现场层通信中的OPC UA – 实践理论

版本1 // 2020年11月

技术手册

概要

产品和系统的数字化为新的软件以及增强软件的解决方案提供了机会，并促成了新的数字服务和商业模式。由于现场层通信协议的异构性，概念实现变得更加困难。尽管当今大多数现场总线系统和实时以太网协议都是由IEC在61784/61158系列实现其标准化，但是支持不同协议的自动化设备之间无法互操作，甚至不能共存于一个公共网络基础设施中。此外，设备信息一直是采用不同的信息模型进行结构化，这使得数据分析成为一项劳累且十分耗时的任务，而且容易出错，特别是在多供应商和多协议环境下。

但是，随着工业4.0和工业物联网（IIoT）时代的到来，无缝互操作趋势逐步加快，要求工业系统的集成独立于供应商，并且支持从传感器到云的端到端的互操作性，包括所有工业自动化的现场级设备用例，例如实时、运动和功能安全。

从传感器到云的标准化通信将支持跨行业的数字转换，包括工厂自动化和过程自动化。最终用户、机器/撬块制造商和系统集成商将受益于简易的系统集成和跨供应商互操作性。对生产数据和工艺条件的无缝访问也将促进生产工艺的可用性和优化。

从技术层角度讲，这种方法需要在多个层面上进行标准化：语义、信息建模、通信协议、数据链路层和物理层，所有这些都被一个通用的网络安全框架所涵盖。信息技术（IT）和工业运营技术（OT）的融合非常重要，它使得IT和OT共享通用的网络基础结构，同时还保证了各种IT和OT应用程序所要求的不同水平的服务质量（QoS）。其中尤为重要的技术是以太网高级物理层（APL）和以太网时间敏感网络（TSN）。APL的无缝以太网连接扩展至现场层，特点包括更长的电缆长度，以及通过两线电源和带有安全性的通讯功能实现了防爆保护。TSN支持在标准以太网上进行确定性通信，这使得IT和OT协议可以共存于通用网络基础结构。

OPC基金会的现场层通讯倡议于2018年11月成立，旨在扩展OPC UA的框架，对不同制造商的控制器和现场设备的语义和行为进行标准化。其涵盖的主要用例包括控制器到控制器，控制器到设备以及设备到设备，支持控制器和设备（控制器到计算和设备到计算）IIoT连接。OPC基金会的多供应商工作组正在进行这些技术工作，工作组定义技术的概念，并说明实现的不同机制。

目录

引言

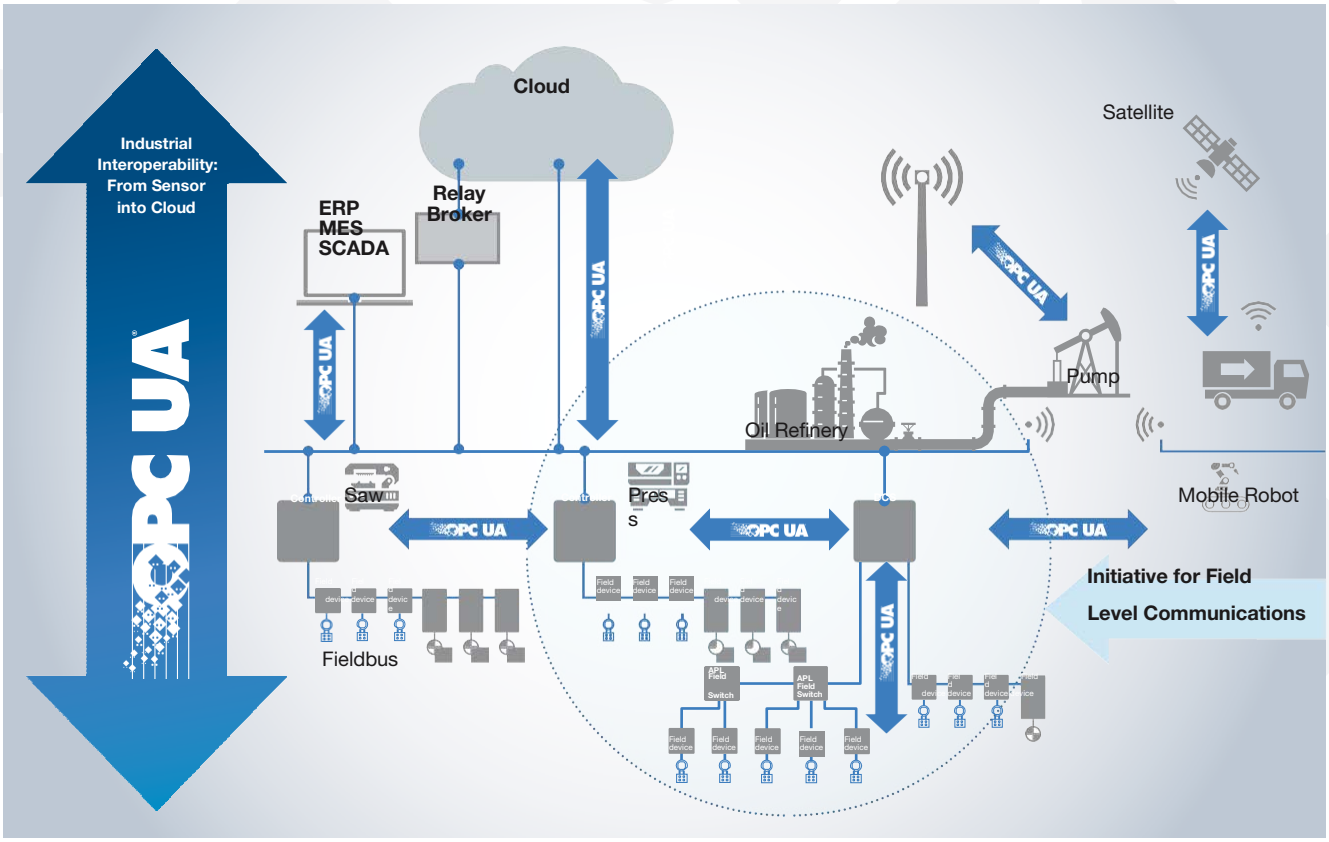
背景

数字化的目标是促进IT技术与OT在整个价值链之间从设计、生产到维护的集成，包括产品、系统、解决方案和服务。一旦实施了数字化，将为产品和系统提供新的及增强的软件解决方案，最终促成新的数字服务和商业模式。

早前的产品，传统产品和解决方案通常无法通过当今几乎无处不在的基于IP的网络进行连接，如今的物联网（IoT）为这些OT产品、系统和解决方案整合了各种技术。

虽然以太网提供了事物“相互联系”的能力，但它们仍然需要一种通用的通信方式，标准化的数据连接性和互操作性满足了这一需求。

简单来说，以标准化数据连接为核心的工业物联网（IIoT）可以从两个角度来看：水平通信和垂直通信。水平通信的示例如：车间系统之间的控制器到控制器（C2C）的数据连接。垂直通信的一个示例是设备到云的数据传输。



图表 1: OPC UA用例和现场层通信倡议

在这两种情况之下，OPC基金会的OPC统一架构（OPC UA）标准提供了一个安全、可靠和强大的基础，促进基于标准的数据连接和互操作性。多年来，为实现这一目标，许多公司和合作组织在OPC基金会的组织下展开合作，并在未来继续扩大合作。为改善水平和垂直的数据连接，一个关键方面是网络融合，即支持用于IT和OT通信的通用网络。基于IEEE 802.1的以太网时间敏感网络（TSN）支持受限延迟和不稳定的通信。此外，各种数据流和流量类型也可以借由通用的网络基础设施进行传输，同时保证了不同应用程序对带宽、等待时间、抖动和可靠性的各种要求。因此，TSN在支持IT和OT的融合中起着关键作用。以太网高级物理层（APL）是推动网络融合的另一项关键技术，因为APL为过程自动化（包括危险区域）中的传感器和执行器提供无缝的以太网连接。

现场层通信倡议

2018年，在德国纽伦堡举行的SPS IPC Drives 展上，OPC基金会正式启动现场层通信倡议。FLC倡议基于标准的IIoT通信解决方案，旨在将OPC UA扩展到现场级别，实现传感器、执行器、控制器和云之间的开放和统一，从而满足工厂自动化和过程自动化中的所有要求（见图1）。因此，通过OPC UA扩展到现场级别，OPC基金会将逐步实现成为全球工业互操作性标准的愿景。针对所有相关的工业自动化用例，包括实时、功能安全和运动，都提供了现场级设备之间独立于供应商的端到端互操作性，所有这些都需要安全的信息交换。

IT和OT正在融合现场层通信倡议，旨在实现以下四种融合:

1. OPC UA应用程序融合，多个供应商的多个OPC UA自动化设备共享一个网络。
2. OT融合，使用不同OT协议的多个供应商系统和设备共享一个网络。
3. IT/OT融合，即在一个网络中，多个供应商的控制器、设备、应用程序和操作系统均使用整合的IT和OT协议。
4. IT/OT组织的融合，IT和OT的组织之间界限模糊，管理遵循共同的战略和流程。

目标读者

本技术手册适用于工程经理、自动化工程师、技术产品经理和技术销售代表，他们希望对OPC基金会的现场层通信技术方法和基本概念有一个整体的了解。

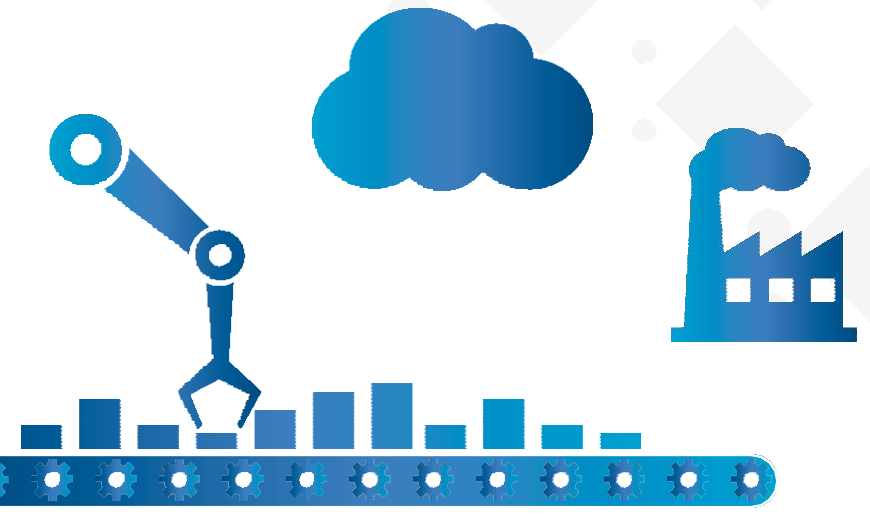
阅读导引

为了指导读者阅读本手册，下面给出了本手册各个部分的结构和内容概述：

1. **技术系统说明**（第8 – 13页）
   概述扩展的OPC UA框架——支持工厂自动化和过程自动化中各用例的技术方法。给出了有关系统架构、软件交互和通信模式的详细信息，重点介绍在第一版规范中解决的控制器到控制器（C2C）用例和目标网络架构。

2. 第二部分**“自动化组件模型”**（第14 – 17页）
   概述如何使用资产模型和具有功能实体的功能模型对自动化组件建模的方法。提供有关连接、连接配置数据和连接管理器的详细信息，同时也包含了在多个自动化组件之间交换数据的关键概念。

3. 在**“离线工作流程和模型”**部分（第18 – 24页）中，介绍控制系统工程师的工作流程，以便在现场调试之前启用C2C用例。解释两个描述符的概念：产品描述符-自动化组件产品相关的数据，配置描述符-包含产品相关部件和一个或多个配置组件。还包含了两个使用配置描述符的示例，演示在具有一个线路控制器和三个包含TSN和不包含TSN的从属控制器的场景中的工作流程。



4. **安全与保护** （第25 – 28页）
   解释了在职能实体原则与标准相结合的情况下如何安全的交换应用数据。安全提供商和安全消费端都使用安全来交换安全数据，这是一种安全的传输协议，便于在各个关键应用中使用。然后解释在建立连接和数据交换时如何保护连接以防止恶意攻击。

5. 在**传输**一节（第29 – 31页）中，描述支持通信行规及其与传输层和网络访问层相关的结构。此外，解释了当多个设备支持不同通信行规时是如何影响互操作性。最后，描述以太网高级物理层（APL）和以太网时间敏感网络（TSN）的重要性，以及它们在OPC UA扩展到现场层时所起的重要作用。

6. 最后部分**总结与展望**（第31页）
   概述了现场层通信倡议的主要成就和今后的工作目标，支持工厂自动化和过程自动化的所有相关用例和应用场景。此外，解释将采取哪些措施，能更容易的实现此项技术以及跨供应商的互操作性。

技术系统说明

系统架构

OPC UA是一套安全、可靠、独立于制造商和平台并用于工业通信的数据交换标准。OPC UA以制造商、用户、研究机构和集团之间密切合作制定的规范为基础，实现了系统中安全可靠的信息交互。尽管如此，现在仍缺乏一种机制来满足特定OT的相关要求，如功能安全、确定性和冗余，用于制造工厂和过程自动化工厂的设备和控制器之间的信息交换（见图2）。

现场层通信倡议的技术工作包含以下主题：

- → 定义控制器和设备所通用的自动化组件的基本模型
- → 为通用功能定义系统行为和序列。如引导、建立连接等。
- → 对应用层行规的统一和标准化，如运动控制、功能安全、系统冗余
- → 信息模型的标准化，在线或离线场景下的现场级设备模型，例如设备描述、诊断等。

- → OPC UA配套规范的集成
- → 支持以太网TSN的确定性通信和 IT/OT的融合
- → 包括TSN在内的以太网网络中与实时操作相关的应用程序行规的映射
- → 定义层面、行规和一致性单元，确保测试后能够实现跨供应商的互操作性
- → 定义认证程序

