

工业4.0与网络安全

联网生产时代的风险管理

德勤咨询有限公司的供应链与制造运营业务组助力公司了解并把握机遇，利用工业4.0技术实现商业目标。我们将凭借对增材制造、物联网及分析学的洞见，依据日新月异的先进制造业实践，协助公司重新评估其员工、流程与技术。

目录

引言 | 2

数字化供应网络 | 5

不断演变的供应链与网络风险

智能工厂 | 7

应对智能生产时代的新型网络风险

联网物品 | 12

风险触及实体物品

在工业4.0时代保持安全性、警惕性与韧性 | 16

尾注 | 17

德勤中国联系人 | 19

引言

第四次工业革命为联网的智能制造和数字供应网络带来一项新的运营风险：网络风险。工业4.0时代中，由于企业运营具有互联互通的特性，企业数字化转型的步伐加快，网络攻击的影响比以往任何时候都更加广泛，制造商和供应网络可能尚未准备好应对风险。为了在工业4.0时代充分解决网络风险，企业网络安全战略应保证安全性、警惕性和韧性，并从一开始就充分结合组织与信息技术战略。

2009年，恶意软件曾操控某核浓缩工厂的离心机，导致所有离心机失控。该恶意软件又称“震网”，通过闪存驱动器入侵独立网络系统，并在各生产网络中自动扩散。通过“震网”事件，我们看到将网络攻击作为武器破坏联网实体工厂的可能。¹这场战争显然是失衡的：企业必须保护众多的技术，而攻击者只需找到一个最薄弱的环节。

但非常重要的一点是，企业不仅需要关注外部威胁，还需关注真实存在却常被忽略的网络风险，而这些风险正是由企业创新、转型和现代化过程中越来越多地应用智能互联技术所引致的。否则，企业制定的战略商业决策将可能导致该等风险，企业应管控并降低该等新兴风险。

工业4.0时代，智能机器之间的互联性不断增强，风险因素也随之增多。工业4.0开启了一个互联互通、智能制造、响应式供应网络和定制产品与服务时代。借助智能、自动化技术，工业4.0旨在结合数字世界与物理操作，推动智能工厂和先进制造业的发展。²但在意图提升整个制造与供应链流程的数字化能力并推动联网设备革命性变革过程中，新产生的网络风险让所有企业都感到措手不及。针对网络风险制定综合战略方案对制造业价值链至关重要，因为这些方案融合了工业4.0的重要驱动力：运营技术与信息技术。

随着工业4.0时代的到来，威胁急剧增加，企业应当考虑并解决新产生的风险。简而言之，在工业4.0时代制定具备安全性、警惕性和韧性的网络风险战略将面临不同的挑战。当供应链、工厂、消费者以及企业运营实现联网，网络威胁带来的风险将达到前所未有的广度和深度。

在战略流程临近结束时才考虑如何解决网络风险可能为时已晚。开始制定联网的工业4.0计划时，

就应将网络安全视为与战略、设计和运营不可分割的一部分。

本文将从现代联网数字供应网络、智能工厂及联网设备三大方面研究各自所面临的网络风险。³在工业4.0时代，我们将探讨在整个生产生命周期中（图1）——从数字供应网络到智能工厂再到联网物品——运营及信息安全主管可行的对策，以预测并有效应对网络风险，同时主动将网络安全纳入企业战略。

图1：智能生产的生命周期与网络风险

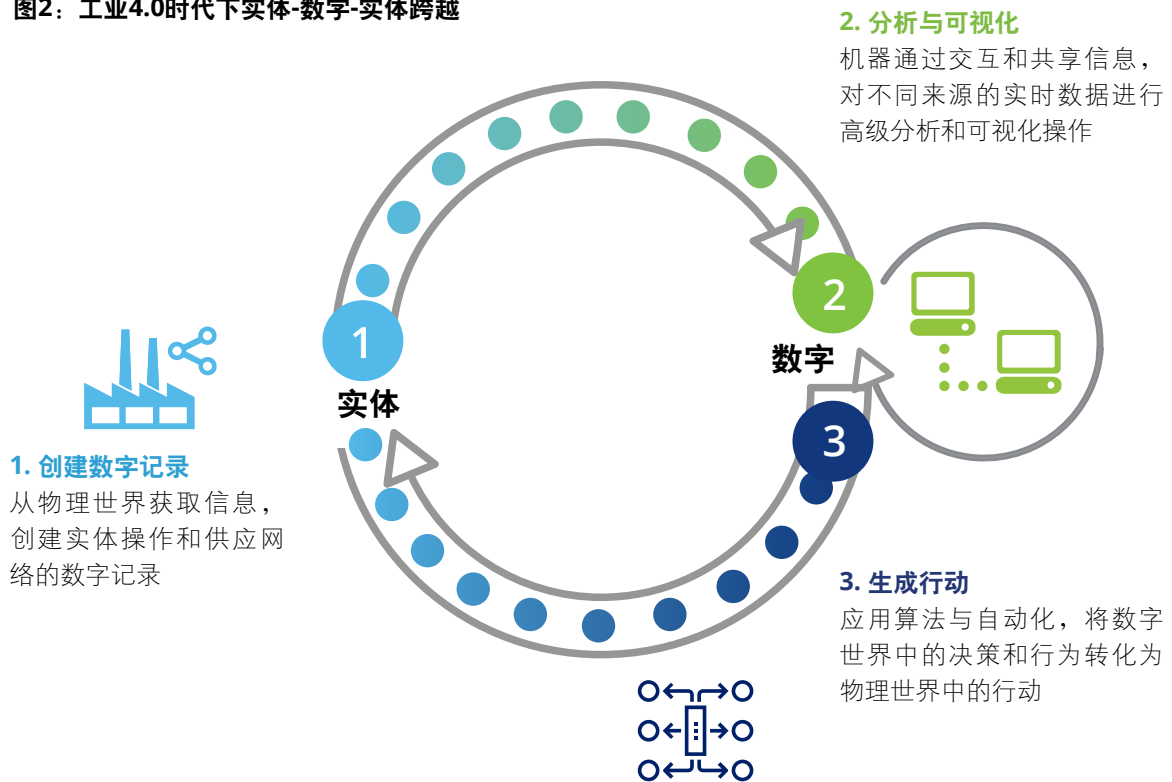
生产生命周期阶段	安全性、警惕性、韧性类别	网络需求	目标
数字供应网络 	安全性、警惕性、韧性	数据共享	确保系统完整，避免泄露私人所有数据
	安全性、警惕性、韧性	供应商处理	在无法验证流程时保持信任
智能工厂 	警惕性	健康与安全	确保员工和环境安全
	警惕性、韧性	生产与流程韧性/效率	确保连续生产和关键系统恢复
	警惕性、韧性	检测并主动解决问题	保护企业品牌与声誉
	安全性、韧性	系统的可操作性、可靠性与完整性	支持使用多个供应商和软件版本
	警惕性、韧性	效率与成本规避	利用远程站点诊断与工程建设，减少运营成本，增强灵活性
	安全性	监管与合规	确保流程的可靠性
联网物品 	安全性	产品设计	利用安全软件开发生命周期，生产可操作的安全设备
	警惕性	数据保护	在整个数据生命周期内确保敏感数据安全
	韧性	修复攻击影响	迅速恢复运营和安全的同时将事故影响降至最低

