

基于 OPC UA TSN 技术的工业数据通讯解决方案

原作者

Dietmar Bruckner¹, Rick Blair², Marius-petru Stanica³, A. Astrit Ademaj⁴, Wesley Skeffington⁵, Dirk Kutscher⁶, Sebastian Schriegel⁷, R. Wilmes⁸, Karl Wachswender⁹, Ludwig Leurs¹⁰, M. Seewald¹¹, Rene Hummen¹², E-C. Liu¹³, S. Ravikumar¹⁴

(1. 贝加莱工业自动化; 2. 施耐德电气; 3. ABB; 4. TT Tech; 5. 通用电气; 6. 华为技术; 7. Fraunhofer IOSB-INA; 8. 菲尼克斯电气; 9. 英特尔; 10. 博世力士乐; 11. 思科; 12. 赫斯曼; 13. 摩莎; 14. KalycitoInfotech)

编译

宋华振, 周晓霞, 朱亮

(贝加莱工业自动化(中国)有限公司, 上海 200233)

摘要: 在工业自动化系统集成中, 不同厂商一般都有自己的数据通讯标准和协议。目前工业数据通讯领域由基于以太网的各类现场总线系统主导, 虽然它们有着相似的要求和细分市场, 但是它们的实施和生态系统差别却很大。价值链中的利益相关者通常在其特定技术的决策方面并不完全一致, 因此, 终端客户和设备制造商不得不购买和掌握诸多产品和技术, 这就大大提高了使用成本。时间敏感网络 TSN 与 OPC UA 的结合, 能够实现从现场层、控制层、管理层直到云端的数据通讯。OPC UA TSN 作为独立于某一特定厂商的后继技术, 将 IT 和 OT 无缝融合到现场总线项目中, 可以获得良好的适用性并实现更高水平的自动化配置。我们发现, 通过选择正确的一系列功能特性, 它能够满足今天和未来的工业通讯要求, 同时在此期间还可利用标准以太网硬件的成本效益。当保持每种方法的独特性能时, 由 AVB 演变而来的 TSN 网络基础架构还同时能够执行各类工业通讯任务。OPC UA 是针对嵌入式应用的源自 OPC 通信标准的一项重大演进。被描述为发布/订阅的最新进展则更进一步, 旨在为嵌入式设备在较小空间内优化性能。增加了用于描述数据的元模型, 以及用于交换和浏览信息的通讯基础架构。此外, OPC UA 还带有一个内置的安全模型, 可以根据即将出台的标准, 如 IEC 62443 来帮助实施安全系统。我们期望, OPC UA TSN 将会很快被认为是工业自动化领域内的游戏规则改变者, 成为建立从传感器到云端的整体通讯基础架构的首要也是唯一的候选者。

关键词: 工业数据通讯; OPC UA TSN; IT 和 OT 无缝融合; 循环周期; 数据链路层

中图分类号: TN915 **文献标识码:** B

Solution of Industrial Data Communications Based on OPC UA TSN

Original Authors

Dietmar Bruckner¹, Rick Blair², Marius-petru Stanica³, A. Astrit Ademaj⁴, Wesley Skeffington⁵, Dirk Kutscher⁶, Sebastian Schriegel⁷, R. Wilmes⁸, Karl Wachswender⁹, Ludwig Leurs¹⁰, M. Seewald¹¹, Rene Hummen¹², E-C. Liu¹³, S. Ravikumar¹⁴

(1. B&R Industrial Automation; 2. Schneider Electric; 3. ABB Automation Products; 4. TTTech Computertechnik; 5. General Electric Company; 6. Huawei Technologies; 7. Fraunhofer IOSB-INA; 8. Phoenix Contact Electronics; 9. Intel Corporation; 10. Bosch Rexroth; 11. Cisco Systems; 12. Hirschmann Automation and Control; 13. Hirschmann Automation and Control; 14. Kalycito Infotech)

Editors and Translators

SONG Hua-zhen, ZHOU Xiao-xia, ZHU -liang
(B&R Industrial Automation (China) Co., Ltd., Shanghai 200233)

Abstract: In industrial automation system integration, generally, each of manufacturers has own standard and protocol for data communication. At present, industrial data communication domain is dominated by Ethernet-based diverse fieldbus systems, although they share similar requirements and market segments, but their implementations and ecosystems are very different.

Stakeholders in the value chain are usually not completely consistent in their decisions for particular technologies, therefore, end customers and device manufacturers have to purchase and master numerous products and technologies; as a result, the cost of using is greatly increased. The combination of time-sensitive network (TSN) and OPC UA is able to realize the data communications from field layer, via control layer and management layer and till to the cloud. By means of OPC UA TSN, that as a specific vendor-independent successive technology, IT and OT are fused into the project of fieldbus seamlessly, thus a well applicability can be obtained and an automation configuration with higher level can be realized. We have found that, by choosing a series of correct functional features, OPC UA TSN is able to meet the industrial communication requirements both for today and the future, meanwhile the cost benefits of standard Ethernet hardware can be utilized in the mid-term. The TSN network infrastructure as an evolution of AVB is simultaneously able to carry out all types of industrial communication tasks, while maintaining the individual properties of each method. OPC UA is a major evolution from the OPC communication standards targeting embedded usage. The latest evolution described as Publish/Subscribe goes further and is aimed at embedded devices, optimizing performance in small footprints. A meta model and a communication infrastructure are added, the former for describing data, and the latter for exchanging and browsing information. Moreover, OPC UA comes with a built-in security model that helps implement secure systems in accordance with upcoming standards like IEC 62443. We anticipate that OPC UA TSN will quickly reveal itself as a changer of game rule in the field of industrial automation, become the first and only candidate for establishing a holistic communication infrastructure from the sensor to the cloud.

