硬件安全在实现工业4.0愿望中的作用

Erik Halthen
ADI公司

工业4.0愿望和网络安全含义

涉及工厂数字化的工业4.0对工业市场领域的组织领导者来说有着不同的意义，随着工厂设备变得智能化和互联，数字化影响可能对网络安全产生广泛的影响。例如，这可能意味着对您的工厂进行转型以提高自主性和定制能力，从而提高运营总成本并为客户带来更高价值。这还可能意味着系统和子系统供应商正在使工厂设备变得更加智能，以实现更大型多单元系统内部和各企业系统之间制造单元的实时决策和自主交互。根据您希望利用工业4.0解决方案的方式，采用这些解决方案的策略将取决于它们将在价值链中的整合位置以及在工厂内的整合深度。

工厂的数字化正在改变价值链的各个方面，并直接影响企业的顶线和底线。最常讨论的是创新，它可以解锁新的收入来源，例如新产品、新服务或二者的某种组合。数字化生产、处理的使用以及边缘数据的分析都需要新的产品创新，而元数据的收集则产生了优化控制、维护和使用的新服务。数字化生产的两个方面都存在于价值链的不同部分，直接影响收入表现。另一方面，降低成本的举措侧重于提高供应链效率和优化运营绩效。这些改进要求在自己的工厂中采用功能更强大的产品和服务。实现工业4.0的线下效益必须要采用新产品创新。根据人们利用工业4.0解决方案的方式，网络安全策略将发生变化，以确保在工厂中成功采用和扩展数字解决方案。

网络安全策略也将根据普遍数字解决方案在工业控制回路边缘的整合方式而有所变化。传统的工业自动化架构迥然不同，并且依赖于将现场设备的控制与工厂的其他信息系统、服务和应用隔离，以防范网络安全威胁。此外，实际的现场设备通常是具有有限数据交换和边缘处理的点对点解决方案，这就限制了任何一个设备对系统造成的网络安全风险。颠覆这种典型的架构并非易事，需要采用分阶段的方法。工业4.0解决方案的积极采用者将需要确定他们希望在工厂中整合新技术的深度，并推动实现这些愿望的网络安全策略。新的工业自动化架构有望显得与众不同。传统上使用普渡模型或类似模型将工厂划分为五个不同的级别，而未来的工厂架构可能并不等同于这一模型。未来的现场设备将检测和执行与制造执行和控制相结合。这些设备不仅会在工厂中联网成一个整合互联架构，而且其中一些设备将直接连接到企业系统、互联网和云服务，这极大地增加了任何一台设备给系统带来的网络安全风险。无论以何种方式感知未来的工业4.0架构，实现最终目标都将采用多管齐下的方法和网络安全策略，该策略与在工厂中整合数字解决方案的意识强度有关。