在第一版规范（ 版本1.0 ）中，重点是控制器到控制器C2C用例，包括使用OPC UA 客户端/服务器和 OPC UA PubSub，结合点到点的程序和基本的诊断来进行标准和安全的实时数据交互。目标网络架构如图 3 所示。

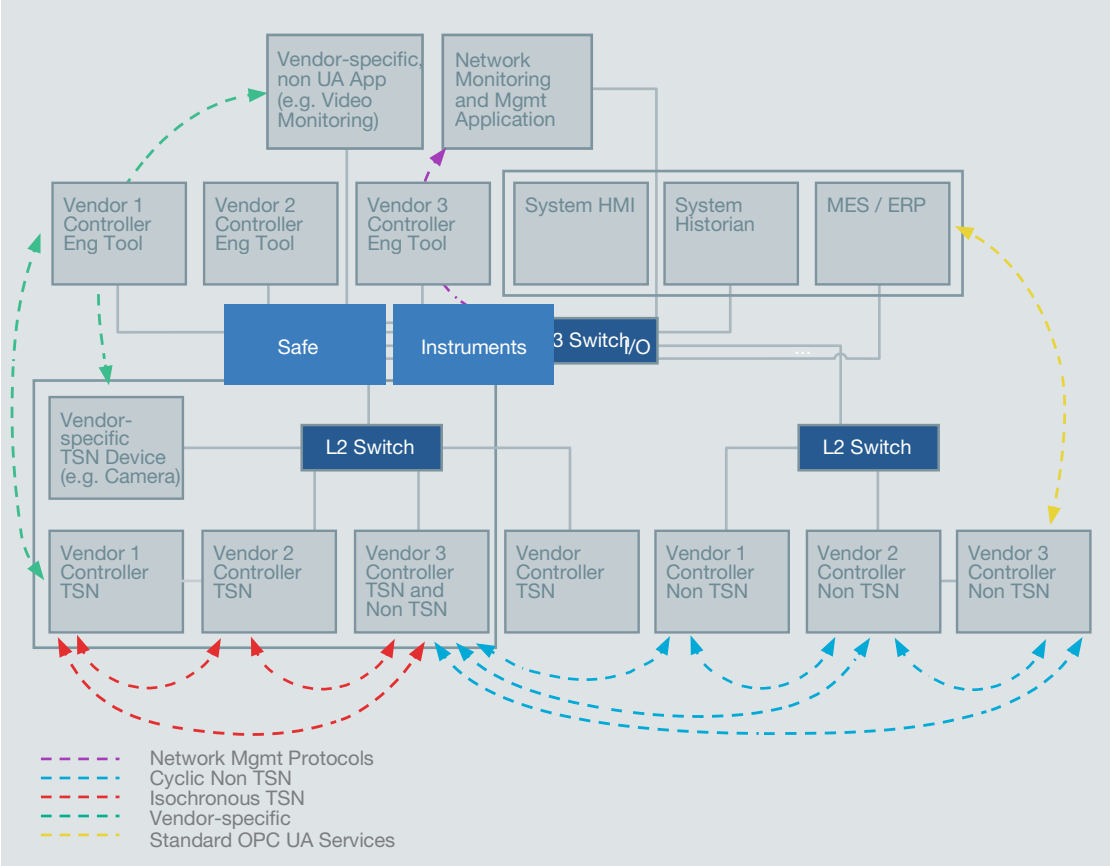


Figure 3: Controller-to-Controller supported network architecture

交互模型

在图4所示的交互模型中，控制器表示通常的可编程自动化控制器(PAC) 、可编程逻辑控制器（PLC）或分布式控制器到控制器（DCS）。如今，自动化设备通常连接到控制器上，可以像感应开关一样简单，也可以像Coriolis流量计或伺服驱动器一样复杂。计算是指运行在各种硬件平台上的独立软件应用程序，从边缘网关到云中的刀片服务器。控制器和设备有许多共同的属性“自动化组件”中的功能适用于两者。

→ 控制器到计算

在计算平台上运行软件是当今创新的一个主要领域。无论是在仪表板中管理信息、长期过程优化、预测设备诊断还是数字孪生，它们都需要从控制器中提取信息。OPC UA如今占主导地位，几乎每个主要控制器厂商都在其控制器或设备上直接安装OPC UA。

。

→ 控制器到控制器

工厂主和系统集成商正在使用从不同的机器/撬块制造商处购买的设备来组装复杂的操作系统。他们可能会发现，每一个都安装了来自不同供应商的控制器。因此需要一个简单的方法来在多个供应商之间建立控制器到控制器的通信。到目前为止，这一问题还没有在工业自动化中得以解决，由现场层通信倡议创建的控制器到控制器解决方案将是第一个为所有类型的自动化应用提供标准和安全通信的互操作性实时解决方案。

→ 控制器到设备

传统的现场总线方法是让控制器与模块、驱动器伺服器、仪器和其他智能自动化组件的子网通信，这在工业自动化社区中得到了很好的理解。尽管在部署解决方案时，它对网络体系结构和拓扑结构有约束，但工业自动化技术共享网络，现场层通信倡议将提供满足甚至超过IEC 61784规范所提供的控制器到设备的通信能力。

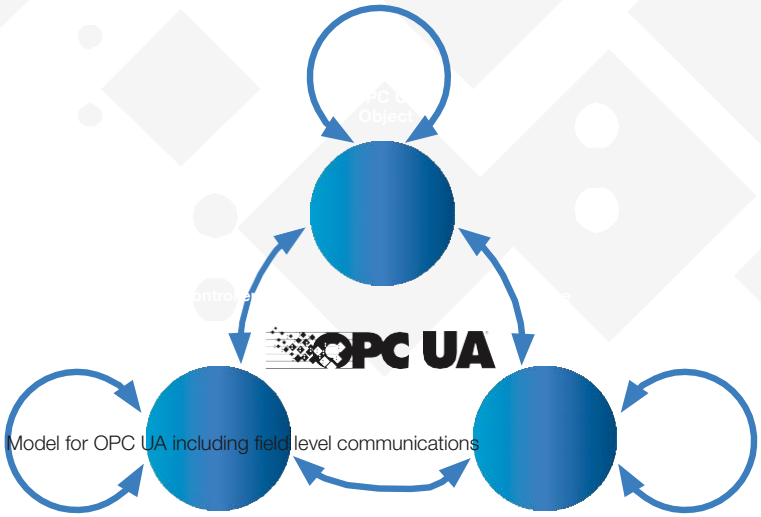


Figure 4: Interaction Model for OPC UA including field level communications

→ 设备到设备

通过整合多个车间技术的最佳实践，以及协调终端设备里的应用行规，跨伺服驱动器共享刚性负载等应用程序将实现更加容易的互操作性部署方式。

→ 设备到计算

控制器通常充当设备的代理，为这些设备提供含有丰富信息的数据，在某些情况下可以控制对这些信息的访问。然而，随着设备变得越来越复杂，有用变量以及内部和外部测量变得越来越多，将控制器作为代理变得越来越不符合实际。例如，通过控制器已无法扩展每个设备路由中的千个变量。现场层通信OPC UA将定义必要的语义和元数据，将来自设备的信息语境化，在开放的体系结构中应用不同软件应用程序，控制器将不再是个瓶颈。

→ 计算到计算

这些应用程序包括系统到网关、云到云的连接、可互操作的制造业操作管理等等。现场层通信倡议将在服务、信息建模和互操作性的基础上，使用并建立的这些服务、信息建模和互操作性，在过去十年里推动了OPC UA在计算应用程序里的成功。虽然预计现场层通信倡议不需要进一步发展计算对计算应用程序的能力，但这些应用程序将继承并受益于现场层级所带来的协调作用。

通信模式

控制器到控制器通信的一个例子，供应商的混合模块集成到另一个供应商的系统中，各供应商都选择来自不同厂商的控制器，并使用自己的ECO设备系统（见图5）。机器和分布式自动化系统也有类似的例子。

Figure 5: Controller-to-controller example

现场层通信OPC UA支持两种新的方法，即不妨碍现有的客户端/服务器机制，利用OPC UA PubSub在机器之间交换数据：

→ 单向通信

单向一词来自应用程序数据流。每台机器的设计人员创建一个信息输出的配置描述符，这些信息可用于配置各项功能（如更新速率、安全性等）供其他控制器配置时使用。然后，其它机器的设计人员可以导入这些描述符，输入自己的机器，用来启用通信并自定义代码实现这些数据的正确应用。

→ 双向通信

双向通信模型扩展了单向通信，并继承了单向通信的所有属性。

在这一模型中，设计人1修复了控制器发送（(输出)和接收(输入)的数据和格式）。其他控制器（及其设计器）有责任向设计人1的控制器发起通信，并以设计人1所要求的格式提供/处理信息。在单向通信中，机器双方是对称的，机器1和机器2的设计者执行完全相同的功能，以便在两个控制器之间建立双向通信。在双向通信模型中，一方定义设备的输入和输出，另一方建立双向连接-两个机器控制器在通信中执行不同的功能:

- → 机器1设计人定义双向交互的数据，但控制器不启动任何通信。
- → 机器2控制器启动所有通信，但设计者必须确保它以机器1可用的应用程序代码传输信息，并接收信息。

在此用例中，机器1的行为与I/O模块的行为非常相似。

通信配置

标准化配置描述符用于控制器工程的设备之间交换通信配置。工程设备和控制器可以一起自动创建所有必要的信息模型条目，自动建立与其他控制器的连接，并自动处理故障。安装后的通信配置中可能需要一点灵活性，特别是在将多个相同的机器或橇装设备交付给单个应用程序的情况下（见图6）。机器设计人必须控制允许配置的级别，实际的配置可以由通用的OPC UA客户端完成。在这个例子中，有两台相同的设备是从供应商1购买的，另两台相同的设备是从供应商2购买，每台设备在安装后不改变功能或操作，但我们并没有事先设定它们如何相连，而且也没有预先标注设备一旦安装后它的网络标识。在调试时，必须给每台设备（或更具体地说，每台设备中的控制器）一个网络标识(例如：主机名或IP地址)，并且使用通用OPC UA客户端的另一个供应商的设备中的控制器必须具有网络标识。

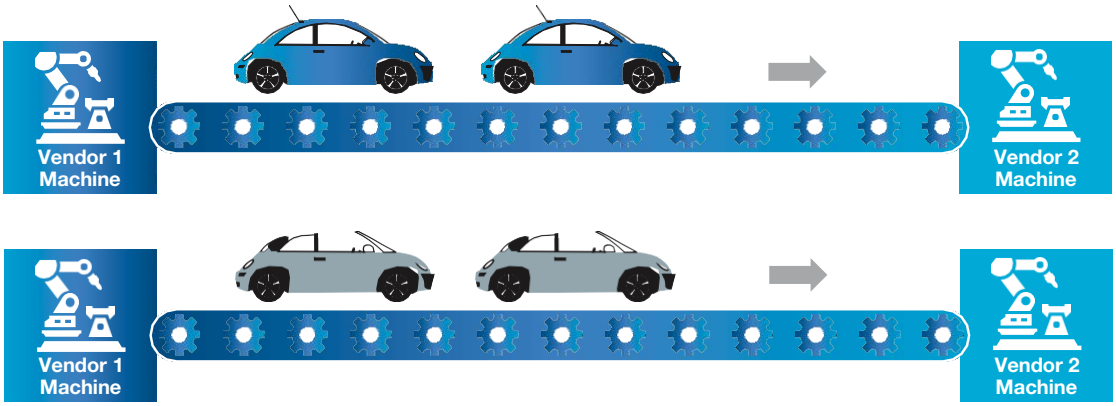


Figure 6: C2C Example with two identical lines (Case 1)

在下面的示例中，两个相同的混合橇集成到供应商1的均质器中（参见图7）。与前面的示例一样，供应商2控制器中的网络标识必须与供应商1的控制器互联。但是，必须提供进一步的信息给到每一个供应商2的橇。

因为供应商1的控制器提供两个独特的连接器‘a’到供应商2的橇，其功能相同，但携带的数据不同。这两个供应商2的橇控制器的对话必须通过供应商1控制器的网络标识和关联的连接内部标识。

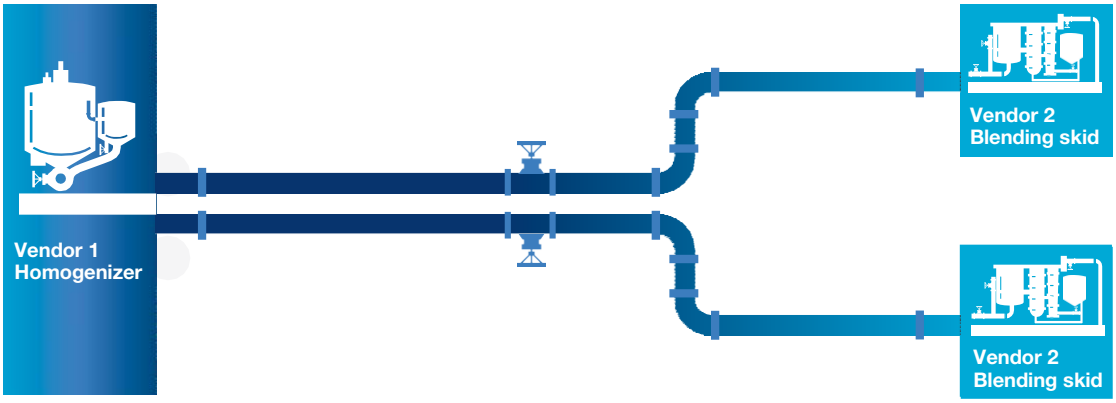


Figure 7: C2C Example with two identical skids in the same line (Case 2)

自动化组件模型

自动化组件 – 功能模型与资产模型

现场层的OPC UA必须使用规定的OPC UA信息模型公开其信息。该模型基于自动化组件(AC)，它们是执行一个或多个功能的实体，这些功能是自动化设备的一部分(例如：控制器、驱动器、仪器、I/O设备)（见图8）。所有ACs都可以建模为一个或多个资产和/或一个或多个功能实体。此外，AC包含描述AC支持的网络接口和网络，以及其通信服务的信息。

AC的规模取决于供应商。它可以小到一个独立的I/O设备，也可以大到一个房间大小的复杂机器。.

