HongKe 虹科

[EBOOK]

你需要知道的实用OPC UA安全技术

每个人的OPC UA系列指南

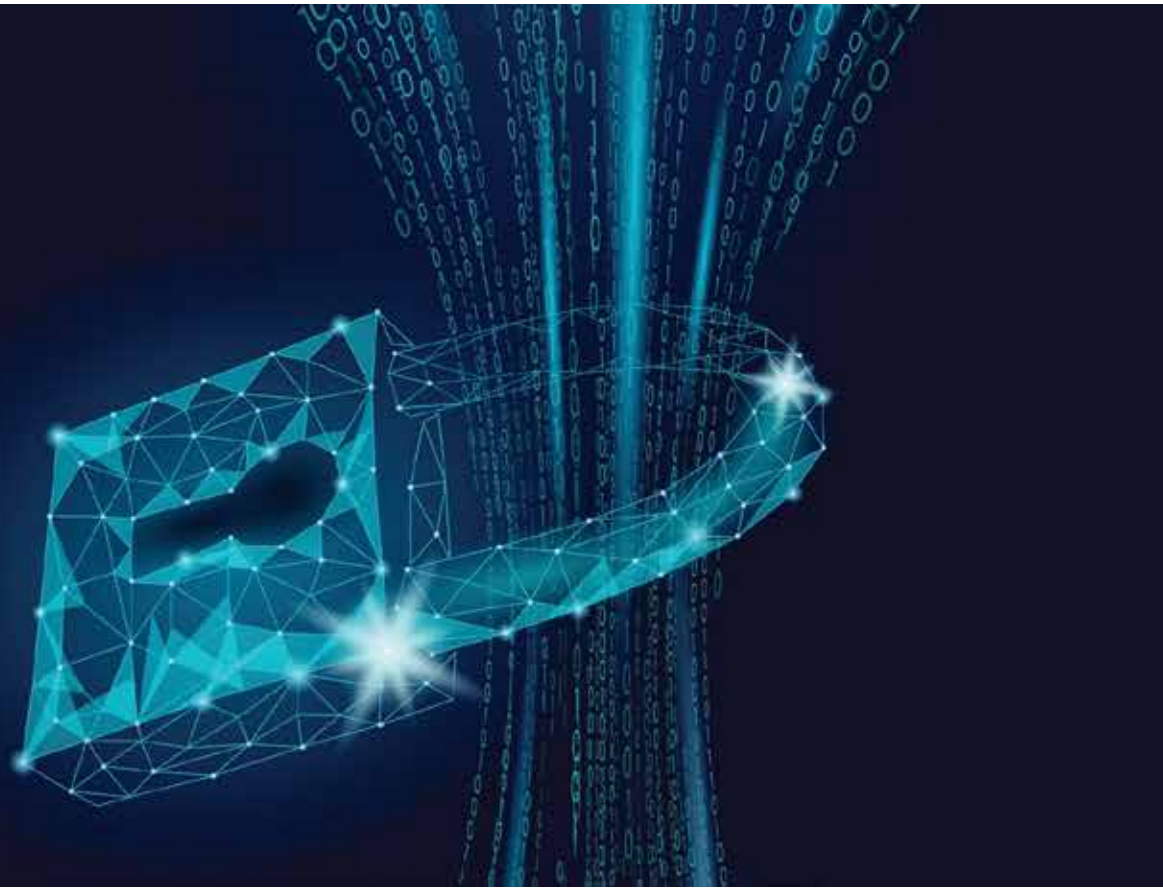
Matrikon® Powering Interoperability | Beeond

OPC UA

目录

OPC 安全: 概述

IIoT/工业4.0且状个玫守入摘拥云措佛怍



数字业务转型，OPC UA和安全性

新兴的工业物联网（IIoT）时代的数字化业务转型正在成为所有行业企业的关键竞争优势。

了解有关第四次工业革命的技术以及如何安全地使用它们至关重要。尤其是由于企业对更深入的车间可见性的依赖性日益增强，也导致网络攻击的频率，规模和复杂性急剧增加。

OPC UA在实现IIoT，工业4.0（I4.0）和中国制造2025方面起着基础性作用，部分原因是自下而上内置的有效数据安全性。

Ebook提供了OPC UA关键安全主题的高级概述，因此非技术读者可以快速了解该主题及其背后的相关安全概念。

缩小 IT与OT 的差距

挑战：满足IT和OT安全需求

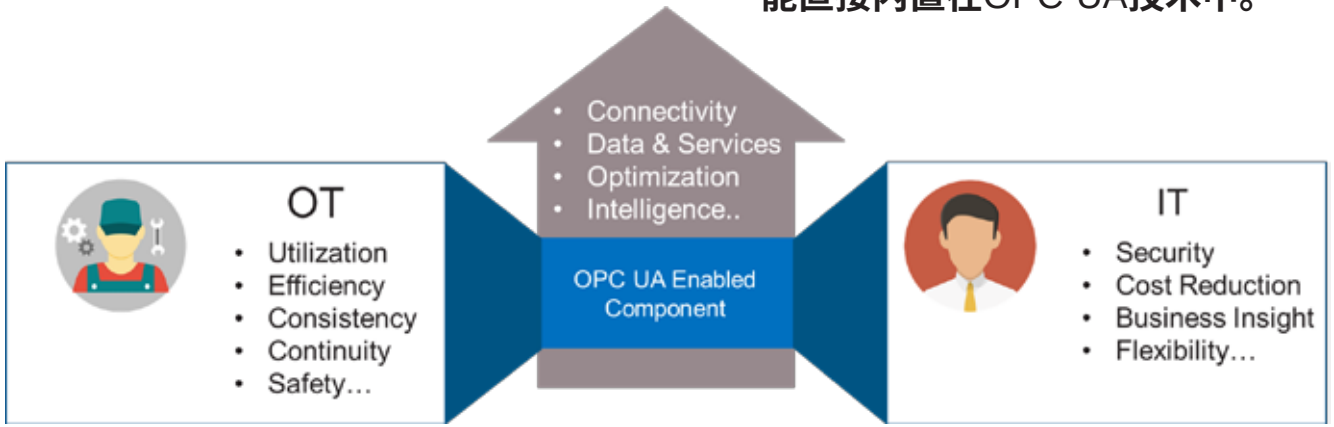
数字化要求整个企业中的人员和系统以安全的方式随时访问他们所需的OT数据。

最终，IT和OT有着相同的目标来保证他们的系统的安全，但是他们对安全的不同方面有不同的优先级区分（见下图）。传统上，这些组织很难在适当满足IT和OT安全需求的同时，共同提供数字业务时代所要求的数据可见性级别。

解决方案: **OPC UA**

OPC UA标准起源于OT世界，但它是从零开始发展的，目的是在每个步骤中正确实施IT安全最佳实践。这样做是为了最大程度地提高OPC UA系统的可信赖性，因此可以在企业范围内安全使用OPC UA数据。

通过满足IT和OT的安全需求，OPC UA使每个组织都可以专注于其指令，而不必担心对方在做什么。这是可能的，因为正确的功能直接内置在OPC UA技术中。



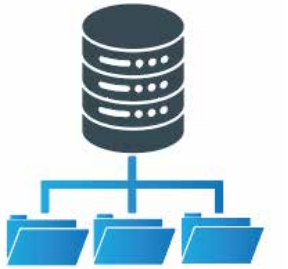
OPC UA 安全 vs. OPC Classic

从成功的OPC Classic标准中学到的经验教训中，OPC基金会拥有20多年的经验，完全重写了OPC UA中安全性的工作方式。各种深入的第三方测试已成功确认，安全性已成为OPC UA的关键优势之一。

OPC UA 安全范围

考虑到“网络安全”术语的广度和深度，重要的是要弄清楚OPC UA提供哪些类型的安全性。 对于Ebook而言，从高层次的角度进行处理比较有建设性，而不是深入研究OPC UA适用和不适用详尽的安全术语清单。

简而言之，OPC UA主要涉及将文本丰富的数据从点A传输到点B。因此，了解数据如何处于三种基本状态之一：静态，处理中和动态。OPC UA安全性更多与动态数据有关。



静态数据

处理中数据

OPC UA 安全重点:

动态数据

动态数据（DIM）侧重于验证两个实体、在它们之间建立信任、在它们之间跨网络和域（包括防火墙和）安全地传输适当数据所需的安全措施，并支持用于定期分析的有效审计跟踪。

数据保证

为了维护安全性，全世界许多组织已经着手来研究，定义和维护网络安全最佳实践。 尽管有许多这样的标准和建议，但是如果您将它们归结为基础，它们将集中在相同的核心安全概念上。下面显示了两个最受欢迎的概念。

