质安全角度减少企业所面临的工控安全风险隐患。同时,推动工控厂商加快开展产学研用联合攻关,形成强安全性的工业控制系统和解决方案。

三是服务方推动,促进企业贯标能力广泛提升。各行业组织应加大力度推动工控安全标准的研制、验证和宣贯培训,引导企业开展自评估、自诊断和自对标;贯标服务机构加强服务能力建设,为工业企业提供有力的技术支撑、信息发布和测评服务。

新形势下,制造业高质量发展需要信息化与安全双轮驱动,以正确的安全防护观念为引导,构建多方参与、协同保护的发展格局。五所将继续加大投入,进一步提升工控安全技术水平和服务能力,发挥桥梁纽带作用推动政产学研用各方携手共进,推动《指南》落地落实,广泛提高我国工业企业工控安全防护水平,为制造业高质量发展提供坚实保障。