数字化制造企业与工业4.0

工业4.0技术让数字化制造企业和数字供应网络整合不同来源和出处的数字化信息，推动制造与分销行为。信息技术与运营技术整合的标志是向实体-数字-实体的联网转变。工业4.0结合了物联网以及相关的实体和数字技术，包括数据分析、增材制造、机器人技术、高性能计算机、人工智能、认知技术、先进材料以及增强现实，以完善生产生命周期，实现数字化运营。

工业4.0的概念在物理世界的背景下融合并延伸了物联网的范畴，一定程度上讲，只有制造与供应链/供应网络流程会经历实体-数字和数字-实体的跨越（图2）。从数字回到实体的跨越——从互联的数字技术到创造实体物品的过程——这是工业4.0的精髓所在，它支撑着数字化制造企业和数字供应网络。

图2：工业4.0时代下实体-数字-实体跨越



资料来源：综合研究中心

德勤大学出版社 | dupress.deloitte.com

即使在我们探索信息创造价值的方式时，从制造价值链的角度去理解价值创造也很重要。在整个制造与分销价值网络中，通过工业4.0应用程序集成信息和运营技术可能会达到一定的商业成果。

了解更多信息，请阅读“工业4.0与制造业生态圈：探索互联企业世界”。³

数字化供应网络

不断演变的供应链和网络风险

有关材料进入生产过程和半成品/成品对外分销的供应链对于任何一家制造企业都非常重要。此外，供应链还与消费者需求联系紧密。很多全球性企业根据需求预测确定所需原料的数量、生产线要求以及分销渠道负荷。由于分析工具也变得更加先进，如今企业已经能够利用数据和分析工具了解并预测消费者的购买模式。

通过向整个生态圈引入智能互联的平台和设备，工业4.0技术有望推动传统线性供应链结构的进一步发展，并形成能从价值链上获得有用数据的数字供应网络，最终改进管理，加快原料和商品流通，提高资源利用率，并使供应品更合理地满足消费者需求。⁴

尽管工业4.0能带来这些好处，但数字供应网络的互联性增强将形成网络弱点。为了防止发生重大风险，应从设计到运营的每个阶段，合理规划并详细说明网络弱点。

在数字化供应网络中 共享数据的网络风险

随着数字供应网络的发展，未来将出现根据购买者对可用供应品的需求，对原材料或商品进行实时动态定价的新型供应网络。⁵由于只有供应网络各参与方开放数据共享才可能形成一个响应迅速且灵活的网络，且很难在保证部分数据透明度的同时确保其他信息安全，因此形成新型供应网络并非易事。

因此，企业可能会设法避免信息被未授权网络用户访问。此外，他们可能还需对所有支撑性流程实施统一的安全措施，如供应商验收、信息共享和系统访问。企业不仅对这些流程拥有专属权利，它们也可以作为获取其他内部信息的接入点。

这也许会给第三方风险管理带来更多压力。在分析互联数字供应网络的网络风险时，我们发现不断提升的供应链互联性对数据共享与供应商处理的影响最大（图3）。


为了应对不断增长的网络风险，我们将对上述两大领域和应对战略逐一展开讨论。

数据共享：更多利益相关方将更多渠道获得数据

企业将需要考虑什么数据可以共享，如何保护私人所有或含有隐私风险的系统和基础数据。比如，数字供应网络中的某些供应商可能在其他领域互为竞争对手，因此不愿意公开某些类型的数据，如定价或专利品信息。此外，供应商可能还须遵守某些限制共享信息类型的法律法规。因此，仅公开部分数据就可能让不良企图的人趁机获得其他信息。

企业应当利用合适的技术，如网络分段和中介系统等，收集、保护和提供信息。此外，企业还应在未来生产的设备中应用可信的平台模块或硬件安全模块等技术，以提供强大的密码逻辑支持、硬件授权和认证（即识别设备的未授权更改）。

图3：智能需求与风险

生产生命周期阶段	安全性、警惕性、韧性类别	网络需求	目标
数字化供应网络 	安全性、警惕性、韧性	数据共享	确保系统完整，避免泄露私人所有数据
	安全性、警惕性、韧性	供应商处理	在无法验证流程时保持信任

德勤大学出版社 | dupress.deloitte.com

将这种方法与强大的访问控制措施结合，关键任务操作技术在应用点和端点的数据和流程安全将能得到保障。

在必须公开部分数据或数据非常敏感时，金融服务等其他行业能为信息保护提供范例。目前，企业纷纷开始对静态和传输中的数据应用加密和标记等工具，以确保数据被截获或系统受损情况下的通信安全。但随着互联性的逐步提升，金融服务企业意识到，不能仅从安全的角度解决数据隐私和保密性风险，而应结合数据管治等其他技术。事实上，企业应该对其所处环境实施风险评估，包括企业、数字供应网络、行业控制系统以及联网产品等，并根据评估结果制定或更新网络风险战略。总而言之，随着互联性的不断增强，上述所有的方法都能找到应实施更高级预防措施的领域。

供应商处理：更广阔市场中供应商验收与付款

由于新伙伴的加入将使供应商体系变得更加复杂，核心供应商群体的扩张将可能扰乱当前的供应商验收流程。因此，追踪第三方验收和风险的管治、风险与合规软件需要更快、更自主地反应。此外，使用这些应用软件的信息安全与风险管理团队还需制定新的方针政策，确保不受虚假供应商、国际制裁的供应商以及不达标产品分销商的影响。消费者市场有不少类似的经历，易贝和亚马逊就曾发生过假冒伪劣商品和虚假店面等事件。⁶

区块链技术已被认为能帮助解决上述担忧并应对可能发生的付款流程变化。尽管比特币是建立货币历史记录的经典案例，但其他企业仍在探索如何利用这个新工具来决定商品从生产线到各级购买者的流动。⁷创建团体共享历史账簿能建立信任和透明度，通过验证商品真实性保护买方和卖方，追踪商品物流状态，并在处理退换货时用详细的产品分类替代批量分拣。如不能保证产品真实性，制造商可能会在引进产品前，进行产品测试和鉴定，以确保足够的安全性。