基于这些核心概念，OPC UA从头开始开发，以正确使用算法和体系结构组件，并可以由供应商正确实现。 这一点很重要，因为标准通常会陷入在纸面上看起来不错但在现实世界中难以实施甚至不可行的陷阱。

CIA 联合组

保密

发送的数据仅对预期的收件人可见

完整性

可以检测到对发送数据的修改

可用性

授权人员在需要时可以使用数据

AAA 框架

真实性

人员或系统的身份得到保证。

授权书

实体之间的所有活动均根据各自具有的权限进行控制

可审核性

不可否认性–所有数据请求和接收均已记录且无可争议。

安全威胁和测试

通过定义CIA联合组和AAA框架，可以映射最常见的网络攻击类型，以显示其针对数据保证的哪些方面。

下表显示了哪些威胁攻击了数据保证条目的哪个方面。OPC UA安全性针对这些攻击类型的有效性已通过独立的第三方实验室的全面测试并成功通过。不出所料，安全威胁及其对策不断发展。

OPC UA标准旨在方便地对其安全机制进行更新，以确保其提供有效的"面向未来"的安全性。

Threat	Authentication	Authorization	Confidentiality	Integrity	Auditability	Availability
Message Flooding						X
Eavesdropping			X			
Message Spoofing		X		X		
Message Alteration		X		X		
Message Replay		X				
Malformed Messages				X		
Server Profiling	X	X	X	X	X	X
Session Hijacking	X	X	X			
Rogue Server	X	X	X		X	X
Compromised User Credentials		X	X			

定义

- 消息洪泛：**攻击者向目标系统发送一系列请求，以尝试消耗足够的服务器资源以使系统对合法流量不响应。**
- 窃听：**在未经他人同意的情况下收听私人对话或交流。**
- 邮件欺骗：**恶意方冒充网络上的另一台设备或用户对网络主机发起攻击，窃取数据，传播恶意软件或绕过访问控制。**
- 消息更改：**一种网络利用，对目标上的数据或传输中的数据进行更改。这可能包括更改数据包头地址以将消息定向到其他目的地或修改目标计算机上的数据。**
- 消息重播：**一种网络攻击，其中捕获有效的数据传输，然后重播以影响系统操作。**
- 格式错误的消息：**也称为协议模糊检查，格式错误的消息（语法错误的消息）被发送到目标服务器或客户端，以中断服务。**
- 服务器配置文件：**收集有关服务器或基础设备的信息，以获取有关基础结构的数据（例如，正在使用哪种类型的PLC）。**
- 会话劫持：**TCP会话劫持攻击受保护网络上的用户会话。会话劫持的一种类型称为"中间人攻击"，攻击者使用嗅探器可以观察设备之间的通信并收集传输的数据。**
- 恶意服务器：**恶意服务器是网络上不受网络人员管理控制的服务器。**
- **泄露的用户凭证：用户凭证已被用户以外的其他人访问（未经其知情或同意），并且他们能够登录到该用户的帐户。**

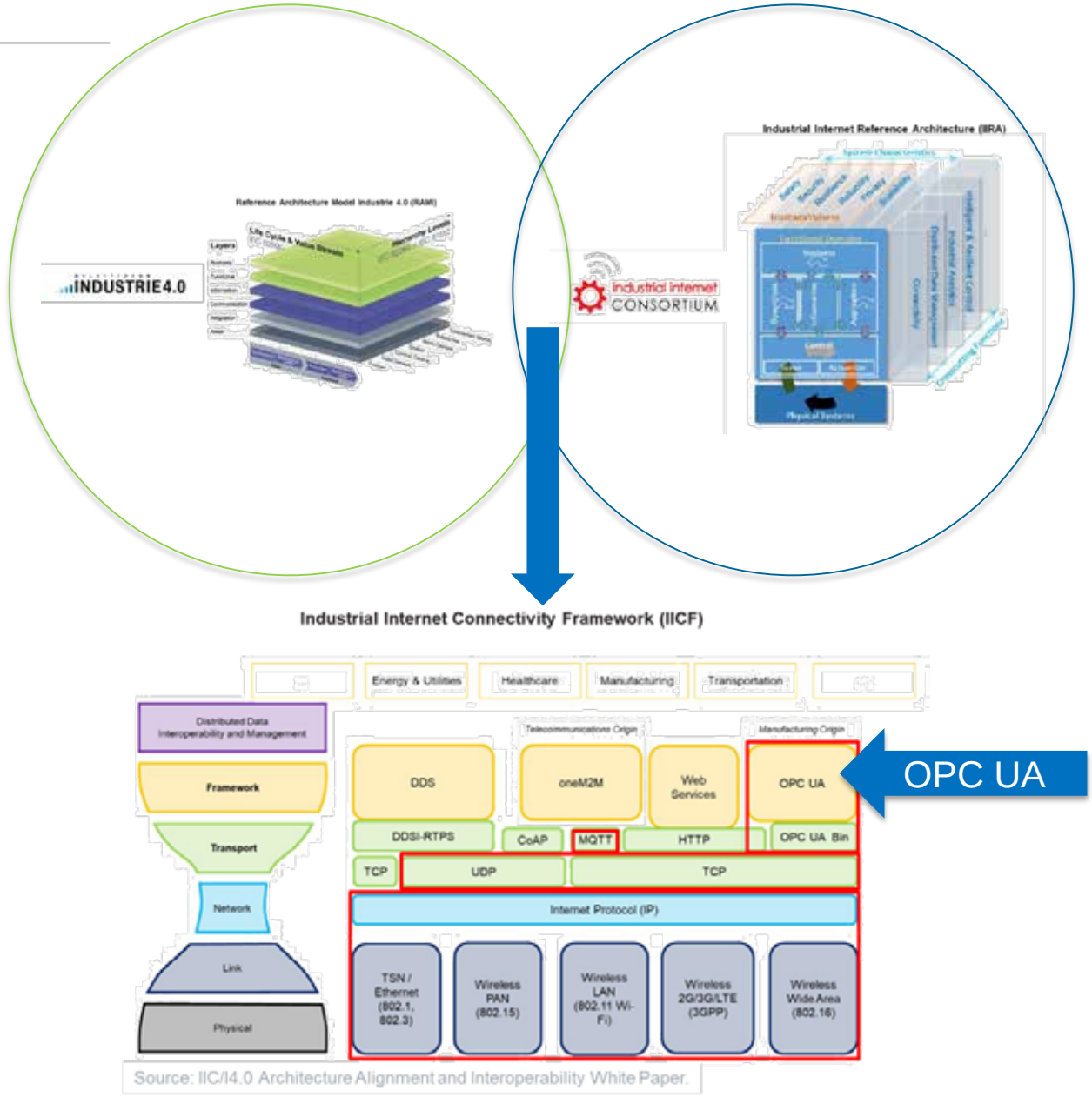
关键行业组织认可 OPC UA

各种组织解决了使工业物联网（IIoT）可行和可持续的范围和复杂性。 他们的目标是确定必要的核心规范集，以共同作为构建IIoT解决方案的一致基础。

关键联盟的两个示例包括工业互联网联盟（IIC）和工业4.0平台（I4.0）。

这些组织彼此独立且具有不同的主题范围，它们开始合作以协调其复杂的IIoT框架，以在全球范围内最大化IIoT的互操作性。

部分基于其强大的端到端安全性以及经过全面的第三方测试，OPC UA规范被IIC，I4.0和全球许多其他组织（例如，开放平台自动化论坛（OPAF），中国制造2025）选择为核心标准。



Source: IIC/I4.0 Architecture Alignment and Interoperability White Paper.