Keywords: industrial data communication, OPC UA TSN, seamless fusion of IT and OT, cycle period, data link layer (DLL)

0 引言

在工业自动化系统集成中，客户的系统编程和组态软件工具，当然也包括数据通讯协议，通常由组成该系统的 PLC 或 DCS 供应商提供，不同厂商一般都有自己的数据通讯标准和协议。目前工业数据通讯领域由基于以太网的各类现场总线系统主导，虽然它们有相似的要求和细分市场，但是它们的实施和生态系统差别却很大。它们中的大多数都拥有相应的联盟组织，由一家大的市场参与厂商引导和资助，并推动技术的发展。价值链中的利益相关者通常在其特定技术的决策方面并不完全一致，因此，终端客户和设备制造商面临着众多产品和技术需要生产、运行、诊断、维护和储备。虽然对产品和服务的可用性基本满意，但是应对多个解决方案会产生高昂的成本，并限制了 IoT 能力。时间敏感网络 TSN 从实质上说是一种能使以太网具有实时性和确定性的新标准。比如 Profinet 不适合连接云端和移动设备，OPC UA 不适合用于现场级通讯控制，但 TSN 能把诸如 Profinet 等实时以太网现场总线和 OPC UA 共享到同一个通讯设施上，识别底层 IO，实现从现场层、控制层、管理层直到云端的数据通讯。OPC UA TSN 作为独立于某一特定厂商的后继技术，将 IT 和 OT 无缝融合到现场总线项目中，可以实现比以往更高水平的自动化配置。此外，由于 OPC UA 和 TSN 并非紧密地与某一特定厂商绑定，从而可大大减少出于非技术原因的人为干预，其适用性也要比过去不同的现场总线宽广得多。

1 工业数据通讯

1.1 工业自动化系统数据通讯的金字塔结构

今天的工业数据通讯主要是按照自动化系统金字塔来组织的，可参见图 1 (a) 到 (c)。在塔顶的计算机层，使用标准的 IT 协议（互联网协议¹）。对于机器间和过程通讯（分布式控制器层）而言，相较传统的基于以太网的 M2M 现场总线系统（PROFINET³、EtherNet/IP⁴、CC-Link IE⁵），OPC UA（IEC 62541²）所发挥作用的重要性正在迅速提高。在机器内部（设备和传感器层），具有硬实时能力（也被称为实时以太网）的协议占据主导地位⁶。根据市场份额，最重要的协议是 EtherCAT⁷、PROFINET IRT⁸、POWERLINK⁹ 和 Sercos III¹⁰。虽然这些技术有着共同的要求，但是它们的实施差别很大。因此，比较它们是一件复杂的事情，并且很大程度上取决于预期的应用（过程控制、运动、I/O、集中式和分布式控制等）。努力比较各种实时以太网协议在多个类别中的性能已经由 Ethernet POWERLINK 标准化组织（EPSG）¹¹ 承担。

相关注释与参考链接：

¹https://en.wikipedia.org/wiki/internet_protocol_suite

²<https://opcfoundation.org/about/opc-technologies/opc-ua/>

³<http://www.profibus.com/technology/profinet/>

⁴<https://www.odva.org/Technology-Standards/EtherNet-IP/Overview>

⁵<https://www.cc-link.org/en/cclink/cclinkie/index.html>

⁶全球范围内，工业以太网和传统现场总线系统目前声称可比的工业通讯市场份额。新的开发主要使用基于以太网的系统，从而导致更高的增长率。具有传统现场总线接口的设备越来越多地被替换，并仅用于传统产品和工厂。

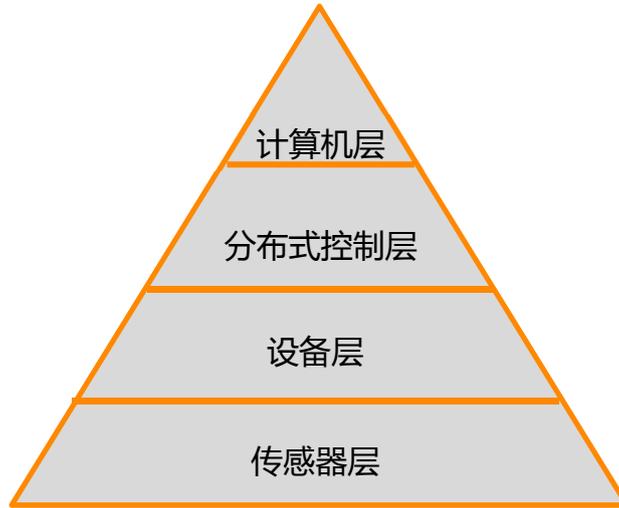
⁷<https://www.ethercat.org/en/technology.html>

⁸<http://www.innovasic.com/news/industrial-ethernet/profinet-rt-vs-profinet-irt/>

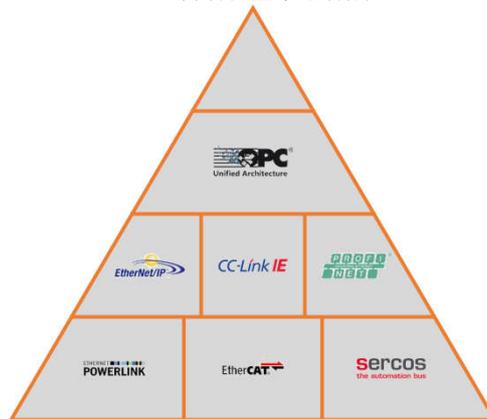
⁹<http://www.ethernet-powerlink.org/en/powerlink/technology/>

¹⁰<http://www.sercos.org/>

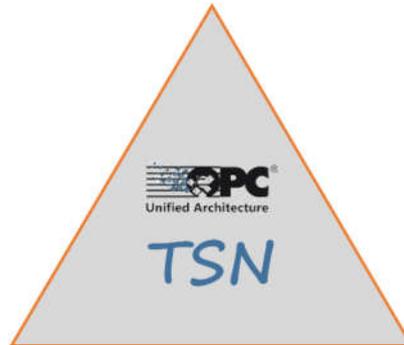
¹¹<http://www.ethernet-powerlink.org/en/downloads/industrial-ethernet-facts/>



