智能生产时代下的网络安全策略研究

梁冬晗[1]，曹亚芳[2]

（1. 国家工业信息安全发展研究中心，北京 100040；2. 山西省经济信息中心，太原 030002）

摘要：智能生产时代下，互联网和物联网的普遍应用、连接性的不断增加，颠覆了传统生产模式的同时，也带来了与之相匹配的网络风险和安全挑战，针对工业领域的安全事件频发，影响愈发广泛。然而网络安全策略却未能引起制造企业的足够重视与支持，网络安全人才匮乏使得制造业不断面临新的网络安全挑战。智能生产环境下的网络安全策略不容忽视，应从一开始就全面融入智能制造战略内容中。

关键词：智能生产；网络安全；数字供应网络；智能制造

中图分类号：F424.3 **文献标志码**：A **文章编号**：1671－1807(2018)01－0139－04

智能生产是指通过使用智能、联网、自动化技术等，使数字世界与物理世界活动相结合，从数字供应网络到智能工厂再到连接对象，将供应链、工厂、客户和运营连接在一起的工业生产过程。其产品集成了动态数字存储、感知和通信能力，承载着在整个供应链和生命周期中所需的各种必要信息。设施由整个生产价值链所集成，且能够根据当前的状况灵活决定生产过程。在智能生产时代下，互联网和物联网的普遍应用，连接性的不断增加，颠覆了传统生产模式的同时，也带来了与之相匹配的网络风险和安全挑战。以美国为首的发达国家高度重视工业领域的网络安全工作。2016年11月，美国国土安全部出版的《保护物联网的战略原则》，提出了加强物联网安全性的方法和建议，并建议通过检查关键嵌入式系统制造商直接或间接在生产中部署的相关风险，制定保护关键嵌入式系统的物联网的安全原则和安全策略。智能生产环境下的网络安全策略不容忽视，应从一开始就全面融入智能制造战略内容中。

1 智能生产时代网络风险和安全挑战问题日益突出

连接性的增加和智能化技术的广泛应用是智能生产时代的一个显著特征，随着制造业各环节越来越多的设备和产品连接到网络中，企业越来越多的使用智能、无线网络和传感器等信息技术、连接技术创新、现代化转型等方式进行生产活动。使得可能出现的网络漏洞随着连接的增加而增加，攻击剖面大大扩大，高度连接的环境意味着网络攻击能产生比以往任何时候都更加广泛的影响，这种影响不断增加且多样化，甚至呈指数级增长。工业领域相关安全事件陆续曝光，如2010年震网（Stuxnet）病毒攻击伊朗核电站，使得8 000台离心机损坏。Stuxnet的复杂性是网络攻击作为武器进入物理工厂最典型的范例；供应链安全方面，2014年Havex利用供应商软件网站的“水坑攻击”影响了欧美1 000多家能源企业；2015年Blackengergy造成了乌克兰境内近三分之一地区持续断电。近日，WannaCry勒索病毒又攻击了日本本田工厂的网络和澳大利亚的交通摄像机，它从5月开始在全球范围内爆发。

1.1 网络贯穿于智能生产生命周期始终，网络风险和安全挑战影响愈加广泛

智能生产生命周期从数字供应网络到智能工厂再到连接对象，当供应链、工厂、客户和运营连接在一起时，网络威胁造成的风险和潜力都将不断扩大。通过在整个生态系统中引入智能、连接平台和设备，促使传统的线性供应链结构进一步发展，从而产生数字供应网络，能够从价值链上的点获取数据以相互通知，能更好地管理和流通材料和产品，更有效的利用资源，供给的产品能更好地满足客户需求。在数字供应网络中，从设计到运营等各个环节相互联系越来越频繁，每个阶段都要妥善规划考虑网络存在的弱点和风险。智能生产生命周期各阶段对网络的需求（如表1）[1]。

收稿日期：2017－09－26

作者简介：梁冬晗（1986－），女，北京人，国家工业信息安全发展研究中心，工程师，数量经济学硕士，研究方向：信息通信产业经济运行；曹亚芳（1985－），女，山西吕梁人，山西省经济信息中心，经济师，研究方向：产业经济和区域经济。