信任是数据共享与供应商处理之间的关联因素。企业从事信息或商品交易时，需要不断更新其风险管理措施，确保真实性和安全性；加强监测能力和网络安全运营，保持警惕性；并在无法实施信任验证时保护该等流程。

在这个过程中，数字供应网络成员可参考其他行业的网络风险管理方法。某些金融和能源企业所采用的自动交易模型与响应迅速且灵活的数字供应网络就有诸多相似之处。它包含具有竞争力的知识产权和企业赖以生存的重要资源，所有这些都与数字供应网络一样，一旦部署到云端或与第三方建立联系就容易遭到攻击。金融服务行业已经意识到无论在内部或外部算法都面临着这样的风险。因此，为了应对内部风险，包括显性风险（企业间谍活动、蓄意破坏等）和意外风险（自满、无知等），软件编码和内部威胁程序必须具备更高的安全性和警惕性。事实上，警惕性对监测非常重要：由于制造商逐渐在数字供应网络以外的生产过程应用工业4.0技术，网络风险只会成倍增长。

智能工厂

智能生产时代的新型网络风险

随着互联性的不断提高，数字供应网络将面临新的风险，智能制造同样也无法避免。不仅风险的数量和种类将增加，甚至还可能呈指数增长。不久前，美国国土安全部出版了《物联网安全战略原则》与《生命攸关的嵌入式系统安全原则》，强调应关注当下的问题，检查制造商是否在生产过程中直接或间接地引入与生命攸关的嵌入式系统相关的风险。¹⁰

“生命攸关的嵌入式系统”广义上指几乎所有的联网设备，无论是车间自动化系统中的设备或是在第三方合约制造商远程控制的设备，都应被视为风险——尽管有些设备几乎与生产过程无关。¹¹考虑到风险不断增长，威胁面急剧扩张，工业4.0时代中的制造业必须彻底改变对安全的看法。

联网生产带来新型网络挑战

随着生产系统的互联性越来越高，数字供应网络面临的网络威胁不断增长扩大。不难想象，不当或任意使用临时生产线可能造成经济损失、产品质量低下，甚至危及工人安全。此外，联网工厂将难以承受倒闭或其他攻击的后果。有证据表明，制造商仍未准备好应对其联网智能系统可能引发的网络风险：2016年德勤与美国生产力和创新制造商联盟（MAPI）的研究发现，三分之一的制造商未对工厂车间使用的工业控制系统做过任何网络风险评估。¹²

可以确定的是，自进入机械化生产时代，风险就一直伴随着制造商，而且随着技术的进步，网络风险不断增强，物理威胁也越来越多。但工业4.0使网络风险实现了迄今为止最大的跨越。各阶段的具体情况请参见图4。

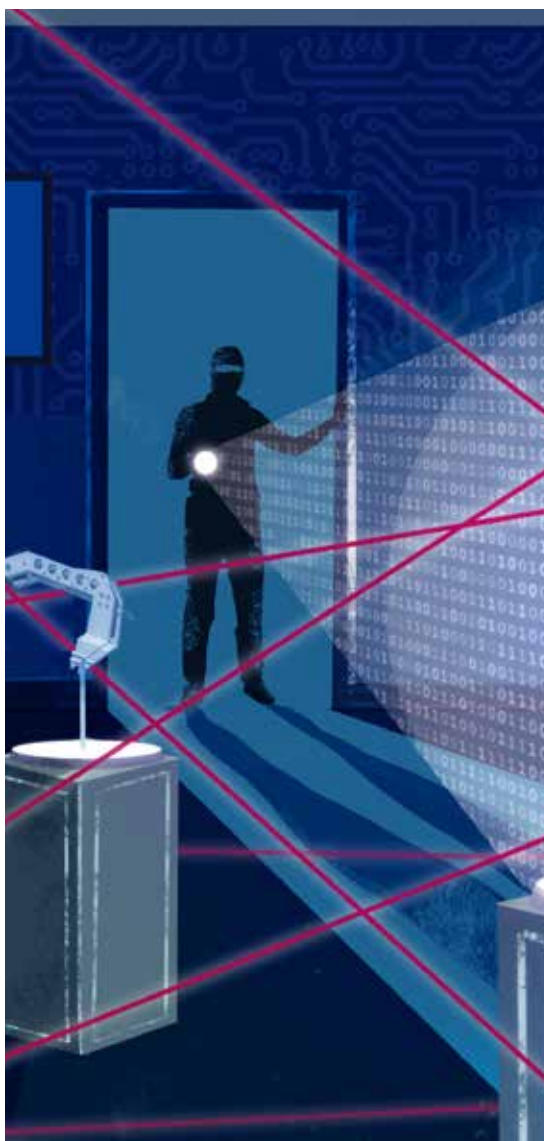
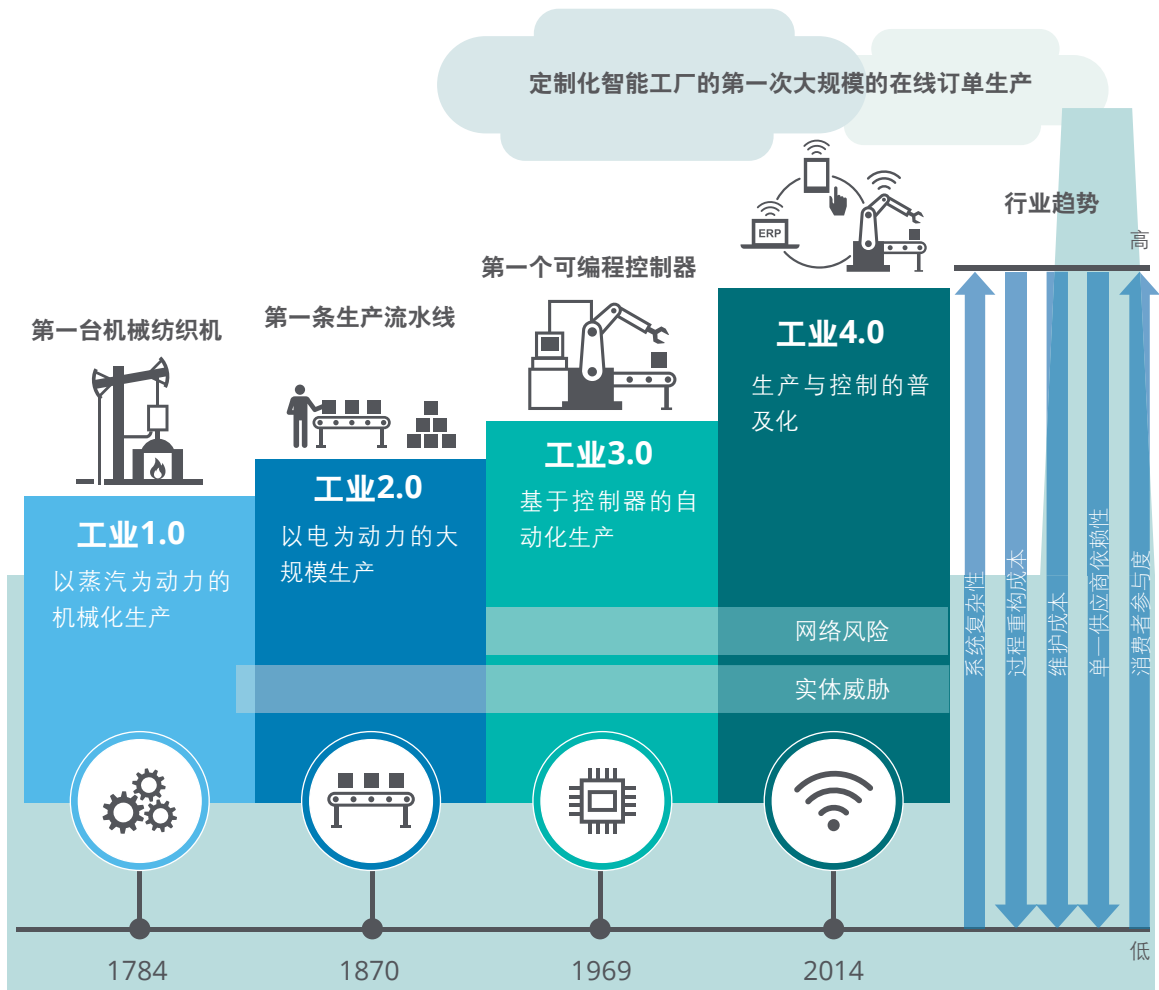