(a) 自动化金字塔各层



(b) 现今自动化金字塔中独特的生态系统



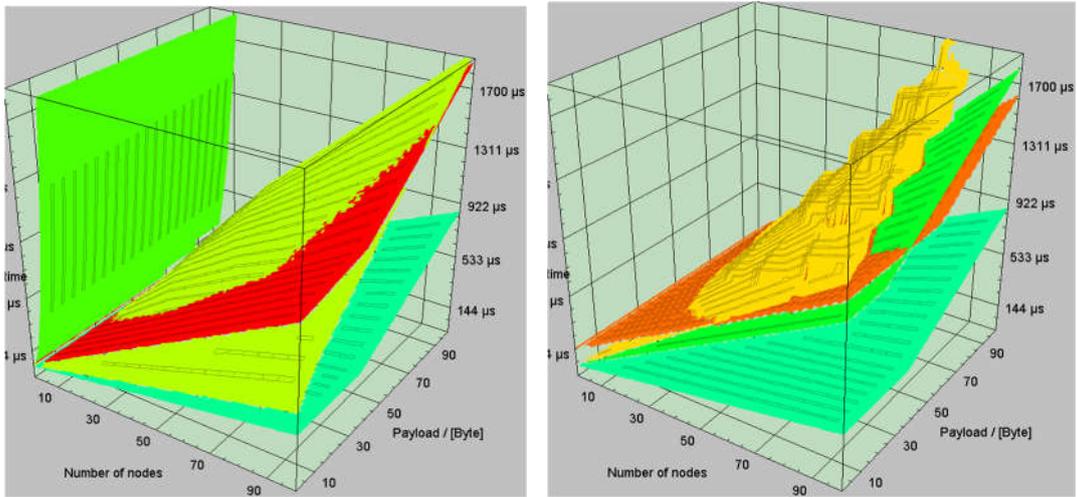
(c) 使用 OPC UA (和 TSN) 实现从传感器到云端的全面通讯

图 1 自动化金字塔-不同层面的通讯需求

1.2 主流通讯协议的循环周期比较

多年来，一直倾向于根据它们各自的功能集比较工业以太网技术。

1.2.1 最小循环周期比较@100Mbit

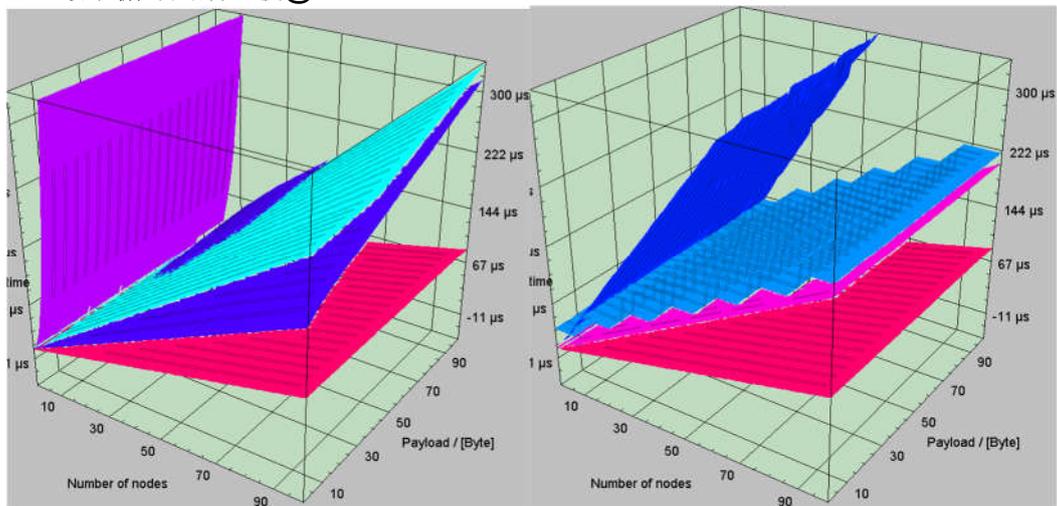


(a) 浅绿色: Modbus/TCP
 黄绿色: SERCOS III
 红色: POWERLINK
 水绿色: OPC UA TSN

(b) 深橙色: Profinet IRT[®]
 绿色: EtherNet/IP
 淡橙色: EtherCAT[®]
 水绿色: OPC UA TSN

图 2 最小循环周期比较@100Mbit

1.2.2 最小循环周期比较@1Gbit

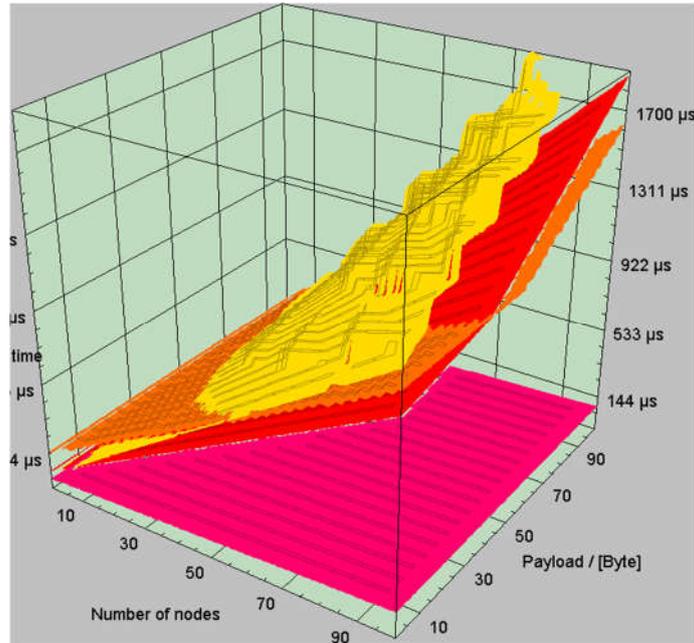


(a) 紫色: Modbus/TCP
 深蓝色: SERCOS III
 淡蓝色: POWERLINK
 品红色: OPC UA TSN

(b) 灰蓝色: Profinet IRT[®]
 粉红色: EtherNet/IP
 中蓝色: EtherCAT[®]
 品红色: OPC UA TSN

图 3 最小循环周期比较@1Gbit

1.2.3 OPC UATSN @1Gbit 的最小循环周期与现有技术比较



深橙色: Profinet IRT^{*)}
 淡橙色: EtherCAT^{y)}
 红色: POWERLINK
 品红色: OPC UA TS

图 4 最小循环周期与现有技术比较 OPC UATSN @1Gbit

从 1.2.1 到 1.2.3 可知, 图 2a 和图 2b @100Mbit, 图 3a 和 3b @1Gbit, 图 4 则显示了 OPC UATSN @1Gbit 与现今的 100Mbit 技术的比较, 直至设备最多 100 个, 有效载荷最大 100 byte。以下参数已被使用:

