



图 1 新的制造方法和单件生产的可能性对像 UL 这样的安全和认证企业的核心业务也有影响

安全

工业 4.0 世界的前提是安全

增材制造和工业 4.0 单件生产等全新制造方法对安全和认证企业的核心业务也产生了影响。

文 | Ingo M. Rübenach



更多精彩内容请扫描二维码

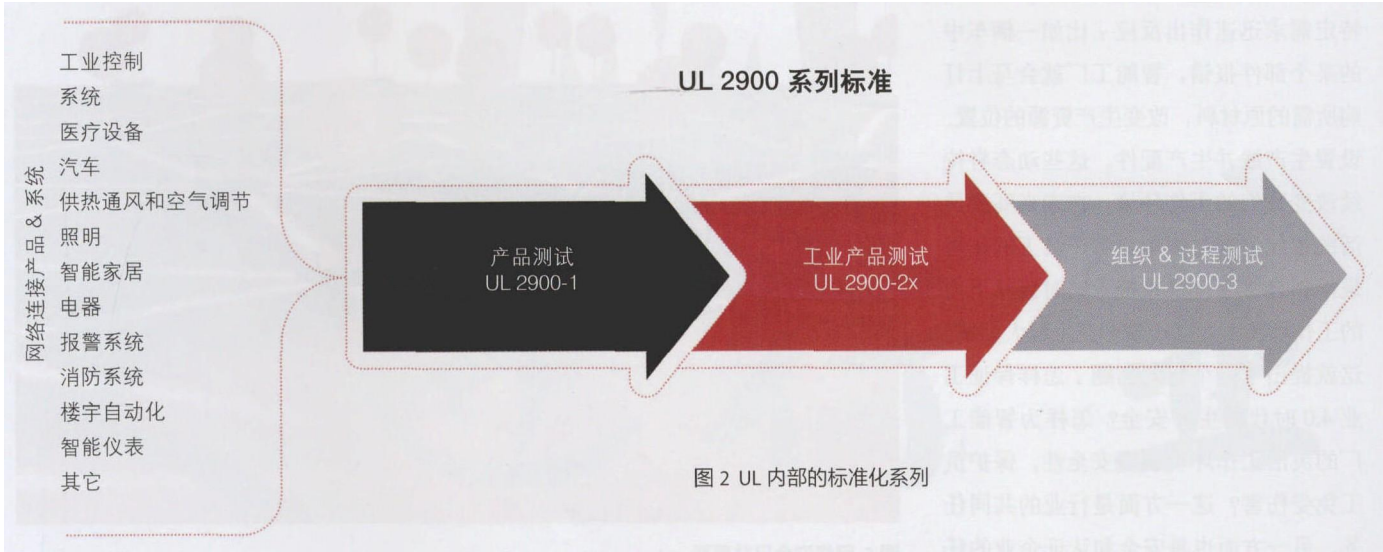
众所周知，工业 4.0 这一概念提出的要求不亚于第四次工业革命，仔细观察那些与工业 4.0 联系在一起、通过新的技术和业务模式产生深层次变化的领域，用革命性的震荡描述它们确实不算夸张。革命这个词语就已经预示了所有参与者都将面对的一个决定性的挑战，不论是经营企业、客户、政策和立法、监管和制定标准的部门还是像 UL 这样的认证服务者：每次革命开始时能预见

的是旧秩序消失，但新规则最终是什么样子还没有人知道。

革命需要安全

不论是称其为物联网、智能制造还是像德国称之为工业 4.0，生产过程和产品的数字化其实是一个革命性的转变，制造设备出自全面联网的网络物理系统，同时不断成长的物联网，即越来越多的产品联网也会对各行业的商业模式产生

巨大影响。2010 年有大约 50 亿人使用联网，到 2020 年将增加 500 亿联网物品，贸易领域将像金融、汽车、高科技和能源行业一样被全面数字化波及，在许多行业中，传统业务模式逐渐消失，它们越来越容易受到攻击，此外从计量到智能手表和其他穿戴设备的智能工厂的发展对安全提出了全新的要求，对于生产商和供应商而言，安全是工业 4.0 实施过程中的核心组成部分。



个性化产品

在智能制造世界，在未来的智能工厂中，生产过程将完全不同，智能工厂的制造告别了标准化的老工业模式，汽车行业已经让人们看到了这一趋势：很久以来就不再是为每个客户都提供相同的黑色 T 型福特车，而是配置高度个性化的车辆。在工业 4.0 时代，整齐一致的工业产品彻底成为过去，增材制造工艺（3D 打印）提供了几乎无限的个性化可能：单件生产。这也对 UL 这样的安全和认证公司的核心业务有影响（图 1），自从 120 多年前在美国作为承销商实验室成立后，UL 就一直在开发保护生活和工作环境的安全解决方案的标准和创新。如果现在要在美国市场上出售充电器，就需要针对现有标准取得许可，这样的认证过程，即符合有关安全标准的验证，只要充电器有原型或之前的产品。但如果产品的批量只有一件，内部质量保证和外部认证就会面临全新的、只能以国际化尺度去应对的挑战，对 UL 来说，解决围绕工业 4.0 的安全问题是企业自成立以来就一直追求的“安全使命”的必然延续，不过可以预见的是，工业 4.0 也将明显改变认证公司的核心业务。