图4：每次工业革命后网络与物理威胁的发展



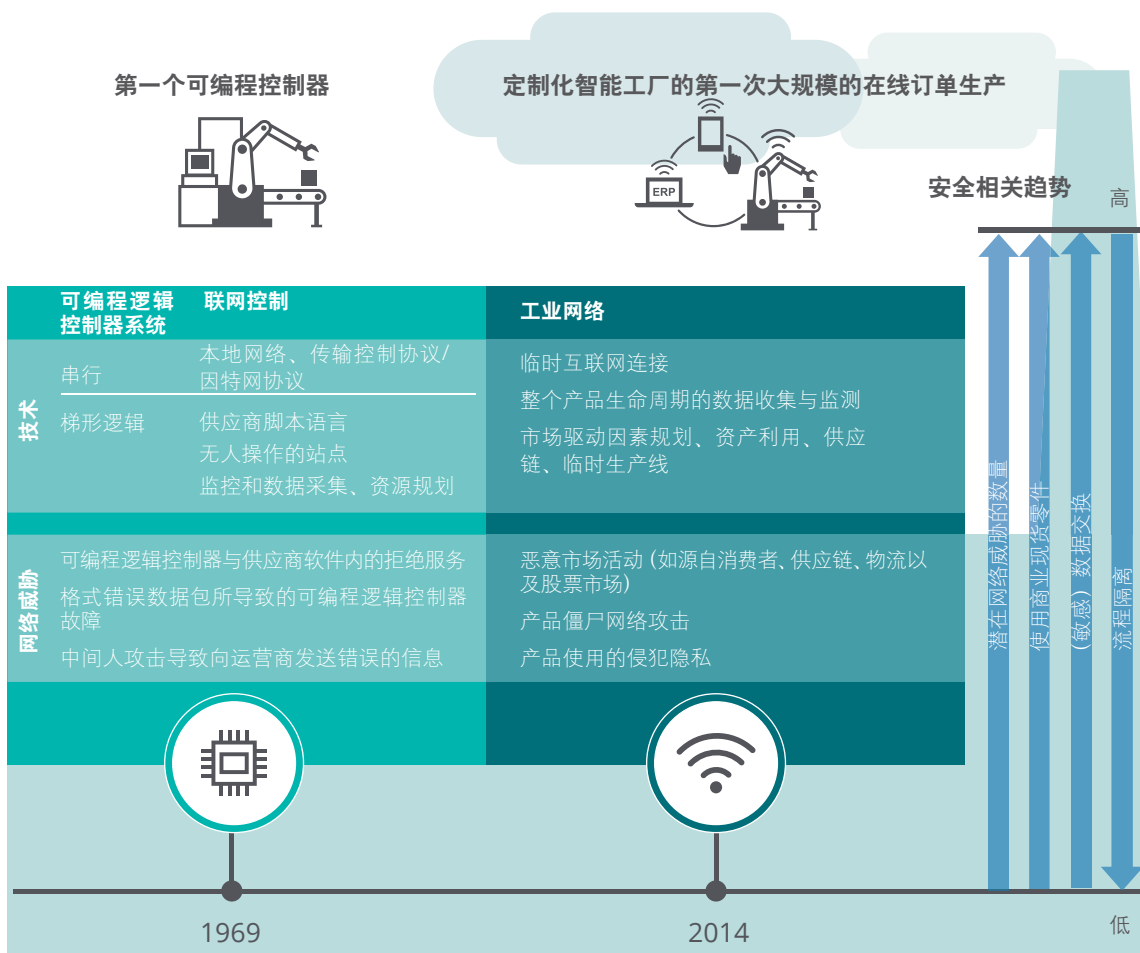
资料来源：德勤

德勤大学出版社 | dupress.deloitte.com

从运营的角度看，在保持高效率和实施资源控制时，工程师可在现代化的工业控制系统环境中部署无人站点。为此，他们使用了一系列联网系统，如企业资源规划、制造执行、监控和数据采集系统等。这些联网系统能够经常优化流程，使业务更加简单高效。并且，随着系统的不断升级，系统的自动化程度和自主性也将不断提高(图5)。

这些网络攻击将可能对生产、消费者、制造商以及产品本身产生更广泛、更深远的影响。

图5：工业控制系统中技术与相关网络威胁的发展



注释：

- 本地网络 (LAN)
- 传输控制协议/因特网协议 (TCP/IP)
- 监控和数据采集 (SCADA)
- 企业资源规划 (ERP)
- 拒绝服务 (DoS)
- 可编程逻辑控制器 (PLC)
- 中间人攻击 (MitM)

