工业物联网安全与核心技术国产化

倪光南
（中国科学院计算技术研究所，北京 100190）

摘　要：以工业控制系统为切入点，详细分析了工业物联网面临的安全问题和国家网络安全战略，阐述了核心技术国产化的重要性。针对工业物联网的核心技术之一——桌面计算机技术，论述了打破 Wintel 体系垄断的必要性及有利条件，给出了 2 条替代 Wintel 体系的途径和关键技术，综合分析了我国安全可控桌面计算机技术体系现状和应用成果，最后为我国网络安全和信息化技术的未来发展提出了几点建设性意见。

关键词：工业物联网；安全；工业控制系统；Wintel；国产化
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.2096-3750.2018.00046

Security of the industrial Internet of things and localization of the core technology

NI Guangnan
Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190, China

Abstract: With the industrial control system as the breakthrough point, the security problems and national network security strategy of the industrial Internet of things were analyzed in detail, and the importance of the localization of the core technology was expounded. Taking the desktop computer technology, which was one of the core technologies of the industrial Internet of things, as an example, the necessity and favorable conditions for breaking the Wintel system monopoly was expounded, two ways and key technologies to replace the Wintel system were given, and the present status and application results of the security controlled desktop computer technology system in China was analyzed. Finally, suggestions for the future development of China's network security and information technology were put forward.

Key words: industrial of Internet of things, security, industrial control system, Wintel, localization

1　引言

近年来，物联网的发展迅猛，使各种实际应用不断落地，促进了社会经济发展，并逐步改变人们的生活方式，在国际范围内已得到普遍认可。我国也出台了相应的发展规划，物联网已经成为新一代信息技术的重要组成部分，其发展趋势十分明显。美国 2016 年公布的《2016-2045 年新兴科技趋势——领先预测综合报告（2016 年 4 月）》认为，到 2045 年将会有包括移动手机和可穿戴设备、医疗器械、电器、工业传感器、监控摄像头、汽车、衣服等超过 1 000 亿的设施与网络连接。这些设施使原来需要劳动力的检测、管理和维修等工作实现全自动化[1]。

我国在物联网领域的发展较快，具备人才、市场、技术等多方面的优势，完全有可能在物联网的某些领域引领潮流，从跟跑者变成领跑者。但需要注意的是，我国在物联网的基础设备方面还存在短板，而美国等发达国家在这方面很有优势[2-5]。例如，我国的芯片设计能力发展较快，但制造能力不足。相比之下，我国软件的相关产业则发展较快，因为其主要依赖的是人的智力，对传统的工业基础依赖较少。如果未来物联网的发展能尽量发挥软件优势，并与应用紧密结合，那么我国的物联网发展还是具备一定优势的。

收稿日期：2018-02-26；**修回日期**：2018-05-09

工业物联网是智能制造提升的关键所在。它将具有感知、监控能力的各类传感器、控制器和专用设备以及先进的信息技术不断融入工业生产过程的各个环节，收集数据并执行大量扩展企业能力的任务，从而大幅度提高生产效率与企业竞争力，有助于推动人、社会与自然的协调、和谐发展，最终实现将传统工业提升到智能化的新阶段。因此，我们应当紧密结合《中国制造 2025》战略实施物联网发展，尤其是对工业物联网的建设[6-8]。

然而，随着万物互联时代的到来，物联网的安全问题也日益凸显。有预测称未来 30 年里，随着物联网的发展以及日常生活中越来越多的连接，网络安全将会成为网络行业首要的话题。安全和发展的同步推进非常重要。未来应当争取发展安全、可控的物联网，这需要通过自主创新、掌握关键核心技术来实现。本文将重点关注工业物联网中的工业控制系统面临的安全问题和挑战，并以工业物联网中的核心技术——桌面计算机技术为例，详细分析了核心技术国产化的重要性和应对思路。

