Accelerating Industry 4.0: Extending the Secure Edge in Industrial Control Systems

加速工业4.0：扩展工业控制系统中的安全终端

ADI公司 Erik Halthen

理解工业控制系统的网络安全

工业控制系统(ICS)中的网络安全问题势必延缓工业4.0的采用。许多企业领导者发现ICS网络安全挑战非常难以理解，因为众多因素导致其非常复杂。此外，开发工业控制系统解决方案的工程师可能尚未看到在设备层面的重大网络安全要求。保障工业控制系统安全的传统方法依赖于限制对网络和设备的访问，并通过信息技术(IT)解决方案监控网络流量。在工厂中使用设备的产品负责人会发现如果将网络安全问题视为IT问题，就很容易解决。然而，随着工业4.0的出现，传统方法将不再足以保障工业控制系统的安全。如果公司没有应对终端设备安全问题的策略，ICS网络安全面临的挑战最终将延缓工业4.0的采用。为了采用并充分利用工业4.0，网络安全必将成为企业规划的关键部分。ADI公司认识到工业4.0为市场带来的挑战。尽管工业市场历来变化缓慢，但工业4.0的采用却以创纪录的速度大大超出了预期。伴随着这些变化，网络安全正成为采用工业4.0最具挑战性的障碍之一。ICS网络安全标准和准则已经付诸实施或正在建立中，以确保工厂的安全，但它们没有提供有关如何加速工业4.0计划的指导。我们的使命是通过扩展安全终端并使其更易于实施安全性，使我们的客户能够更快速地采用工业4.0解决方案。

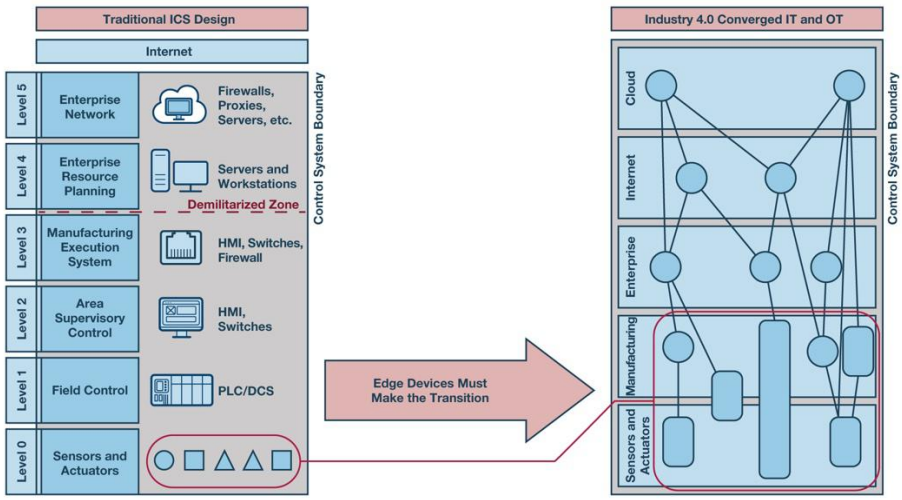

图1.终端设备需要转型以适应工业4.0的采用。

工业4.0正在改变工业　控制系统的网络安全

工业4.0正在改变ICS网络安全问题是有原因的。工业4.0的本质是增加对工厂中设备控制的访问权限和可访问性。这意味着对数据的访问权限增加以扩大透明度，减少网络规划，缩减资本支出，降低运营支出，提高带宽并优化机器互通。增加对控制的访问权限和可访问性意味着工厂系统的网络安全风险评估正在发生变化。ICS网络安全解决方案需要适应不断变化的风险，而传统实施于系统的防范措施（例如设置防火墙和将设备置于闭锁门之后）与工业4.0的目标相背。这意味着需要对设备进行安全加固，以便在确保安全的方法中实现更多功能。为了实现可信数据和安全操作，身份和完整性将成为此领域中每个设备的核心。