- 总线型拓扑, 输出数据 = 40%的输入数据, 交叉通信用于 20%的设备
- 转发延迟@100Mbit: TSN: 3μs, 开关: 10 μs, PLK: 0.76 μs, EC: 1.35 μs, SER: 0.63 μs
- 转发延迟@1Gbit: TSN: 780 ns, 开关: 2 μs, PLK: 0.76 μs, EC, 0.85 μs, SER: 0.63 μs
- 25%的设备是由 20 个插片式模块化 I/O 组成 (仅影响 EtherCAT)

品红色和水绿色平面的实现使用了 OPC UA Pub/Sub, 它在原始以太网上采用了帧聚合技术。然而, 使用 Pub/Sub over UDP/IP 可能会显示不可区分的平面, 而使用单帧可能会增加有效载荷的循环周期超过约 50 bytes。

图 4 显示, 具有千兆位物理层的 OPC UA TSN 的有利实施优于现有解决方案 (基于 100M bit) 大约 18 倍。

有关注释:

^{*)} Profinet IRT 的循环周期始终是 31.25 μs 的倍数

^{y)} 循环周期平面上的隆起代表使用新的以太网帧

表 1 计算循环周期的符号

术语	符号	单位
最小循环周期	Γ	s
传输延迟	τ	s
网络设备延迟	l	s
传播延迟	δ	s
链路容量	C	Bits/s
有效载荷	x	bytes
网络设备数量	n	-

然而, 更重要的是, 特别是在运动控制应用中技术的性能, 它根据为特定应用实现的最小循环周期^[1]进行测量。它可以被看作是最具挑战性的度量, 如果一项技术满足这项要求, 它也可以在

实时性要求较小的环境中得以利用。可实现的最小循环周期是 PLC 发送全部输出至其从站¹²并接收到所有输入所需的时间。重要的是，所有从站都要在相同的循环¹³内接收到来自于 PLC 的输出。[2]介绍了一个基本的方法，用于估算几种技术的最小循环周期。它们的贡献包括显示相应的最小循环周期的二维图作为设备数量的函数。以下将提供基本机制的综述。EtherCAT（简称：EC）和 Profinet IRT（PN）在所分析的技术之中，将要作为采用帧聚合和基于交换式以太网的技术的例子。

循环周期的第一个组成部分是链路传输延迟（符号，见表 1）。这是指通过一条具有特定链路容量的线路发送所有帧所需的时间。集总帧的基本方程是：

$$\tau = \frac{8(\text{header} + \max(\text{remainder}, n \times \text{subheader}))}{C}$$

remainder 是填充最小尺寸的以太网帧（84 bytes，包括帧间距）所需的 bytes 数量。具体针对 EC 而言，公式可转换为¹⁴：

$$\tau = \frac{8(40 + \max(44, n \times (x + 12)))}{C}$$

应当注意的是，这个公式只考虑了一个帧。如果最大的以太网帧大小不够，必须发送至少一个最小尺寸的帧。另外，由于设备订阅有效载荷不能跨多个帧分割，因此最大的以太网帧大小将不会达到，数据将不得不在第二（第三，...）帧中发送。

循环周期的第二个组成部分是帧通过网络基础架构包括电线在内的传播延迟。对于 EC 而言，帧通过整个网络发出并送回，导致最小循环周期为：

$$\Gamma = (2n - 1)l + 2n\delta + \tau$$

有关注释：

¹² 所有传感器和执行机构也被称为“节点”。

¹³ 有赞同转移循环的论据，即循环开始和结束于与 PLC 相比具有规定偏移量的从站。但是，这种优化取决于技术和应用，因此省略一般的比较。

¹⁴ 方程中的特定数字总是表示 header 的大小、最小以太网帧中的有效载荷空间和订阅消息 header 的大小。相关详细解释，请参阅其它脚注中的协议定义。

对于 PN，必须考虑每个节点各帧，致使每帧¹⁴ $\tau = \frac{8(38 + \max(46, 6 + x))}{C}$ 。

这将假定帧预定依次到达 PLC，然后第一个从站的帧通过一个基础架构加上一根电缆。这导致最小循环周期为：

$$\Gamma = \delta + l + n \times \tau$$

这里介绍的所有方程都假设了简单的情况，其中输入和输出数据量相等，拓扑结构为完美的总线型。然而在实际应用中，这种比较取决于许多其它参数：

- 输入数据与输出数据的比率
- 具有直接交叉通信的设备的百分比
- 利用不同的循环周期
- 拓扑结构（总线型、星型、环型），以及设备之间的跳数
- 带有自己背板总线的模块化 I/O 的可用性