2　工业物联网的安全问题

如图 1 所示，工业物联网是智能制造体系和工业互联网的主体，而工业物联网包含智能工厂，作为智能工厂主要成分的工业控制系统（以下简称工控系统），其安全对工业物联网的安全有重大意义。工业控制系统作为军工国防科技、电网电力、石油石化、电信、煤炭、民航、航运等国家命脉行业的重要基础设施，在网络信息安全攻防战日趋激烈的今天，面临着持续攀升的安全风险。安全漏洞的不断涌现，将影响正常的生产秩序，甚至会危及人员健康和公共财产安全。

2.1　工业控制系统安全形势

工业控制系统是由服务器、终端、前端的实时操作系统等共同构成的网络体系，因此其安全问题不仅包括直接用于控制的实时操作系统设备的安全，还包括物理层、网络层、主机层、应用层等传统信息安全问题。在工业控制系统中，大多数工业控制软件都是运行在通用的操作系统上的，系统漏洞无法避免，安全性没有保障；另外，大多工业控制网络都属于专用内部网络，即使安装反病毒软件，也不能及时更新病毒数据库，给病毒、恶意代码的扩散留下了空间。 据了解，2010 年伊朗核设施遭受“震网”病毒攻击导致无法正常运行，该事件是世界上首例“网络超级武器”事件，直击伊朗核工业。由此可见，针对工业控制系统的攻击行为，已经对国家安全和社会发展产生深远的影响。事实上，不仅是“震网”病毒，近年来相继涌现出的著名恶意软件如“火焰”病毒、“Havex”病毒、“超

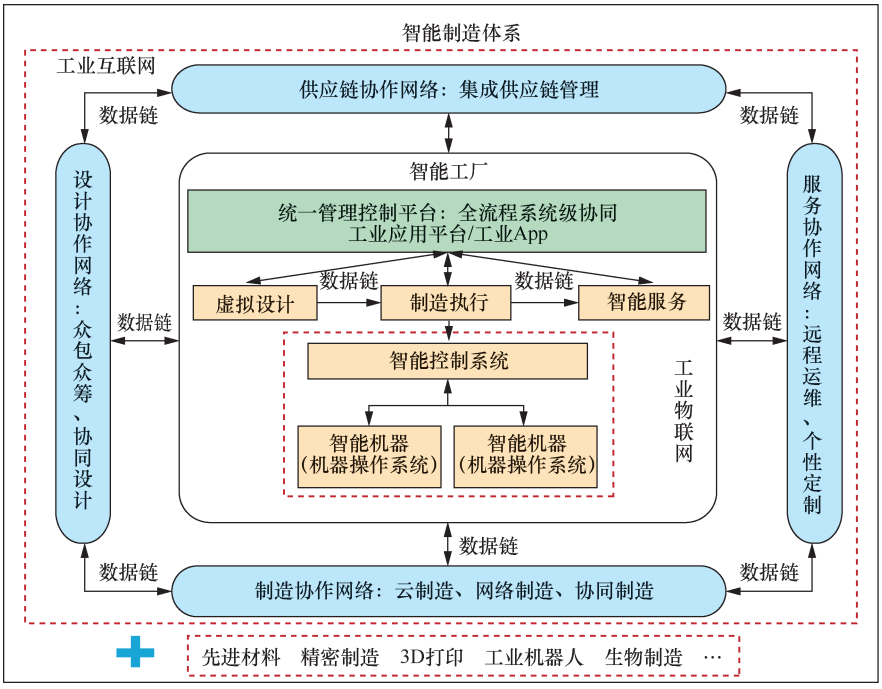

图 1　智能制造体系

级电厂”病毒、“BlackEnergy”病毒等，也将攻击重心向石油石化、电网电力等国家命脉行业领域倾斜，工业控制系统面临的安全形势越来越严峻。

我国工业控制系统大多集中在北京、上海、广州和东部经济发达地区。工业控制系统漏洞的类型分布广泛，包括跨站脚本、数字错误、代码注入等27 种以上。其中，缓冲区溢出、信息泄露和输入验证分列漏洞类型前三甲，如图 2 所示。截至 2016 年 12 月，据国家信息安全漏洞共享平台（CNVD）、美国 CVE、ICS-CERT、NVD 发布的漏洞数据统计，与工业控制系统相关的漏洞多达 984 个，2010 年后工业控制相关漏洞增长较快，年增长率达到 15%左右，2016 年新增工业控制安全漏洞为 181 个，安全形势非常严峻。

