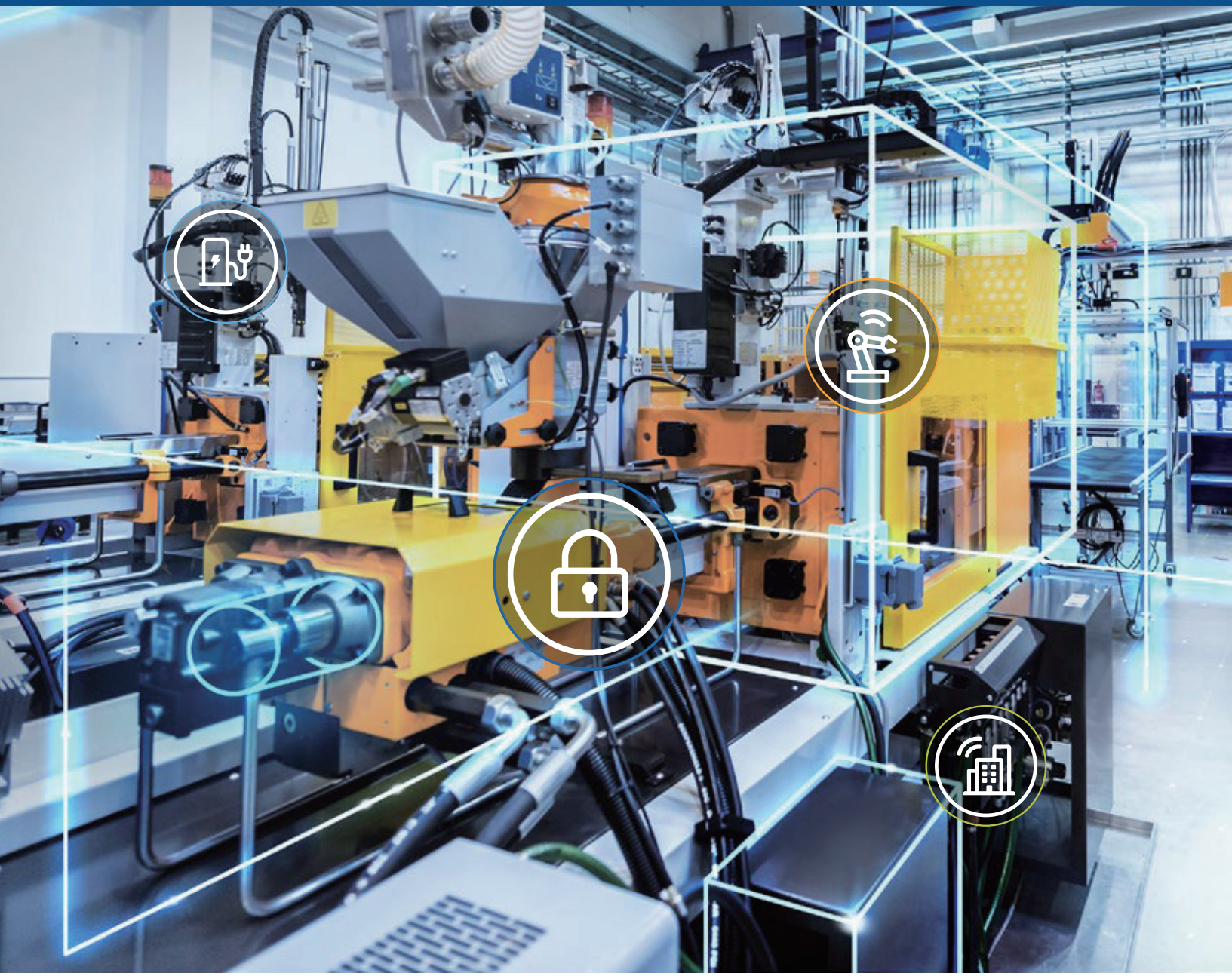
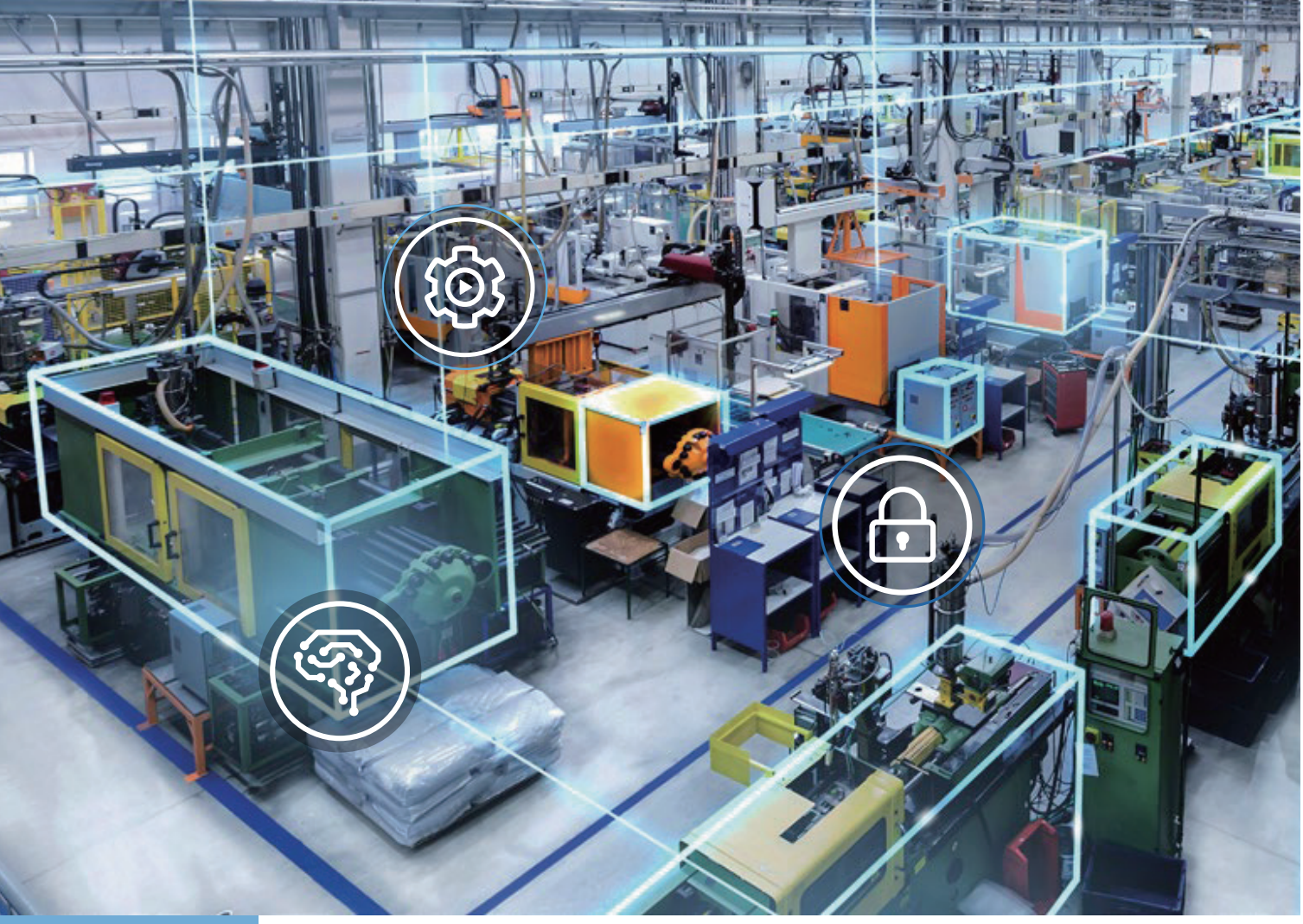
保障工业物联网安全