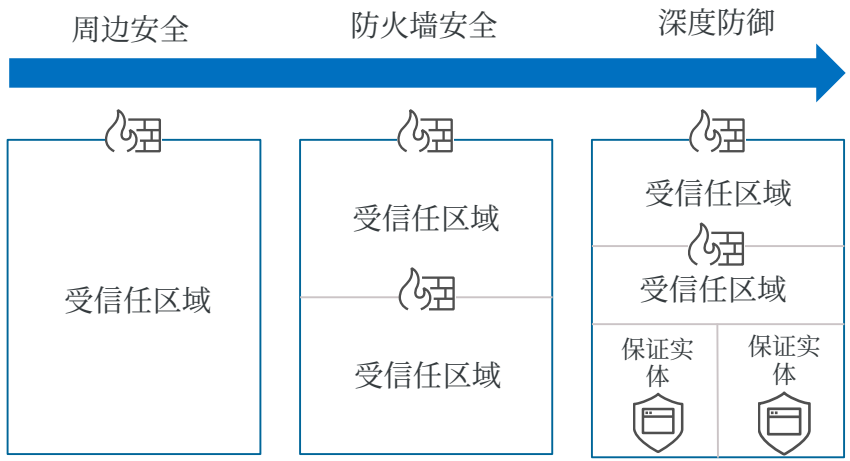
深度防御

实现深度防御安全性的IT最佳实践方案旨在通过在整个给定体系结构中混合使用不同类型的安全措施来最大程度地提高系统对各种攻击的弹性。每种不同类型的安全性都会增加另一层复杂性，从而在闯入者渗透到系统中时使其速度变慢。虽然最终可以击败每个系统，但花费更多的时间才能增加攻击失败或被发现并加以抵抗的机会。

OPC UA**直接符合深度防御的理念，利用多种安全机制。 通过使用这些安全功能，启用了**OPC UA**的应用程序可增强它们所组成的基础架构的整体安全性。**

OPC UA**中的一些安全机制包括：**

- 加密
- 签收
- 支持审核
- 认证与授权
- 密码安全
- 防火墙兼容性
- 另外的许多其他机制



对车间数据的日益增长的依赖导致对基础数据系统的攻击增加。为了解决这个问题，IT安全已经从外围样式安全演变为“源头安全”的理念。 OPC UA**是专为深度防御而设计的。**

灵活的OPC UA传输支持

OPC UA**支持深度防御范例的另一种方式是，可以使用不同的传输方式跨网络承载**OPC UA**数据。**

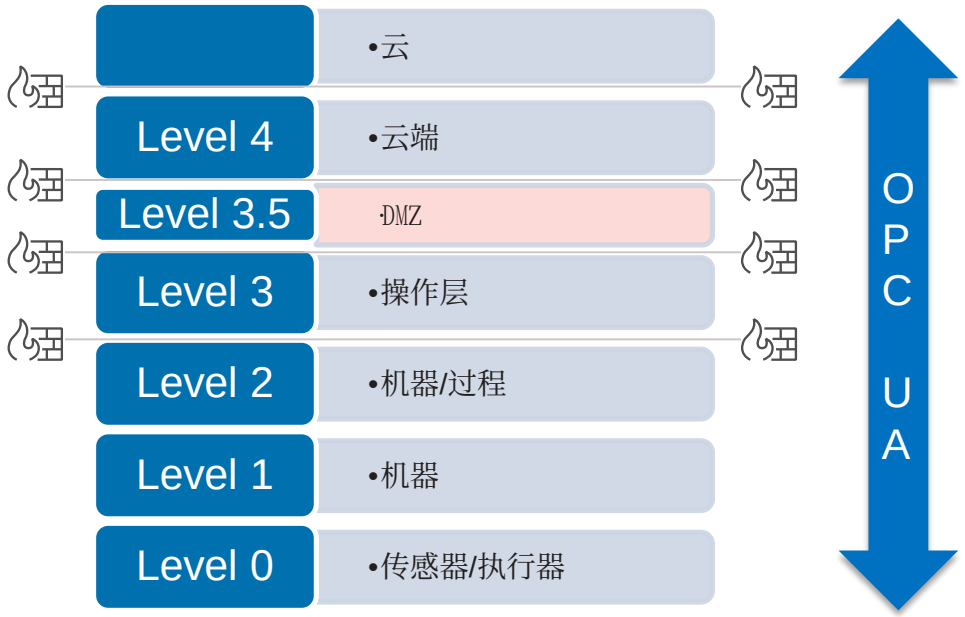
每个受支持的传输最适合用于不同的体系结构和环境（例如，LAN vs Cloud**），但使用相同的**OPC UA**信息模型。**

OPC UA – Secure Data Connectivity for Every Situation

Type	OPC UA Mechanism	End-to-End Security	Transport	Two Way	One Way	LAN	WAN (Cloud)	Firewalls & DMZ
Point-to-Point	Client-Server	✓	TCP	√		√	√	√
Peer-to-Peer	PubSub	✓	UDP		√	√		√
Cloud	PubSub	✓	MQTT		√		√	√

企业范围内的数据连接

在世界范围内，工业网络是建立在普渡参考模型的基础上的，普渡参考模型将不同的设备、设备和网络划分为通常通过防火墙和非军事化区域（DMZ）分隔的区域。



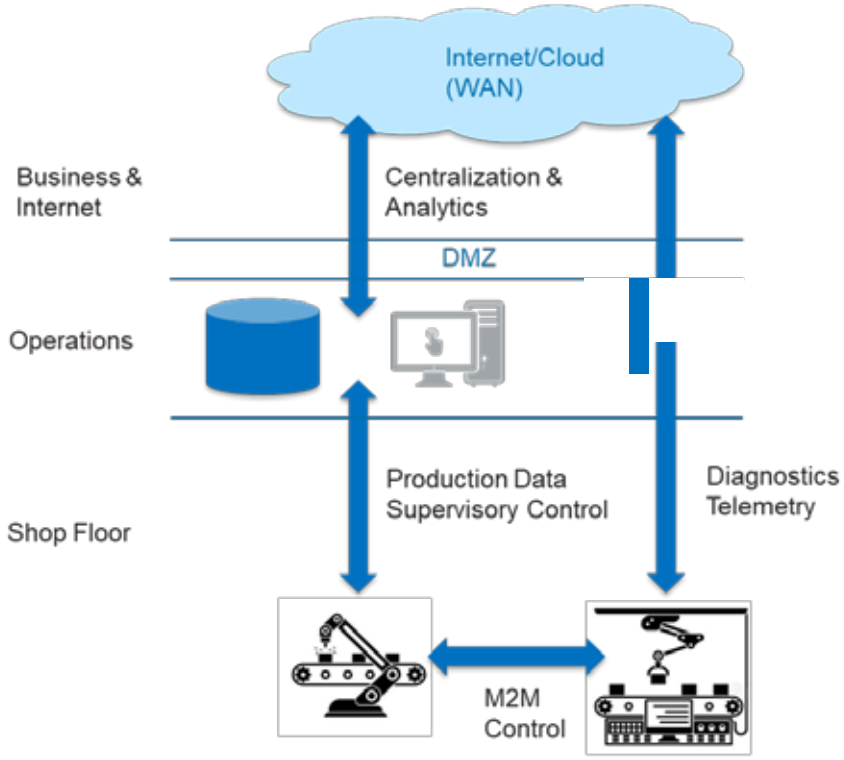
在IIoT时代，普渡网络模型继续占据主导地位，但在某些情况下，企业也在云设置中添加了传感器，从最低级别的数据直接发送到云，绕过了普渡网络的其他部分。

OPC UA**支持现有的普渡网络安全基础设施的数据通信，并可以通过新出现的直接到云的通信。**

OPC UA 支持安全的数据连接

OPC UA**支持在每个网络层内部和之间的安全通信。**OPC UA**还提供相对于特定连接点所需的内容进行优化安全性和效率的通信选项。**

例如：OPC UA**支持使用最合适的通信传输技术（**TCP、UDP、MQTT**等），这取决于数据的来源和去向。**



策略，证书和加密

OPC UA使用许多基于标准的安全机制，如证书、算法、密码、散列等。这些机制的组合被组织成OPC UA安全策略，这些策略被设计成随着时间的变化而变化。随着世界的变化，OPC UA支持的安全机制也在通过定义策略变化。

任何被视为不安全的机制都可以通过新策略否决任何相关的策略，并添加新的、更强健的机制。这允许互操作性，但也允许适应性和“未来验证”。供应商可以轻松地添加对新策略的支持，新策略被定义并弃用不再被认为安全的策略。