谁负责 3D 打印？

尽管如此，悬而未决的问题还占大

多数，目前既没有说明谁要为增材制造过程的安全负责，也不知道谁对产品有法律保证义务：是三维打印机的制造商、原料供应商还是三维打印机的用户？增材制造的质量保证和认证面临的最大挑战之一是针对材料、工艺和产品建立适当的标准。保证增材制造产品质量的第一步在于检查和确定原材料，比如金属 3D 打印主要使用金属粉末作为原料，其性质对最终产品的质量有很大影响：不论是粉末的化学组成、颗粒的大小分布还是流动性和温度，粉末原料的密度也对成品的孔隙率有重要影响。此外贯穿整个过程的检测同样必不可少，以便制

造过程在所要求的公差范围内进行，当然成品检测也是必需的，增材制造的质量保证、验证、产品检测和认证方面还有很大空缺，UL 支持 ISO 和 ASTM 等组织在增材制造领域的标准化工作，但目前在实际工作中还有很多未知数（图 2）。工业 4.0 的一个重要方面是高度的自我组织，它是未来智能工厂中制造的标志，全新网络物理系统的智能足以使生产过程自己定义和自主控制。

智能工厂的生产安全

网络物理智能工厂将是高度灵活的（图 3），凭借全面的垂直整合能够针对

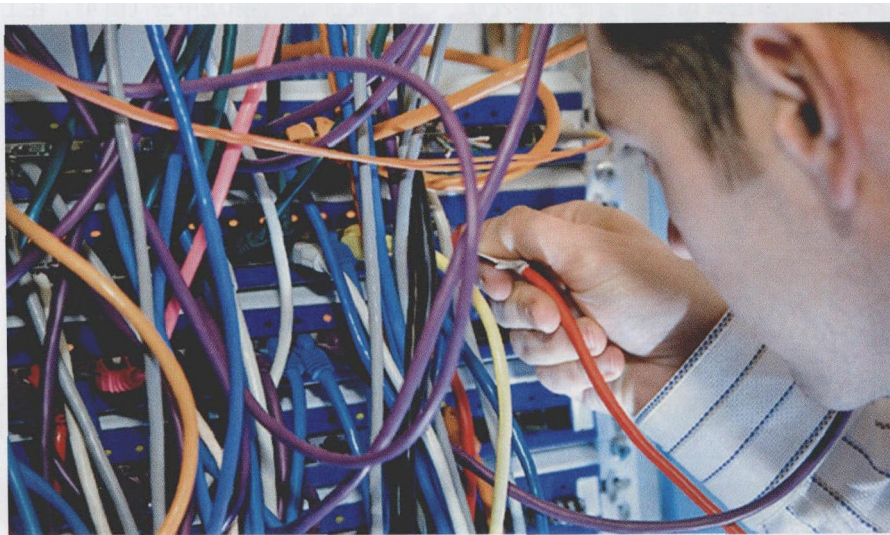


图 3 物联网产品和系统总览

特定需求迅速作出反应：比如一辆车中的某个部件报错，智能工厂就会马上订购所需的原材料，改变生产资源的位置、设置生产线并生产配件，这些动态将持续改变我们的工作环境，在未来高度灵活智能制造过程中，生产员工的作用是控制自主工作的系统，同时极具活力的工作环境会对生产安全产生很大影响，这就提出了一个重要问题：怎样保证工业 4.0 时代的生产安全？怎样为智能工厂的灵活工作环境创造安全性，保护员工免受伤害？这一方面是行业的共同任务，另一方面也是安全和认证企业的任务，研究怎样有效定义和保证这方面的安全性。

工业 4.0 的网络物理系统不仅将智能工厂作为焦点，还要建立整个供应链的密切联网和全面垂直整合，整个价值生产链上的生产商必须比以往任何时候都更加密切地相互合作，与工业协会、决策者甚至竞争对手的合作也将起到一定作用。在工业 4.0 的世界，问题不再是蜘蛛有多强，而是它的网有多强大，随着供应链的横向整合，另一个问题出现了：数据究竟属于谁？谁是受益者？工业 4.0 是大数据的世界，谷歌的力量在于能够访问珍贵的数据财富，在这种情况下数据保护和数据安全有了新的意义。明确法律规定是立法者的任务：哪些人有哪些权限访问和控制供应链的哪些过程和哪些数据基础？谁负什么责任？