可信的嵌入式系统解决方案





工业物联网（IIoT）正在改变工业运营的方式。其核心要义是采集数据进行分析并转化为可行动的见解，从而解决问题，更快地做出决策。但工业物联网的设备和基础设施可能成为高价值的网络攻击目标——安全泄露可能导致经济、安全甚至环境的威胁。恩智浦认为安全必须从一开始就考虑进来，从而实现最佳保护。因此，我们坚持不懈地专注于安全工程专业知识、利用经过验证的流程并深刻理解最新的发展趋势，从而为您提供满足安全需求的可信解决方案。

工业物联网：转型的驱动力

各个行业在数字化转型中催生出各种新应用，从无人驾驶运输和智能处理系统，到无人干预、自主运行的机器人。IIoT技术正在电力和能源、工厂、楼宇和医疗行业中广泛部署。执行器、传感器节点、伺服驱动器、视觉系统和可编程逻辑控制器等相互连接的设备——工业的“物”——共同构成工业通信网络，使各设备能够共享大量数据。

工业物联网系统生成、处理和收集的大量敏感数据，需要得到保护并以安全的方式处理。

有些设备可感知、分析、获取数据，并与自动化控制系统实时通信。例如边缘设备，它具有片上计算和机器学习能力，能够立即做出决策。有些执行器能通过操作开关或阀门并收集其数据，可直接影响工业生产过程。这些边缘设备具有计算能力，可以直接影响生产过程，而不需将数据传送于整个系统中。

还有些边缘设备收集数据并发送到中心枢纽进行处理和整合，并将信息发送到云端。这些信息可以由基于云端的应用进行分析和处理，然后再反馈到边缘设备以提高生产效率。

高效IIoT系统的优势包括能效更高、成本更低、产品质量更佳、决策更优化，设备停机时间更少。毫不奇怪，数字化正在所有领域不断扩展，有望在供应链中的多个组织之间实现互联。

设计IIoT架构

虽然IIoT系统差异很大，但它们具有相似的架构特征。物联网设备在制造和物流收集的数据通过网关流向运营管理、监控和数据采集系统（SCADA）和制造执行系统（MES）。它们将原始数据整合并转换为信息，供边缘应用本地分析，或发送到基于云的数据中心进行分析，或两者兼有。