目前，针对工业控制系统的定向攻击正成为敌对势力和网络犯罪集团实施渗透攫取利益的重点对象，极有可能对涉及国计民生的重要基础设施造成严重损害。我国工业控制系统的安全威胁主要来自工业控制设备的高危漏洞、国外设备后门、高级持续性威胁（APT）、工业网络病毒、工业互联网应用的风险。究其原因，主要包括如下 4 个方面。

1) 互联网化带来内部威胁

① 与外部系统互联互通，如基于通信的列车自动控制系统（CBTC, communication based train control system）与综合监控系统（ISCS, integrated supervisory and control system）、乘客信息系统（PIS, passenger information system）、广播（PA, public address）系统等。

② 无纸化办公的方式使重要信息存在内网中，信息容易被窃取、泄露。

③ 多种电子信息管理系统的使用给轨道交通信息网络带来了信息安全风险。

④ 研究表明，70%的信息安全事故来自企业内网，主要包括误用和滥用。

2) 网络攻击多种多样

① 网络攻击手段日趋多样，典型的手段包括 DoS/DDoS 攻击、外部入侵、IP 欺骗、网络嗅探、木马攻击和垃圾信息等。

② 主要攻击手段由单一手段向多种手段结合的综合性攻击方向发展。

3) 工业控制设备脆弱性

① 工业控制设备（PLC、DCS、SCADA）和工业控制协议中普遍存在安全漏洞，主流工业控制设备厂商无一幸免。

② 进口工业控制设备后门广泛存在，操作站和冗程师站存在较多远程维护端口和后门。

③ 核心控制系统和设备严重依赖进口。

4) 行为审计与管理缺乏

① 入侵行为看不见、安全事件查不到、关键资产不掌握、安全风险不了解。

② 缺少对流量的实时监控和记录，就无法发现高级持续威胁。

③ 缺少对安全防护设备的综合管理和运维，各设备没有形成安全合力。

④ 安全管理不完善。

⑤ 缺少安全防护应急处置。

2.2　增强工控系统安全的国家网络安全战略

网络空间安全已成为陆海空天之外的第五大国家主权领域空间，保卫网络安全就是保卫国家主权。在此背景下，2016 年 4 月 19 日，习近平总书记关于网络安全和信息化工作的讲话要求：树立正确的网络安全观；加快构建关键信息基础设施安全