德勤大学出版社 | dupress.deloitte.com

资料来源：德勤

从安全的角度看，鉴于工业控制系统中商业现货产品的互联性和使用率不断提升，大量暴露点将可能遭到威胁。与一般的IT行业关注信息本身不同，工业控制系统安全更多关注工业流程。因此，与传统网络风险一样，智能工厂的主要目标是保证物理流程的可用性和完整性，而非信息的保密性。

但值得注意的是，尽管网络攻击的基本要素未发生改变，但实施攻击方式变得越来越先进(图5)。事实上，由于工业4.0时代互联性越来越高，并逐渐从数字化领域扩展到物理世界，网络攻击将可能对生产、消费者、制造商以及产品本身产生更广泛、更深远的影响(图6)。

图6：智能工厂的需求与风险

生产生命 周期阶段	安全性、警惕性、 韧性类别	网络需求	目标
智能工厂 	警惕性	健康与安全	确保员工和环境安全
	警惕性与韧性	生产与流程韧性/效率	确保连续生产和关键系统恢复
	警惕性与韧性	检测并主动解决问题	保护企业品牌与声誉
	安全与韧性	系统的可操作性、可靠性 与完整性	支持使用多个供应商和软件版本
	警惕性与韧性	效率与成本规避	利用远程站点诊断与工程建设，减少运营 成本，增强灵活性
	安全性	监管与合规	确保流程的可靠性

德勤大学出版社 | dupress.deloitte.com

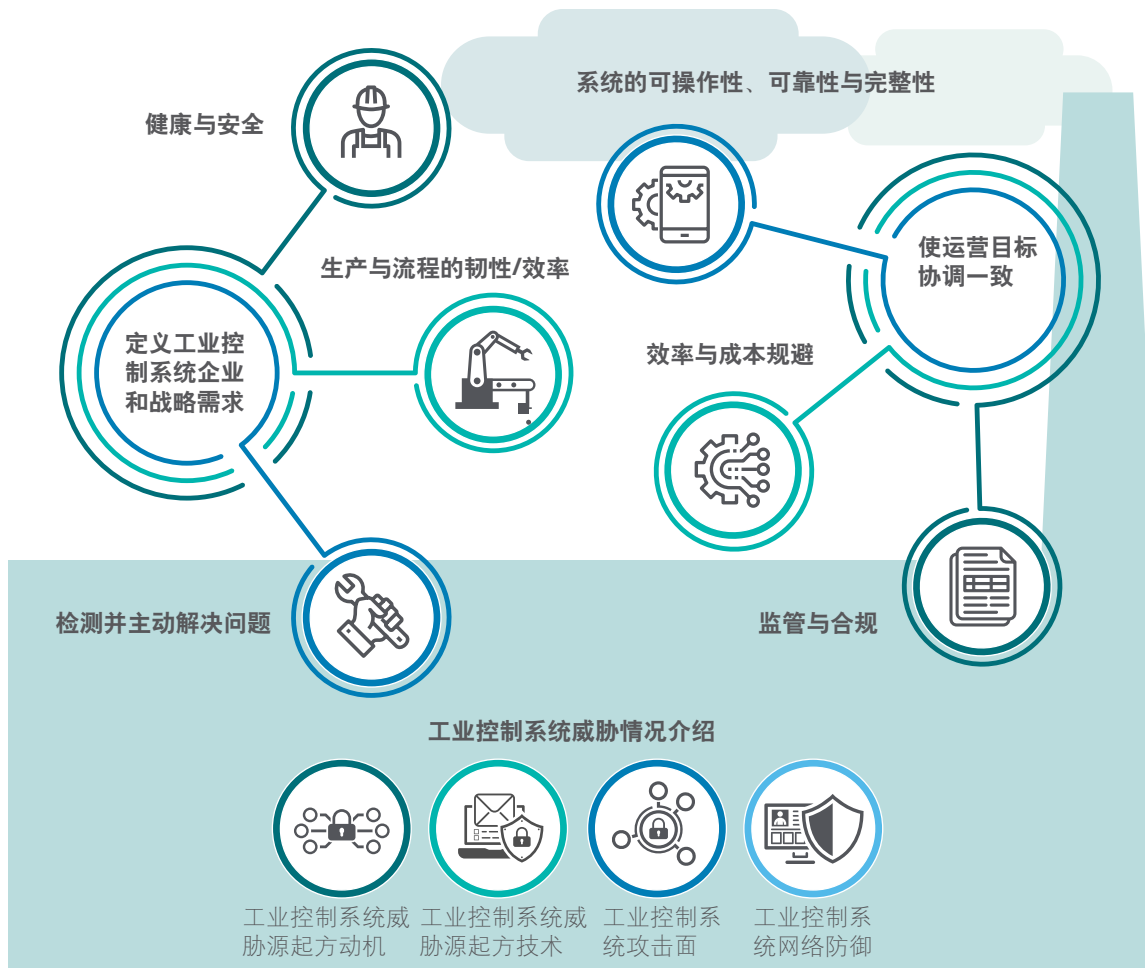
结合信息技术与运营技术： 当数字化遇上实体

制造商实施工业4.0 技术时必须考虑数字化流程和将受影响的机器和物品，我们通常称之为信息技术与运营技术的结合。对于工业或制造流程中包含了信息技术与运营技术的公司，当我们探讨推动重点运营和开发工作的因素时，可以确定多种战略规划、运营价值以及相应的网络安全措施（图7）。

首先，制造商常受以下三项战略规划的影响：

- 健康与安全：**员工和环境安全对任何站点都非常重要。随着技术的发展，未来智能安全设备将实现升级。
- 生产与流程的韧性和效率：**任何时候保证连续生产都很重要。在实际工作中，一旦工厂停工就会损失金钱，但考虑到重建和重新开工所花费的时间，恢复关键流程可能将导致更大的损失。
- 检测并主动解决问题：**企业品牌与声誉在全球商业市场中扮演着越来越重要的角色。在实际工作中，工厂的故障或生产问题对企业声誉影响很大，因此，应采取措施改善环境，保护企业的品牌与声誉。

图7：智能工厂的业务驱动与威胁环境



资料来源：德勤

德勤大学出版社 | dupress.deloitte.com

第二，企业需要在日常的商业活动中秉持不同的运营价值理念：

- **系统的可操作性、可靠性与完整性：** 为了降低拥有成本，减缓零部件更换速度，站点应当采购支持多个供应商和软件版本的、可互操作的系统。
- **效率与成本规避：** 站点始终承受着减少运营成本的压力。未来，企业可能增加现货设备投入，加强远程站点诊断和工程建设的灵活性。