管理和控制运营的传统运营技术（OT）系统是“隔空”的环境，意思就是系统没有连接到外部网络。然而，在当今的各个行业中，信息技术（IT）和运营技术（OT）之间的界限已经模糊，互联的IT系统（可处理电子邮件和数据）开始与独立的OT系统相结合。二者结合好处众多，比如通过提高系统性能的透明度，降低厂商运营成本；助力电力公司根据实时用量及费率情况，为客户提供合约系统。

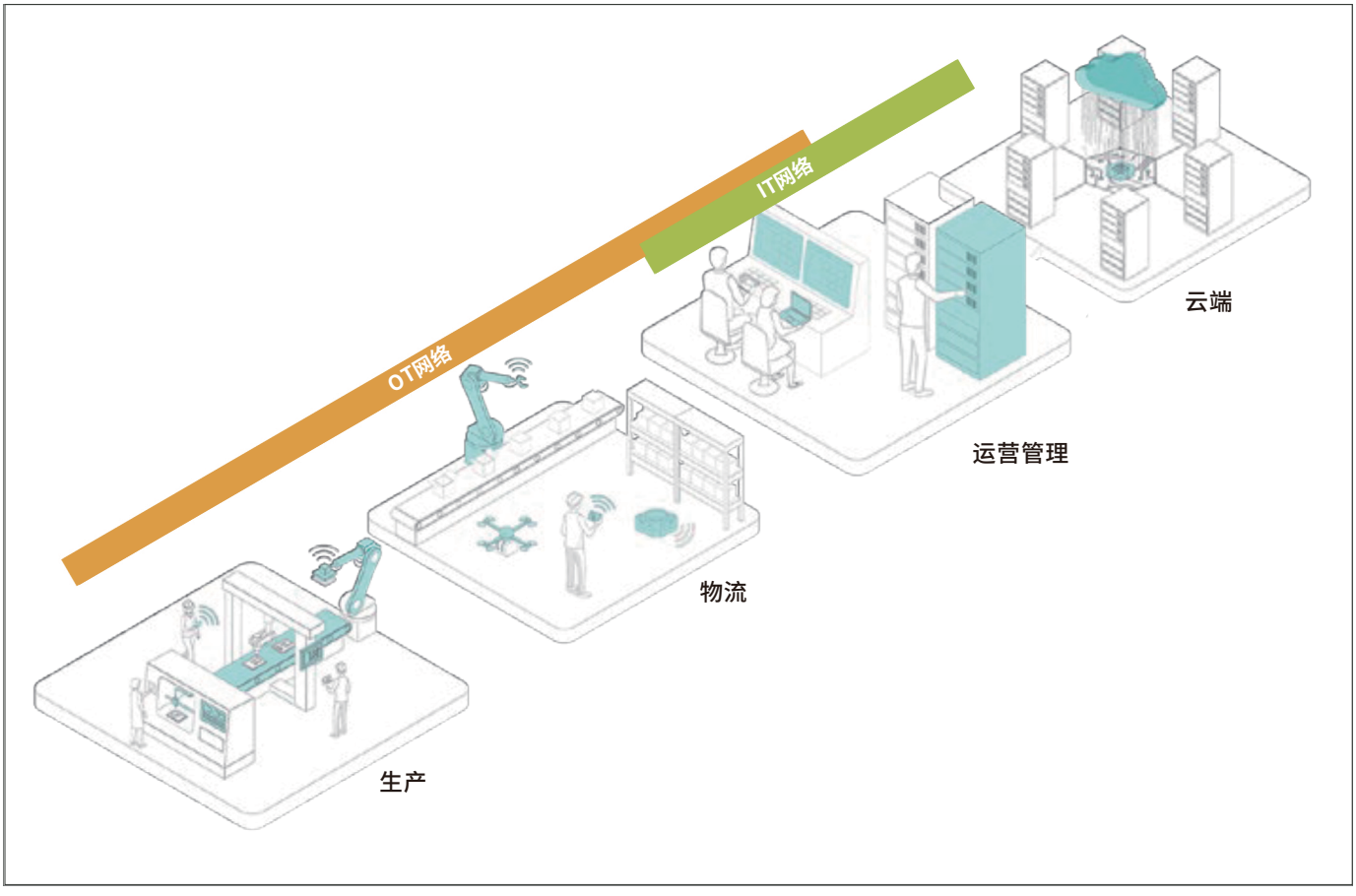


图1. IT和OT网络的融合具有显著的优势，但增加了大规模网络袭击的可能性，可能影响到整个供应链。

网络攻击面扩大，业务风险加大

IT和OT的结合可能扩大基础设施中几乎每个层级（从企业资源规划到工厂车间）的潜在攻击面。

例如，某组织可以访问供应商的计算机系统，以了解物流和供应情况。由于涉及大量互联设备和系统，网络攻击面就扩大了，甚至可以作为入口，侵入财务和流程管理系统，甚至是基于云的系统。犯罪分子的手段越来越高超，可以确定系统中最薄弱的环节，并利用它来引导对整个互联设备网络的攻击。