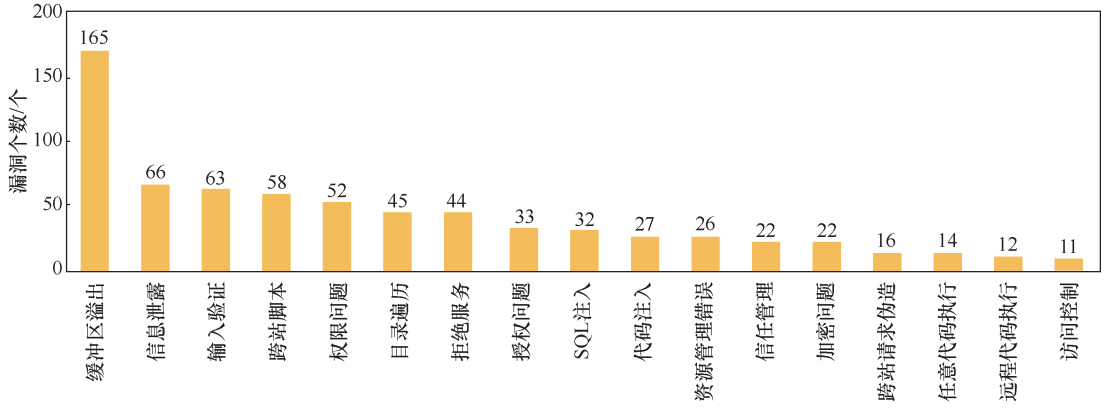

图 2　2000-2016 年公开工控漏洞主要类型

保障体系；全天候全方位感知网络安全态势；增强网络安全防御能力和威慑能力[9]。2016 年 11 月 3 日，工业和信息化部正式发布《关于印发<工业控制系统信息安全防护指南>的通知》。2016 年 11 月 7 日，《中华人民共和国网络安全法》正式颁布。2017 年 1 月，《信息安全技术网络安全等级保护基本要求第 4 部分：物联网安全扩展要求》征求意见稿在国家标准化管理委员会网站发布。2017 年 12 月发布的《工业控制系统信息安全行动计划（2018-2020 年）》中提到，2018-2020 年的工作重点和目标是建成全国在线监测网络、应急资源库、仿真测试、信息共享、信息通报平台，态势感知、安全防护、应急处理能力显著提升。可见，国家层面已出台多项政策，为应对工业控制系统的安全问题指明了方向。当前，我国工业控制系统受到核心技术限制、系统结构复杂、缺乏安全与管理标准等诸多因素影响，运行在工业控制系统中的数据及操作指令随时可能遭受来自敌对势力、商业间谍、网络犯罪团伙的破坏。因此，“政、产、学、研、用”各界人士应该积极响应国家号召，掌握核心技术。本文以工业物联网中的关键技术之一——桌面计算机技术为例，分析核心技术国产化的必要性和可行路径。

3　打破 Wintel 体系垄断的必要性及有利条件

众所周知，信息化时代各个领域都离不开桌面计算机的应用，尤其是智能制造领域，然而目前在世界桌面计算机领域占据垄断地位的仍然是 Wintel 体系，即由微软公司的 Windows 操作系统和英特尔公司的 CPU 构成的计算机技术体系，两者是桌面计算机领域的关键核心技术，采用 Wintel 体系就必然在这 2 项核心技术上受制于人，既无法保障网络安全，也无法保障产业发展。微软公司宣称到 2020 年 1 月将结束对 Windows7 的技术支持，旨在迫使用户采用 Windows10。鉴于 Windows10 不可控，政府和重要领域不能使用，使得加快推进以国产 Linux 操作系统替代 Windows 迫在眉睫，也再一次印证掌握核心技术的重要性。

习近平总书记在论述网络强国建设时提出：“加快推进国产自主可控替代计划、构建安全可控的信息技术体系、实施网络信息领域核心技术设备攻坚战略等举措”。在卫星导航领域，我国已经能用北斗卫星导航系统替代全球定位系统（GPS, global positioning system），在桌面计算机领域应以此为榜样，加快推进用安全可控的桌面计算机技术体系替代 Wintel 体系。

Wintel 已走过 20 多年的历程，无论是作为技术体系还是商业联盟，它都已明显地走向衰落，具体表现如下。

1) 在云计算和服务器领域，采用开源 Linux 操作系统和非 Intel CPU 的数据中心越来越多，在这个领域 Wintel 已经没有优势。

2) 即使在 Wintel 长期垄断的桌面领域，其市场份额也在缩减。据统计，目前 Mac OS 占据 9.02%的份额，Linux 占据 2.12%的份额，另外，谷歌公司的 Chromebook 在美国教育市场已占据 50%的份额。当前，中国推进对 Wintel 的替代也将加速这种趋势。

3) 随着移动生态系统的迅速发展，移动生态变得越来越重要，大大削减了 Wintel 在生态系统方面的优势。

4　替代 Wintel 体系的途径

如何应对 2020 年微软公司结束对 Windows7 技术支持的困境、如何保障停止服务的 Windows7 系统的安全，是各界困扰和迫切需要解决的问题，笔者认为有以下 2 种途径。

1) 依赖于微软的 Windows7 加固途径：由某些厂商与微软公司合作。

2) 不依赖于微软的途径：Windows7 主机可信免疫防御解决方案、智能动态防御技术解决方案。

下面将分别针对以上途径，对有代表性的解决方案进行阐述。

4.1　依赖于微软的 Windows7 加固方案

WindowsXP 停止服务后，某些安全厂商与微软合作，在一定期限内提供“加固”WindowsXP 版，如 360 公司推出的“360XP 盾甲”，这种方式也许会在 Windows7 停止服务后重现，但是这种方式的主动权仍在微软公司手中，用户也需花费一定的代价，既是被动的，又不能一劳永逸。