请参阅此处的当前安全策略列表：
https://apps.opcfoundation.org/profilereporting/

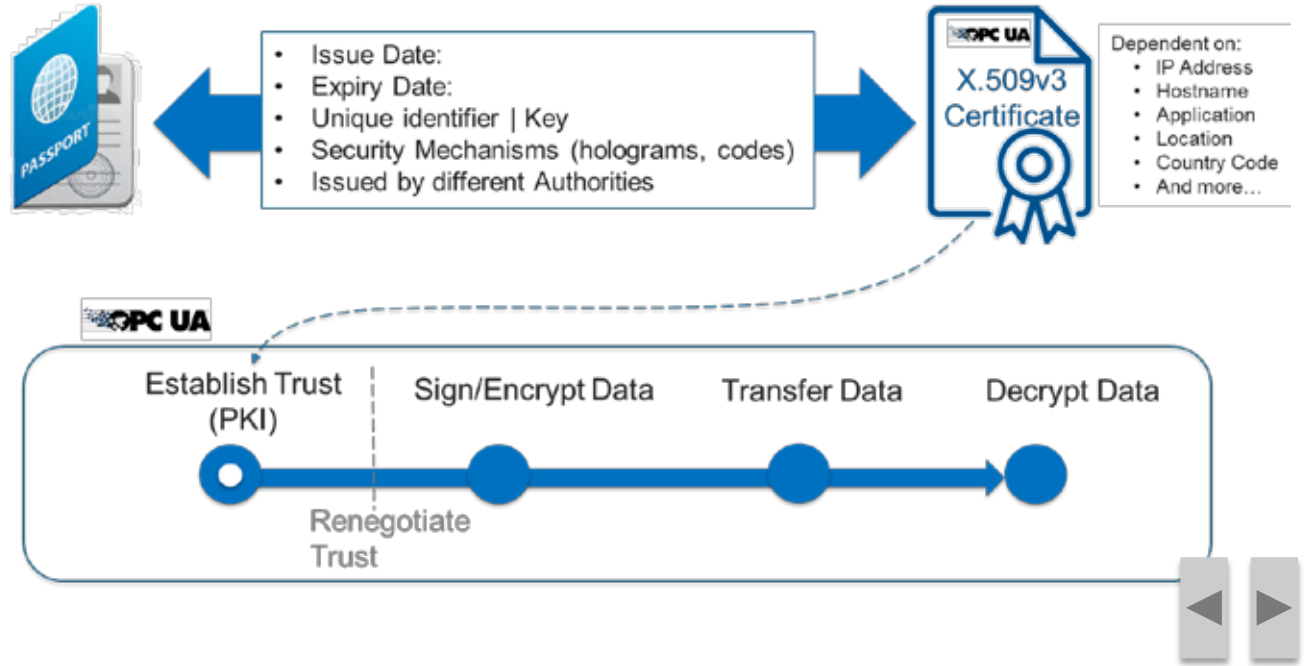
X.509 v3证书

在实体之间建立信任的过程中，IT系统通常使用X.509 v3证书，以便安全地交换数据。

通过在OT环境中采用IT安全机制，OPC UA缩小了IT与OT之间的差距。这允许对IT和OT基础设施进行共同管理，从而降低成本并提高整个组织的可靠性。

一个类比：X.509证书就像护照。由当局签发的护照，包含姓名、地址、出生日期、签发日期和有效期等关键信息。当您旅行时，您的护照用于与各个国家当局建立信任。证书的工作方式相同，只是它们用于在两个系统之间建立信任，以便可以交换数据。X.509证书还包含有关证书颁发地点的信息，如IP地址、主机名、应用程序、位置、国家代码等。

OPC UA使用X.509v3证书以及附加的OPC UA相关字段和公共密匙基础设施（PKI）来建立系统之间的信任。通过在定义的通信序列中交换证书，系统可以建立信任并开始交换加密信息。颁发和管理证书非常重要，必须与OT（保持系统运行）和IT（保持系统安全）保持一致。



点对点：跨防火墙的安全OPC UA数据交换

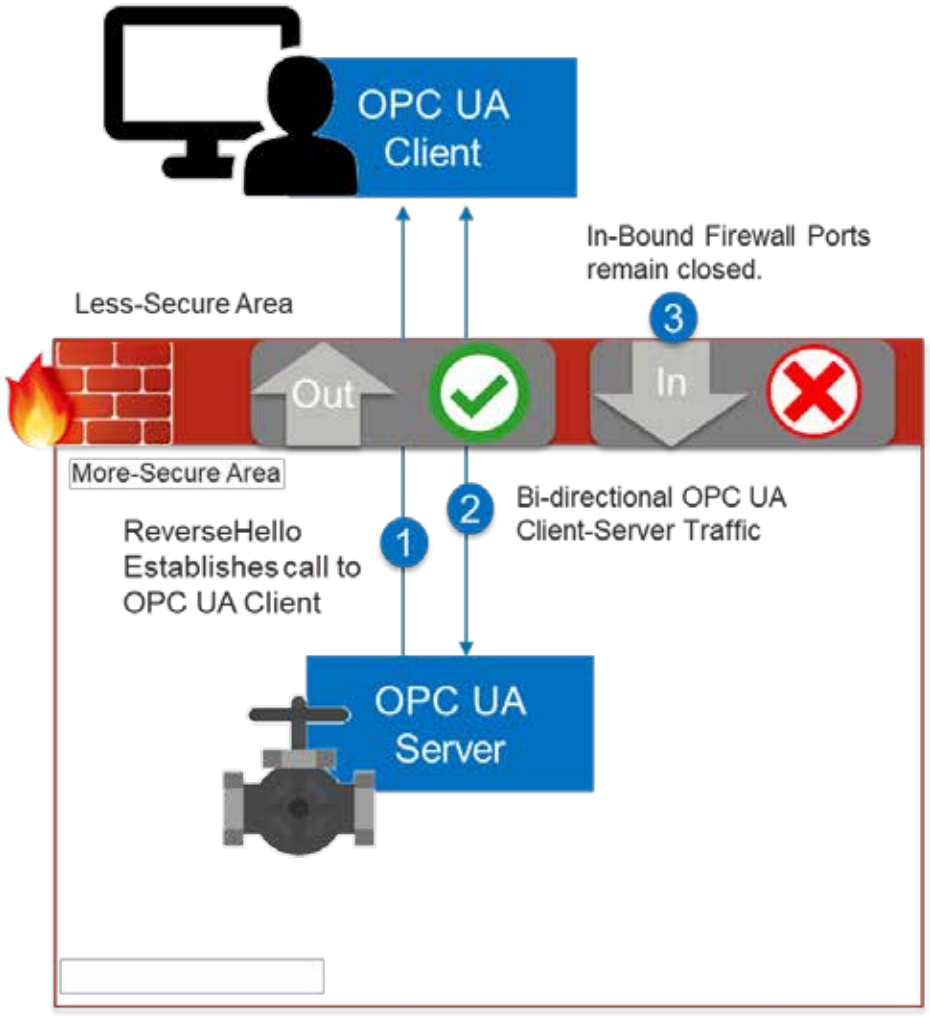
挑战：IT安全最佳实践要求关闭绑定的防火墙端口，因为这样可以最大限度地减少外部攻击的威胁。传统上，这对从业务端访问OT数据构成了障碍，通常需要打开“受信任”的绑定端口。OPC UA消除了这个问题。

解决方案：OPC UA反向连接

右边的图显示了一个OPC UA服务器，它位于一个受防火墙保护的更安全的区域，防火墙的内部端口是关闭的。这可以防止防火墙以外的系统（不太安全的区域）通过防火墙进行呼叫。

OPC UA1.04版本引入了一种“反向Hello”功能，允许OPC UA服务器通过一个外部防火墙端口启动与OPC UA客户端的通信。一旦OPC UA客户端确认收到反向Hello，两个组件之间的安全通信就可以自由进行。

这种跨防火墙通信的方法非常重要，因为NIST和NERC等安全组织正在指示其成员关闭所有绑定的防火墙端口。OPC UA 反向hello的安全特性允许当前业务所需的功能，并以高度安全的方式允许它。



云：端到端安全与逐跳安全性

OPC UA或MQTT？

人们经常问是使用MQTT还是OPC UA。实际上，MQTT和OPC UA是不可直接比较的。OPC UA是一个互操作平台，而MQTT是一个传输协议。除了为各种数据传输设计以外（包括MQTT），OPC UA还包括许多其他特性，例如基于标准的信息建模，这些特性是企业范围内信息交换和系统间互操作所必需的。

MQTT上的OPC UA提供真正的端到端安全性

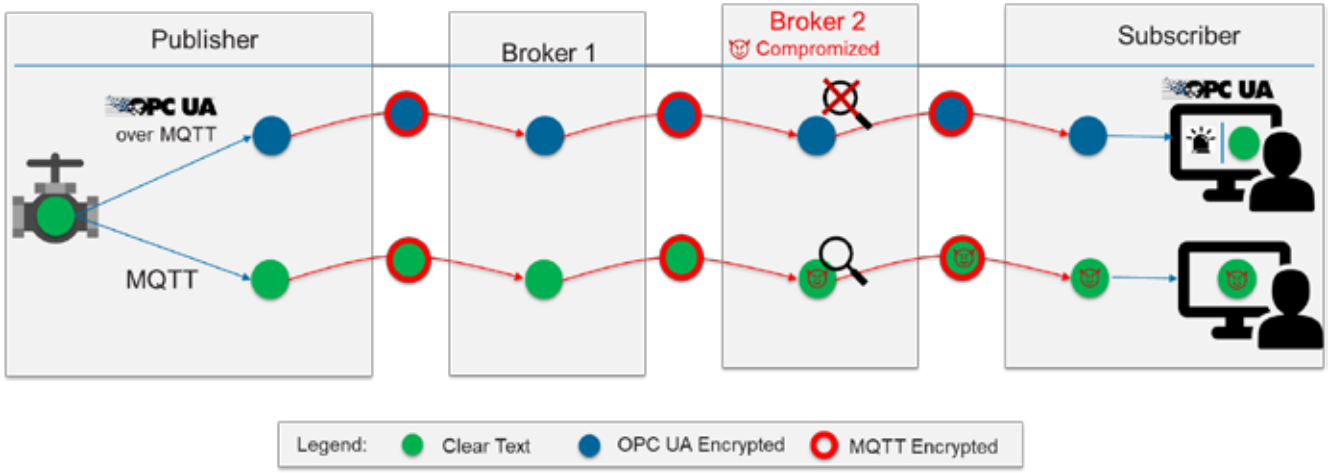
从安全的角度来看，“ MQTT上的OPC UA”和MQTT本身是不同的。下面显示的示例说明了从发布服务器发送的数据可以通过两条路径到达订阅服务器。一个是在MQTT上使用OPC UA，另一个单独使用MQTT。