表 1　智能生产生命周期各阶段的网络需求

生产周期的阶段	网络内容	网络需求
数字供应网络	数据共享	确保系统的完整性，因此无法访问私有专有数据
	供应商处理	当流程无法验证时，确保信任
智能工厂	健康和安全	确保职工和环境的安全
	生产和工艺弹性且有效率	确保生产不间断且能恢复关键系统
	仪器仪表和主动解决问题的能力	维护企业的品牌和声誉
	系统的可操作性、可靠性和完整性	支持使用多个供应商和软件版本
	效率和成本回避	通过远程诊断和控制来降低运营成本且提升灵活性
	监管和职责调查	确保过程可靠性
连接物体	生产设计	在开发生命周期中使用安全软件来实现生产功能和设备安全
	数据保护	在数据生命周期中保持敏感数据的安全
	面对攻击的修复能力	最小化事件的影响，同时快速恢复操作和安全性

来源：德勤。

1.2　网络漏洞随着连接性的增加而增加，智能制造攻击剖面不断扩大

智能工厂则面临从设备层、控制层、网络层、应用层、工业云、到数据层等方面的网络风险和安全挑战（如表 2）。据 2016 年德勤 MAPI 的研究发现，三分之一的制造商还没有对工厂里的工业控制系统进行任何网络风险评估。

表 2　智能工厂面临的网络风险和挑战

攻击面	网络风险和安全挑战
设备层	智能制造领域网络中伺服驱动器、智能输入输出系统、智能传感器、仪表、智能产品的安全挑战，包括：所用芯片安全、嵌入式操作系统安全、编码规范安全、第三方应用软件安全以及功能安全等，这些设备均可能存在漏洞、缺陷、规范使用、后门等安全挑战。
控制层	机床数控系统、PLC、运动控制器、所使用的控制协议、控制平台、控制软件等方面，其在设计之初可能未考虑完整性、身份校验等安全需求，存在输入验证，许可、授权与访问控制不严格，不当身份验证，配置维护不足，凭证管理不严，加密算法过时等安全挑战。
网络层	各类数控系统、PLC、应用服务器通过有线网络或无线网络连接，形成工业网络，工业网络与办公网络连接形成企业内部网络，企业内部网络与外面的云平台连接、第三方供应链连接、客户的网络连接。主要安全挑战包括：网络数据传递过程的常见网络威胁（如：拒绝服务、中间人攻击等），网络传输链路上的硬件和软件安全（如：软件漏洞、配置不合理等），无线网络技术使用带来的网络防护边界模糊等。
应用层	支撑工业互联网业务运行的应用软件及平台的安全
工业云	云平台及服务也面临着虚拟化中常见的违规接入、内部入侵、多租户风险、跳板入侵、内部外联、社工攻击等内外部安全挑战。
数据层	智能制造工厂内部生产管理数据、生产操作数据以及工厂外部数据等各类数据的安全问题，不管数据是通过大数据平台存储、还是分布在用户、生产终端、设计服务器等多种设备上，海量数据都将面临数据丢失、泄露、篡改等安全威胁。

1.3　网络安全未能引起制造企业的足够支持，网络安全人才匮乏

企业对网络安全支持力度不够。尽管现在制造企业越来越重视公司的网络风险状况，高级管理层致力于改善网络环境，但据德勤数据统计，42％的网络风险管理人员表示在公司获得资金支持关键网络计划仍然是一个挑战。据卡巴斯基实验室调查显示，2016 年，每两家工业控制系统公司中，就有一家经历过 1～5 次安全事故。平均来看，无效的网络安全给工业机构平均造成每年 497 000 美元的损失。尽管大多数工业机构认为自己已经准备好应对网络安全事故，但他们的这种自信似乎并不充分。

员工对网络安全的意识薄弱也是一大威胁。企业内部人员有意识或无意识的行为，可能破坏工业系统、传播恶意软件、忽略工作异常等，因为网络的广泛使用，这些挑战的影响将会急剧放大，针对人的社会工程学、钓鱼攻击、邮件扫描攻击等大量攻击都利用了员工无意泄露的敏感信息。