工业4.0包括可以相互通信并与外部世界通信的IIoT设备。
如果不加以保护，这些设备将成为远程攻击的目标。
对单个设备的恶意攻击有可能牵连其他连接的设备。

许多看似无害的互联设备都存在被网络罪犯利用的漏洞。例如，商业访问控制系统中的漏洞可能让黑客获取到用户凭据、控制门禁并发起拒绝服务（DoS）攻击。犯罪分子利用工厂内安全性较差的可编程逻辑控制器（PLC），向其控制的机器发送错误数据，致使生产线陷入瘫痪。

恶意攻击者利用目标设备路径（它提供了PLC乃至IT网络之间的连接），向生产系统链条的上游移动。在某些情况下，安全至关重要，假设核电站遭到网络袭击，后果将不堪设想。

工业环境的首要安全目标是保障工人安全和系统可用性。

许多现代网络攻击都是来自钓鱼邮件中的“社交引擎”。IT和OT系统的结合，让恶意软件有了从IT系统转移到OT系统的渠道。

不同的生命周期和遗留设备

以前的恶意攻击不像现在这样普遍，由于设备更迭，且网络中融入了不同的安全等级，当时建立在工业设施中的工业物联网系统在不断演进。甚至可能出现供应厂商倒闭，产品在生命周期结束之前就已无法得到支持的情况。

此外，旧有产品的处理能力或内存不足以处理OTA更新或技术人员实施的更新，但它们控制的系统却因为成本过高或影响过大，也无法更换。OT系统内运行旧版操作系统的个人计算机或物联网平台将使有效根除恶意软件变得更加复杂，尤其在不断演变的安全威胁面前保护系统安全时。生产线停机成本也是一个考虑因素，也是所有者不愿意进行此类升级的原因。

虽然现代设备中漏洞并不常见，但一些遗留嵌入式设备中的漏洞会生成初始序列号（ISN）——计算机或互联网连接设备之间传输控制协议（TCP）的基本特征，使数百万的物联网设备易受攻击。ISN随机生成，可防止第三方入侵通信。然而，部分遗留设备生成的序列号可以找到规律，黑客能预测并发起DoS攻击。此外，入侵者可以访问通信并注入恶意代码。

勒索软件的目标

网络罪犯认为“工业”是勒索软件有利可图的目标。生产线停机可能导致每分钟数千美元的损失。证据表明，在一半的案例中，勒索软件网络攻击得手后，受害方支付了赎金。在一项对交通、能源、化工、智能楼宇和智慧城市等关键基础设施领域的1100名IT和OT安全专业人员的独立调查中，超过60%的人支付了赎金。其中超过一半的人至少支付了50万美元。对这些部门的网络恐怖袭击可能会造成灾难性的环境影响，甚至造成人员伤亡。很明显，随着这个世界的数字化不断加快，工业网络安全会是一个非常重要的领域。

各个行业都会受到勒索软件的攻击，但对制造业的影响尤为严重。2020年，制造业遭受的攻击比前一年增加了300%。

[来源：NTT 2021 Global Threat Intelligence Report]

工业界的反击

政府建立新法案

2019年6月生效的《欧盟网络安全法案》为所有OT产品和服务建立了欧洲网络安全认证框架。其范围包括欧盟网络威慑、法律强化、犯罪者识别、国际合作和外交、政治应对。欧洲网络安全机构（ENISA）加入了这一新框架，建立了标准化和认证之间的联系。

在美国，国家工业安全计划（NISP）也采取了类似举措。此外，2022年的《加强美国网络安全法案》（SACA）于2022年3月签署立法。法案要求关键基础设施运营商在72小时内向网络安全和基础设施安全局（CISA）报告“重大网络事件”，并在24小时内报告勒索软件赎金情况。