MQTT上的OPC UA

当发布者通过MQTT广播OPC UA消息时，数据在通过MQTT发送之前由OPC UA加密（这也可以加密有效负载）。当MQTT消息到达代理时，MQTT有效负载将被解密，但OPC UA加密的数据将保持加密状态，因为只有订阅者才能在收到时对其进行解密。因此，受损的代理将无法访问数据。

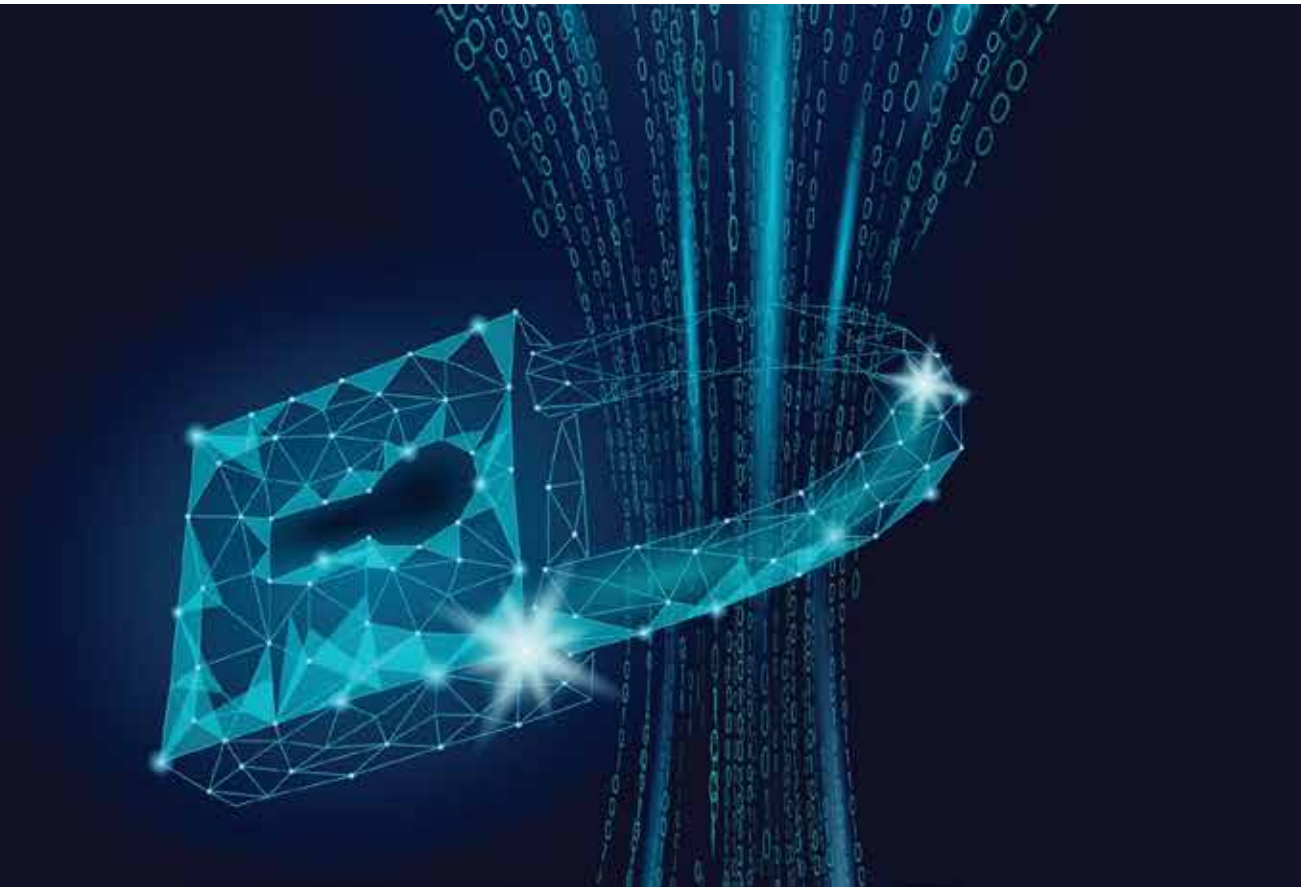
只有MQTT

当使用MQTT发送消息时，每个代理都会在加密并继续发送原始数据之前对公开原始数据的消息进行解密。如果链中的代理被破坏，这会带来潜在的安全威胁。



实施OPC UA的最佳实践

易箭牛恶命建反亲告氢忽争附



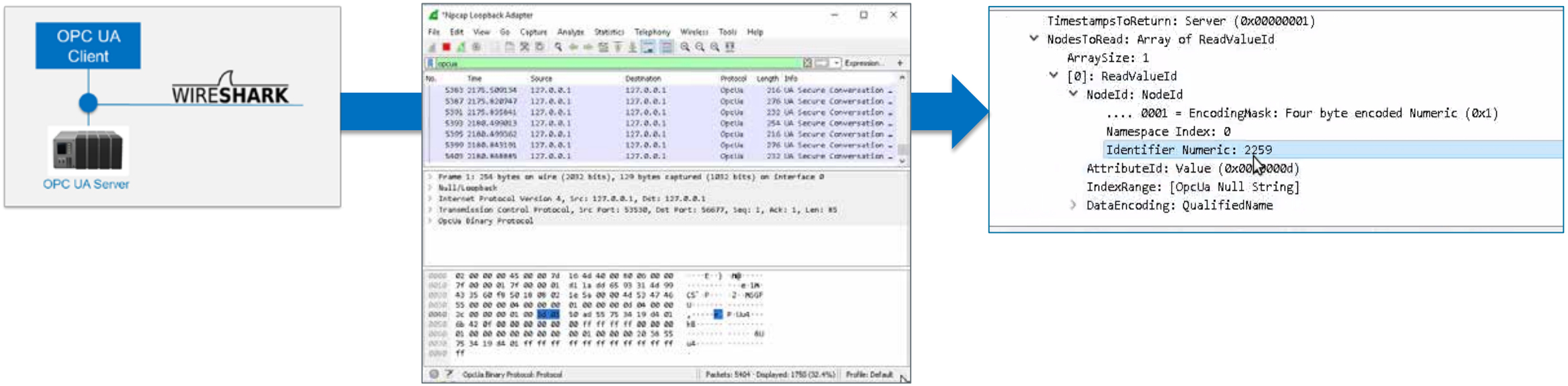
黑客工具和OPC UA安全

黑客工具随时使用

今天很多黑客工具都很容易获得，新的工具也会定期发布。当专业黑客变得越来越复杂时，这些黑客工具的可用性使得技术知识很少的人有可能对未受保护的真实工业设施构成真正的威胁。因此，利用OPC UA中定义的安全特性是非常重要的。

虽然OPC UA可以通过签名和加密为您的数据提供强大的安全性，但如果您选择不使用它，则可以使用各种免费可用的工具（例如Wireshark）轻松读取您的所有数据。

Wireshark使用简单，支持多种协议，包括OPC UA。在正确的人手中，这样的工具对于OPC UA开发人员监视和诊断网络通信很有价值。但在错误的人手中，它们可以被用来监视和潜在地危及不安全的通信。



开发人员和最终用户的安全检查表

开发者

为了进入安全的OPC UA解决方案市场，开发人员（技术供应商）必须花时间和精力在遵循OPC UA最佳实践的前提下进行开发和测试。下面是一个清单，可以将其用作开发安全应用程序的指南。

最小化清单

- 获得有关OPC UA开发和最佳实践的培训
- 选择专业的商业SDK–为什么？支持的商业SDK是经过高度测试、调整、支持和维护的。掌握最新的安全算法是必不可少的。
- 使用支持良好代码覆盖率的工具
- 执行静态代码分析（Clang、CppCheck、PCLint等）
- 执行互操作性测试