- **监管与合规：** 不同的监管机构对工业控制系统环境的安全与网络安全要求不同。未来企业可能需要投入更多，以改变环境，确保流程的可靠性。

工业4.0时代，网络风险已不仅仅存在于供应网络和制造业，同样也存在于产品本身。由于产品的互联程度越来越高——包括产品之间，甚至产品与制造商和供应网络之间，因此企业应该明白一旦售出产品，网络风险就不会终止。¹⁴

互联物品

风险触及实体物品

预计到2020年，全球将部署超过200亿台物联网设备。¹⁵其中很多设备可能会被安装在制造设备和生产线上，而其他的很多设备将有望进入B2B或B2C市场，供消费者购买使用。

2016年德勤与美国生产力和创新制造商联盟(MAPI)的研究结果显示，近一半的制造商在联网产品中采用移动应用软件，四分之三的制造商使用Wi-Fi网络在联网产品间传输数据。¹⁶基于上述网络途径的物联通常会形成很多漏洞。物联网设备制造商应思考如何将更强大、更安全的软件开发方法应用到当前的物联网开发中，以应对设备常常遇到的重大网络风险。

尽管这很有挑战性，但事实证明，企业不能期望消费者自己会更新安全设置，采取有效的安全应对措施，更新设备端固件或更改默认设备密码。比如，2016年10月，一次由Mirai恶意软件引发的物联网分布式拒绝服务攻击，表明攻击者可以利用这些弱点成功实施攻击。在这次攻击中，病毒通过感染消费者端物联网设备如联网的相机和电视，将其变成僵尸网络，并不断冲击服务器直至服务器崩溃，最终导致美国最受欢迎的几家网站瘫痪大半天。¹⁷研究者发现，受分布式拒绝服务攻击损害的设备大多使用供应商提供的默认密码，且未获得所需的安全补丁或升级程序。¹⁸需要注意的是，部分供应商所提供的密码被硬编码进了设备固件中，且供应商未告知用户如何更改密码。当前的工业生产设备常缺乏先进的安全技术和基础设施，一旦外围保护被突破，便难以检测和应对此类攻击。¹⁹

风险与生产相伴而行

由于生产设施越来越多地与物联网设备结合，因此，考虑这些设备对制造、生产以及企业网络所带来的安全风险变得越来越重要。受损物联网设备所产生的安全影响包括：生产停工、设备或设施受损如灾难性的设备故障，以及极端情况下的人员伤亡。此外，潜在的金钱损失并不仅限于生产停工和事故整改，还可能包括罚款、诉讼费用以及品牌受损所导致的收入减少（可能持续数月甚至数年，远远超过事件实际持续的时间）。下文列出了目前确保联网物品安全的一些方法，但随着物品和相应风险的激增，这些方法可能还不够。

传统漏洞管理

漏洞管理程序可通过扫描和补丁修复有效减少漏洞，但通常仍有多个攻击面。攻击面可以是一个开放式的TCP/IP或UDP端口或一项无保护的技术，虽然目前未发现漏洞，但攻击者以后也许能发现新的漏洞。

减少攻击面

简单来说，减少攻击面即指减少或消除攻击，可以从物联网设备制造商设计、建造并部署只含基础服务的固化设备时便开始着手。安全所有权不应只由物联网设备制造商或用户单独所有；而应与二者同样共享。

更新悖论

生产设施所面临的另一个挑战被称为“更新悖论”。很多工业生产网络很少更新升级，因为对制造商来说，停工升级花费巨大。对于某些连续加工设施来说，关闭和停工都将导致昂贵的生产原材料发生损失。

很多联网设备可能还将使用十年到二十年，这使得更新悖论愈加严重。认为设备无须应用任何软件补丁就能在整个生命周期安全运转的想法完全不切实际。²⁰ 对于生产和制造设施，在缩短停工时间的同时，使生产资产利用率达到最高至关重要。物联网设备制造商有责任生产更加安全的固化物联网设备，这些设备只能存在最小的攻击表面，并应利用默认的“开放”或不安全的安全配置规划最安全的设置。

制造设施中联网设备所面临的挑战通常也适用基于物联网的消费产品。智能系统更新换代很快，而且可能使消费型物品更容易遭受网络威胁。对于一件物品来说，威胁可能微不足道，但如果涉及大量的联网设备，影响将不可小觑——Mirai病毒攻击就是一个例子。在应对威胁的过程中，资产管理和技术战略将比以往任何时候都更重要。

人才缺口

2016年德勤与美国生产力和创新制造商联盟(MAPI)的研究表明，75%的受访高管认为他们缺少能够有效实施并维持安全联网生产生态圈的技能型人才资源。²¹随着攻击的复杂性和先进程度不断提升，将越来越难找到高技能的网络安全人才，来设计和实施具备安全性、警觉性和韧性的网络安全解决方案。

网络威胁不断变化，技术复杂性越来越高。搭载零日攻击的先进恶意软件能够自动找到易受攻击的设备，并在几乎无人参与的情况下进行扩散，并可能击败已遭受攻击的信息技术/运营技术安全人员。这一趋势令人感到不安，物联网设备制造商需要生产更加安全的固化设备。

多管齐下，保护设备

在工业应用中，承担一些非常重要和敏感任务——包括控制发电与电力配送，水净化、化学品生产和提纯、制造以及自动装配生产线——的物联网设备通常最容易遭受网络攻击。由于生产设施不断减少人为干预，因此仅在网关或网络边界采取保护措施的做法已经没有用(图8)。

从设计流程开始考虑网络安全

制造商也许会觉得越来越有责任部署固化的、接近军用级别的联网设备。很多物联网设备制造商已经表示他们需要采用包含了规划和设计的安全编码方法，并在整个硬件和软件开发生命周期内采用领先的网络安全措施。²²这个安全软件开发生命周期在整个开发过程中添加了安全网关(用于评估安全控制措施是否有效)，采用领先的安全措施，并用安全的软件代码和软件库生产具备一定功能的安全设备。通过利用安全软件开发生命周期的安全措施，很多物联网产品安全评估所发现的漏洞能够在设计过程中得到解决。但如果可能的话，在传统开发生命周期结束时应用安全修补程序通常会更加费力费钱。²³

图8：互联物品规划与风险

生产生命 周期阶段	安全性、警惕性、 韧性类别	网络需求	目标
互联物品 	安全性	产品设计	利用安全软件开发生命周期，生产可操作的安全设备
	警惕性	数据保护	在整个数据生命周期内确保敏感数据安全
	韧性	修复攻击影响	迅速恢复运营和安全的同时将事故影响降至最低

