



图 1 只要涉及到工业 4.0 概念，就必须考虑到安全问题，且这种安全考量应该沿着整个产品价值链展开

信息安全

工业 4.0 对安全要求很高

当前人们对自动化技术的讨论离不开工业 4.0 概念，信息安全议题是工业 4.0 面临的一个根本性挑战，设计整体解决方案时就必须以安全设计为宗旨，考虑信息安全要素（图 1）。

文 | LUTZ JÄNICKE

手工单件的生产在经历了几个阶段之后，过渡到了工业批量生产，这种过渡不仅能够降低每个产品的单位成本，还能提高产品质量（图 2）。然而，这往往会以牺牲生产灵活性为代价，只有在生产数量较多时，才能摊低前期投入的生产成本。

工业 4.0 方案的目的在于将 IT 完全

渗透到价值链的每个步骤和产品整个生产周期，从而进一步提高企业生产效率和灵活性，由设计开始，经过订单处理和生产，直至售后服务。

工业 4.0 的目标和计划

其它行业已经提出了工业生产可能发展的方向，通信领域正朝着对内容和

服务供应商有利的方向发展，通信网络供应商将失掉其重要性（和利润）。带有程序的 PC 和传统的笔记本电脑将败给平板电脑和应用程序，汽车共享将取代传统的汽车拥有模式。

IT 行业中的相关发展趋势显而易见：一方面，软件代替硬件，专用服务器将由虚拟服务器取代，服务器所需的

硬件环境将通过软件制作的解决方案得到进一步发展。另一方面，这些变化并不仅仅存在于 IT 本身，传统云计算定义的外部服务也会对此进行补充或替代，所有这些例子的共同点是发展方向转移到了内容和服务上，而不再注重传统的物质媒介。

于是出现了下面这些问题：未来人们还会购买冲床、工具或是冲孔机么？机床制造商会自己提供这些么？亦或是由一个专门的服务商来提供？如果允许供应商进行状态监测优化，价格是否会降低？对此需要收集哪些数据？这些数据应该存储到哪里？又该属于谁呢？

工业 4.0 互联网的意义在于参与者往往不仅是供应商，同时本身也是客户或操作者。产品特点、设计数据、软件、价格和状态参数等相关信息未来一定会跨越企业界限，实现水平交换。

数码产品容易被复制

为了在小批量生产的情况下也能高效完成产品生产，必须根据生产件数变化做到生产准备成本最小化，为此生产系统必须能够对自身进行基本设置，从而适应这一产品，该产品必须以数字形式存在，这需要将整个产品生产周期数字化，即从产品概念，到售后服务，直至产品退出市场（图 3）。

知识、方案和数据，即与产品和工艺过程相关的知识产权（Intellectual Property），将随着产品的数字化具有越来越重要的意义。全面数字化的产品实用而高效，但与此同时也容易被复制，例如，用 3D 打印机制做一次打印成型的产品，该产品有可能被多次打印出来；滥用自动订货的供应链系统也有可能造成严重损失。工业 4.0 的高效基于中央 ERP 系统被相互独立的分散子系统所替

代，但这些系统需要相同的安全防护水平。反过来通过收集到的已预订或已供应组件的相关数据，或通过评估状态监测过程中积存的运行数据可以获取许多当前生产的信息，并能从中推导出客户或供应商的经济状况。

最近，德国机械设备制造业联合会（VDMA）针对工厂自动化 IT 安全的调查结果非常不理想，仅有一半左右的机械设备制造企业了解相关标准，且只有 1/3 的企业落实了相关措施，与此同时，29% 的企业指出自己遭受过安全事故导致的生产损失。

在工业以太网概念的影响下，工业设备的网络化近几年得到了高速的发展，由于以前生产网络在很多情况下都不会或只是小范围地与外部网络建立连接，所以 IT 安全议题在此发展过程中只扮演着次要角色。然而，如今在实践中不难发现