AC由资产模型和功能模型两大类组成。资产模型通常描述物理项，但也可以包括非物理项，如固件或许可证。资产模型基于DI信息模型(OPC10000-100-第100部分：设备信息模型)，扩展了现场层通信倡议的用例。功能模型描述了一个逻辑功能。功能模型由一个或多个具有封装特性的功能实体组成，这些功能实体可以包括输入/输出变量、通信和设备参数以及通信连接。功能实体(FE)从硬件中抽象出来，允许将应用程序移植到新的硬件。

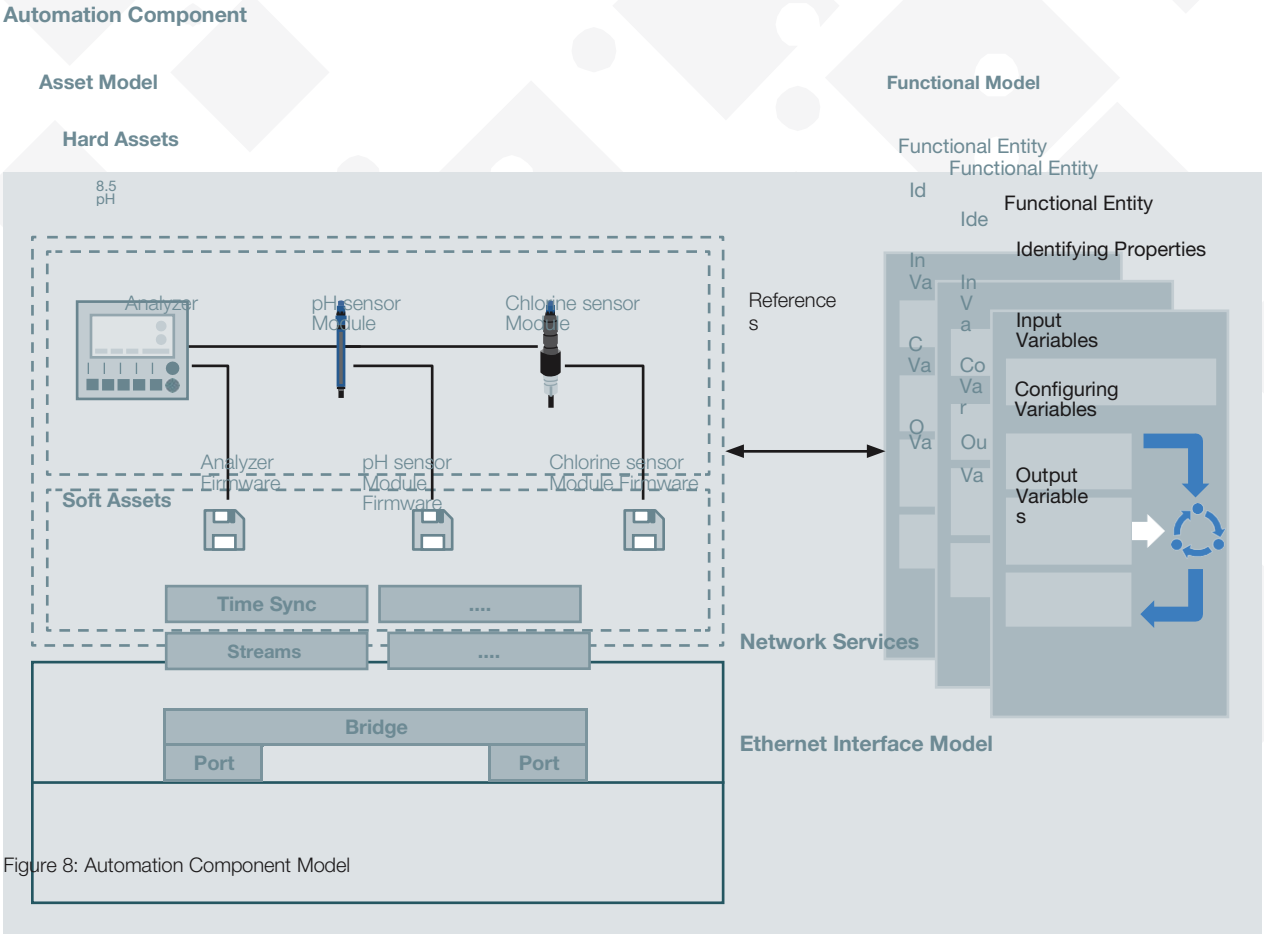


Figure 8: Automation Component Model

功能实体引用的相关设备或执行的设备，其应用程序可以满足任何硬件的要求。例如，双轴驱动器可以基于某个包括两个功能实体的设备。

从功能实体到通信关系

功能实体（FE）是AC的一个元素，它表示AC的某一个功能（参见图9）。例如包括应用程序执行引擎、运动轴控制、传感器、继电器、I/O控制和变频驱动控制。在AC中可以有多个FE。

连接是交换一组定义的过程数据和数据质量的一种逻辑结构。在连接中，一个或多个PubSub数据集写入器和数据集读取器负责与其他功能实体交换数据。

使用PubSub交换过程数据支持以下三种连接类型：

1. 单向通信
2. 单向通信心跳机制
3. 双向通信

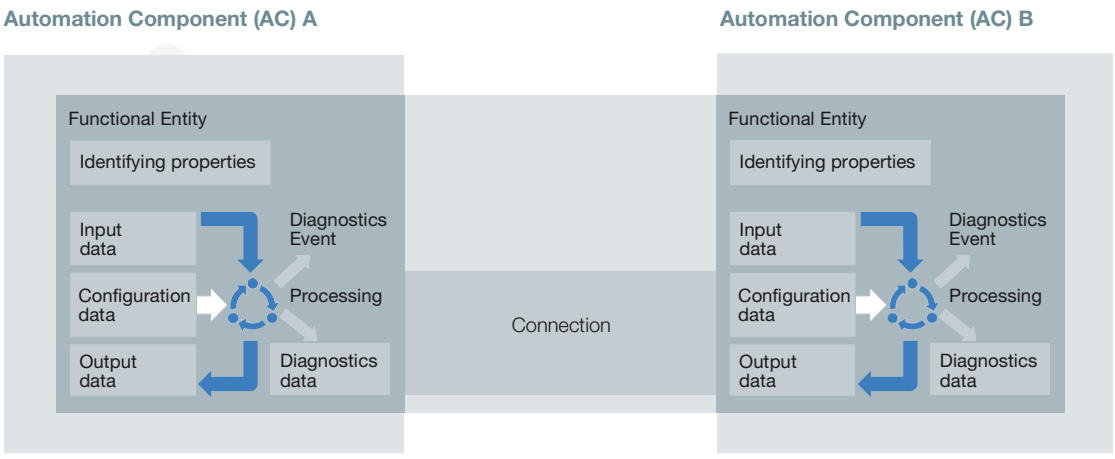


Figure 9: Connections between Functional Entities

连接管理器的角色

连接管理器(CM)负责在FE之间建立连接服务。它使用连接配置数据，如对象的通信地址、更新率和QoS设置，一个或多个通信对象的通信设置（参见图10）。

CM能够建模为各种不同的实体。该实体通常驻留在AC中，AC通过内部机制启动连接，但也可以选择外部实体。

连接配置数据由以下参数组成:

- 连接端点描述
  - 本地地址，包括位于AC上的OPC UA服务器地址和连接功能实体的浏览路径
  - 远程地址
- 单播或多播的选择
- QoS选项及其参数(包括TSN)
- 处理数据
  - 发布间隔（用于数据发布者）
  - 消息接收超时（用于数据订阅者）
- 故障检测
  - 发布时间间隔
  - 消息接收超时
- 连接超时（用于清理）
- 兼容性验证参数

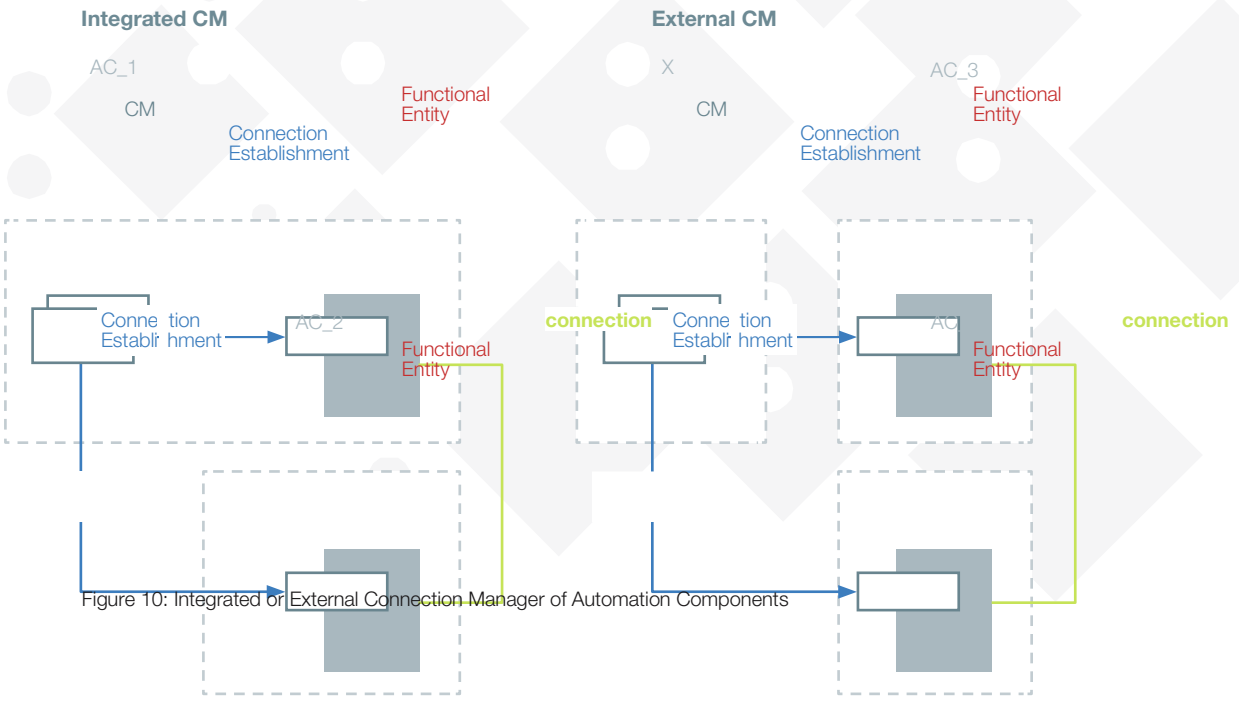


Figure 10: Integrated or External Connection Manager of Automation Components

连接状态机

连接管理器(CM)必须在两个平行对等的端点上建立连接。对于每个端点，都需要一个单独的连接状态机（参见图11）。

对于两个端点的联合操作，人们提出CM并行执行两个端点的状态机，这意味着在一个端点和另一个端点上逐步地执行。这将有助于简化通信的启动。此连接状态机扩展了OPC10000-14第6.2.1章定义了PubSub状态机，它只处理PubSub连接的单个状态，并不处理如何达到此状态。连接最初是使用Client/Server机制设置，这一交换建立了双向PubSub连接，例如交换兼容性验证、所有权和参数。此后，准备和操作PubSub连接。在功能实体的信息模型中定义每个连接的连接状态机。

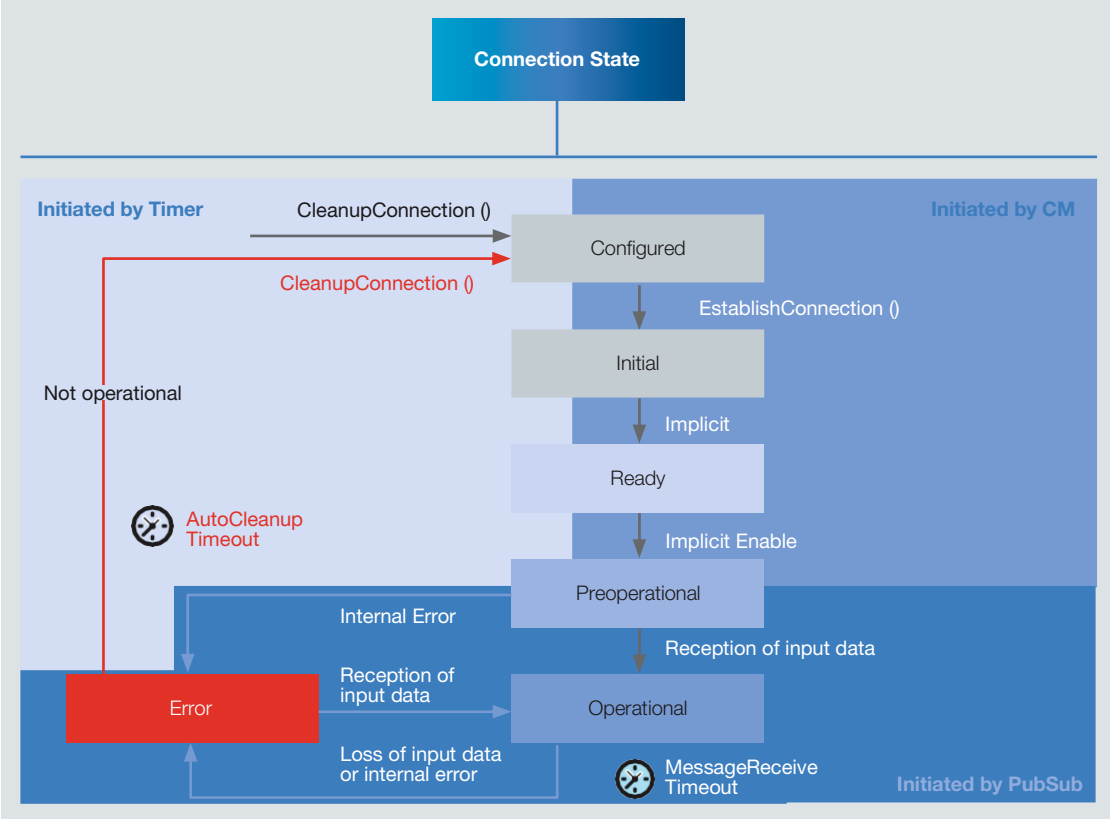


Figure 11: Connection State Machine

离线工作流和模型

导言

离线工程是自动化系统开发、运行和维护的重要组成部分。允许用户在硬件系统部署之前理解自动化系统的操作，一旦硬件系统到位，用户能够了解如何可靠和正确地执行系统的控制功能。用户将能够模拟自动化系统的更改和更新。