德勤大学出版社 | dupress.deloitte.com

从联网设备端保护数据

物联网设备所产生的大量信息对工业4.0制造商非常重要。基于工业4.0的技术如高级分析和机器学习能够处理和分析这些信息，并根据计算分析结果实时或近乎实时地做出关键决策。这些敏感信息并不仅限于传感器与流程信息，还包括制造商的知识产权或者与隐私条例相关的数据。事实上，德勤与美国生产力和创新制造商联盟 (MAPI) 的调研发现，近70%的制造商使用联网产品传输个人信息，但近55%的制造商会对传输的信息加密。²⁴

生产固化设备需要采取可靠的安全措施，在整个数据生命周期内，敏感数据的安全同样也需要得到保护。因此，物联网设备制造商需要制定保护方案：不仅要安全地存放所有设备、本地以及云端存储的数据，还需要快速识别并报告任何可能危害这些数据安全的情况或活动。

保护云端数据存储和动态数据通常需要采用增强式加密、人工智能和机器学习解决方案，以形成强大的、响应迅速的威胁情报、入侵检测以及入侵防护解决方案。

随着越来越多的物联网设备实现联网，潜在威胁面以及受损设备所面临的风险都将增多。现在这些攻击面可能还不足以形成严重的漏洞，但仅数月或数年后就能轻易形成漏洞。因此，设备联网时必须使用补丁。确保设备安全的责任不应仅由消费者或联网设备部署方承担，而应由最适合实施最有效安全措施的设备制造商共同分担。

应用人工智能检测威胁

2016年8月，美国国防高级研究计划局举办了一场网络超级挑战赛，最终排名靠前的七支队伍在这场“全机器”的黑客竞赛中提交了各自的人工智能平台。网络超级挑战赛发起于2013年，旨在找到一种能够扫描网络、识别软件漏洞并在无人干预的情况下应用补丁的、人工智能网络安全平台或技术。美国国防高级研究计划局希望借助人工智能平台大大缩短人类以实时或接近实时的方式识别漏洞、开发软件安全补丁所用的时间，从而减少网络攻击风险。

真正意义上警觉的威胁检测能力可能需要运用人工智能的力量进行大海捞针。在物联网设备产生海量数据的过程中，当前基于特征的威胁检测技术可能会因为重新收集数据流和实施状态封包检查而被迫达到极限。尽管这些基于特征的检测技术能够应对流量不断攀升，但其检测特征数据库活动的能力仍旧有限。

在工业4.0时代，结合减少攻击面、安全软件开发生命周期、数据保护、安全和固化设备的硬件与固件以及机器学习，并借助人工智能实时响应威胁，对以具备安全性、警惕性和韧性的方式开发设备至关重要。如果不能应对安全风险，如“震网”和Mirai 恶意程序的漏洞攻击，也不能生产固化、安全的物联网设备，则可能导致一种不好的状况：关键基础设施和制造业将经常遭受严重攻击。²⁵

攻击不可避免时，保持韧性

恰当利用固化程度很高的目标设备的安全性和警惕性，能够有效震慑绝大部分攻击者。然而，值得注意的是，虽然企业可以减少网络攻击风险，但没有一家企业能够完全避免网络攻击。保持韧性的前提是，接受某一天企业将遭受网络攻击这一事实，而后谨慎行事。

韧性的培养过程包含三个阶段：准备、响应、恢复。

- **准备。**企业应当准备好有效应对各方面事故，明确定义角色、职责与行为。审慎的准备如危机模拟、事故演练和战争演习，能够帮助企业了解差异，并在真实事故发生时采取有效的补救措施。
- **响应。**应仔细规划并对全公司有效告知管理层的响应措施。实施效果不佳的响应方案将扩大事件的影响、延长停产时间、减少收入并损害企业声誉。这些影响所持续的时间将远远长于事故实际持续的时间。
- **恢复。**企业应当认真规划并实施恢复正常运营和限制企业遭受影响所需的措施。应从事后分析中汲取到的教训用于制定之后的事件响应计划。

具备韧性的企业应在迅速恢复运营和安全的同时将事故影响降至最低。在准备应对攻击，了解遭受攻击时的应对之策并快速消除攻击的影响时，企业应全力应对、仔细规划、充分执行。

在工业4.0时代保持安全性、警惕性和韧性

推动网络公司发展至今日的比特 (0和1) 让制造业的整个价值链经历了从供应网络到智能工厂再到联网物品的巨大转变。随着联网技术应用的不断普及,网络风险可能增加并发生改变,也有可能价值链的不同阶段和每一家企业有不同的表现。每家企业应以最能满足其需求的方式适应工业生态圈。

企业不能只用一种简单的解决方法或产品或补丁解决工业4.0所带来的网络风险和威胁。如今,联网技术为关键商业流程提供支持,但随着这些流程的关联性提高,可能会更容易出现漏洞。因此,企业需要重新思考其业务连续性、灾难恢复力和响应计划,以适应愈加复杂和普遍的网络环境。

法规和行业标准常常是被动的,“合规”通常表示最低安全要求。企业面临着一个特别的挑战——当前所采用的技术并不能完全保证安全,因为干扰者只需找出一个最薄弱的点便能成功入侵企业系统。这项挑战可能还会升级:不断提高的互联性和收集处理实时分析将引入大量需要保护的联网设备和数据。

企业需要采用具备安全性、警惕性和韧性的方法,了解风险,消除威胁:

- **安全性。**采取审慎的、基于风险的方法,明确什么是安全的信息以及如何确保信息安全。贵公司的知识产权是否安全?贵公司的供应链或工业控制系统环境是否容易遭到攻击?
- **警惕性。**持续监控系统、网络、设备、人员和环境,发现可能存在的威胁。需要利用实时威胁情报和人工智能,了解危险行为,并快速识别引进的大量联网设备所带来的威胁。
- **韧性。**随时都可能发生事故。贵公司将会如何应对?多久能恢复正常运营?贵公司将如何快速消除事故影响?