4.2　Windows7 主机可信免疫防御解决方案

以北京可信华泰信息技术有限公司为例，可信计算安全体系架构如图 3 所示，包括硬件层、操作系统层、应用层。硬件层指可信芯片。操作系统层主要指可信软件基（TSB），TSB 是基于可信计算机平台的硬件资源，提供支持可信计算目标的可信服

务，通过度量与认证保证系统软件和环境的可信性。应用层包括可信安全管理平台和可信软件库，其中，可信安全管理平台是协助用户实现安全策略管理、安全组织管理、安全运作管理和安全技术框架的中心枢纽，它是一种安全管理的形式，其职能分成管理层的职能和技术层的职能，能有效地将企业的策略管理、安全组织管理、安全运作管理和安全技术框架结合在一起，保持一致性。

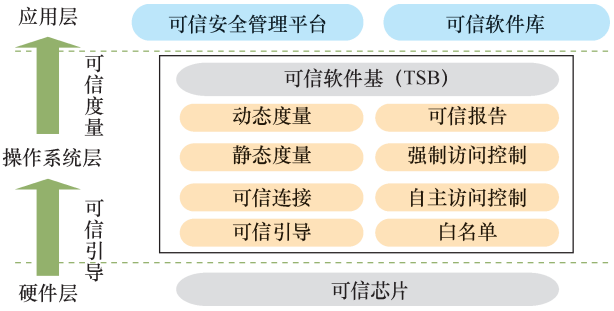

图 3　可信计算安全体系架构

主动免疫可信 3.0 体系结构如图 4 所示。

4.3　智能动态防御技术解决方案

以北京卫达科技有限公司为例，从设计思路、关键技术的角度阐述智能动态防御技术解决方案。

4.3.1　智能动态防御体系设计思路

智能动态防御的策略是构建一种动态的、异构的、不确定的网络，通过部署运行网络、主机系统增加其随机性，减少确定性、相似性、静态性，从而增加攻击者的攻击难度与代价。智能动态防御通过随机调动网络、主机系统自身原有资源的冗余性、异构性和空间分布性来构成安全机制，从而大大提高网络系统的弹性。

该技术颠覆了传统的信息安全观：“期望创造一个绝对安全的、没有漏洞的信息系统”，以“破坏网络攻击能够实施的基础条件，主动、动态地改变网络防御策略，从根本上阻止网络攻击的发生”为目标[9]。