慧于心、简于行 ——魏德米勒 u-remote

Weidmüller 

定制化的规划、快速的安装、安全可靠的启动、更少的停机时间：如果您向往更高效的自动化设备，我们创新的 I/O 解决方案 u-remote 会给您留下深刻的印象。

IP20 系统 u-remote 为您实现：

- 更小的机柜 —— 超薄的设计，更少的馈电模块
- 更快的安装 —— 免工具装配，模块化设计，集成 Web 服务器
- 高效的维护 —— 通道上 LED 及模块 LED 状态指示

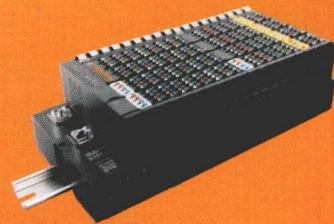
慧于心，简于行 —— 魏德米勒 u-remote

浏览 www.weidmueller.com.cn/u-remote 了解更多关于魏德米勒 u-remote 信息

Let's connect. 携手·共赢

魏德米勒电联接(上海)有限公司

电话: 86 21-22195008 网址: www.weidmueller.com.cn/u-remote



▲反馈服务编码 M2590

许多工厂网络已经连接到互联网，例如，远程维护应用正在发挥作用。尽管这些网络应用中的一部分是在计划和控制下进行的，但在更多情况下，负责人对这种网络互联并不知情。专有系统和协议能够有效阻碍攻击者入侵的这一假设也在蠕虫病毒出现后被否定了，当前流行的安全扫描器，如 Metasploit，采用了 Scada 系统的专用模块，像 Shodan 这样的网络扫描仪会专门搜索工业控制系统。

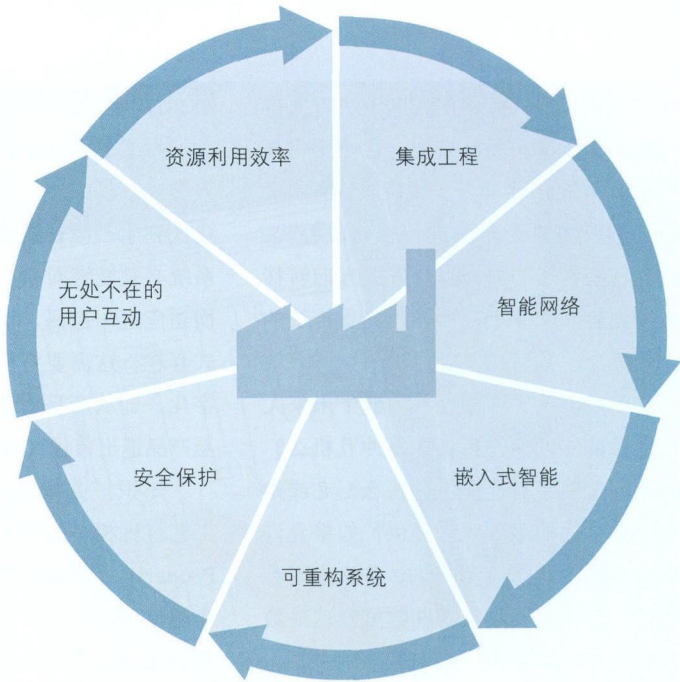
入侵经常在办公室发生

针对这种发展态势，如今已经出现了各种应对举措，以改善这种状况。正如分析结果所示，除了采用技术方案解决问题外，无论何时信息安全意识都是最重要的。

工业 4.0 所需的全面网络整合必定能克服现实存在的办公 IT 和工业 IT 组织分离的问题，如果一个工程师在办公室制定出的设计数据要被用到生产中，甚至可能被其它公司使用，那么相应的安全方案就必须做到全面而综合。更高效率且有目的性的入侵往往是通过初始入口进入办公环境的，从第一个入口点开始，深入公司内部的入侵将逐步展开，如果工业 4.0 要求做到全面网络化，那么不久将无法再对不同领域的安全措施进行划分。