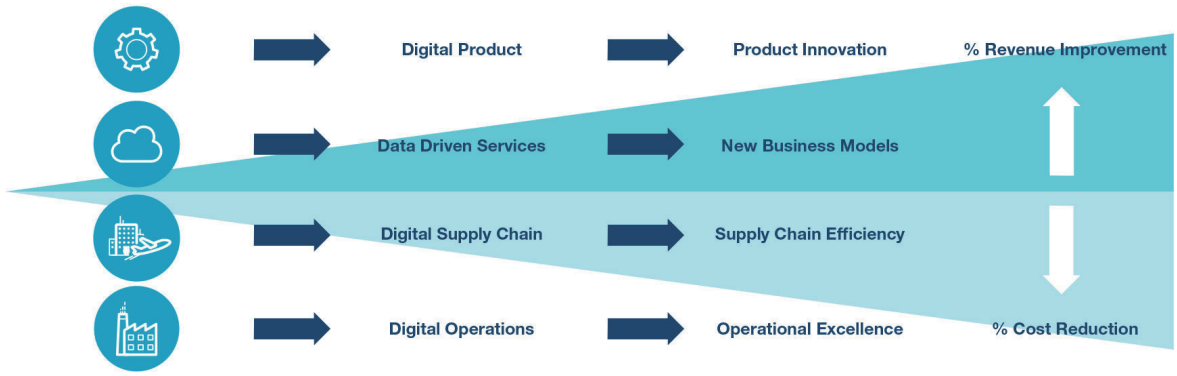

图1. 工厂的数字化正在改变价值链的各个方面，并直接影响企业的顶线和底线。

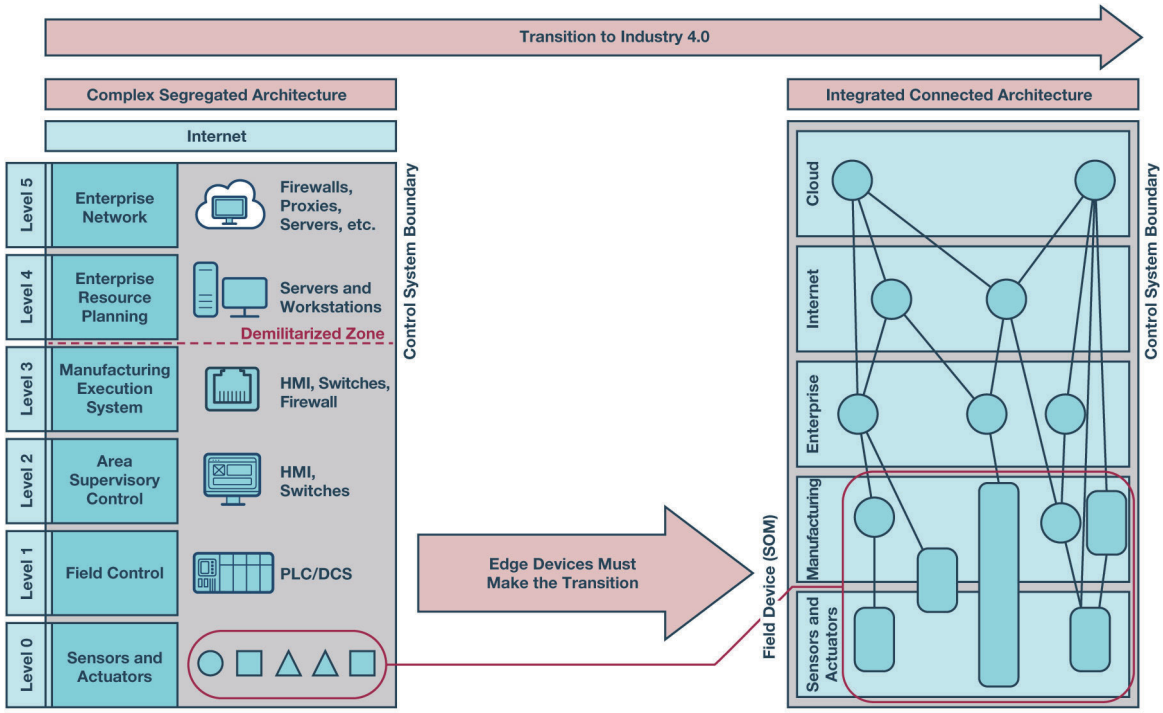

图2. 过渡到完全数字化的工业4.0工厂。

实现网络安全工业4.0的三个步骤

对于完全整合解决方案后，工业4.0会是什么样子，有很多不同的观点。有些人认为传统的工厂设计将基本保持完整，而另一些人的观点则更加激进，认为新工厂将难以被传统标准认可。但每个人都认为工厂正在发生变化，而且不会在一夜之间发生。这种过渡有一些明显的原因，但主要原因是目前现场设备的使用寿命。这些设备的设计运行时间超过20年，并可以继续运行更长时间。可以努力改造这些设备以实现额外的功能和连接，但是它们将受到其硬件设计的限制，并且工厂系统架构将不得不补偿它们的不足之处。从网络安全角度来看，这些设备将始终受到限制并存在网络风险。安全设备需要安全的架构和系统设计方法。对具有安全功能的设备进行改造只是权宜之计，将始终留下网络安全漏洞。完全过渡到数字化工厂将要求设备实现高安全水平，并增强这种安全水平以便能够抵御网络攻击，同时不影响它们实时共享信息和做出决策的能力。弹性即从困难中快速恢复的能力，会对网络安全的实施方式和实现网络安全工业4.0的必要步骤产生巨大影响。