网络安全技术人才匮乏也是制造商面临的重大挑战。据 2016 年德勤-MAPI 研究发现，75％的受访

主管认为他们缺乏有效实施和维护安全的生产生态系统所需的技术人才资源。

1.4 网络攻击不断向智能制造领域渗透，高级持续性威胁不断进化

由于工业系统关系到国计民生，近年来已成为网络黑客们研究攻击的重点对象。根据美国工业控制系统网络应急小组的报告显示，2015 年处置的工业系统相关的安全事件高达 295 件，其中关键制造占比 33%，能源行业占比 16%。攻击者目标可能是偷取重点智能制造企业的产品设计资料、产品应用数据等，也可能是在关键时刻让智能制造企业生产停止、良品率下降、服务不及时等给企业造成直接损失，攻击者精心策划、为了达成既定目标，长期持续的进行攻击，其攻击过程包括收集各类信息收集、入侵技术准备、渗透准备、入侵攻击、长期潜伏和等待、深度渗透、痕迹消除等一系列精密攻击环节。

2 智能生产时代的网络安全策略应是安全的、警觉的和修复能力强的

随着连接技术的广泛使用，网络风险不断增长和变化，对于从数字供应网络到智能工厂再到连接对象价值链上每个环节的每个阶段，网络风险可能都会有所不同。智能生产生命周期各环节的网络安全策略是不尽相同的，但基本涵盖了安全性、警觉性和复原力三方面。

2.1 既能开放数据共享，又要保护私有专有数据

在数字供应网络中，数字技术有能力推动供应链元素的融合，但随着从设计到运营等各个环节相互联系越来越频繁，网络风险也相应扩大。它允许基于购买者和供应商的供需状态对产品和材料进行实时、动态定价。但是这种响应敏捷的灵活网络只有通过供应网络中所有参与者的开放数据共享才能实现，这就产生了重大的障碍，在允许某些数据的透明度和维护核心技术和机密等其他信息的安全性之间难以平衡。

2.2 既能在网络上支付验收，又要避免受到网络威胁欺诈

由于供应网络各个环节紧密的合作关系加强了企业之间的关联性，且开放的环境和动态的特征，成员之间可以进行高效率、低成本的信息共享，且能在网络平台上进行支付验收，简化了支付和验收流程。在数字供应网络中，如何保证商品的真实性，提供真实的物流信息、产品信息等，为买卖双方提供保护，从而免受欺诈性供应商、国际制裁的供应商和次品分销商的威胁。

2.3 保证智能工厂生产过程的可用性和完整性，增强事故的复原力和复原效率

智能工厂的目标主要集中在物理过程的可用性和完整性上，而不是信息的保密性。对于生产和制造设施，重要的是最大限度地提高制造资产利用率，同时最大限度地减少停机时间。对于制造商而言，至关重要的是确保连续生产，对于一些连续运转的设施，关机和停机可能导致昂贵的原材料损失。随着生产设备增加了物联网设备的集成应用，考虑物联网设备对制造生产和网络安全风险变的更加重要，受损的物联网设备的安全隐患包括生产停机、设备或设施的损坏等系列问题，关键流程恢复所需的重建和重新启动能力，也就是生产和工艺流程的复原力和复原效率是智能制造环节的网络安全挑战。

总而言之，虽然在整个智能生产过程打造安全和警觉的网络环境，能够应对大多数攻击者形成有效震慑，然而建设对所有攻击都完全免疫的网络环境是不现实的。如果攻击不可避免的来临时，应具备积极制定应对方案并快速修复的能力，尽量降低事故带来的影响。

3 智能生产时代的网络安全保障工作思路

3.1 将网络安全纳入智能生产生命周期的规划，规范网络安全管理控制机制

在智能生产的规划环节就将网络安全纳入到设计中，在企业内部管理中成立专门负责网络安全管理的机构，对构建网络安全环境给予资金支持，定期对智能生产网络进行合规性安全检查。建立一个关键利益相关者的跨职能团队，包括信息技术，运营技术，研发，财务和风险管控等方面；创建所有连接设备清单，进行统一规划管理；评估与关键合作伙伴建立的创新网络风险及与工业生态系统相关的第三方网络风险。

3.2 利用人工智能、深度学习等技术进行威胁监测检测，建立实时自动网络防御系统

利用人工智能技术扫描网络，识别软件漏洞并在无人为干预的情况下应用补丁，从而降低网络风险。建立实时自动化的网络防御系统，并且能够快速且大量的应对新的攻击手法，来应对频发的网络攻击，并降低攻击出现到防御生效之间的时间差。