蠕虫病毒就是针对这种问题的一个很好的例子，入侵者利用控制装置，通

图 3 该产品必须以数字形式存在，这需要将整个产品生产周期数字化，即从产品概念，到客户服务，直至产品退出市场



过输入错误的驱动参数来损坏机械系统，遭到入侵的不仅仅只有控制装置，还有制造出相应修改控制程序的设计系统，入侵所用的入口点是运行设计软件的办公操作系统。只有采用一种全面的方案才能够阻止这些入侵，所以数据通信协议和格式的设计必须能够测定信息流，这样一来，加密就成了一把双刃剑，一方面最全面的端到端加密能够最大程度地实现防窃听通信，但另一方面却不再能够检查哪些信息被转送，使入侵或信息泄露事件更难察觉。

安全识别通信对象和产品十分重要，这一任务既有技术性质又有组织性质，目前通常采用不对称加密技术完成安全

识别，在此过程中要对带有证书的公共密钥进行归类。过去的种种例子显示，证书的签发是一个重大挑战，如果授权给众多独立的签发者，那么管理起来会很困难，但却能限制对签发者发起的入侵；如果只授权给少数大的签发者，那么管理起来会更加简单，但却更难符合超越大型组织的安全技术要求。

及时将安全性纳入计划

跨公司的网络互联可以做到实时信息交换，这种互联需要一种能够适应信息灵敏性的信任基础，为此有必要对安全水平进行适当的评估，当前情况显示出的冲突是可预见的，许多运营商对远程维护有很大顾虑，尽管远程维护有可能提高效率，但还是遭到了拒绝，出于安全考量，不允许举行在线网络会议，如果网络安全负责人无法接受这些，工业 4.0 将不可能获得成功。

此外还需要注意用户体验，尽量规避一些干扰性的限制，这对确保功能安全 (Safety) 有着重大作用，尽管这些作用大多是在局部。考虑信息安全可能会对经济产生较大影响，但不会明显危及员工个人。出于上述原因可以清楚地看到，工业 4.0 的安全方案不应该是后期增补的，设计整体解决方案时就必须以安全设计为宗旨，对安全方案加以考虑。[MM]

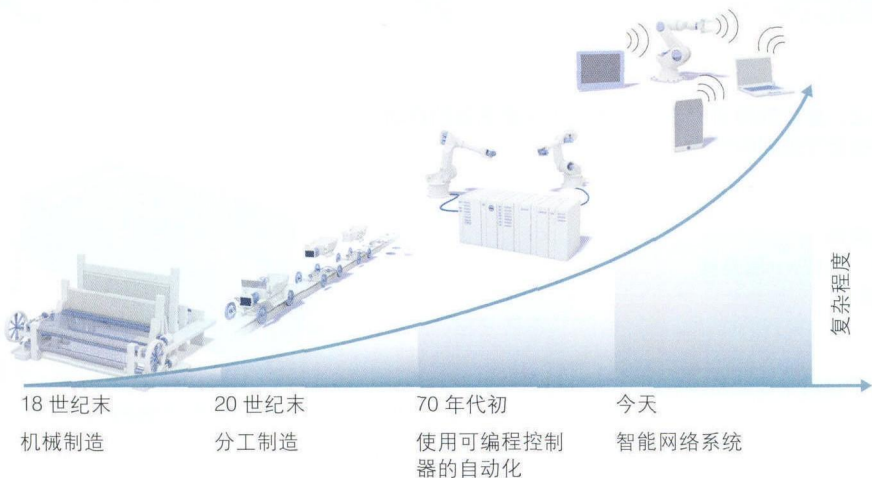


图 2 手工单件的生产在经历了几个阶段之后，过渡到了工业批量生产，这种过渡不仅能够降低每个产品的单位成本，还能提高产品质量