在对硬件系统更改并确保在此之前达到用户的期望并提高系统的性能。

本章描述了在离线工程阶段使用AC描述构件的配置工作流。

下图是离线工程描述符使用工作流步骤的概述。

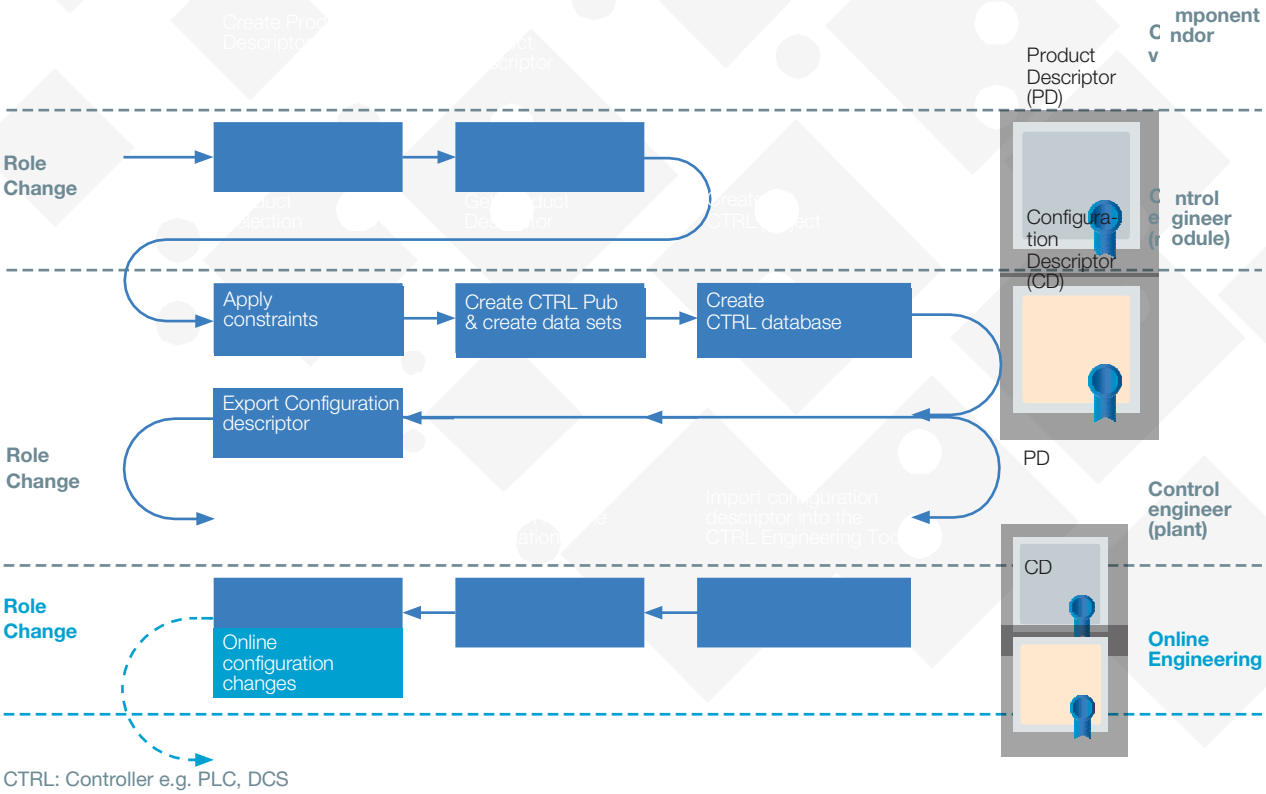


Figure 12: Overview of the workflow steps for offline engineering descriptor(s) usage

描述符的定义

通常来讲，AC的描述符是一组文档，其中包含OPC UA信息模型和用于配置潜在的其他有用信息。信息可以是一个AC或一组AC（如机器、机器模块或橇）。AC描述符以打包文件的格式(zip文件包)交付，支持为离线工程提供和共享信息。描述符中的一个或多个数字签名可以为内容提供完整性。

AC描述符的文档可分为信息模型和附件文档。信息模型文档定义AC的信息模型，而附件文档为工程和部署过程补充（和可选的特定供应商）材料。

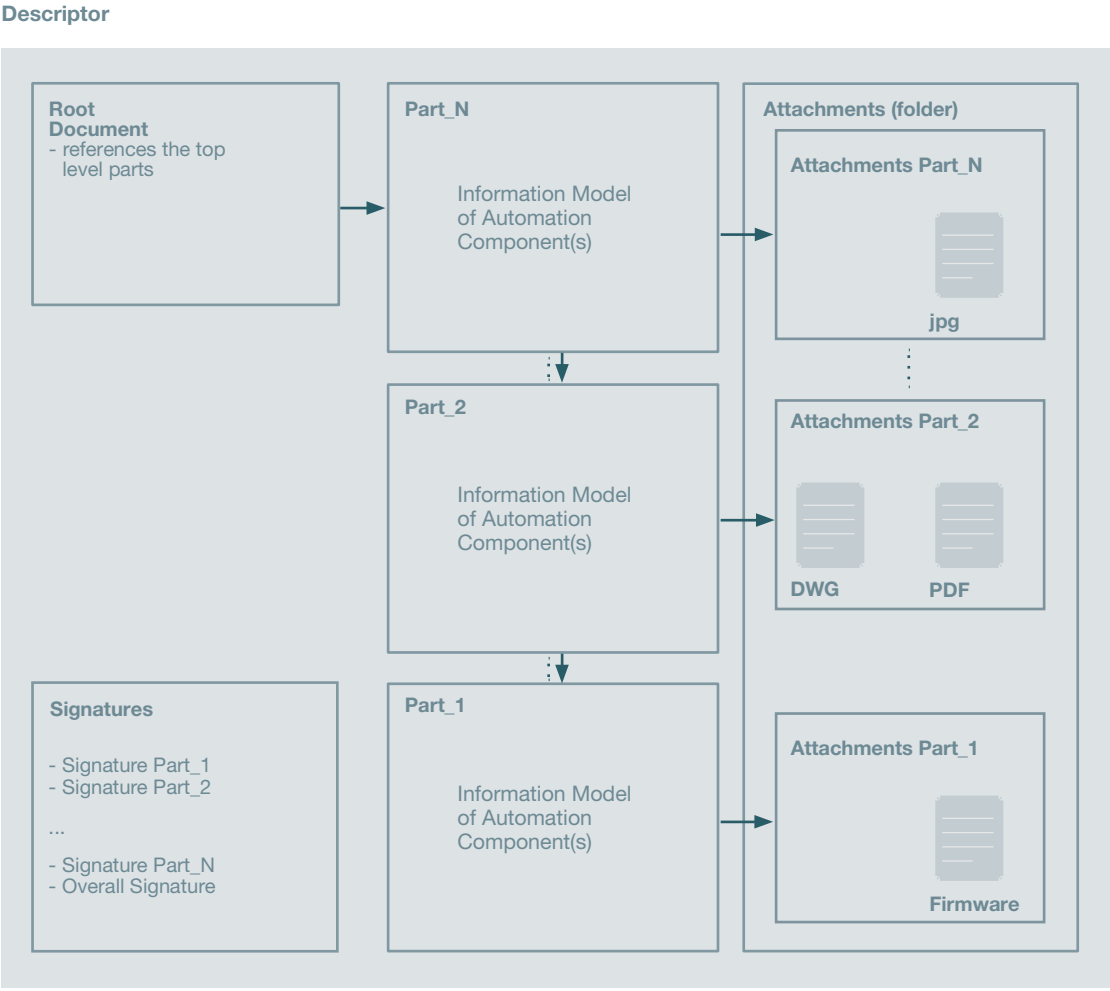


Figure 13: Generic Descriptor Package or Generic Descriptor

如图13所示，内容分为两部分。每个部分可以由不同的工程师设计，并有其特定的工程步骤。零件系统形成一个层次结构，其中上层（后面）部分依赖于下层(较早)部分，添加或覆盖(如果允许的话）前一部分中创建的信息。

信息模型的内容由一个或多个自动化ML(AML)文档组成。AutomationML (AML)是一种基于供应商中立的XML格式，用于存储和变更工程信息。接下来描述两个AC描述符的例子。

产品描述符

产品描述符是包含AC产品数据的特定AC描述符（参见图14）。通常，产品描述符由AC供应商提供。将产品描述符导入工程工具是AC工程的第一步。在大多数情况下，产品描述符包含后面的描述符中（例如：配置描述符，见图15）作为第一部分。

产品描述符说明AC资产的标识、结构和功能。对于字段或I/O设备，描述符还可以包含有关资产组件功能的信息。

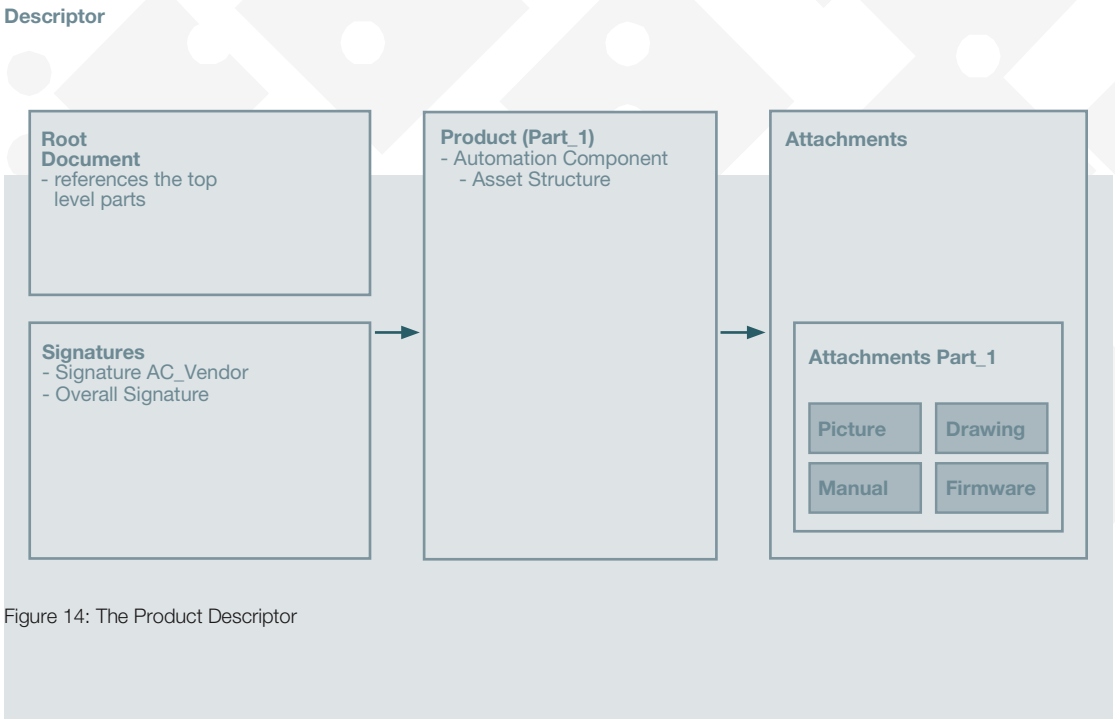


Figure 14: The Product Descriptor

配置描述符

图15所示的配置描述符具有一个产品部件（Part_1）和一个或多个配置部件（Part_2）的描述符。配置描述符是在工程过程中创建的，通常是为了与另一个工程工具共享AC的信息。

配置描述符的配置部分定义了功能实体、通信数据集、服务质量(QoS)和建立连接所需的数据(如OPC UA Pub单播或多播地址)。此外，对于现场层或I/O设备，配置部分还可以包含参数数据。

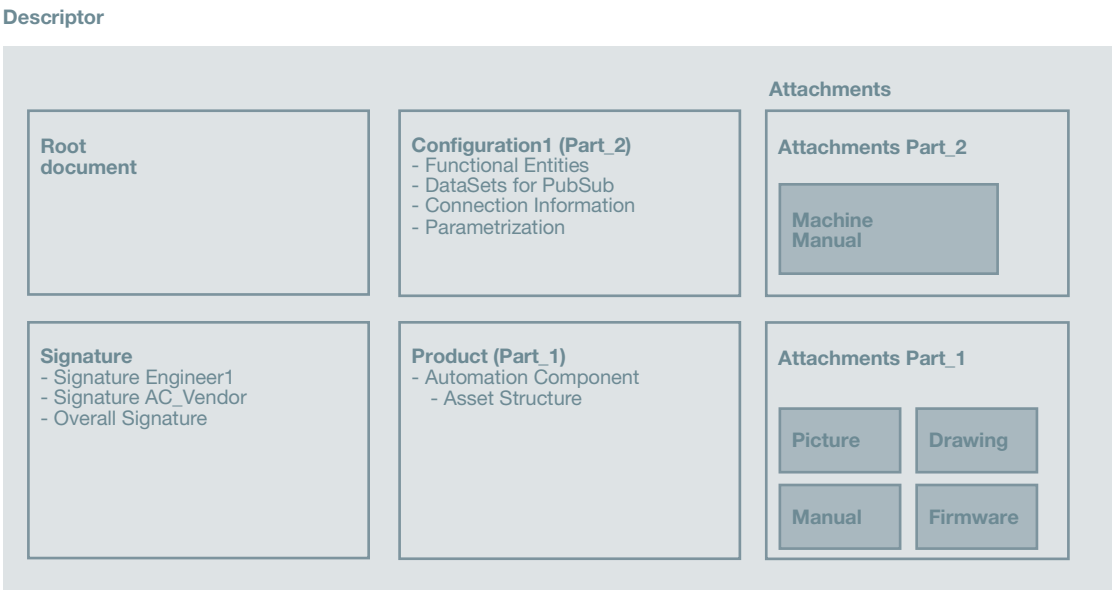


Figure 15: The Configuration Descriptor

工作流示例

本节将展示如何在脱机环境下使用描述符，以及描述符如何表示一个或多个ACs。在下面的两个例子中，在自动化系统中设置一个线路控制器(LC)并向3个下属控制器(PLC/DCS)实施总体控制。在第一个示例中，使用没有TSN的标准以太网通信。第二个示例中的系统则支持TSN通信。