假设更具现实价值的结果如图 2a –图 2b（使用 100 Mbit）所示。使用不同的链路容量（1 Gbit）明显改变了这种情况，因为只有循环周期的传输延迟成分–而非网络基础结构成分–可以减少 10 倍（见图 3a - 3b）。因此，对基础结构具有较大依赖性的技术（EtherCAT、Sercos III、POWERLINK）在使用千兆位时的性能平均提高了 4 – 6 倍。相比之下，基于交换式以太网的技术（EtherNet/IP、Profinet IRT）可将足够大的有效载荷提高 7 – 10 倍。对于较小的有效载荷，短帧的传输延迟可能比基础结构的延迟小，导致总线中最小循环周期的下限较低。今天针对 Gbit 的 COTS 直通式交换机具有 2 μs 范围内的转发延迟（图 3b），这意味着最小帧大小为 250 bytes（= 2000 bits）（忽略电缆上的传播延迟）。发送较小的帧不会进一步减小循环周期。因此，在具有较高性能要求的应用中，转发延迟短的设备至关重要。OPC UA TSN 循环周期的计算是上面介绍的两种方法的组合。具有 Pub/Sub 值的帧传输延迟–由于帧聚合和高效的帧格式–变为¹⁴：

$$\tau = \frac{8(51 + \max(33, n \times (x + 3)))}{C}$$

总的最小循环周期变为：

$$\Gamma = \delta + l + \tau$$

可以注意到，相比今天建立在各种参数组合上的解决方案，可实现的循环周期更低，大约低了 18 倍（参见图 4）。若现今的现场总线技术机制不变，相比具有千兆位电路的假想设备则低了近 2 倍（参见图 3a – 3b）。

1.3 工业数据通信类型

开发新的 OPC UA TSN 系统的公司拥有多种 TSN 标准，从中可以为他们的应用选择正确的功能特性。这通常涉及到尝试尽可能接近地匹配传统技术的行为。外推到整个工业自动化市场，这告诉我们，为了得到广泛采用，一个解决方案必须同时支持所有当前使用的工业通信类型。

今天的技术实现了各种通信类型。它们大多数都考虑到了区分周期性和非周期性通信，而在它们实际属性的细微差别方面又有所不同—从每个循环拥有不同发送、传播和接收周期的硬实时通信；到有或无时间同步的周期性通信；到多种来源的非周期性通信，其中 TCP/IP 就是一个越来越重要的例子。在有些情况下，网络控制、诊断信息和用户控制消息有不同的优先级。我们已经评估了这些，并得到了一个超集。通过工业通信系统实现通讯的通信类型可以概括在下面的表 II 中。一个融合的网络需要支持所有这些类型（例如，见图 10），即使不在特定应用中使用。用于实施的形成机制的选择需具备全球化标准；这里介绍目前讨论的一个提案。

注意：TSN 的主要特点是不同通信类型共存的可能性，同时保留实时通信的定时特性。一些现有的“实时”（EtherNet/IP、Profinet）网络使用通信规划和 QoS 来保证在设备运行良好条件下的行为。由于将 TSN 用作数据链路层，因此这些技术可以更好地利用带宽效率，因为 TSN 无条件保护了高优先级的通信（请参阅[3]中 ODVA 的性能考虑，表 1）。

2 设置

计算理论性能估计和定义通信类别要求是一回事—具有硬件和/或软件限制的现实世界实现是完全不同的事情。百兆工业以太网技术已经达到了非常高的成熟度，这意味着几乎所有的现有设备都能够提供全面的网络性能。对于千兆技术而言，事实并非如此。如上所述，千兆将交换网络的性能提高了约 10 倍。帧聚合、优化标头和超低直通延迟可以进一步提高约 2 倍。为了在真正的产品中利用该性能，其许多组件都需要进行优化。

许多原型设备已经实施并由作者测试，例如在 IIC 试验台上。其中两个原型已被用于本文中评估：一个是基于运行 Linux 的单端口工业 PC，另一个嵌入式的形式为模块化 I/O 模块的头站，具有两个外部网络端口，也运行 Linux OS。图 5 描述了使用这些设备的测试设置的主要拓扑结构；图 6 则表现了设备构成。它包含 200 个嵌入式节点（贝加莱），具有数字量 I/O 模块和一个工业 PC。另外，它包含五个高清摄像头（Mobotix）和一个标准工业面板。此外还用到了工业 TSN 交换机（TTTEch）。200 个设备部署在四条总线中，每条线 50 个设备。可实现的性能报告在第 7 部分中。

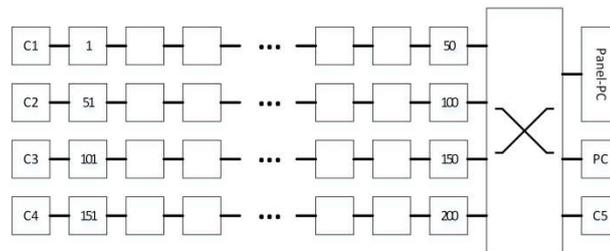


图 5 测试设置的主要拓扑结构



图 6 测试设置的设备构成

3 标准和技术

3.1 概述

图 7 提供了 OPC UA TSN 所使用的协议和服务的概述以及它们如何适应 ISO/OSI 参考模型的各层。以下将讨论各层的要求和特性。

3.2 物理层

以下的物理介质是工业网络中使用最广泛的，因此大多数厂商都会提供：

基于铜

- Fast Ethernet (100BASE-T/T1)
- Gigabit Ethernet (100BASE-T/T1)

基于光纤

- Fast Ethernet (100BASE-T/T1)
- Gigabit Ethernet (100BASE-T/T1)

对于过程自动化，已经成立了一个工作组来开发十兆单双绞线以太网（10SPE）。该介质可以促使以太网传播至更小和成本更敏感的传感器和执行机构设备以及 Zone 1 危险区。

表 2 工业通信类型

第 3 - 9 列表示每种类型的要求

ID	工作名	保证	应用同步至网络	相位协调的动作	定期/零星	带宽预留	数据大小	需要冗余机制	通信整形 [§]
I	同步	截止期限	Y	Y	P	Y	受限	无缝	Qbv
II	网络控制	优先级	Y	-	S/P	-	小	不相关	SP ^y
III	周期性	有界延迟 ^z	可选		P	Y	受限	无缝	Qbv
IV	音频/视频	有界延迟 ^z	N/A		S/P	Y ^y	受限	常规	Qbv+Qav+SP ^y
V	报警/事件	带宽	-	-	S/P	Y ^y	未知	常规	Qbv+SP ^y
VI	管理/诊断	带宽	-	-	S	Y ^y	未知	常规	Qbv+SP ^y
VII	预留				用户特定				
VIII	尽力而为	无	-	-	S/P	-	未知	常规	无