4.3.2　智能动态防御关键技术

北京卫达科技有限公司研发的“幻境”智能动态防御技术体系如图 5 所示，涉及的主要关键技术包括如下 6 种。

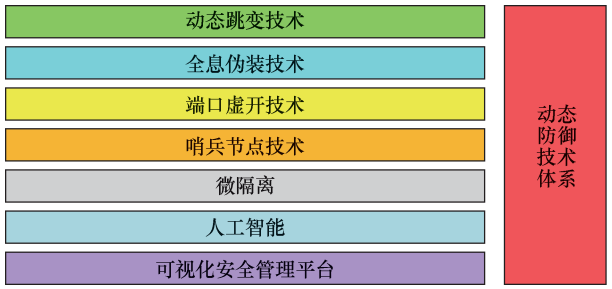

图 5　“幻境”智能动态防御技术体系

1）动态跳变技术：网络身份不断随机变化，使攻击者无法有效识别目标节点，更不可能锁定目标实施攻击，从根本上阻止网络攻击行为的发生。

2）全息伪装技术：将不同网络节点进行数字化描述，全息虚拟大量动态变化的伪装节点，动态随机地改变网络节点属性和网络拓扑结构，迷惑攻击者认知。

3）端口虚开技术：每通过虚拟开启一些诸如 445、139、3399 端口，混淆黑客攻击的进入端口，诱导黑客进行攻击。

4）哨兵节点技术：开放一些容易被黑客攻击的常用服务来诱捕攻击者；实时监测不符合动态变换规则的异常网络行为。

5）微隔离：每个终端节点被单独定义为一个独立的逻辑网络，实现二层隔离的同时快速定位、封

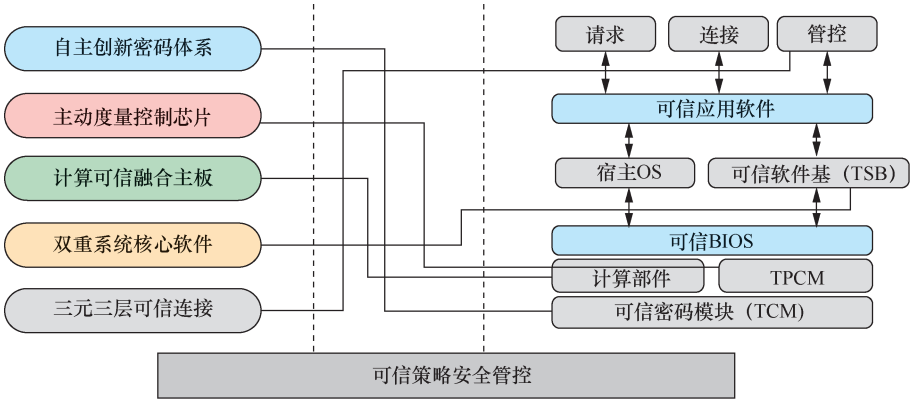

图 4　主动免疫可信 3.0 体系结构

堵攻击。

6) 人工智能：利用机器学习形成行为记忆，能够有效感知网络运行状态，动态改变防御策略。

5 我国安全可控桌面计算机技术体系

当前，国产桌面计算机技术架构是“1+3”：国产 Linux 操作系统 + 3 种国产 CPU（申威/飞腾/龙芯），作为国产安全可控信息技术体系的核心，有关厂商现正着手制订一个统一的“桌面操作系统参考平台”。为了改进国产体系的生态，国产 Linux 操作系统将具备“安卓运行沙箱”功能，率先实现移动和桌面生态的融合。我国安全可控的桌面计算机技术体系主要构成如表 1 所示。

习近平总书记在国家安全工作座谈会上要求“加大核心技术研发力度和市场化引导”，这里，将“核心技术研发”和“市场化引导”联系在一起，具有重大意义。人们常说“软件到 3.0 版才好用”，这对硬件也基本适用，说明任何核心技术如不通过大量使用，没有进入市场的良性循环，就不能发展成熟。

这个过程一般要经历“不可用”“可用”“好用”3 个阶段，特别是处在“不可用”阶段时，如果没有市场化引导，很可能无法进入市场，没人应用，也就不可能得到改进和发展。

因此，必须强调市场化支持（如通过政府采购），使这些开始“不可用”的技术也能得到应用的机会，并在应用中发现问题，不断改进，最终从“不可用”发展到“可用”“好用”。

目前，国产桌面计算机技术体系已达到“可用”。在 2016 年“科技三会”上，航天科工集团作为中国大企业集团的代表，曾介绍了集团实施自主可控替代计划的经验。该集团“商密网”是目前规模最大的全国产软硬件构成的信息系统，已部署了 20 000 台全国产桌面电脑，采用云计算模式，由包括“航天昆仑数据库一体机”在内的国产服务器提供云服务，并引入了采用航天元心移动操作系统的安全手机支持移动办公。该“商密网”已稳定运行了 2 年左右，用户体验与原先采用外国软硬件的系统相仿，这说明依托创新，国产并不等于落后。

航天科工集团“商密网”的成功表明，国产软硬件已基本达到可用水平，也表明通过技术创新、模式创新等，国产自主可控替代计划是切实可行的。建议政务信息化大力推广航天科工集团“商密网”这样的自主可控云服务。

6 结束语

我国网络安全和信息化技术的明显短板是在集成电路的制造、工艺和设计工具等方面，国家已设立了上千亿的集成电路发展基金，还有很多民间基金加入，希望能尽快赶上去。此外，大型软件（如