要克服的第一个主要障碍是要遵守新的网络安全行业标准和最佳实践。要在不断变化的工厂内实现合规，需要采用不同的方法。传统方法应用信息技术(IT)安全解决方案来隔离、监视和配置网络流量，将无法在工业4.0工厂中提供所需的弹性。随着设备实现互联并共享实时信息，将需要硬件安全解决方案来实现自主实时决策，同时保持工厂的弹性。随着网络安全方式的变化，组织也需要适应以迎接新的挑战。许多组织正在进行重组以构建网络安全能力，既可以从传统的工程组织单独管理，也可以整合到整个组织的项目团队中。建立一个能够实施网络安全解决方案策略以满足行业标准和最佳实践的组织是实现工业4.0愿望的第一个重要步骤。

在组织采用新兴安全标准建立稳固的基础之后，以及当他们有能力管理跨产品生命周期和跨组织边界的安全要求时，他们就可以专注于在工厂单元内提高自主性。只有当工厂中的设备变得足够智能，能够根据接收的数据做出决策时，才能实现自主。网络安全方法是一种系统设计，构建能够证实信任数据生成来源的数据的边缘设备。最后有信心通过网络安全系统提供实时决策，该系统能够接受来自现实世界的输入信息、评估其可信度并自主行动。

最后一个问题是建立一个不仅连接到云，而且通过云服务与其他工厂系统同步运行的工厂。这需要更广泛地采用数字解决方案，由于完全过渡到数字工厂所需的时间，最终这将成为最后的障碍。目前的设备已经连接到云，但在大多数情况下，这只是为了接收数据。然后分析这些数据，并从工厂车间远程做出决策。这些决策的结果可能是加速或延迟维护或微调自动化过程。今天，由于现场控制在工厂本地进行并与企业系统隔离，因此很少会从云端执行这些决策。随着工厂车间采用更多的自主性，通过云服务监控工厂以及跨企业系统共享实时信息将更为重要。

图3. 工厂车间的自主性采用。

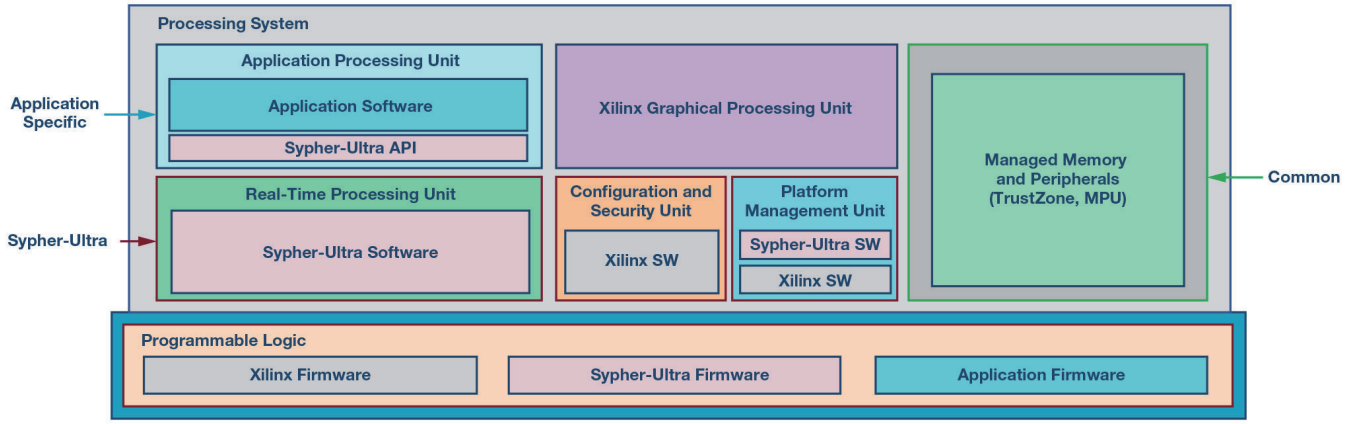

图4. ADI公司的Sypher-Ultra实施。

通过硬件安全性实现互联工厂

工业标准正在推动对硬件安全性的需求，这些标准实现了更高的安全水平，能够在工厂中实现互联解决方案。增加控制的访问和可访问性意味着新风险，如果不将设备级安全性与硬件信任根相结合，则传统IT安全解决方案无法抵御这些风险。当设备连接到网络时，这些设备就成为整个系统的接入点。这些接入点中的任何一个可能造成的损害都会扩展到整个网络，并且可能使关键基础设施易受攻击。依赖防火墙、恶意软件检测和异常检测的传统安全方法需要不断更新和配置，并且容易出现人为错误。在今天的环境中，应假设对手已经在网络中。为了抵御这些对手，需要采取深度防御和零信任方法。为了最大程度地确保互联设备正常运行，设备中需要硬件信任根。今天在设备中建立正确的硬件关联对于未来向数字工厂过渡至关重要。