下面是用例的工作流，包括对工作流状态的逐条描述(例如，在方括号中注明[1]):

线路控制器系统以及3个非TSN子控制器

在离线工程阶段，LC的工程工具可以用于创建[1]配置描述符或配置描述符包(CDP):

→ C_1 LC CDP用于导入C_1工程工具
→ C_2 LC CDP用于导入C_2工程工具
→ C_3 LC CDP用于导入C_3工程工具

每个CDP都包含配置LC和C_X（X=1、2、3）之间通信所需的信息（参见图16）。除了配置信息之外，CDP还包含一个索引，帮助浏览存储信息和作者的数字签名（在这种情况下，系统集成商开发工程师）。

当CDP[2]导入其中某一控制器的工程工具时，控制工程师检查签名的有效性，并使用CDP索引浏览和查找发布信息—这使控制工程师能够在控制器内部

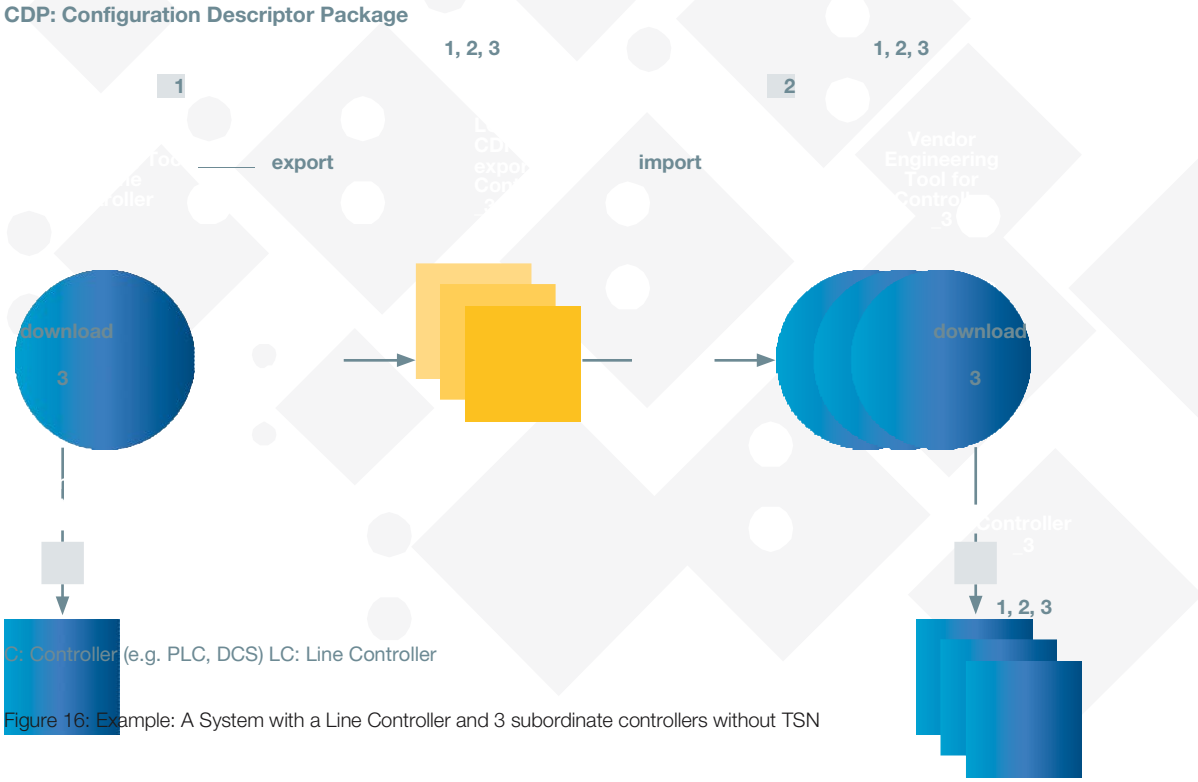


Figure 16: Example: A System with a Line Controller and 3 subordinate controllers without TSN

设置相应的订阅和连接对象。一旦控制工程师完成C_X项目，硬件(PLC/DCS)连接成功，就可以通过C_X工程工具[3]部署配置。

线路控制器系统和三个带有TSN的子控制器

在离线工程阶段，LC的工程工具可以用于创建[1]配置描述符或配置描述符包(CDP):

- → C_1 LC CDP用于导入C_1工程工具
- → C_2 LC CDP用于导入C_2工程工具
- → C_3 LC CDP用于导入C_3工程工具

每个CDP都包含配置LC和C_X（X=1、2、3）之间通信所需的信息（参见图16）。除了配置信息之外，CDP还包含一个索引，帮助浏览存储信息和作者的数字签名（在这种情况下，系统集成商开发工程师）。

每个控制器的CDP—除了第一个示例中的信息之外—还包括TSN机制为每个控制器(C_1、C_2和C_3)提供的QoS功能和需求)。QoS功能是控制器的产品描述符的一部分(也包含在CDP中)，而QoS需求是配置描述符的一部分。

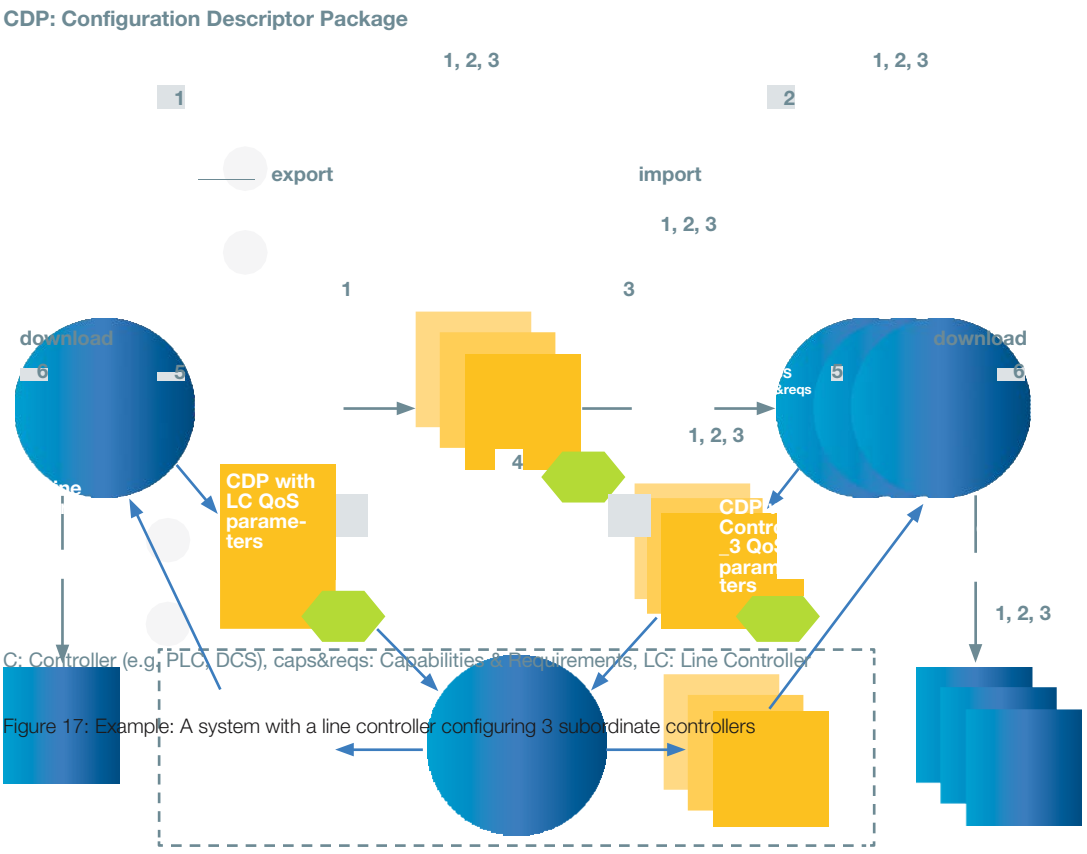


Figure 17: Example: A system with a line controller configuring 3 subordinate controllers

当CDP[2]导入到其中一个控制器的工具时，控制工程师开始检查签名的有效性，并使用CDP索引浏览和查找发布的信息。这使得控制工程师能够在控制器中设置相应的订阅和连接对象。

所有控制器(LC、C_1、C_2和C_3)的QoS功能和需求从CDPS导入到离线中央网络配置(CNC)[3]用以计算TSN配置(例如：QoS参数/TSN流配置数据)。

计算输出输入的QoS参数/TSN流设置描述符一对应每一个控制器C_X。这些描述符再次导入C_X和LC工程工具中[5]。

一旦控制工程师完成了C_X项目与硬件(PLC/DCS)连接，就可以从C_X工程工具[6]开始部署配置。

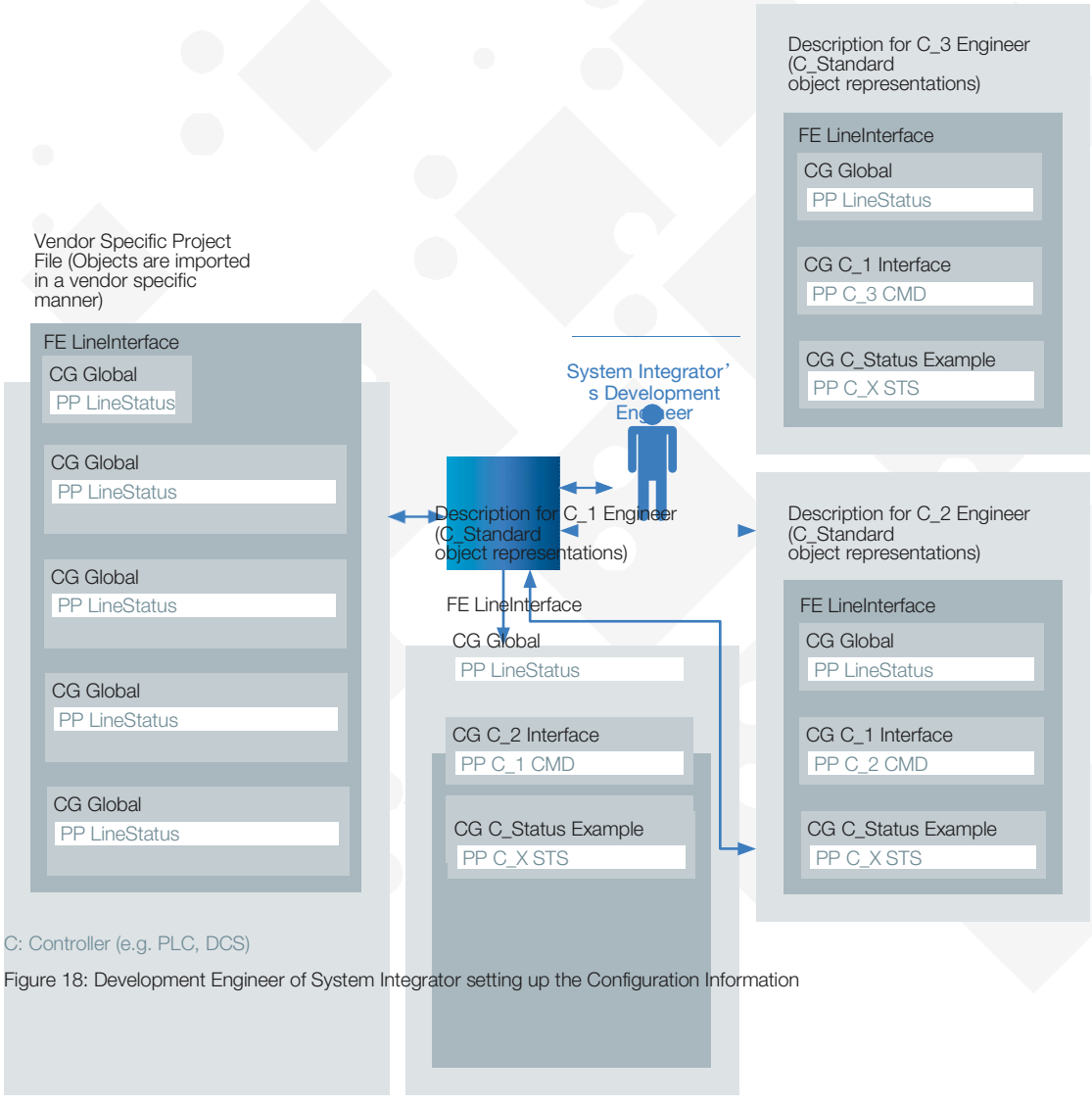


Figure 18: Development Engineer of System Integrator setting up the Configuration Information

安全通信

OPC UA安全规范(OPC10000-15-第15部分：安全)描述了使用OPC UA机制交换安全数据的服务和协议。它扩展了OPC UA，满足IEC61508和IEC61784-3系列标准中对功能安全定义的要求。
实现上述功能后就可以检测到低一级网络层中的所有类型的通信错误。

如果检测到信息错误，将与安全层共享此信息，然后安全层将采取适当地操作，例如切换到安全状态。OPC UA安全性与应用程序无关，不会对应用程序数据的结构和长度提出要求。.