表 1　我国安全可控的桌面计算机技术体系主要构成

技术	代表企业
操作系统	中标麒麟、普华、天津麒麟、深度、思普、一铭、红旗、技德
CPU	龙芯、飞腾、申威、众志
BIOS	百敖、太极
可信 3.0	可信联盟旗下已有上百家企业
虚拟化	华三、华为、云宏、深信服、同方、浪潮、有孚
数据库	南通、达梦、金仓、神通
中间件	东方通、金蝶、中创、普元、中和威
网络安全	华为、启明星辰、深信服、绿盟、360、亚信、卫士通、卫达
办公套件、流式文档	金山、福昕
企业管理软件	用友、金蝶、数码大方、宝信
浏览器	360、搜狗、QQ、百度
输入法	搜狗、QQ、百度、讯飞
排版、印章、版式文档	方正、文泰、蒙泰、福昕、书生
系统集成	浪潮、东软、中软、太极、同方、神码、东华、航信
第三方机构	软交所、有关测评中心、有关标准化机构

EDA、CAD/CAM 等工业软件）也是短板，开发这类软件周期很长，需要尽早进行部署。当前可以采用虚拟化技术，通过云服务解决某些大型软件不能在本地运行的问题[10]。

自主可控不等于安全，但不自主可控一定不安全。自主可控、掌握核心技术意味着不存在后门，可以主动增强安全（即能掌控源代码，自己分析研究），发现漏洞后可以主动打补丁；而不自主可控意味着丧失主动权，在网络攻击下完全处于被动挨打地位。所以应当将自主可控作为网络安全的必然要求，这样才能构建安全可控的信息技术体系。

参考文献：

[1] GUINARD D, TRIFA V, KARNOUSKOS S, et al. Interacting with the SOA-based Internet of things: discovery, query, selection, and on-demand provisioning of Web services[J]. IEEE Transactions on Services Computing, 2010,3(3):223-235.

[2] KYUSAKOV R, ELIASSON J, DELSING J, et al. Integration of wireless sensor and actuator nodes with it infrastructure using service-oriented architecture[J]. IEEE Transactions on Industrial Informatics, 2013,9(1):43-51.

[3] LIU H, GAN Y, YANG J, et al. Push the limit of Wi-Fi based localization for smartphones[C]//International Conference on Mobile Computing and NETWORKING. 2012: 305-316.

[4] VASIN P. Blackcoin's proof-of-stake protocol v2[S]. White Paper, 2014.

[5] KWON J. Tendermint: consensus without mining[S]. GitHub Draft v6, 2014.

[6] IDDO B, CHARLES L, ALEX M, et al.Proof of activity: extending Bitcoin's proof of work via proof of stake[J].IACR,2014:452.

[7] SOMPOLINSKY Y, ZOHAR A. Accelerating Bitcoin's transaction processing, fast money grows on trees, not chains[J]. IACR Cryptology ePrint Archive, 2013:881.

[8] LI B, SALTER J, DEMPSTER A G, et al. Indoor positioning techniques based on wireless LAN[C]// IEEE International Conference on LAN. 2007:13-16.

[9] 崔传桢, 田霞. 卫达安全, 构建网络安全智能动态防御系统[J]. 信息安全研究, 2017(12): 1058-1066.
CUI C Z, TIAN X. VEDA, establishing the AI dynamic defense system for cyber security[J]. Journal of Information Security Research, 2017(12): 1058-1066.

[10] 倪光南. 构建安全可控的信息技术体系[N].经济参考报, 2018.
NI G N. Building a safe and controllable information technology system[N]. Economic Information Daily, 2018.

[作者简介]

倪光南（1939-），男，中国科学院计算技术研究所研究员，中国工程院院士。几十年来一直从事计算机及其应用的研究与开发工作，曾参与研制我国自行设计的第一台电子管计算机（119 机）。20 世纪六七十年代开展汉字处理和字符识别研究，首创在汉字输入中应用联想功能。近年来，致力于中国推广 Linux 等开源软件、推广国产 CPU、国产软件和文档格式国家标准 UOF 等开放标准，并为促进制订有关产业政策建言献策。