工业市场中有许多不同的标准，为工业控制系统安全性的实施提供指导。例如，NIST为美国管理的市场提供安全指导。IEC 62443是针对欧洲管理的国际市场的安全标准草案。这是两个最主要的标准，为工业控制系统安全性的实施和安全状况评估提供了有用的准则；但是，它们并没有就如何加速工业4.0的采用提供指导。IEC 62443目前没有提供有关在PLC下实施安全性的任何准则，最近成立的ISA99工作组旨在解决IEC 62443框架内工厂底层的网络安全问题。当前，为了实现系统可接受的安全状态，必须在未达到足够安全级别的设备上实施防范措施。这

些防范措施通常依赖于诸如防火墙之类的方法来限制访问，并切断或隔离易受攻击的设备。将来，设备需要达到更高的安全级别才能实现向工业4.0的过渡。

ADI公司：扩展工业控制系统的网络安全终端

ADI公司在扩展安全终端方面拥有独特的优势。我们的传统市场空间位于物理终端，即将现实世界转换为数字信号并生成数据的地方。这使我们有机会通过在信号链中更早地提供身份和完整性来建立可信数据，并构建安全终端的全新定义。传统上，安全终端始于工业控制系统安全框架中的网关、PLC乃至服务器。这种观点让人联想到工厂的传统IT网络安全观点，而它仍然存在于整个工业领域中。在信号链中将安全终端进一步向下扩展，其前景非常有吸引力，因为这使得基于该数据的决策具有更高的可信度。在信号链中越早建立身份和完整性，就可以在驱动决策的数据中建立更高的信任和可信度。

ICS网络安全无法以一体适用的解决方案来应对，必须采用深入的防御方法并根据系统的风险评估加以应用。随着以太网应用于终端，ADI公司的策略是扩展ICS网络安全的深度。实现工业4.0需要工厂采用新的连接方法。这意味着以太网已经并将继续在工业控制系统中发挥更大的作用。ADI公司的安全策略是关注以太网连接的位置，因为这会显著改变网络中任何一台设备对系统的影响。我们当前的工业以太网解决方案和TSN解决方案系列一直是公司安全开发的重点。近期，可提供双端口、多协议连接的fido5000 RapID®平台将能够实现多项安全功能，包括提供密钥生成/管理、安全启动、安全更新和安全存储器访问，从而防止网络绑定攻击。此产品系列路线图包括单芯片解决方案，该方案具有硬件可信根、安全设备生命周期管理、安全通信/相互身份验证和防篡改保护。随着工业领域不断采用智能化程度更高的传感器，工厂连接将越来越向下扩展，从而推动了设备层面额外的安全需求。ADI公司致力于开发安全产品组合，以便使ICS安全解决方案的采用更加轻松，并在终端建立信任，以便加速工业4.0的采用。

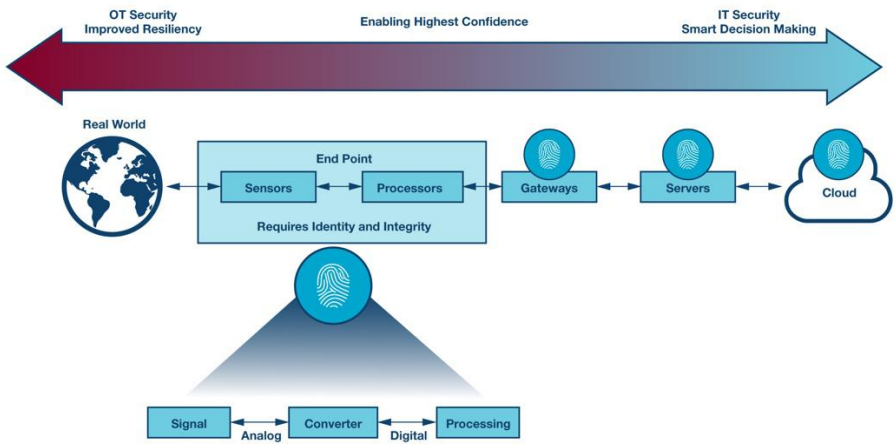

图2.实现最高可信度的决策：就在实现从物理到数字转换的地方。

作者简介

Erik Halthen作为Sypris Electronics（2016年被ADI收购）的一员，在网络安全解决方案方面拥有丰富的背景知识。Erik就职于ADI网络安全卓越中心，担任工业解决方案的安全系统经理。Erik充分利用自己担任防务行业网络安全项目经理时积累的经验，重点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。