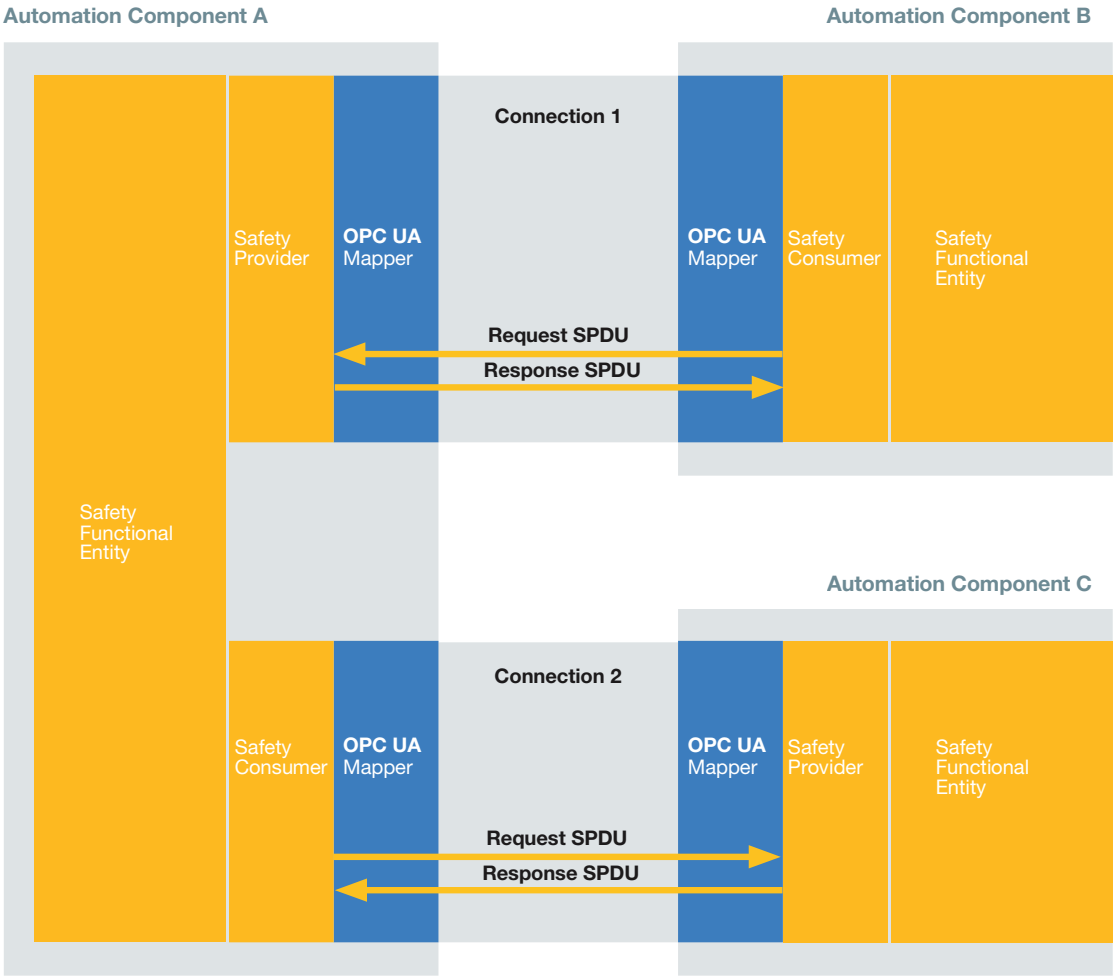


Figure 19: Safety connections between Automation Components

现场层通信安全

在这些连接之上，OPC UA安全使用标准的连接并附加安全的传输协议。为了通过安全的数据连接来扩展功能实体之间标准的数据交换（参见图19）。此原则将评估工作划分为安全传输功能，因此与此相关的连接就不需要任何额外的安全评估。

安全功能实体包括标准和安全的输入和输出变量。功能实体内部的安全应用程序也必须以安全的工作流程开发。

安全应用程序可直接与安全提供商/安全用户连接，后者通过安全协议交换数据。OPC UA映射用于连接安全层与底层的通信，并支持安全提供者和安全用户之间的通道。

最基本的安全通信类型是双向通信，即一个AC(A)上的安全应用程序将数据发送到另一个AC(B)上的安全应用程序。安全用户启动并请求SPDU的通信。安全提供商反馈接收到的ID和计数器，添加所请求的安全数据后，通过校验和确保所有数据，然后再对SPDU做出响应。

一个AC可以是安全用户，同时也可以是安全供应商。安全提供商和安全用户之间的连接可以在运行时建立或终止，允许不同的用户在不同的时间连接到同一个安全提供商。

安全提供商状态图

安全提供商通过一个非常简单的状态机来实现。 它只是等待请求，如果收到请求，就会发出安全电报。所有安全检查将在安全用户方进行。

安全用户状态图

安全用户通过启动安全数据交换、等待响应、并根据IEC61784-3检查潜在的通信错误（完整性、及时性、真实性）。此后，安全数据将提供给AC内部的安全应用程序。如果发生通信错误，将向安全应用程序提供故障安全替代值，并提示错误。

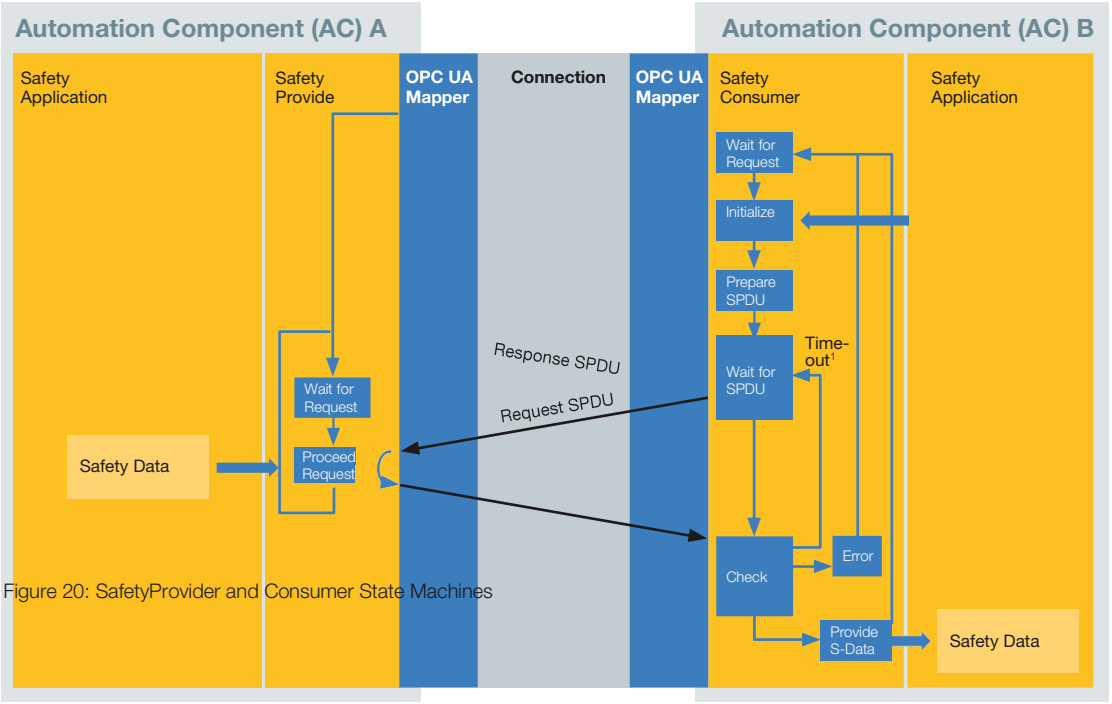


Figure 20: SafetyProvider and Consumer State Machines

1 To avoid running into safety timeout, SPDUs may also be protected by end-to-end latency guarantee.

安全性

现场层通信的安全性

每个现场层的连接，都是通过Client/Server和PubSub通信指定了标准的OPC UA安全机制进行身份验证和可选加密。连接是在完成OPC UA安全会话之后输入，利用带有证书和私钥的非对称密码建立起来(参见图-21)。

在此阶段，连接的认证和对称密钥的交换建立完成。此后，连接管理器（CM）即可通过此安全会话维护连接，并确定连接的操作状态。

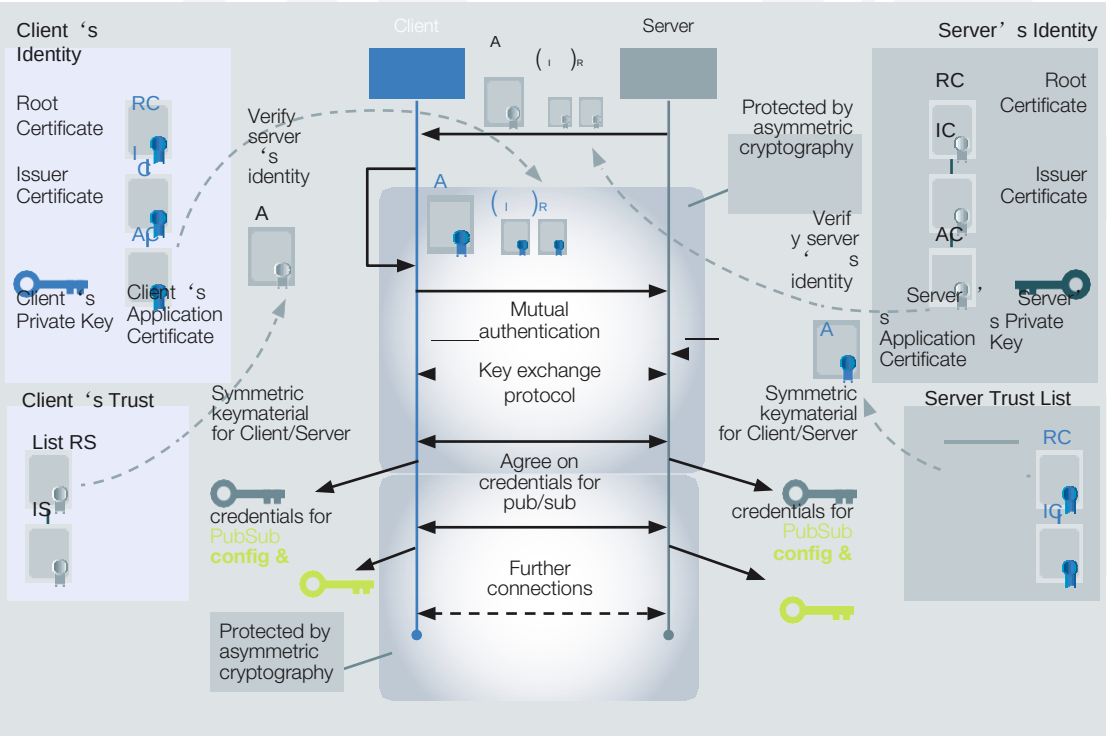


Figure 21: Mutual authentication plus obtaining credentials for PubSub

数据传输

通信

当前，现场级通信设备的系统架构可以与PubSub通信一起使用两个通信行规，该行规至少由四个通信层构建（参见图22）。

现场级通信所实现的所有OPC UA ACs将能够支持一个或多个通信行规，包括任何一个或所有可选的行规。每个行规都可以在任意一个连接的基础上使用。因此，如果控制器符合多个行规，控制系统工程师可以对连接选取最佳的方案。

→ 行规 A

行规A可以优化为3层网络，它通常部署在由许多机器、配件和单元所组成的整个工厂当中。行规A连接可以提供最灵活的网络体系结构，但相比行规B的连接会消耗更多的网络带宽和资源。

在各层以及 UDP UADP 传输层，如果建立了 IP 路由，安装在 IP 网络中的任何两个行规 A 的组件都可以互操作。配置了行规A的ACs可以选择TSN网络访问层，以便在TSN域中能够互操作（参见第 35 页等）。

由于UADP传输层不兼容，行规A和行规B的连接不能互操作，因此AC必须实现两者以支持所有用例中的互操作性。

→ 行规 B

行规B针对第2层网络进行了优化，通常应用在单个设备、单元或机器中；使用行规B的连接可以获得最有效的网络带宽和性能，但无法通过第3层的交换机或路由器运行。

如果一个 AC 支持 TSN 网桥层并使用嵌入式以太网桥来实现，那么它也应该配置 TSN 网桥层。

If an AC supports the TSN bridge facet and is implemented with an embedded Ethernet bridge, then it shall implement the TSN Bridge Facet.