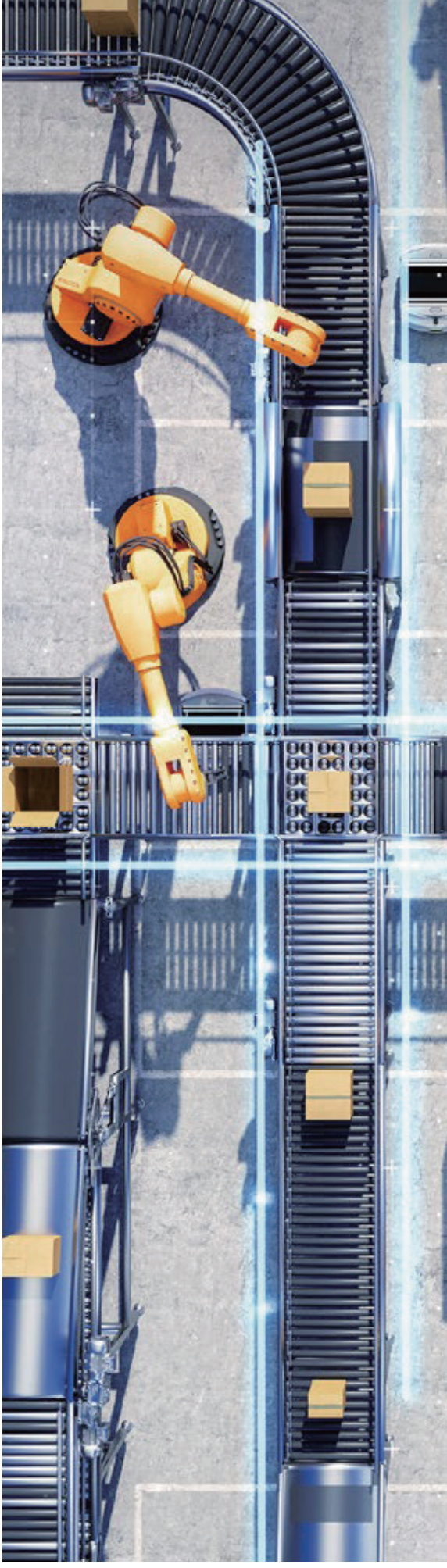
IEC 62243：实现产品合规

IEC 62443是一系列国际标准，旨在解决工业自动化和控制系统（IACS）中运营技术的网络安全问题。恩智浦及其他行业安全专家共同开发了该系列标准，标准分为几个部分，涵盖从设备级到IACS级的程序和技术要求。

IEC批准62443系列标准为“横向标准”，这意味着主题专家开发特定于行业的OT网络安全标准时，它们将被用作标准基础。标准提前为安全的各个方面提供了框架，可防止因使用大量行业标准而引起的混淆，并创建了统一、可互操作的安全方法，例如，基于IEC 62443建立的电梯网络安全标准。除了控制系统可能包含的技术外，IEC 62443系列还包括程序“最佳实践”指南，风险评估和威胁对策，以及组织创建其网络安全管理系统（CSMS）的基准。

标准分为四个部分：

- **第一部分** 涉及使用的术语和方法。
- **第二部分** 介绍了不同角色（如工业设施）的方法和安全流程。
- **第三部分** 讨论了系统的网络安全技术要求。目标受众是系统集成商。
- **第四部分** 是关于在产品生命周期的所有阶段的网络安全整合，并规定了组件本身（如嵌入式设备）的技术要求。



恩智浦的安全设计方法，简化62443标准合规流程

恩智浦拥有广泛的安全专业知识，并利用其在智能卡、政府电子护照和汽车应用领域的高级安全元件方面的经验，满足产品的安全需求。恩智浦严格测试其站点、系统和流程。除了确保安全组件的完整性外，恩智浦在组织内部培养了安全意识文化，使安全成为公司DNA的一部分。

恩智浦不仅有记录在案的安全程序，还将其付诸实践，并已达到IEC 62443-4-1的成熟度3级（ML3）。该认证的范围涵盖恩智浦的业务创建和管理（BCaM）产品开发过程和产品安全事件响应过程（PSIRP）。恩智浦的BCaM框架是一个产品开发过程框架，涵盖了成功推出新产品的所有协调过程，包括新技术和软件。BCaM框架包括一个以安全成熟度过程（SMP）为中心的安全模块；确保产品符合安全标准，包括IEC 62443。有了这样一个模块化的过程结构，恩智浦能够推出符合IEC 62443要求的新产品。

物联网平台安全评估标准（SESIP）

除了IEC 62443等安全标准外，恩智浦认为，一个满足工业物联网安全、足以应对各类复杂挑战的认证标准，可以加强产品的整体安全性。

GlobalPlatform于2020年宣布了一项新的认证标准——物联网平台安全评估标准（SESIP）。这使第三方安全认证成为可能，意味着设备制造商可以证明其声称的设备安全性。我们的客户可以更方便地知道他们能够信任哪些器件。

SESIP以实用、易用和易复用而闻名，并由国际公认的行业组织支持。它通过使用常识方法，映射到主要标准，并包含了一个分级的、有安全配置文件的库，使设备制造商更容易验证其产品的安全性。

平台定义

SESIP汇集了安全系统应实现的常见安全需求。如果某组件要集成到其他设备中，例如安全微处理器、连接库和为运行互联应用提供基础的操作系统，则可以复用组件的认证。

范畴

SESIP威胁模型旨在保护设备上的个人数据，例如身份验证凭据。它还保护传输中的数据、作为应用或平台一部分的软件代码，以及与产品标识、配置、系统运行和设备生命周期相关的数据。