由于企业越来越重视工业4.0所带来的商业价值,企业将比以往任何时候更需要提出具备安全性、警惕性和韧性的网络风险解决方案。

尾注

1. Kim Zetter, "An unprecedented look at Stuxnet, The world's first digital weapon," *Wired*, November 3, 2014, <https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/>.
2. For further information about Industry 4.0, see Brenna Sniderman, Monika Mahto, and Mark Cotteleer, *Industry 4.0 and manufacturing ecosystems: Exploring the world of connected enterprises*, Deloitte University Press, February 22, 2016, <https://dupress.deloitte.com/content/dupress/dup-us-en/focus/industry-4-0/manufacturing-ecosystems-exploring-world-connected-enterprises.html>.
3. For further information about digital supply networks, see Adam Mussomeli, Stephen Laaper, and Doug Gish, *The rise of the digital supply network: Industry 4.0 enables the digital transformation of supply chains*, Deloitte University Press, December 1, 2016, <https://dupress.deloitte.com/content/dupress/dup-us-en/focus/industry-4-0/digital-transformation-in-supply-chain.html>.
4. Ibid.
5. Bridget McCrea, "The evolution of supply chain collaboration software," *Logistics Management*, September 2015.
6. Aron Hsiao, "Top ten risks eBay sellers face," *Balance*, January 8, 2016, <https://www.thebalance.com/top-ten-risks-ebay-sellers-face-1140349>.
7. Harriet Green, "Serving up a better burger: How IoT and blockchain will reinvent the global supply chain," *Venture Beat*, October 30, 2016, <http://venturebeat.com/2016/10/30/serving-up-a-better-burger-how-iot-and-blockchain-will-reinvent-the-global-supply-chain/>.
8. Stuart Trouton, Mark Vitale, and Jason Killmeyer, *3D opportunity for blockchain: Additive manufacturing links the digital thread*, Deloitte University Press, November 16, 2016, <https://dupress.deloitte.com/content/dupress/dup-us-en/focus/3d-opportunity/3d-printing-blockchain-in-manufacturing.html>.
9. Judith Evans, "Cyber criminals target trading algorithms," *Financial Times*, February 22, 2015, <https://www.ft.com/content/f8556c92-b1d9-11e4-8396-00144feab7de>.
10. US Department of Homeland Security, *Strategic principles for securing the Internet of Things*, November 15, 2016; and *Security tenets for life critical embedded systems*, November 20, 2015.
11. The term "life-critical embedded system" extends to any embedded system across all industries that need to protect human life, prevent loss or severe damage to equipment, and prevent environmental harm.
12. Trina Huelsman et al., *Cyber risk in advanced manufacturing*, Deloitte and MAPI, 2016, <https://www2.deloitte.com/us/en/pages/manufacturing/articles/cyber-risk-in-advanced-manufacturing.html>.
13. Sniderman, Mahto, and Cotteleer, *Industry 4.0 and manufacturing ecosystems*.
14. Brenna Sniderman et al., *The design of things: Building in IoT connectivity: The Internet of Things in product design*, Deloitte University Press, September 12, 2016, <https://dupress.deloitte.com/content/dupress/dup-us-en/focus/internet-of-things/connected-products-designing-for-internet-of-things.html>.
15. Ron van der Meulen, "Gartner says 6.4 billion connected 'things' will be in use," *Gartner*, November 10, 2015, <http://www.gartner.com/newsroom/id/3165317>.
16. Huelsman et al., *Cyber risk in advanced manufacturing*.
17. Nicky Wolf, "DDoS attacks that disrupted Internet was largest of its kind in history, experts say," *Guardian*, October 26, 2016, <https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet>.

18. Alex Hern, "Chinese webcam maker recalls devices after cyberattack link," *Guardian*, October 24, 2016, <https://www.theguardian.com/technology/2016/oct/24/chinese-webcam-maker-recalls-devices-cyberattack-ddos-internet-of-things-xiongmai>.
19. Matthew E. Luallen and Barbara Filkins, *Results of SANS SCADA Security Survey*, SANS Institute, February 2013, <https://www.sans.org/reading-room/whitepapers/analyst/results-scada-security-survey-35135>.
20. Sniderman et al., *The design of things*.
21. Huelsman et al., *Cyber risk in advanced manufacturing*.
22. Broadband Internet Technical Advisory Group, *Internet of Things (IoT) security and privacy recommendations*, November 2016, [http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_\(IoT\)_Security_and_Privacy_Recommendations.pdf](http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf).
23. Sniderman et al., *The design of things*.
24. Huelsman et al., *Cyber risk in advanced manufacturing*.
25. Nicole Perlroth, "Hackers used new weapons to disrupt major websites across U.S.," *New York Times*, October 22, 2016, <http://www.nytimes.com/2016/10/22/business/internet-problems-attack.html>.

德勤中国联系人

董伟龙

中国工业产品与服务行业领导人
电子邮箱: rictung@deloitte.com.cn

薛梓源

中国科技风险咨询服务领导合伙人
电子邮箱: tonxue@deloitte.com.cn

关于德勤全球

Deloitte (“德勤”)泛指一家或多家德勤有限公司(即根据英国法律组成的私人担保有限公司,以下称“德勤有限公司”),以及其成员所网络和它们的关联机构。德勤有限公司与其每一家成员所均为具有独立法律地位的法律实体。德勤有限公司(又称“德勤全球”)并不向客户提供服务。请参阅 www.deloitte.com/cn/about 以了解更多有关德勤有限公司及其成员所的详情。

德勤为各行各业的上市及非上市客户提供审计及鉴证、管理咨询、财务咨询、风险咨询、税务及相关服务。德勤透过遍及全球逾150个国家与地区的成员所网络为财富全球500强企业中的80%左右的企业提供专业服务。凭借其世界一流和高质量的专业服务,协助客户应对极为复杂的商业挑战。如欲进一步了解全球大约263,900名德勤专业人员如何致力成就不凡,欢迎浏览我们的Facebook、LinkedIn 或Twitter专页。

关于德勤中国

德勤于1917年在上海设立办事处,德勤品牌由此进入中国。如今,德勤中国的事务所网络在德勤全球网络的支持下,为中国本地和在华的跨国及高增长企业客户提供全面的审计及鉴证、管理咨询、财务咨询、风险咨询和税务服务。德勤在中国市场拥有丰富的经验,同时致力为中国会计准则、税务制度及培养本地专业会计师等方面的发展作出重要贡献。敬请访问 www2.deloitte.com/cn/zh/social-media,通过德勤中国的社交媒体平台,了解德勤在中国市场成就不凡的更多信息。

本通信中所含内容乃一般性信息,任何德勤有限公司、其成员所或它们的关联机构(统称为“德勤网络”)并不因此构成提供任何专业建议或服务。在作出任何可能影响您的财务或业务的决策或采取任何相关行动前,您应咨询合格的专业顾问。任何德勤网络内的机构均不对任何方因使用本通信而导致的任何损失承担责任。

©2018。欲了解更多信息,请联系德勤中国。
CQ-118CN-17



这是环保纸印刷品