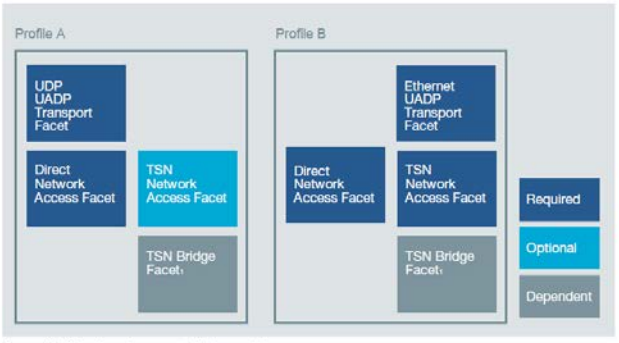


Figure 22: Structure of communications profiles

图22: 通信规则架构

行规B需要TSN网络访问层的支持，包括网络直接访问层和以太网 UADP 传输层。配置在同一个TSN域中的任何两个行规B组件都可以互操作。
为了支持非TSN以太网网络环境下的操作，行规B连接还支持网络直接访问层。

传输层和网络访问层

→ 传输层

OPC UA规范中第14部分（OPC 10000-14）发布并定义了以太网UADP和UDP UADP传输层，第7部分行规（OPC 10000-7）则可以用于当前。

→ 直接网络访问层

在直接网络访问层定义了非TSN以太网的点对点或组播技术，以及使用PCP或DSCP优先级机制的通信。这意味着使用此连接将不会受限于基础架构，且支持所有类型的托管和非托管交换机，包括TSN交换机。在负载量大的网络中，交换机缓冲区可能会拥堵并出现数据丢包，或者可能会产生延迟和抖动，从而导致数据包传输太迟，应用程序无法控制。

→ TSN网络访问层

TSN网络访问层是直接网络访问层的超集，使用了TSN以太网点对点或TSN流组播技术。在此层面上使用带有TSN网桥的任何两个终端都可以保证零拥塞丢包和有限的网络延迟和抖动。即使在负载量很大的TSN网络中，高优先级流也不会受到这种负载的影响。

→ TSN网桥层

具备TSN桥接这一特征的网络接口就称为TSN网桥层。现场层通信计划致力于支持IEC/IEEE 60802 TSN工业自动化规范。预计在TSN的工业网络中运行的所有工业以太网变量和 IT 设备都将符合此规范，允许它们公平地共享网络资源。

TSN要求所有桥接（嵌入在AC或基础设施交换机中）符合IEC/IEEE60802标准。如果AC配置了TSN网络资产并实现了嵌入式交换机，那它必须配置TSN网桥方面，并且其交换机必须符合IEC/IEEE 60802的网桥。在单个网络中连接多个TSN域以及通过网络路由器扩展TSN域的机制尚未标准化。

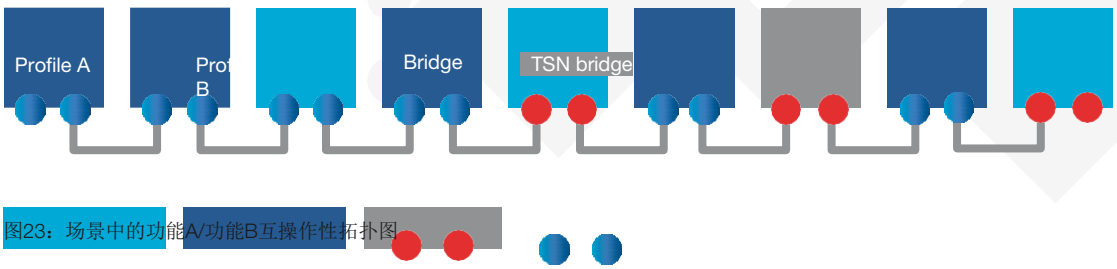


图23：场景中的功能A/功能B互操作性拓扑图

互操作性矩阵

图23显示了ACs的潜在配置，它说明了所有可能的网络行规互操作性用例（同时允许必需的和可选的配置）。

表1显示了哪些ACs是可互操作，并指出了该互操作性的诸多限制。

互操作性仅适用于两个组件交换数据的能力。还有其他属性，通常与设备的完整功能相关，即满足应用程序要求的能力。

例如，如果设备2和6是运动设备，互操作性不需要其系统达到成功控制特定应用程序所需的更新速率、延迟和抖动。

如果设备1和7已经实现了对功能A和功能B的支持，那么设备1将与所有设备兼容（见图24），因此如表2所示。

	Device 1	Device 2	Device 3	Device 4	Device 5	Device 6	Device 7	Device 8
Device 1		Yes	No[1]	Yes[2]	No[1]	Yes[3]	No[4]	No[1]
Device 2			No[1]	Yes[2]	No[1]	Yes[3]	No[4]	No[1]
Device 3				No[1]	Yes	No[1]	No[1]	Yes[5]
Device 4					No[1]	Yes[3]	No[4]	No[1]
Device 5						No[1]	No[1]	Yes[5]
Device 6							No[4]	No[1]
Device 7								No[1]

Table 1: Interoperability matrix (Device 1 supporting Profile B)

[1] Different communication profiles
[2] All devices between devices implement an embedded IEC/IEEE 60802 compliant bridge
[3] Does not use TSN QoS
[4] Layer 2 communications cannot traverse a router
[5] UDP communications are routable

	Device 1	Device 2	Device 3	Device 4	Device 5	Device 6	Device 7	Device 8
Device 1		Yes	Yes	Yes	Yes	Yes[3]	Yes	Yes

Table 2: Interoperability matrix (Devices 1 and 7 supporting both, Profile A and Profile B)

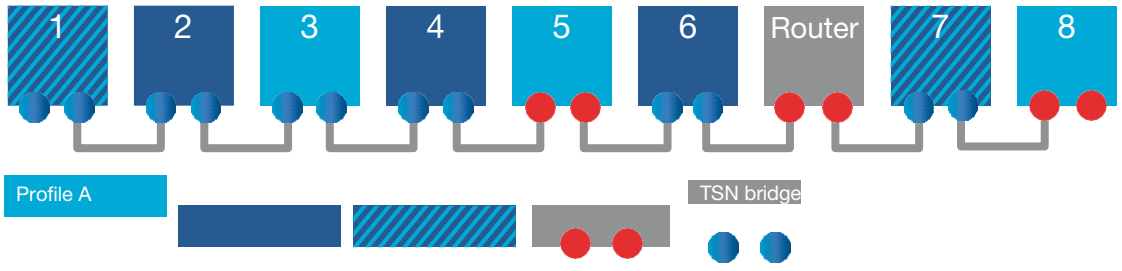


Figure 24: Topology to illustrate interoperability in a mixed Profile A/Profile B scenario

以太网 – 高级物理层

OPC UA这一框架与传输无关，因此可以与不同的底层协议（如TCP、UDP、MQTT等）和物理层一起使用。为了将OPC UA扩展到流程工业的现场层，OPC UA与以太网高级物理层（APL）相结合，这将在稍后的规范版本中即在控制器到设备用例中解决。

以太网 – 高级物理层 [1]

如图25所示，APL是基于10BASE-T1L的单对以太网（SPE）的增强物理层。它通过10 MBit/s、高达1000 m的全双工电缆进行通信。它在逻辑上扩展了以太网，为工厂的可靠运营提供更高性能。以太网APL物理层，能够支持OPC UA或任何其他高级的协议。

以太网APL的设计支持各种拓扑结构，例如具有可选冗余或“弹性”的干线和支线。以太网APL明确指定了点到点与构成“网段”的通信组件之间的连接。因此，以太网APL交换机隔离了网段之间的通信。这消除了诸如串扰之类的干扰，使得本机的通信免于受不同网段上设备故障的影响。

以太网-APL 定义了两种通用类型的网段：

- → “Trunk”为长达 1000 m 的长电缆提供高功率和信号电平。
- → “Spur”具有较低的功率，其安全性最长可达 200 m (2-WISE)。

2-WISE 代表双绞线内在安全的以太网。此 IEC 技术规范 IEC TS 60079-47 (2-WISE) 定义了所有危险区域和分区的本质安全保护。对于用户来说，这包括一些简单步骤即无需计算就可以验证网络本质安全。

以太网-APL将以太网与双绞线安装技术相结合。使得以太网-APL成为更易于部署的现场通用标准，从具有危险区域0/1分区的过程工厂，再到采用工厂自动化和过程自动化技术的网络工厂。因此，将以太网-APL作为 OPC UA 现场设备的物理层是将OPC UA成功部署到过程自动化应用中的现场级别的关键驱动因素。

ethernet-apl™
advanced physical layer

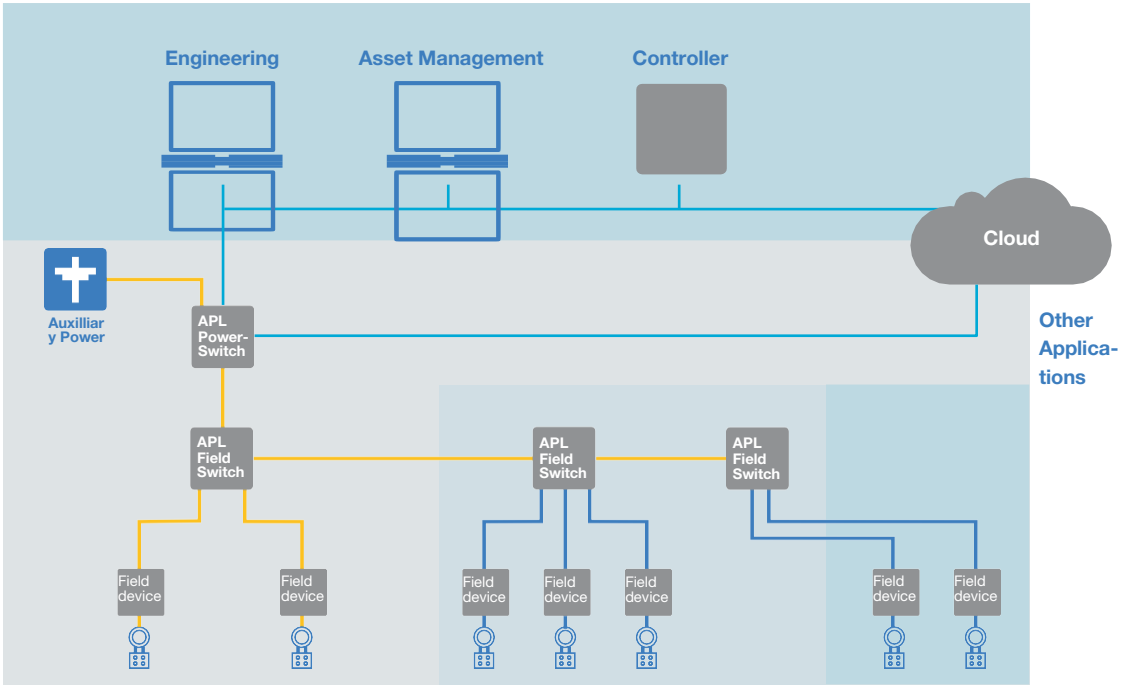


Figure 25: Example topology for long cable reach

[1] Extract from "ethernet-apl advanced physical layer. Ethernet to the field" https://opcfoundation.org/wp-content/uploads/2020/06/Ethernet-APL_Ethernet-To-The-Field_EN.pdf

实时通信模型

服务质量（QoS）的概念

QoS是一种网络控制机制，它可以为不同的设备或数据流提供各种优先级，或者根据应用程序的请求保证数据流性能水平。如果网络性能作为关键要素，QoS可以保护高优先级的应用程序，尤其是实时控制程序。

在TSN出现之前，工业自动化网络中提供 QoS 的最常见方法是为不同类型的流量提供差异化服务。这一方法通过对流量进行分类，并使用优先级排队等工具，更好地处理了某些类型的流量，从而对所选流量类型实现更快的处理、更高的平均带宽和更低的平均丢失率。然而，这仅是一种统计偏好，无法做到稳定和快速的保证。不同类型的工业以太网流量（如运动、I/O 和 HMI）对延迟、丢包和抖动有不同的要求，服务策略应该针对这些类型的流量区分服务。

现场层通信倡议为现场层定义了识别重要的OPC-UA 流量规定，包括第 3 层 DSCP（差分服务代码点，在 IETF RFC 2474 等中定义）和第 2 层 CoS（服务等级，在IEEE 802.1Q中定义) 标签，用于非TSN网络的管理。

TSN通过为特定类型的流量保留网络资源，并提供标准化机制来保证服务质量。此类网络必须能映射到网络应用程序或中间件，如OPC UA PubSub。应用程序的QoS要求OPC UA应该是可配置的，且与底层网络技术没有或有较少的依赖关系。通过对应用程序隐藏的网络细节，应用程序生成器可以更轻松地将OPC UA应用程序从一种网络技术迁移到另一种网络技术，甚至可以通过不同的网络技术互连OPC UA应用程序。

TSN QoS 机制

IEC/IEEE 60802 TSN 工业自动化行规由IEEE 802.1TSN 工作组提出，它定义了一组QoS机制，用于工业自动化网络的融合。融合网络有望实现运营技术 (OT) 与信息技术 (IT) 应用程序的通信，其中包括 PROFINET 或 EtherNet/IP 等传统现场总线，以及工厂运营中的通信，例如 HMI/SCADA/MES 与 PLC，从而实现了共享网络基础设施，不会妨碍彼此的操作。对于许多工业控制应用而言，意味着它必须满足某些带宽、延迟和截止期限等要求，尤其是在竞争同一网络资源的情况下。

流量类型与QoS

为了使不同的应用程序能够在同一网络上运行，基础设施组件必须提供一种能够传输不同类型流量QoS的方法。现场层通信倡议定义的流量类型可以使用相同的基础设施，可以融合不同类型的 OT 流量（例如过程控制、工厂自动化以及快速运动和 I/O 控制）和 IT 流量。

定义了以下通道类型：

- → 网络控制
- → 循环控制
- → 事件控制
- → 配置与诊断
- → 用户定义
- → 其他

这些流量类型的系统范围实现允许在同一网络上实现工厂自动化、过程控制、IT流量和尽力而为流量的融合。

TSN域和通信关系示例

今天，工业自动化系统的许多网络架构遵循一定的物理和逻辑相分离的域或区域。这种分离通常是组织或技术要求的结果，例如，来自不同供应商的单个组件或整个机器的互连，每个供应商都配备了其验证过的通信网络和配置，或实施了安全的最佳实践，或以网络冗余来达到进一步增强网络QoS。在使用TSN 时，逻辑上的分离也可能是必不可少的一步。