更高级的清单

- 执行模糊测试
  - 简单易用的16字节标头和有效负载协议（可通过先进工 具如AFL或商用工具实现）
  - 具有大量应用范围OPC UA的复杂性
  - 需要专业知识和努力确保彻底的测试，以避免对错误预估一定能通过测试
- 执行同行代码评估
- 咨询安全专家/顾问
- 获得OPC UA认证

最终用户

在调试OPC UA解决方案时，正确管理安全环境工件和资产非常重要。在开始实施之前，应调查以下问题：

- 数据流-哪些数据需要流向何处？
- 数据保护—需要保护哪些内容？目前什么是安全的？
- 硬件功能-组件是否有足够的CPU/RAM用于加密？
- 网络拓扑-是否需要跨防火墙的额外跃点？
- 用户权限管理-谁需要做什么？他们现在有什么权限？
- 证书管理-与IT部门协调证书管理

回答完这些问题并准备好选择供应商解决方案后：

- 确保供应商在购买之前和之后为其产品提供支持
- 检查OPC UA产品是否经过认证
- 培训员工如何使用OPC UA
- 阅读OPC基金会的“OPC UA的实用安全建议”(www.opcfoundation.org)

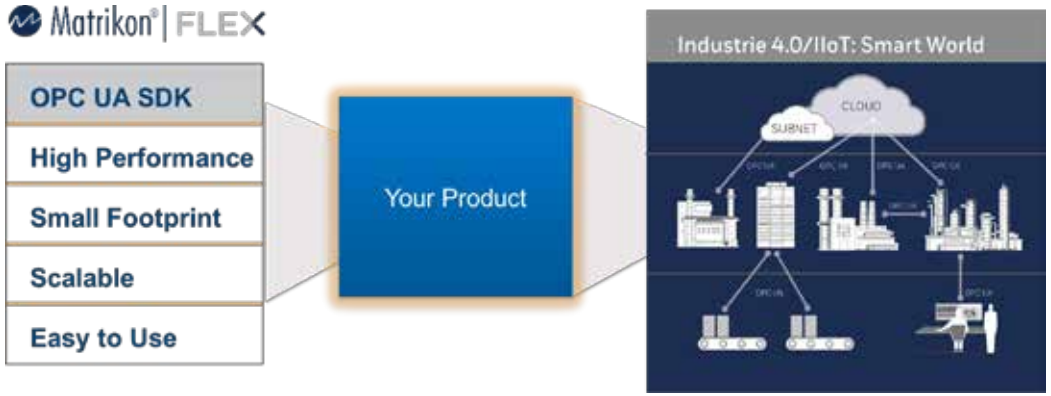
使用专业的OPC UA SDK

适用于所有项目的专业OPC UA工具包
考虑到整个软件开发生命周期，领先的供应商不仅寻找提供最佳OPC UA实现的工具包，而且还需要在OPC UA不断发展的过程中得到支持。

Matrikon Flex OPC UA SDK**就是专业OPC UA工具包的一个例子。这种高性能的软件开发工具包使离散和流程行业的开发人员能够轻松地使用OPC UA启用其应用程序和设备，而无需担心工具包是否保持最新、SDK实现本身的安全测试，也无需担心在需要时是否能获得支持。**

选择OPC UA SDK时附加的SDK关键属性包括：

- ü OPC UA**认证-安全测试和认证**
- ü **完全支持OPC-UA标准丰富的信息建模能力、HA、AC、DA等。**
- ü **硬件独立-从小型32位微处理器到全尺寸多核CPU**
- ü **操作系统（OS）全兼容：运行在Windows、Linux、RTOS和没有任何操作系统的系统上**
- ü **具有高度的可扩展性：从小型嵌入式应用程序到功能强大的工作站，拥有数百万OPC UA节点**
- ü **足够灵活，便于设备（机器对机器或M2M）之间的通信，以及车间、办公场所和企业云应用程序之间的通信。**



一句话：经验表明，预先选择合适的专业OPC UA SDK有助于供应商以更好的产品更快地进入市场，并有助于供应商及其最终客户避免麻烦。

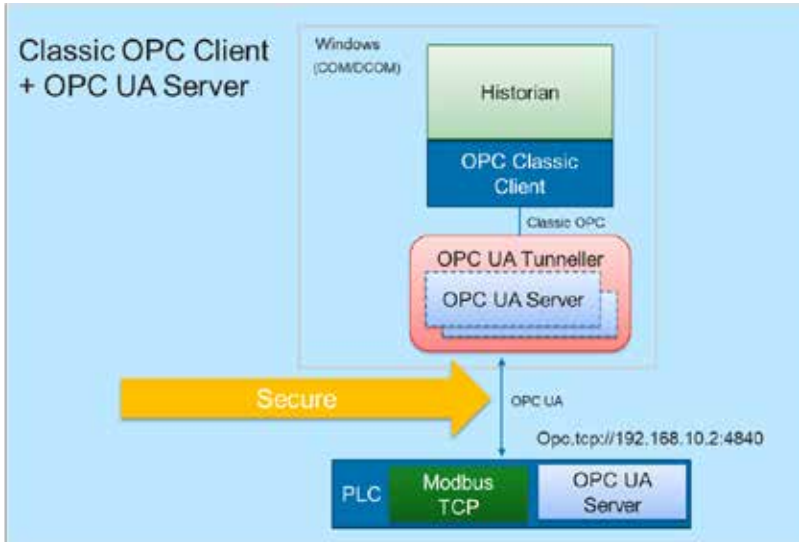
分阶段迁移到OPC UA

OPC Classic拥有庞大的安装基础，因此大多数企业将分阶段逐步向只有OPC UA基础设施迁移。

虽然OPC Classic不能直接与OPC UA应用程序一起工作，但是可以将OPC Classic通信升级为OPC UA，以便底层OPC数据源可以与新的本地OPC UA应用程序混合。

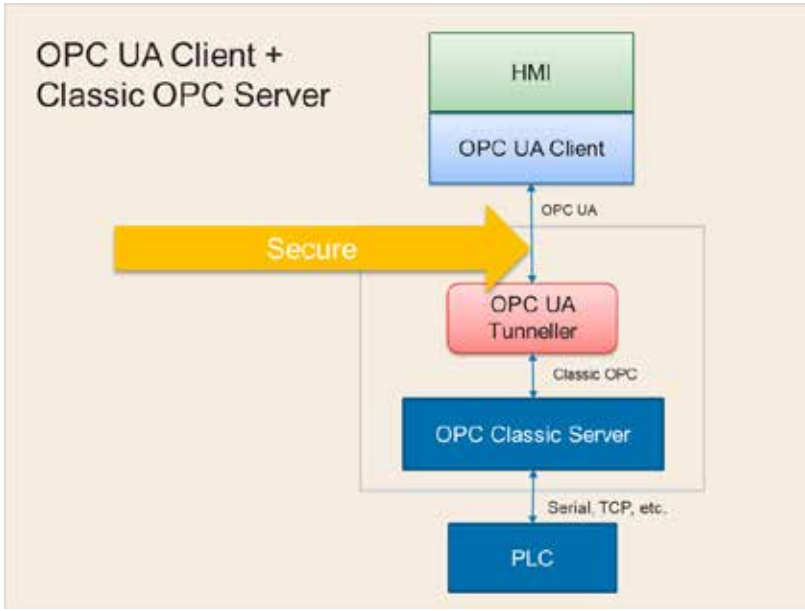
这由于新技术，使OPC Classic和OPC UA共存于一个共同的体系结构成为可能。这对于了解最终用户希望如何开始采用OPC UA系统，但不能简单地摆脱其遗留系统至关重要。

其中一个工具是Matrikon®OPC UA Tunneller，用于促进各种OPC Classic到OPC UA的结合。



Classic OPC客户端和OPC UA服务器部署

上图说明了Matrikon OPC UA Tunneller在OPC Classic客户端和OPC UA服务器之间的使用。



OPC-UA客户端和Classic OPC服务器

下图说明了Matrikon OPC UA Tunneller在OPC UA客户端和OPC Classic服务器之间的使用。

供应商采用策略-更快、更低的风险和成本

IIoT采用的5个步骤

IIoT通过OPC UA可以帮助您提高效率并获得竞争优势。实际的IIoT五步过程是结构化和有组织的，这将帮助最终用户快速高效地实现价值。该过程将会有：

- ü 更快的上市时间 - 分阶段方法可以快速实现价值
- ü 降低风险和开发成本 - 专家指导和培训是降低开发风险和成本的关键
- ü 竞争性IIoT产品 - OPC UA认证产品为您和您的客户提供竞争优势