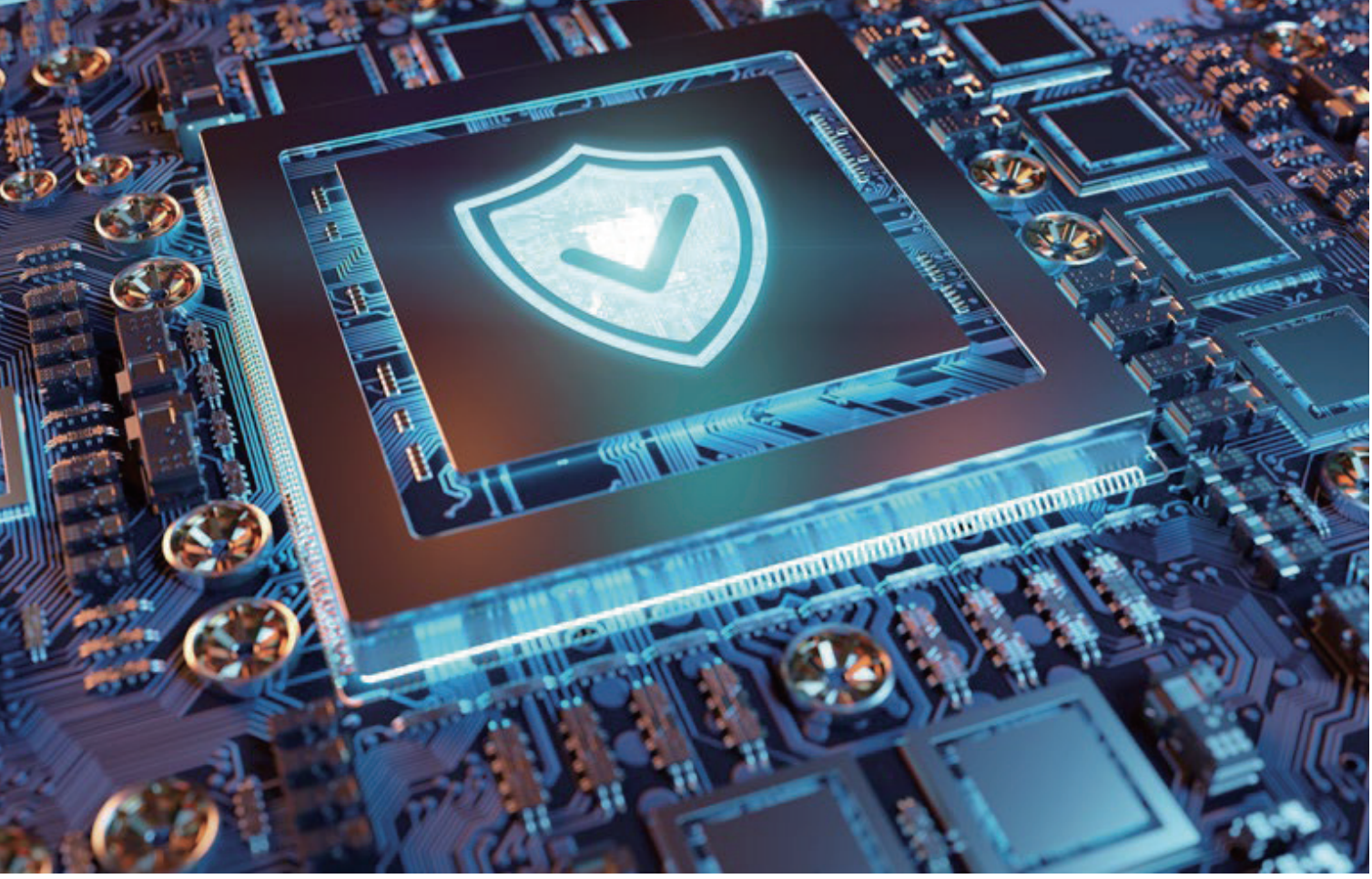
可应对的威胁

预防、恢复和从攻击中学习的能力是组件鲁棒性评估的一部分。评估涵盖基线威胁场景，并可能扩展到更多场景。

安全原语

考虑到现代工业物联网系统网络安全的复杂性，在特定用例中确定必要的产品安全功能可能具有挑战性。为了帮助建立必要的安全级别，恩智浦拥有一套全面的安全定义，有助于以结构化的方式实现安全。这些定义也称为“安全原语（Security Primitives）”，描述了分到不同类别的安全功能，根据给定用例或安全需求的高级概念，帮助选择合适的产品或相关安全标准。
https://www.nxp.com.cn/securityprimitives

恩智浦的安全原语提供了一个起点，帮助您以结构化的方式将安全需求映射到产品中。更多信息请访问 nxp.com.cn/securityprimitives。



恩智浦产品

用例不同，安全性也各不相同。因此，恩智浦提供了内容丰富的EdgeVerse™产品组合，满足广泛的用例和保护需求。客户可根据应用，选择具有集成安全功能的SoC、开箱即用的安全元件或两者的组合。信任供应和云安装服务进一步补充了我们的解决方案。我们的产品组合可以抵御高价值重要系统中的各种风险，从基本软件威胁，直至复杂的硬件攻击。