有关注释：

^x) 未使用的带宽可以被较低优先级的通信使用

^y) 严格优先级通信选择算法

^z) 有界延迟保证包含带宽保证

[§]) 建议，见图 8 例子

3.3 数据链路层

术语 TSN^[4] ^[5]是指由 IEEE 802.1¹⁵ 工作组的时间敏感网络任务组开发的一系列标准。这里值得注意的是，802.1 标准化了以太网交换机（他们称之为“网桥”），802.3 标准化了以太网端点。下列介绍与工业通讯相关的标准：

IEEE 802.1AS-Rev: IEEE 1588-2008 时钟同步标准的协议是为了解决导致 IEEE 802.1AS^[6]中更大的以太网系统而开发和采用的。可惜两者并不兼容。在 TSN 工作组中，正在开发 IEEE 802.1AS (.1ASRev^[7]) 的修订版。此修订版解决了最高级冗余和多时钟域（例如，同时分配工作时钟（同步传输的基础）和挂钟（例如，记录消息））的机制。.1AS-Rev 计划于 2018 年发布；出于互操作性和接近最终方案的考虑，我们强烈鼓励机器、工厂和过程自动化厂商实施.1AS（而不是 IEEE 1588）。另外，802.1AS 是 AVnu 和 IEEE TSN 任务组推动的默认解决方案。

IEEE 802.1Qbv: 用于实时保证的同步传输。它规定了传输窗口¹⁶，以保证有界延迟和较小抖动^[8]。Qbv 也可以周期性地给予出口队列优先接入线路，所以它也可以提供带宽保证。

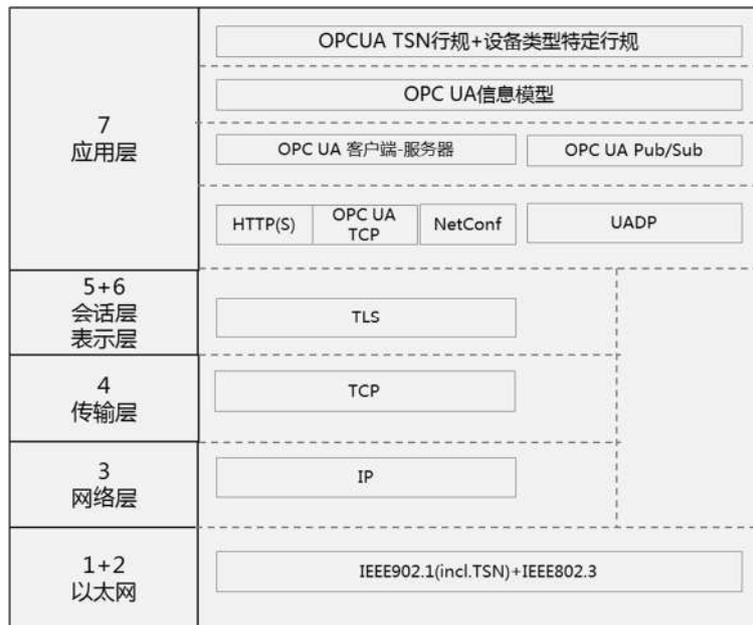


图 7 OSI 参考模型中 OPC UA TSN 的描述

IEEE 802.1Qav: 可用于周期性传输，以保证某些通信类别^[9]拥有带宽预留和有界延迟。主要的应用是音频/视频广播¹⁷。

相关注释和参考链接：

¹⁵<http://www.ieee802.org/1/pages/tsn.html>

¹⁶按照“门开闭”时间值

¹⁷由于采用流预留协议，将它用于循环过程数据交换也具有吸引力，无需事先配置。然而，动态添加的流会影响已配置的流的保证（不会通知它们），这使得很难预测系统（和通信负载）更新的融合网络中更长时间段的行为。

IEEE 802.1Qcc: 该标准提供了用于 TSN 配置的协议、程序和管理对象的规范，主要用于已经运行的系统。描述了以下三种配置模型：

- (1) 完全集中式模型—适用于所有 TSN 机制，在使用 Qbv 时是必备的（见图 8）；
- (2) 完全分布式模型—适用于无需改变调度（或不使用 Qbv 机制）时；
- (3) 集中式网络/分布式用户模型。

由于同步通信经常用于工业网络（见图 10 示例），Qbv 机制的使用是必然的，因此，我们使用完全集中式的配置模型。该模型指定了 CUC（集中式用户配置）和 CNC（集中式网络配置）功能^[10]。CUC(s)指定了关于循环周期和传输的过程数据的用户要求，并将其传输给 CNC。CNC 会计算 TSN 配置，包括通讯调度必须通过使用标准的 YANG¹⁸模型满足要求。CNC 使用基于 YANG 的管理协议（如 NETCONF¹⁹over TLS²⁰）将配置分配给交换机（网桥）。CNC 将端点配置发送到 CUC。RESTCONF²¹应用作 CUC 和 CNC²²之间的通讯协议。CUC 然后将端点配置分发到相应的端点。

TSN Configuration Broker (TCB): Qcc 不会进一步指定协议以及 CUC 和端点之间的功能（因为这是专用的）。当工作在 OPC 基金会 TSN 工作组内针对基于 OPC UA Pub/Sub TSN 的系统标准 CUC 接口上时，所有 CUC 的共同功能已被确定和进一步明确。TSN Configuration Broker (TCB)一方面从端点提取出了不同的 IEEE Qcc 配置模型，另一方面为流预留/实例提供了标准化的功能。TCB 由驻留在端点的 TCB 客户端和集中式 TCB 服务器组成（见图 7）。TCB 客户端与服务器之间的 PTCB 协议非常轻便。除了通常适用于所有 CUC 之外，这是一种接收基本网络配置的有效方式，特别适用于几乎不需要应用程序配置的资源受限设备（因此没有可用的 OPC UA 客户端或服务端）。