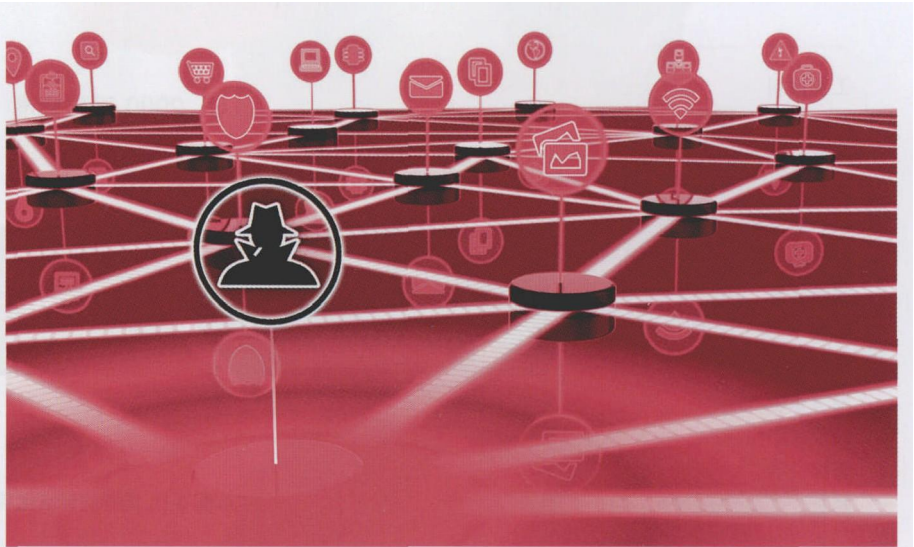


图 5 网络安全日益重要

任何联网都需要网络安全

在工业 4.0 和物联网的世界里，生产设备和产品具有互联网接口不再是例外而是常规，如今所有生产设备都可以不受地点的限制通过 IPad 来控制，这是一个进步，但同时也对安全性提出了全新的要求，如果将来有一个破坏者想改变断路开关的脱扣曲线，造成对人、机器和厂房的损害，比如引起火灾，那他只能通过互联网以黑客的方式进入系统，保护网络物理系统不被未授权的访问和错误控制攻击是一个巨大的挑战，因为新系统全面联网且非常灵活。在此必须实现操作安全、数据保护和信息安全的全新组合，所有这些安全措施都必须集成到组件和系统中去（图 4），在工业 4.0 的范围内，安全不只是抽象的话

题，它更多的是一个非常现实的物理存在，全面联网的生产系统抵御外部攻击的漏洞最后会导致从火灾到触电的物理危险和风险。在网络方面介入网络物理系统也会对其物理方面产生潜在影响，因此 UL 与中立的研究机构合作，将两个安全领域更加密切地结合起来：新的 IT 标准和协议一方面与传统电气安全标准，另一方面与功能性的安全要求相结合。然而，在全面联网和易受攻击的工业 4.0 的安全要求方面还存在很多问题，它们还没有阐述清楚，更不用说找到答案了。

路途遥远

共同为动态工业 4.0 世界和物联网制定适当的安全标准，是研究机构、工业企业以及标准化和认证公司的重大任务，我们肯定还不能理解，未来我们的网络物理系统必须满足哪些标准，在目前还处于第四次工业革命的开始这一形势下，如果我们能够勾勒出众多盲区、确定研究重点并提出明确的问题，就已经收获不小了。实施工业 4.0 时，我们还处于解决相关安全问题的开始阶段，工业 4.0 的智能和全面联网世界带来了全新的机会，为了能够充分利用这个机会，必须控制革命的风险，路途虽然遥远，但值得走下去（图 5）。MM

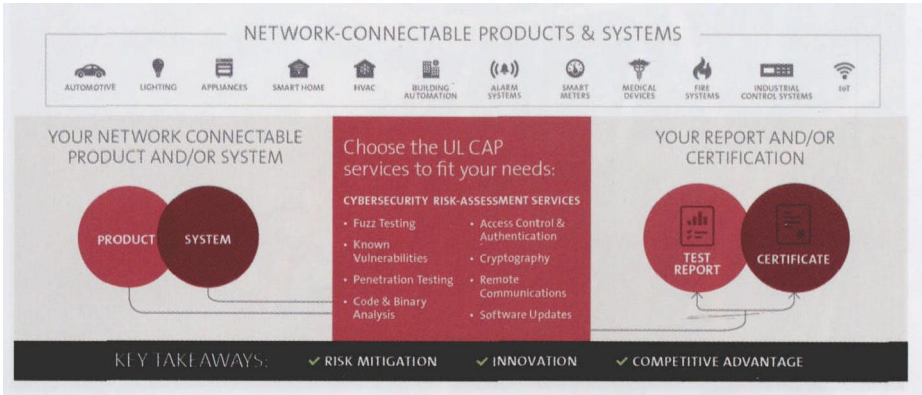


图 4 制造业的基础设施日益复杂