具有集成安全性的MCU和处理器

恩智浦的EdgeVerse™处理平台可应对安全IIoT需求。该平台包含一系列微控制器和处理器，功率、性能可扩展，提供丰富的混合信号和安全集成，以及系统级解决方案和软件支持，从而简化嵌入式开发。

近年来，无论是作为连接端点中的主机控制器，还是IIoT网关或网络解决方案中的配套器件，微控制器基于硬件的安全性已成为嵌入式系统开发的主要设计标准。我们在开发最新的基于Arm® Cortex®-M的微控制器（例如最近推出的LPC5500 MCU系列）时，把安全放在首位。LPC5500 MCU系列集成了一系列基准安全功能，如具有不可变硬件信任根的安全引导、基于SRAM PUF的唯一密钥存储、基于证书的安全调试身份验证。LPC5500的加密加速功能得到进一步增强，使用专用于AES-256和SHA2-256的加速器以及非对称算法（如用于公钥基础设施的ECC和RSA），实现更快的密钥交换。

恩智浦将EdgeLock® secure enclave集成到部分新推出的i.MX应用处理器和i.MX RT跨界MCU中，以提供保护和隔离。这种预配置、自我管理和自主的芯片内安全系统提供了一套丰富的安全服务和平台安全功能，可以进行独立管理，而不会影响处理器或控制器的功能。

恩智浦i.MX RT1180是专门为工业边缘应用构建的跨界MCU，是恩智浦首款包含secure enclave以及5 Gbps直通以太网交换机的产品。其交换机具有多协议支持，可用于时敏网络和实时工业以太网。此外，通过将系统级工业安全要求映射到恩智浦的目标SESIP组件认证中，i.MX RT1180将简化原始设备厂商满足IEC 62443标准方面的努力。

无论是用于机器学习、图形和视觉的专用加速器，还是集成的EdgeLock® secure enclave，我们的i.MX应用处理器系列，包括针对各种低功耗用例的i.MX 8ULP和主流i.MX 9系列，都能满足IIoT应用日益增长的安全需求。

安全元件

EdgeLock SE05x产品系列是一组开箱即用、即插即用安全元件器件，经过通用标准（CC）EAL 6+认证，并在IC级别提供信任根，为IIoT设备提供强大的端到端安全性。EdgeLock SE05x系列是一个即用型解决方案，提供完整的产品支持包，可与Linux、Windows、RTOS和Android等主要操作系统集成。作为对各种MPU和MCU的扩展，该系列器件可简化设计并缩短上市时间。该系列微控制器的设计工具，如用例示例代码和兼容的开发工具包，有助于用户快速集成。

使用EdgeLock SE05x安全元件及其预集成的安全功能，可以简化IEC 62443组件要求的合规工作，同时消除实现安全性的许多复杂性。例如，EdgeLock SE05x为IIoT设备提供了一个安全身份，然后与相互认证、传感器认证、云安装和其他IIoT任务一起使用。这使原始设备厂商能够进一步增强IIoT设备的抗逻辑和物理攻击能力，打造面向未来的设备。

EDGELOCK® ASSURANCE by NXP

EdgeLock Assurance

安全性是恩智浦组件和解决方案的核心。EdgeLock Assurance标志意味着该产品的设计遵循了行业标准。这类解决方案使用验证过的流程开发，并经过了验证评估，因此非常可靠，能帮助您应对各种安全挑战。

更多信息请访问
www.nxp.com.cn/edgelockassurance

安全灵活的物联网服务平台

EdgeLock 2GO

EdgeLock 2GO安全服务平台用于轻松、安全地部署和管理嵌入恩智浦 EdgeLock SE05x 安全元件或EdgeLock A5000安全验证的物联网设备。这种全包式解决方案提供安全设备凭据管理，可用于制造过程，或现场、无线和整个设备生命周期中。EdgeLock 2GO服务基于安全硬件，保护凭据，并与此安全硬件建立安全的端到端连接。安全硬件和服务的组合可以显著减少工业设备的开发时间和拥有成本。有了EdgeLock 2GO，设备厂商不必投资新的制造设备来支持设备安全管理，包括设备安装和生命周期管理。

高于工业4.0的转型：工业驱动开发平台

i.MX RT工业驱动平台提供了利用恩智浦安全产品进行开发的起点，让用户体验到恩智浦在硬件和软件方面为下一代安全和网络弹性工业驱动提供的强大安全性。它具有用于多轴控制的先进电机控制算法和充足的带宽，以支持人机界面（HMI）、确定性以太网时敏网络（TSN）通信、数据记录和故障检测。它旨在通过IEC 62443-4-1、4-2 SL3认证。i.MX RT1170 MCU和板载恩智浦 EdgeLock SE05x安全元件提供了一个现成的多板开发平台，用于评估和验证各种工业应用。