IEEE 802.1CB: 用于为环型和网格拓扑^[11]提供无缝冗余。1CB 允许冗余规划在每个数据流的基础上，这样可以实现比传统冗余解决方案更好的带宽效率。

相关参考链接和注释：

¹⁸<https://tools.ietf.org/html/rfc6020>

¹⁹<https://tools.ietf.org/html/rfc6241>

²⁰<https://tools.ietf.org/html/rfc5246>

²¹<https://tools.ietf.org/html/rfc8040>

²² 如果两者都托管在单个设备（例如工程工具或 PLC）上，那么 CUC-CNC 通讯不一定涉及协议。

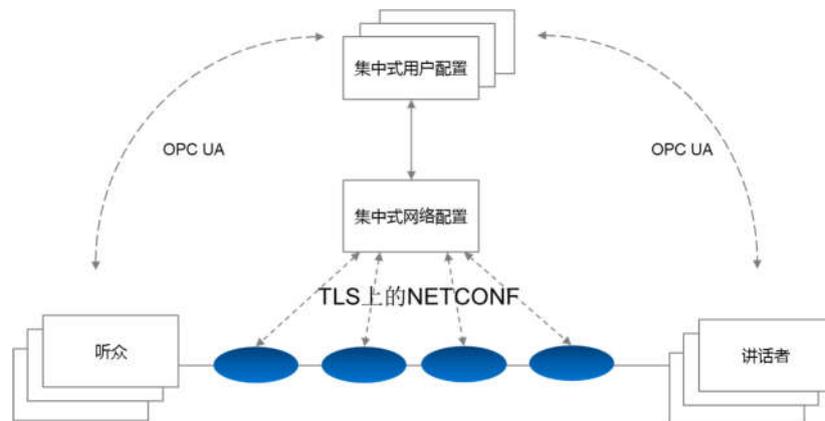


图 8 Qcc 的完全集中式模型（带有 OPC UA 应用程序），取自[4]

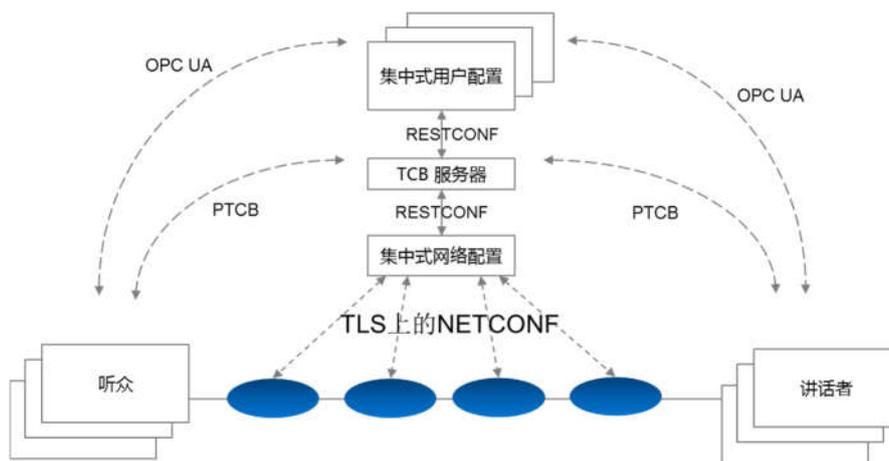


图 9 包含 TCB 的完全集中式模型

更多标准

IEEE 802.1Qbv & IEEE 802.3br（可选）²³

在使用调度（Qbv）机制的情况下，帧抢占^[12] ^[13]可以用来最大化尽力而为业务的吞吐量。抢占不适合尽力而为以外的通信类型，因为它会使这些通信类型的任何保证无效。然而在千兆的情况下，尽力而为的增益微不足道²⁴。

IEEE 802.1CS（可选）

AVB 的流预留协议扩展。该项目刚刚发起。它定义了一个可供选择的–目前不兼容–配置路径（也称为“完全分布式配置模型”），适用于 III 类通信（和尽力而为）的应用，因此在工业应用中的使用有限。

总结

因此，强制性标准是 .1AS(-Rev)、Qbv、.1CB 和具有完全集中式模型的 Qcc，再加上 NETCONF over TLS。AVnu 联盟正在定义实施这些标准的一致性和互用性准则。

3.4 第 3-6 层

对于 OPC UA 客户端/服务器，支持带可选安全（TLS）的 TCP/IP 连接。对于 Pub/Sub 连接，支持 UADP²⁵ over UDP/IP 或直接在原始以太网上的 UADP。安全在 UADP 层中进行处理。UADP（即云协议）的其它传输选择超出了本文的范围。

NETCONF 也使用带 TLS 的 TCP/IP。

对于设备上的固件升级和 Web 应用程序，可选用 HTTP(S)。

3.5 应用层

OPC UA 在应用层上采用，包括支持客户端/服务器和发布/订阅通讯模型。所有设备上的 OPC UA 服务器应支持嵌入式服务器协议。对于资源有限的设备，只能利用发布功能提供数据和 TCB 客户端进行网络配置。

- **客户端/服务器：**用于设备配置、浏览信息模型、记录诊断信息等的通讯模型。对于安全应用程序，设备配置应提供数据完整性（签名）和可选的机密性（加密）。

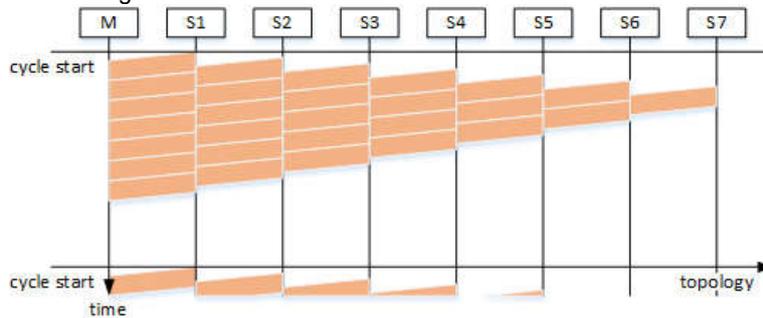
- **发布/订阅（简称：Pub/Sub）：**用于循环传输的通讯模型。通过使用基于 OPC UA 消息的安全，可选签名和/或加密。具有静态数据集偏移的标头协议可用于在终端站中高效地提取数据集。

