doi: 10.7690/bgzdh.2019.09.004

军工行业工业控制系统信息安全风险与对策

习　阳，李　凯，王　潇
（中国兵器工业信息中心，北京 100089）

摘要：针对军工行业工业控制系统面临的信息安全问题，对新业态环境下的信息安全风险进行探讨。阐述军工行业工业控制系统的发展历程，根据军工行业控制系统应用和信息安全的现状，对现有工业控制系统设备、数字化和信息化、信息安全技术标准与有关法规缺失等的信息安全风险进行分析，提出提升军工行业信息安全防护能力的对策。该研究有较高的实用参考价值。

关键词：军工行业；工业控制系统；信息安全
中图分类号：TP302　　**文献标志码：**A

Information Security Risk and Countermeasure of Industrial Control System in Military Industry

Xi Yang, Li Kai, Wang Xiao
(*Information Center of China North Industrial Group Corporation*, *Beijing* 100089, *China*)

Abstract: In view of the information security problems faced by the industrial control system in the military industry, the information security risks in the new industry environment are discussed. This paper expounds the development history of industrial control system in military industry. According to the application of control system in military industry and the current situation of information security, it analyses the information security risks of existing industrial control system equipment, digitalization and informatization, information security technical standards, and the absence of relevant laws and regulations, and puts forward some countermeasures to improve the information security protection capability of military industry. This study has a high practical reference value.

Keywords: military industry; industrial control system; information security

0　引言

信息化与工业化的加速融合使工业控制系统成为世界各国最重要的一类基础设备。军工行业是我国国防建设的保障。我国一直非常重视网络信息安全问题，通过抵御渗透、修复漏洞、查杀木马、反击黑客等手段进行防护，但信息安全形势仍日趋严峻。我国现行的互联网一直使用美国具有控制权的IPV4 或 IPV6 因特网根服务器(10 台在美国，1 台在日本，2 台在欧洲)；因此，我国现在的信息网络在本质上是不安全的。

根据 2017 年 6 月 1 日颁布的《中华人民共和国网络安全法》，工信部在 2017 年先后发布《工业控制系统信息安全事件应急管理工作指南》和《工业控制系统信息安全防护能力评估工作管理办法》[1]，与 2016 年颁布的《工业控制系统信息安全防护指南》形成工控安全管理体系。《中国制造 2025》中也提出了“加强智能制造工业控制系统网络安全保障能力建设，健全综合保障体系”。《国务院关于深化制造业与互联网融合发展的指导意见》把“提高工业信息系统安全水平”作为主要任务之一。2019 年，工信部发布了《工业控制系统信息安全行动计划(2018—2020)》[2]。这一系列国家和政府行为体现了提升我国工业控制系统信息安全防护能力的紧迫性。

笔者就军工行业工业控制系统面临的信息安全问题，从国家政策、法律法规、行业技术标准、技术创新与安全管理等多角度进行分析，提出若干应对措施与建议。

1　军工行业工控系统发展概况

1.1　军工行业工业控制系统发展概述

作为西方国家的禁运对象，我国军工行业工业控制系统的发展主要走自力更生、自主研发的道路。在 20 世纪 70—80 年代，通过技术改造，军工企业重点工序和关键零部件生产基本实现单机自动化，主要控制设备为机床数控系统、单板机、程序控制器等。在 20 世纪 90 年代，军工行业逐步建成了部

收稿日期：2019-04-02；**修回日期：**2019-05-20
作者简介：习　阳(1976—)，男，上海人，工程硕士，高级工程师，从事计算机网络技术及应用、计算机网络信息安全、计算机应用技术研究。E-mail: xiyangit@163.com。

分自动化生产线，其中既有部分引进的程序控制机组或固定产品生产线，又有军工院所与企业联合研制的示范性柔性或准柔性生产线，也建成了高危产品计算机控制演示验证生产线。进入 21 世纪后，军工行业实施了大规模的技术改造和军品科研生产能力建设，经过“十五”到“十二五”3 个“五年计划”的信息化、数字化的发展建设，在一些重点军品领域实现了科研、设计、制造、管理、服务一体化。“十三五”以来，军工行业工业控制系统进入智能化发展阶段；同时，在军工行业内也建立和形成了有关专业的先进工业技术创新中心，计算机控制系统在军工行业进入了广泛应用和发展时期。

1.2 军工行业工业控制系统应用现状

1) 军工行业工业控制系统采用的设备类型。

我国军工行业工业控制系统采用的控制设备主要有：分布式控制系统(distributed control system，DCS)、现场总线控制系统(fieldbus control system，FCS)、可编程逻辑控制器(programmable logic controller，PLC)和 PC 工控机组成的控制系统，具有网络通信接口的数控机床和现场控制计算机构成的生产线控制系统、数据采集与监控系统(supervisory control and data acquisition，SCADA)、智能仪表控制系统、嵌入式控制器构成的单机或机组控制系统和其他专用控制系统[3]。

2) 军工行业工业控制系统网络连接现状。

在我国军工行业的各专业领域或企业之间，工业控制系统的发展和应用水平存在一定差距。一些重点装备领域实现了科研、设计、制造、管理、服务一体化，即全流程的网络化和数字化；一些重点企业建成了由专用网络连接的自动化生产线并实现了生产线或车间级的管控一体化，通过专用接口与企业级管理信息系统实现了信息交换；但仍有较多的自动化生产线、数控系统或自动化机组设备尚未实现网络连接，处于单机或生产线独立运行状态，有关管理信息还靠人工录入和传递。