工业网络安全的未来

网络威胁继续以复杂和令人惊讶的方式演变，遗留设备的风险水平也会随着时间的推移而提高。因此，恩智浦正准备通过推进创新来应对这些新的网络威胁。

后量子时代的加密

量子计算机正在一点一点、缓慢而稳定地发展着。通用量子计算机可以执行复杂的计算，这类计算，对于我们目前能够构建的最强大的超级计算机来说，都是难以解决的。这类计算可以解决优化问题，在GPS、计量学、药物研究和机器学习等领域具有潜在的突破能力。然而，鉴于当前使用的密码系统，量子计算对互联网安全、物联网设备和法律基础设施（乃至对整个社会）的潜在威胁，再高估也不为过。

在这样的量子未来，当今系统和解决方案的安全性可能会被削弱，或完全攻破。此类系统中包含的数据（包括代码）可能会突然泄露。恩智浦的安全工程师和密码学家正在领导后量子加密（PQC）过渡，为NIST PQC标准化工作中的领跑者做出贡献，并确保任何未来推出的PQC标准都要考虑到嵌入式安全的核心要求，例如物理安全实现和资源限制。

IP 保护

知识产权（IP）传统上指为一个想法申请注册专利，保护其相对较长的研发时间，防止被剽窃。在软件场景中，这种保护更复杂，可能涉及数字水印。加数字水印是指在数字文件中以隐藏的方式存储文件中包含的信息。在工业电子领域，特别是机器学习领域，版权信息可能与知识产权有关。

例如，我们可以使用基于机器学习模型的预防性维保应用。该模型包含IP，可以直接复制，从而减少签订维保合同的成本。数字水印是一个很有前途的发展方向，通过保护机器学习模型来防止IP盗窃。

工业物联网设备的网络弹性

网络安全从来不是静态的；事实上，即使是最安全的设备在未来也可能会遭到黑客攻击，这种情况非常正常。为了在这种具有挑战性的场景中也能实现安全性，将保护与检测和恢复机制相结合的多层防御策略至关重要。由此产生的有网络弹性的设备，即使是遭遇当前未知的远程网络攻击，也可以快速恢复到可信状态。最好的情况是，如果设备检测到安全泄露，这种操作会自动运行，但即使没有实现自动化，作为最后手段，管理员也始终能够远程恢复设备。恩智浦的全面网络弹性和恢复策略的概述，请见**nxp.com.cn/cyres**

区块链

区块链技术在工业中的运用越来越多，主要是用来跟踪工业物联网设备产生的日志和交易。这些设备所属的内外实体、组织可能未建立信任关系。区块链使用加密机制确保交易链在任何时候的完整性和不变性，以便各方可以信任发布的信息。

为了确保只有授权设备在区块链中发布交易，交易可以由物联网设备签署，并在接收时由区块链验证。因此，将用于签署交易请求的私钥存储在安全元件（SE）中，对于保证交易的真实性至关重要。恩智浦一直在开发可以利用我们的微控制器的高安全性功能的解决方案，以此支持区块链交易的验证工作。

专有网络

随着工业物联网系统内互联设备数量的增加，与通信相关的安全解决方案越来越重要。越来越多的工业企业使用内部私有网络，其中的数据从不进入公域，从而更好地保护其免受黑客的攻击。专有网络还保证了一致、可靠的覆盖。使用的无线技术可以是传统的802.11 Wi-Fi或蜂窝协议。

未来，Wi-Fi 6和5G很可能会在许多工业物联网系统中发挥作用。与以前的Wi-Fi标准相比，Wi-Fi 6具有更低的功耗和显著的性能提升。5G拥有超可靠的低延迟通信（URLLC），其速度足以支撑一个智能工厂使用增强现实、人工智能和先进机器人技术。这些技术预示着工业4.0的美好未来。恩智浦处在开发和实现这些技术的核心。一个例子是Layerscape®系列处理器，它实现了软件定义的无线设置能够通过专有5G网络传输开放平台通信统一架构（OPC UA）数据。

结语

IIoT为所有工业部门提供了巨大的效率和成本效益，无论是在发电、交通还是智慧城市基础设施领域。为此，所有部门的通信电子设备的数量和复杂性都在增加。这种部署扩大了风险足迹，增加了网络攻击的可能性。

所有工业物联网设计都必须内置强大的网络安全措施，以规避潜在的灾难。保护系统免受恶意攻击需要仔细规划，在设计之初就嵌入安全功能。在设计时就使用安全产品以构建精心规划的可扩展架构的IIoT系统（同时考虑到OT和IT系统的融合），相比不考虑安全架构或连接的IIoT系统，能更好地抵御不断演变的网络攻击。在组织内接受过安全意识文化培训的员工，也将在识别和应对威胁方面发挥至关重要的作用。定期威胁测试和持续审计将带来安全提升和优化，从而提高工业物联网对于网络攻击的抵御能力。

网络安全法规、标准和框架都有助于应对日益增加的威胁，指导各部门的最佳实践，并协助组织创建其网络安全管理系统。恩智浦在安全方面有着悠远的成功经验，它将在未来的安全保障方面发挥至关重要的作用。

文档编号：INDSECWP REV 0