五步流程旨在帮助供应商高效、经济地完成OPC UA实施流程。步骤如下：

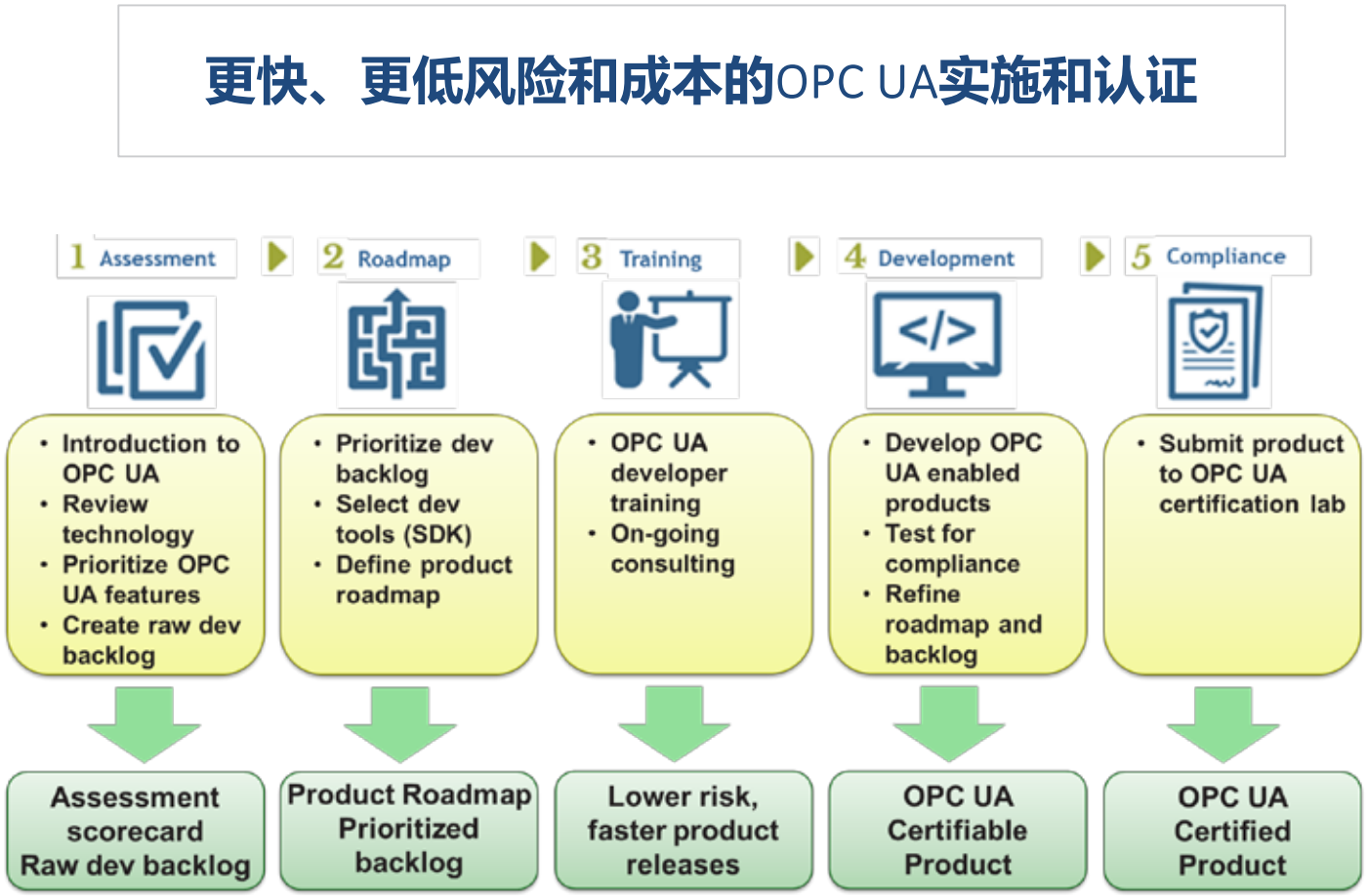
1.OPC UA评估研讨会：评估您的IIoT业务和产品目标。创建评估记分卡，根据OPC UA标准映射您当前的产品功能和目标。

2.OPC UA路线图研讨会：定义OPC UA采用路线图，以便尽可能快速且经济高效地为您的产品提供OPC UA。

3.OPC UA培训：使用Matrikon®FLEX™OPC UA SDK培训您的开发资源，了解如何实施OPC UA规范。

4.开发服务：利用经验丰富的OPC UA开发人员，与您的员工和开发环境合作，快速实施OPC UA标准。

5.合规辅助：确保您的实施符合OPC UA标准。



最终用户采用策略-结构化实用方法

IIoT采用的5个步骤

IIoT通过OPC UA可以帮助您提高效率并获得竞争优势。实际的IIoT五步过程是结构化和有组织的，这将帮助最终用户快速高效地实现价值。该过程将会有：

- ü 帮助您制定一个路线图，将您的组织和供应商推向IIoT
- ü 培训您的IT和自动化人员以及供应商如何实施和支持OPC UA规范
- ü 竟帮助您和您的供应商在您的工厂及其产品中部署和测试OPC UA规范

五步流程旨在帮助最终用户有效，经济地通过IIoT采用生命周期。 强烈建议您的供应商参与此过程。 步骤如下：

1.IIoT战略研讨会：确定您的IIoT目标，战略和优先事项。首先评估您的已安装技术，确定战略供应商及其路线图计划。可交付成果是一个计划，其中包含将工厂和供应商转移到IIoT的优先要求。

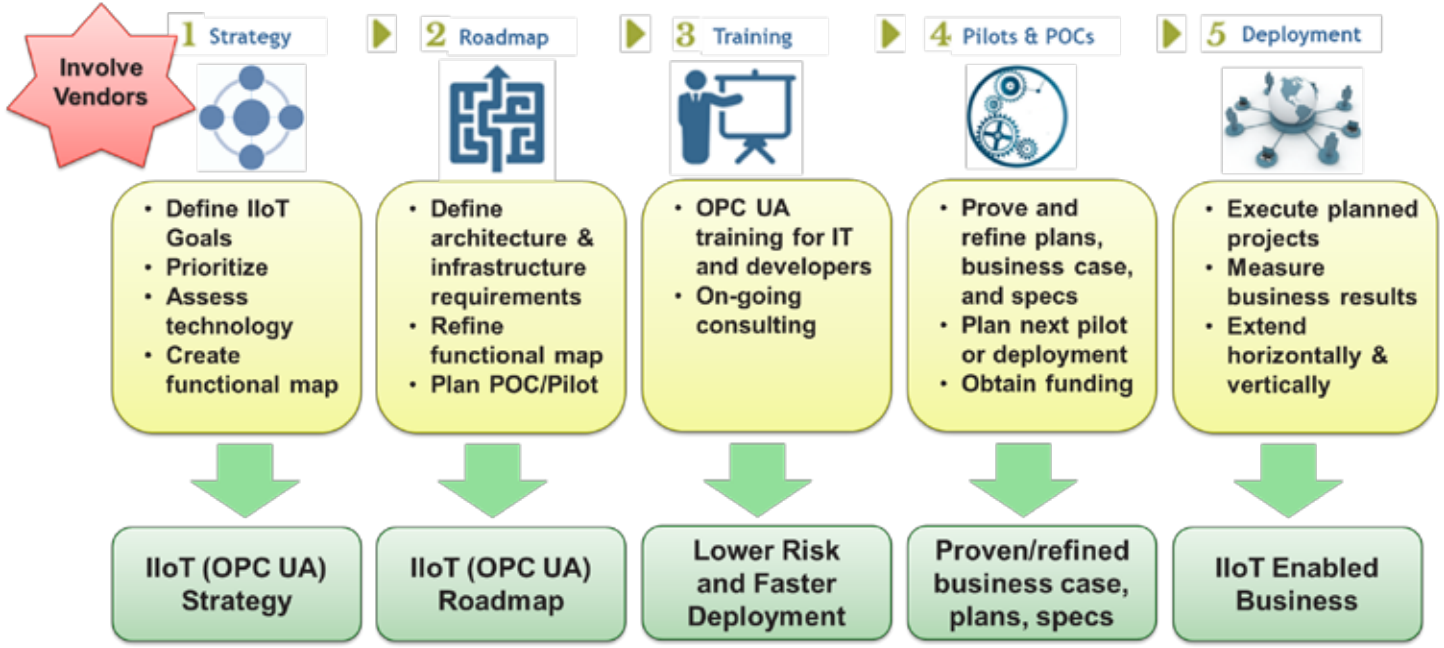
2.IIoT路线图研讨会：定义采用路线图，将您带到一个支持IIoT的工厂，在该工厂中，传统和新的IIoT时代自动化组件共存。