1.3 军工行业工业控制系统信息安全现状

1) 军工行业现有工业控制系统设备潜存极大安全风险。

我国军工行业已有的工业控制系统，无论采用的是通用的或专用的控制设备，还是进口或是国产设备，都缺乏安全防护能力，且设备中的核心硬件和系统软件均可能隐藏有后门或逻辑炸弹[4]。现有控制设备中的网络通信、远程诊断、设备调试和系统维护等接口(包括 USB、光驱等各种通用或专用通信接口)，很容易在执行常规的管控操作时被夹带的病毒入侵，或者被恶意代码作为入侵渠道。

2) 军工行业实现数字化和信息化潜在的信息安全风险。

军工企业为了实现管理与控制的一体化，提高企业信息化合综合自动化水平，实现生产和管理的高效率、高效益，引入了产品数据管理技术(product data management，PDM)、生产过程执行系统(manufacturing execution system，MES)，在管理信息网络与生产控制网络之间通过防火墙实现了数据交换[5]。现有防火墙与网络安全监测设备的防护能力有限，管理层网络连接的信息系统、信息设备，很容易遭到来自企业管理网或互联网的病毒、木马、黑客的攻击，而这些攻击又很有可能穿透管理层与控制层之间的防火墙而入侵底层控制网络。即使是在物理隔离状态下运行的管控一体化系统，安全防范工作偶尔的疏忽便可能导致严重后果。

3) 军工行业工业控制系统信息安全技术标准与有关法规缺失。

在军工行业现行的技术标准体系中，目前还没有针对军工行业工业控制系统的相应设计规范、技术标准、风险控制和安全管控法规，而民用行业工业控制系统信息安全技术标准不能满足军工行业的需求。标准的缺失，严重制约军工行业工业控制系统防护能力的提升。军工行业工业控制系统信息安全技术标准体系不仅应包含军工行业工业控制系统信息安全分级、安全要求、安全实施、安全测评方面的相关标准，而且应包含军工行业工业控制系统设备安全、工业互联网平台安全的相关标准。

2 提升信息安全防护能力的对策

1) 更新观念，落实军工行业工业控制系统信息安全主体责任。

军工行业应在工业化和信息化融合、军民融合发展的新业态环境下，更新安全观念，把工业控制系统信息安全植入企业的安全与风险管控体系中，并切实落实相关举措。在 2018 年发布的《工业控制系统信息安全行动计划(2018—2020)》中要求：军工企业作为关键信息基础设施发展建设规划的制定、建设和运营者，应承担提升工业控制系统信息安全防护能力的主体责任，军工主管部门应履行好监管责任，在信息安全与信息化建设中应做到“同步规划、同步建设、同步运行”。在“三同步”的全

流程中，应从技术、管理和运营等方面全面强化信息安全举措，在原有涉密信息管理中，补充和完善工业控制系统涉密信息安全的有关内容。

2) 大力协同，研究制定军工行业工业控制系统信息安全关技术标准。

建立军工行业工业控制系统信息安全关技术标准体系是一项系统工程，需要组织军工行业相互协作。军工行业工业控制系统信息安全技术标准的研究，将在军工行业工业控制网络安全隔离与信息交换、漏洞检测、网络安全监测及测试评价方法、安全控制应用和安全管理等方面，针对军工行业特殊需求制定相关技术标准，为提升军工行业信息安全防护能力提供技术标准支撑。这些标准一旦建立，就应在“三同步”的全流程中贯彻。

3) 开展军工行业工业控制系统信息安全防护能力评估。

评估军工行业工业控制系统信息安全防护能力，是对行业已经建成的工业控制系统存在的信息安全风险进行摸底排查的有效措施。通过评估，既可清楚行业工业控制系统信息安全的整体情况，又为进行分级分类管理、制定应对整改措施，全面提升信息安全防护能力积累基础信息。为此，笔者建议整合军工行业资源，建立军工行业工业控制系统信息安全防护能力评估队伍。

4) 加速研制核心技术安全可控的军工行业工业控制系统设备。

军工行业在工业控制计算机系统、智能控制技术与智能制造装备、控制与管理软件等专业领域，具有实力雄厚的创新研发和一定的产业化能力，在武器系统信息化、高可靠工业控制系统、高危产品自动化生产线控制系统与设备、应用软件开发和智能制造系统成套解决方案等方面具有专业的研发机构或创新中心，而且熟悉军工行业特殊需求。笔者认为：1) 在现行网络框架下，通过收集整理军工行业工业控制系统信息安全产品白名单存在的缺口，组织现有资源，研发满足军工行业特殊需求，拥有自主知识产权、安全可控、可信可用、具备信息安全防护技术的设备；2) 加速组织我国具有主控权的 IPV9 架构网络标准体系在军工行业工业控制系统中的应用试点，研发与之相关的配套设备和产品。前者是在 IPV4/IPV6 体系下的权宜之计；后者才是彻底解决“互联网核心技术是我们最大的‘命门’”的根本途径。

3　结束语

彻底解决具有主控权的安全网络系统已经十分紧迫。笔者通过技术手段，尽可能堵塞网络后门，修补程序漏洞，防止非法入侵，避免自身敏感信息被窃取；同时，通过严格的管理手段，尽可能不给入侵者提供任何可乘之机。

参考文献：

[1] 2017 国内工业控制系统信息安全十大新闻[Z]. 2017. 12.22. http://www.icsisia.com.

[2] 工信部信软[2017]316 号. 工业控制系统信息安全行动计划(2018—2020 年)的通知[Z]. 2017, 12, 12.

[3] 方来华. 工业控制系统的信息安全研究[C]. 北京: 中国自动化学会, 2008.

[4] 何之栋. 工业控制系统的信息安全问题研究[J]. 工业控制计算机, 2013(10): 1-4.

[5] 林诗美. 工业控制系统信息安全防护方法探讨[J]. 电子制作, 2015(12X): 44.