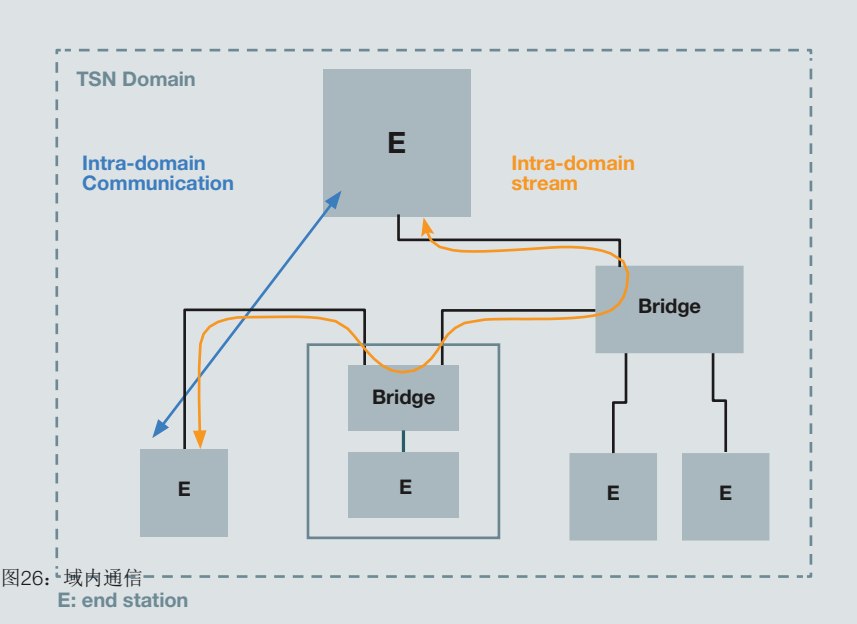


图26：域内通信
E: end station

此外，将TSN划分了不同的域旨在将集中和分布式TSN流保留可以并行运行的方法。

TSN域内和域间通信是严格区分开的。所选的流量预留机制使得工业控制应用可以实现在给定TSN域内，为所选TSN QoS 机制预留网络资源。在融合的网络场景中，您可以利用TSN提供的带宽和时序保证，如图 26 所示。域内通信可用于实现 C2C、C2D 和 D2D 间的通信。

域间通信应用在跨（多个）域的工业控制应用程序数据交换的通信场景中。可用于实现C2C、C2D、D2D的通信。

图 27 显示了用于跨 TSN 域 1、2 和 3 的 C2C 场景的域间通信。

作为域间流量的替代方案，也是连接不同域最先进的方法（例如，代表当今系统中的机器），两个域之间的过程数据交换（例如，域 1 和图 28 中的域 2）也可以通过应用程序级网关与在线通信以及相应的TSN 预留流量在逻辑上进行分离。

表 3 列出了域内或域间通信的通信关系应用示例。TSN 的域间通信代表了与 IEC、IEEE 和 IETF 在未来的合作，因此未在早期版本的 OPC UA 现场级通信规范中描述。 如果应用程序需要域间通信，Profile A 可以确保 AC 之间的互操作通信。

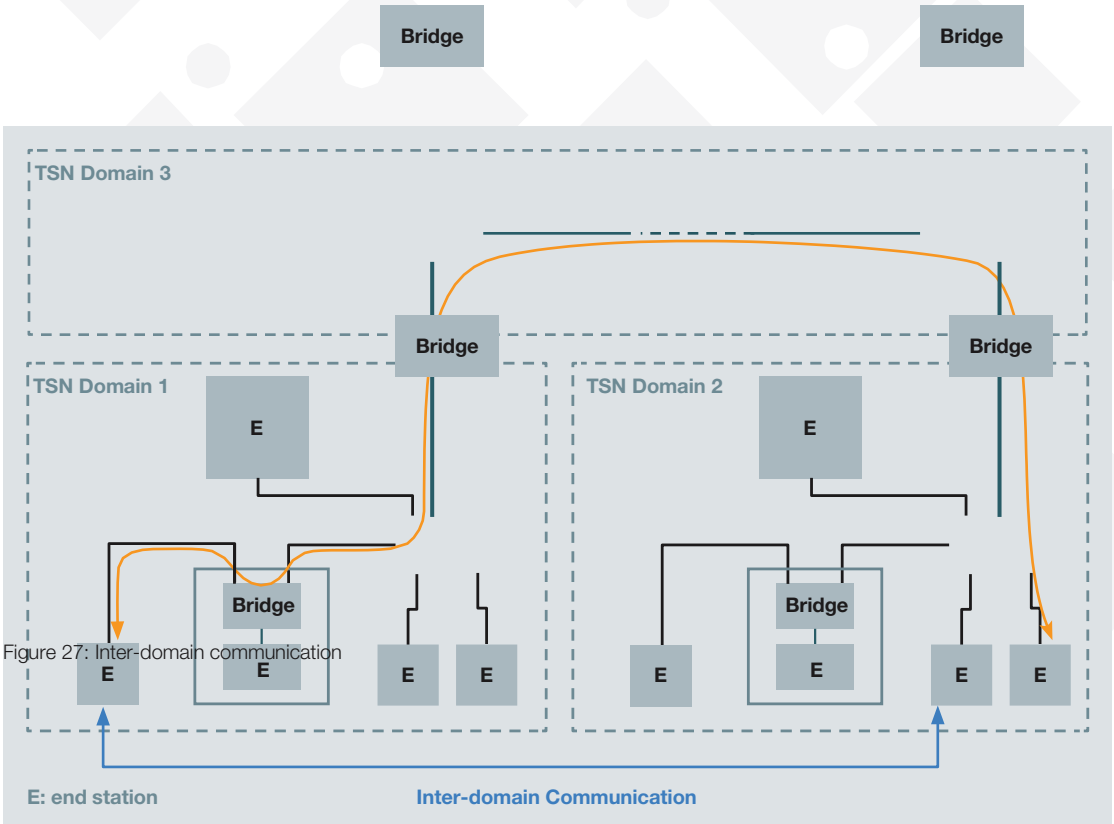


Figure 27: Inter-domain communication

网络管理

现场级通信的网络管理将基于开放的标准， 将使用 模 完 成 。
标准化管理协议来分配成功的网络配置。

实际的配置参数也将在符合 IEEE 标准的数据模型中建

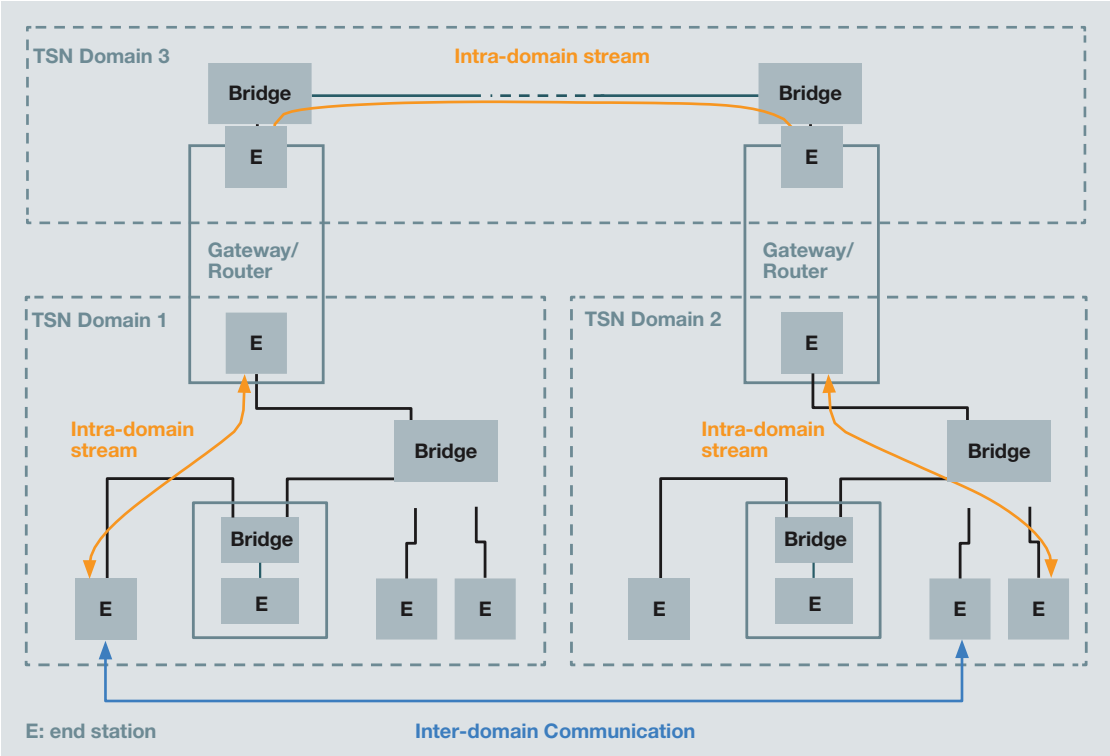


Figure 28: Connection of Domains using application level gateways or DetNet routers

Communication relation	Description/Example
C2D Intra-domain communication	This is probably the most common relationship, when a controller communicates with its peripheral (I/Os, drives, valves, ···)
C2C Intra-domain communication	Communication between multiple controllers in the same TSN Domain
D2D Intra-domain communication	To improve reaction times the devices (I/Os, drives, ···) sometimes need to establish direct communication
C2D Inter-domain communication	controller synchronizes on encoder signal from a different TSN Domain
C2C Inter-domain communication	Interconnection of machines/skids without dedicated gateways (without controller)
D2D Inter-domain communication	synchronization between motions drives in different TSN Domains

Table 3: Examples of communication relationships

总结与展望

本技术手册描述了现场层通信倡议如何扩展OPC UA框架，以促进控制器之间的跨供应商互操作性。通过在不同的用例中实现相关数据交换，包括以安全地更改实时交换的数据和与安全相关的数据。

在首个规范即控制器到控制器用例规范发布之后，规范将扩展到支持控制器到设备（C2D）和设备到设备（D2D）的用例，包括附加功能和专属设备的模型，例如：用于运动、仪器、I/O 和安全设备。

在创建规范的同时，正在生成开源堆栈软件和示例代码，以便可以在现场层通信中轻松采用OPC UA。此外，研发人员正在开发测试规范和测试工具，以提供自动化组件之间的高级跨供应商的互操作性。

通过现场层通信计划的专属扩展，OPC UA与APL、TSN和5G相结合，提供完整、开放、标准化和可互操作的解决方案，既满足了工业通信的要求，同时还提供从现场到云的语义互操作性（见图 29）。

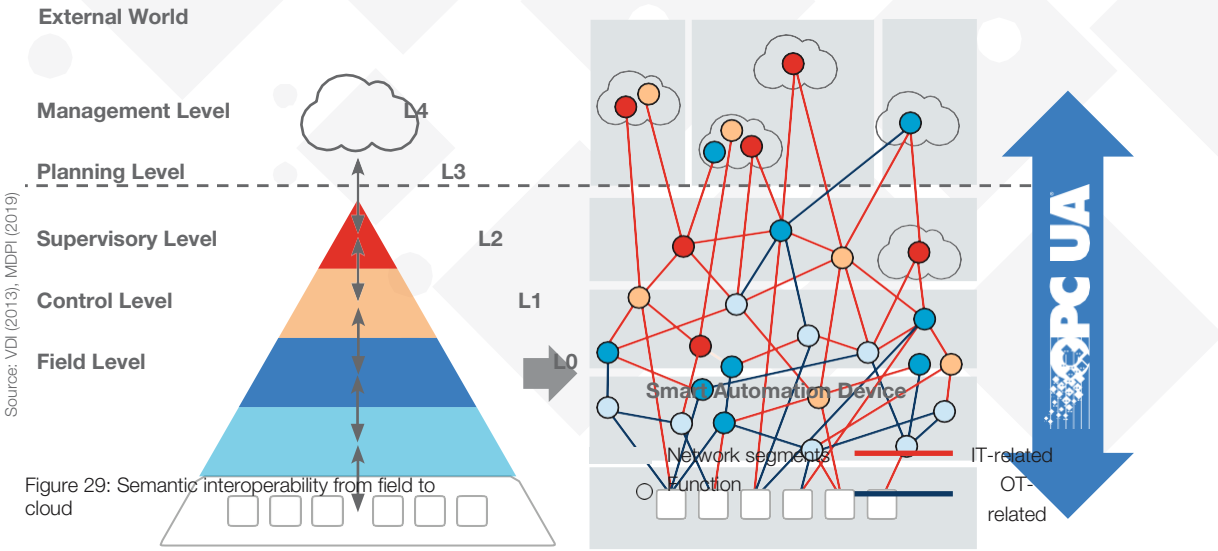


Figure 29: Semantic interoperability from field to cloud

Acronyms

AC	Automation Component
APL	Advanced Physical Layer
C2C	Controller-to-Controller
C2D	Controller-to-Device
CD	Configuration Descriptor
CM	Connection Manager
CNC	Central Network Configuration
CR	Communication Relationship
CUC	Centralized User Configuration
D2D	Device-to-Device
DCS	Distributed Control System
DSCP	Differentiated Services Code Point
ERP	Enterprise Resource Planning
FE	Functional Entity
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IIoT	Industrial Internet of Things
IoT	Internet of Things
IT	Information Technology
L2	Layer 2
L3	Layer 3
MES	Manufacturing Execution System
OE	Offline Engineering
OPC	Open Platform Communication
OPC UA	OPC Unified Architecture
OPCF	OPC Foundation
OT	Operational Technology
PAC	Programmable Automation Controller
PD	Product Descriptor
PCP	Priority Code Point
PLC	Programmable Logic Controller
QoS	Quality of Service
SCADA	Supervisory Control and Data Acquisition
SPE	Single-Pair Ethernet
TSN	Time-sensitive Networking
UADP	Unified Architecture Datagram Packet
UDP	User Datagram Protocol

OPC FOUNDATION HEADQUARTERS
OPC Foundation
16101 N. 82nd Street, Suite 3B
Scottsdale, AZ 85260-1868 USA
Phone: 480 483-6644
office@opcfoundation.org

OPC FOUNDATION EUROPE
opceurope@opcfoundation.org

OPC FOUNDATION CHINA
opcchina@opcfoundation.org

OPC FOUNDATION JAPAN
opcjapan@opcfoundation.org

OPC FOUNDATION KOREA
opckorea@opcfoundation.org

OPC FOUNDATION ASEAN
opcasean@opcfoundation.org

OPC FOUNDATION INDIA
opcindia@opcfoundation.org