通过利用FPGA的Xilinx® Zinq® UltraScale+™ MPSoC (ZUS+)系列，ADI公司开发了Sypher™-Ultra，其通过具有多层安全控制的高保证加密系统，为要生成和处理的数据的完整性提供更高的可信度。它利用ZUS+的安全基础以及ADI公司开发的其他安全功能，助力终端产品满足安全要求，如NIST FIPS 140-2、IEC 62443或汽车EVITA HSM。Sypher-Ultra位于嵌入式ZUS+功能和最终应用之间，为设计团队提供单芯片解决方案以实现安全操作。为了提供高保证安全性，Sypher-Ultra平台采用可信执行环境(TEE)，为静止和传输中的安全数据提供基础。与安全相关的功能主要在实时处理单元和可编程逻辑中执行，使设计团队能够在应用处理单元内轻松添加其应用。该设计使产品团队无需掌握安全设计和认证的所有复杂之处，同时确保能够安全操作。

制定实现更高设备级安全性的途径充满挑战，特别是考虑到上市时间限制要满足数字工厂要求苛刻的实施步伐时。实施安全性极其复杂，需要独特的技能组合和流程。ADI公司的安全平台为设计团队提供了一种解决方案，可以在靠近工业控制回路的边缘实现安全性。为产品设计团队解决实施复杂性，例如安全设计、安全标准认证和漏洞分析，可以大大降低风险，缩短设计时间。ADI公司的解决方案在通用平台上提供易于使用的安全API，可在单个FPGA上实现高保证安全性和更高级别应用的共存。ADI公司的Sypher-Ultra产品允许安全使用Xilinx Zynq UltraScale+ MPSoC (ZUS+)系列来隔离敏感的加密操作，并防止对敏感IP的未授权访问，敏感IP通过边缘的硬件安全性为互联工厂提供路径。

作者简介

Erik Halthen作为Sypris Electronics（2016年被ADI公司收购）的一员，具有深厚的网络安全解决方案背景。Erik在ADI公司网络安全卓越中心工作，担任工业解决方案领域的安全系统经理。凭借其担任防务行业网络安全项目经理的经验，Erik致力于开发能够满足工业物联网的关键市场需求的领先安全解决方案。联系方式：*erik.halthen@analog.com*。

在线支持社区

访问ADI在线支持社区，与ADI技术专家互动。提出您的棘手设计问题、浏览常见问题解答，或参与讨论。

EngineerZone™ ANALOG DEVICES 中文技术论坛

请访问ezchina.analog.com

全球总部
One Technology Way
P.O. Box 9106, Norwood, MA
02062-9106 U.S.A.
Tel: (1 781) 329 4700
Fax: (1 781) 461 3113

大中华区总部
上海市浦东新区张江高科技园区
祖冲之路 2290 号展想广场 5 楼
邮编：201203
电话：(86 21) 2320 8000
传真：(86 21) 2320 8222

深圳分公司
深圳市福田中心区
益田路与福华三路交汇处
深圳国际商会中心
4205-4210 室
邮编：518048
电话：(86 755) 8202 3200
传真：(86 755) 8202 3222

北京分公司
北京市海淀区西小口路 66 号
中关村东升科技园
B-6 号楼 A 座一层
邮编：100191
电话：(86 10) 5987 1000
传真：(86 10) 6298 3574

武汉分公司
湖北省武汉市东湖高新区
珞瑜路 889 号光谷国际广场
写字楼 B 座 2403-2405 室
邮编：430073
电话：(86 27) 8715 9968
传真：(86 27) 8715 9931

analog.com/cn

ANALOG DEVICES 超越一切可能™