3.OPC OPC UA培训：培训您的IT，工程和供应商资源，了解如何部署和实施OPC UA规范，以解决共存，基础设施，信息模型和安全问题。

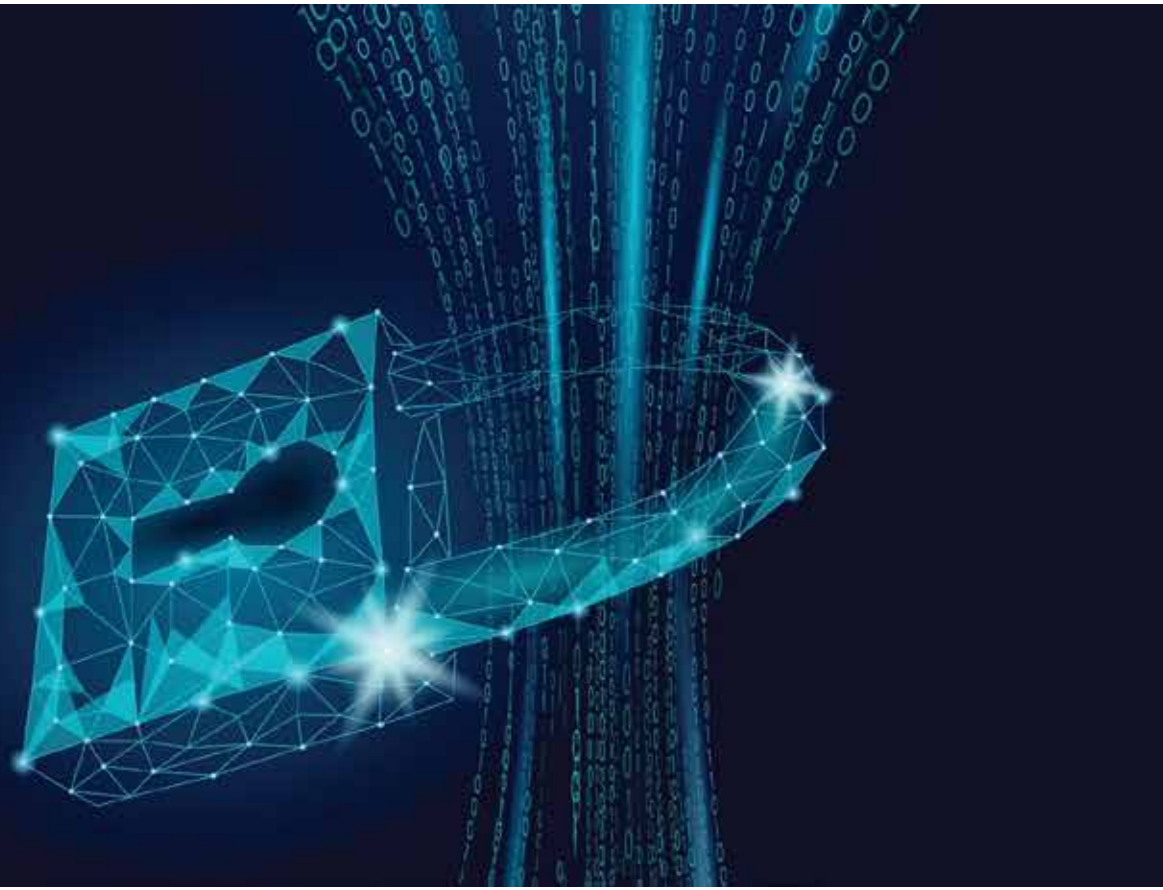
4.Pilots＆POCs：执行试点或概念验证项目，以证明业务案例和关键假设，并完善计划和规范。

5.部署：根据您的OPC UA采用路线图，部署支持OPC UA的应用程序。

系统化IIoT进程以实现更高的投资回报率



资源，作者和赞助商



资源 & 帮助

对于最终用户

工具:

Matrikon® OPC UA Tunneller
- 简单安全实现 OPC UA ß à Classic OPC连接
- 访问: http://www.matrikonopc.com

免费 OPC UA 建模工具 (UMX)
- 访问: www.beeond.net
- GitHub提供开源代码
- 下载 Windows / Linux 可执行文件

咨询: OPC UA 采用的5个步骤

一种结构化和有组织的方法，可降低成本和风险。
(www.beeond.net)

培训: Matrikon OPC UA Workshop

为最终用户和系统集成商完成OPC UA**和**OPC Classic**培训。**
(https://matrikonopc.com/training)

对于供应商和开发者

共苦:

OPC UA SDK Matrikon® FLEX
- 访问: www.MatrikonFLEX.com
- 参数表& demo 版本(Unix / Win)

免费 OPC UA 建模工具 (UMX)
- 访问: www.beeond.net
- GitHub提供开源代码
- **下载** Windows / Linux **可执行文件**

咨询: OPC UA 采用的5个步骤

一种结构化和有组织的方法，可降低成本和风险。
(www.beeond.net)

培训: OPC UA 虚拟教室

深度开发人员培训
查看课程大纲，安排和注册
https://beeond.net/opc-ua-developer-training/

Practical Security Recommendations for building OPC UA Applications

www.opcfoundation.org

About the Authors

Darek Kominek, Matrikon市场总监

在过去的15年中，Darek在Matrikon（霍尼韦尔）担任过各种职位，包括OPC培训，产品管理和战略营销。作为OPC基金会营销控制委员会（MCB）的成员和OPC UA宣传者，Darek与OPC基金会合作伙伴在全球范围内合作，并代表OPC基金会进行演讲。Darek经常撰写有关各种OPC UA主题的论文和文章。加入Matrikon之前，Darek曾在惠普（HP）、通用电气（GE）担任软件工程师，并承担自己的软件咨询业务。Darek是具有阿尔伯塔大学计算机工程学士学位的专业工程师。

Darek.Kominek@MatrikonOPC.com

Rod Stein，Matrikon首席架构师和安全架构师，

在过去的19年里，Rod在许多领导机构担任过职务，包括在Matrikon（霍尼韦尔）的15年。作为技术领导者，他一直参与工业通信和过程控制。目前，Rod管理Matrikon业务团队技术，并在OPC基金会担任过多个职务，包括担任技术咨询委员会成员、OPC UA工作组成员、OPC UA安全工作组成员、OPC UA规范第11部分和第13部分的编辑。Rod拥有计算机科学和数学学士学位以及项目管理文凭。

Rod.Stein@MatrikonOPC.com

Costantino (Cos) Pipero, Beeond公司创始人兼首席技术师

Costantino拥有制造业、工艺和能源行业定义和提供技术解决方案20年的经验。Costantino正在积极合作制定关键行业标准，如ISA95、OPC UA和OpenSCS，并就行业相关主题撰写了文章和书籍。Costanino在从服务器系统到嵌入式设备的OPC和OPC UA开发解决方案方面有着丰富的经验，自1997年以来一直在培训工程师。

Costantino.Pipero@Beeond.net

About the eBook Sponsors

关于 Matrikon® | 增强互操作性

Matrikon是基于控制自动化数据互操作的OPC UA和OPC Classic产品的供应商。Matrikon通过向供应商和最终用户提供可靠和创新的数据互操作性产品、培训和实时支持，使他们能够在工业物联网（IIoT）和工业4.0（I4.0）中实现最佳竞争。

Matrikon为供应商提供了一个专业的OPC UA开发工具包，非常适合在从小型嵌入式设备到大型云应用程序的所有产品线中使用。对于其最终用户客户，Matrikon提供了最有利于企业范围数据共享所需的关键数据工具。Matrikon不仅是一家软件公司，还积极参与标准组织，并与全球客户和合作伙伴建立密切关系，帮助他们在一个日益复杂、竞争激烈和相互关联的世界中，最好地应对业务和技术挑战。

更多信息请访问：*www.matrikonopc.com*

关于Beeond

Beeond公司通过提供IIoT和OPC UA咨询和软件开发服务，在整个生命周期中为技术供应商提供指导和支持，帮助他们更快地实现IIoT兼容。

Beeond遵循一个结构化和有组织的五步IIoT采用流程，因此我们的客户能够快速、经济地实现价值。与传统的软件开发公司不同，Beeond只关注OPC UA及其在嵌入式软件、设备和自动化系统中的实现。他们的经验和专业知识缩短了上市时间，降低了我们客户的项目风险。

我们的价值和利益

- **更快的上市时间** - 分阶段方法可以快速实现价值
- **降低风险和开发成本** - 专家指导和培训是降低风险和成本的关键
- **具有竞争力的IIoT产品** - OPC UA认证产品为您和您的客户提供竞争优势

更多信息请访问：*www.beeond.net*

HongKe 虹科

hkaco.com

公众号

需要详细信息？请通过sales@hkaco.com**联系我们 | 电话**: 400-999-3848

办事处：广州 | 北京 | 上海 | 深圳 | 西安 | 武汉 | 成都 | 沈阳 | 香港 | 台湾 | 美国

Matrikon®