3.3 利用大数据、数据挖掘等技术主动挖掘网络漏洞，构建网络风险识别模型

运用大数据技术主动挖掘漏洞，及时发现未知威胁，对有目的的攻击进行有效阻断。构建网络风险识别模型，通过识别网络通用及专属协议内容，并根据

其中包含的主从关系、访问控制、行为特征、传递途径、命令请求等信息提取非法特征，最后通过加权的方式判断威胁是否存在。

3.4 利用加密、认证签名、区块链等技术保护信息数据，建立安全的信息共享平台

将可信平台模块或硬件安全模块等技术纳入到相关设备中，以提供密码学支持，硬件认证和授权认证等。将其与访问控制相结合，关键任务操作在应用程序点和端点都能得到安全防护，从而保护数据和进程。如果处于休眠中或者通信传输中的数据被拦截或系统被破坏，能够利用诸如加密或者标记化的工具来保护它们。还可以通过区块链技术创建透明可靠的统一信息平台，提高供应链管理的效率，并且保护企业免受欺诈性供应商、国际制裁的供应商和次品分销商的威胁。

参考文献

[1] RENé WASLO，TYLER LEWIS，RAMSEY HAJJ，ROBERT CARTON. Industry 4.0 and cybersecurity managing risk in an age of connected production[EB/OL]. (2017－03－21). https://dupress.deloitte.com/dup－us－en/focus/industry－4－0/cybersecurity－managing－risk－in－age－of－connected－production.html.

[2] 李鸿培，李强. 工业互联网的安全研究与实践[J]. 电信网技术，2016(8)：20－26.

[3] 叶征. “工业4.0”时代网络安全冲击波来势汹涌[J]. 中国信息安全，2015(1)：114－115.

[4] 饶晔. 德国“工业4.0”中的网络安全[N]. 学习时报，2014－07－21(007).

[5] 王德吉. “互联网＋”时代的工业4.0信息安全探索与实践[C]//中国烟草学会2016年度优秀论文汇编——信息化管理主题. 2016：10.

Research on Cybersecurity Policy in the Era of Intelligent Production

LIANG Dong-han[1]，CAO Ya-fang[2]

(1. National Research Center for Industrial Information Security Development，Beijing 100040，China；
2. Shanxi Economic Information Center，Taiyuan 030002，China)

Abstract：In the era of intelligent production，the universal application of the Internet and the Internet of Things，the increasing connectivity，the subversion of the traditional production mode，but also brought with the matching network risk and security challenges，for the industrial areas of security incidents ，The impact of increasingly widespread. However，the network security strategy has not caused enough attention and support of manufacturing enterprises，the lack of network security personnel makes the manufacturing industry continue to face new network security challenges. Intelligent production environment under the network security strategy can not be ignored，should be fully integrated from the beginning into the intelligent manufacturing strategy content. Using a new generation of information technology to ensure the integrity of the intelligent production process，fluency and security.

Key words：intelligent production；cybersecurity；digital supply network；intelligent manufacturing

(上接第97页)

Empirical Analysis of Influencing Factors of Urban Residents' Domestic Water

——Chengdu city as an example

XIONG Sheng-yin

(China Western Economics Research Center，Southwestern University of Finance and Economics，Chengdu 610074，China)

Abstract：In this paper，by analyzing the influencing factors of urban domestic water，according to the present situation of chengdu urban residents living water and take integrated urban population，per capita daily life water consumption，per capita disposable income，water price four representative scalar，through stationarity test and cointegration analysis，using cochran-orcutt iterative correction method to establish the regression model. The results showed that：① urban population increased by 1%，water demand will rise by 0.943%. ②Prices rose 1%，residents' demand for water decreased by 0.016%，and resident income increase the same proportion，demand will rise 0.232%. ③the growth of urban population to the life water consumption is the most significant effect，inhibition rate increases the demand pull function on the water demand more than the income is much smaller. This paper for effective management of urban residents living water，from a given ladder water price，strengthening propaganda，perfecting laws and regulations，Suggestions to promote water-saving technology and so on.

Key words：urban residents；domestic water；influence factors