相关注释：

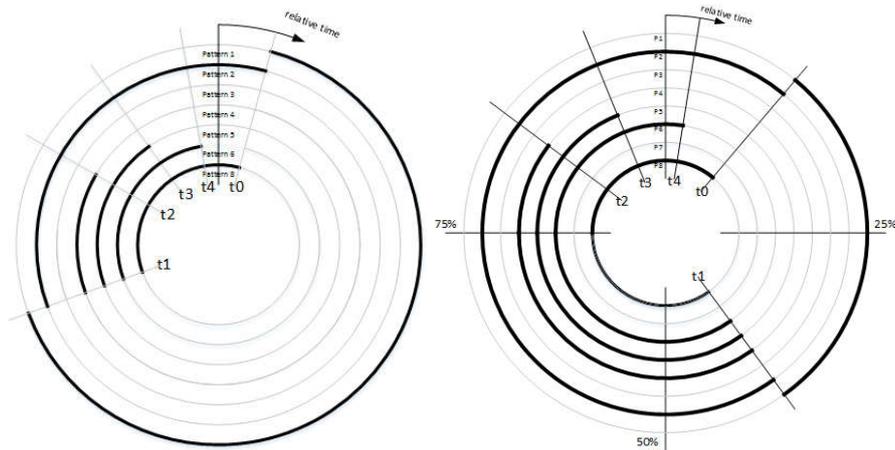
²³ 有两个与帧抢占相关的标准—一个用于网桥（.1Qbu），另一个用于端点（.3br）。

²⁴ 例如，最大尺寸的以太网帧（1.5 kB）需要 12.3 μ s 传输时间。考虑到 1 ms 的共同循环周期，当每个循环抢占一个这样的帧时，带宽利用率可以改善 < 1%。

²⁵ Unified Architecture Datagram Packet



(a) 调度中同步输入帧的时空图



(b).在主站内端口的 Qbv 门控事件 (c).在 S5 左端口的 Qbv 门控事件²⁶

图 10 网络调度示例

图 10 是在第 2 部分介绍的网络的调度示例，只是更小。它有一个主站（M）和七个从站（S₁...S₇）。在类型 1 中，所有从站都向主站发送相同大小的帧（图 10a）。调度计算是这样的，帧一个接一个不停地达到主站，在那里第一个从站在循环开始处发送它的帧。图 10b 显示了主站内端口的 Qbv 配置，它在那里接收帧（循环开始于 90°）。类型 1 的门在循环开始（t₀）不久打开，并保持打开，直到接收到所有帧后关闭（t₁）。在这段时间里，没有其它门打开。之后，类型 2-8 的门同时打开。类型 2 在所有剩余时间内保持打开，给予网络控制通信最高优先级（如果发生这种通信）。接下来，类型 4 的门关闭（t₂），给予类型 5 一些时间，具有最高优先级等等（t₃、t₄）。图 10c 显示了 S5 左端口的 Qbv 配置²⁷。类型 1 的门向朝向主站的三个帧（t₀...t₁）打开，随后打开其它类型的门。因此，在整个网络中²⁸，类型 4 至 6 和 8 的带宽保证是相同的。

相关注释：

²⁶ 所示调度代表尽量在网络中的每个位置可能利用“异步”带宽的最佳调度。但是，为了提高计算调度时的计算效率，整条线路可以使用与图 8a 相同的调度。

²⁷ 图 8a 和 8b 所示的各个调度均基于设备的各个时间。但是，预计设备间的同步足够支持这种方法，而且—简单起见—谈及一个网络共同的循环开始时间。

²⁸ 在这个例子中，类型 4 至 6 和 8 的保证是一样的约 8%。相同的尺寸仅用于描述，可能没有实际用例。

3.6 其它所需功能特性

ISO/OSI 参考模型（图 7）提供了一个涉及 OPC UA TSN 技术的协议栈的快速概览。为了满足工业通讯系统要求，需要以下其它功能特性：

设备角色：第 5 部分介绍了协调 OPC UA TSN 设备的网络启动和操作所需的功能特性。角色（几乎）独立于运行的硬件。

状态机：工业网络中的终端站必须有统一的行为，它根据状态机定义（见第 IV 部分）。这使得中心实例（即网络管理节点）协调整个网络成为可能。许多工业以太网解决方案实施的状态机基于 CiA 的想法^[4]。

拓扑检测：实时通信的调度需要了解网络拓扑结构。拓扑可以在配置工具中进行检测（使用 LLDP²⁹）和导入，或离线创建。CNC（第 5 部分）使用此信息来计算 Qbv 和 Qav 的配置。

直通交换：在交换式网络上可实现的循环周期性能很大程度上取决于帧传输的延迟（见 1.2 部分）。特别是对长的总线型或环型拓扑构成了挑战。因此，直通交换（一旦地址信息被解码就转发一个帧）³⁰ 构成了现场设备中 3 端口交换机不可或缺的一个功能特性。在使用千兆物理层时，转发延迟包括远低于 1 μs 的 PHYs 是必需的，即

$$l_{target} = 800ns$$

设备子协议：在工业通讯系统中，每个 OSI 层都需要确保互操作性。违反互操作性的最低层构成了整个系统互操作性的最高层，独立于任何更高层。传统工业以太网系统仅共享相同的物理介质（电缆、插头），即层 1。该事实已经引起了很多顾客的不满，因为原来的营销信息是以太网是以太网，所以它们都应该兼容。为了防止 OPC UA TSN 技术陷入相同的困境，其目标是使用所有七

个 OSI 层（用于设备间通讯）共同实施，此外还具有标准的设备子协议和特定类型的设备子协议。今天，针对安全、驱动器、IO 和控制器到控制器通讯的标准化子协议正在考虑中。

设备描述文件：在 OPC UA 领域内，一个设备由其服务器实例来表示，其功能特性可以“随时”在线浏览。虽然在线浏览对一些工业用例就足够了，它们具有很高的重复程度，如连续机器制造，但仍要求离线方法用于对设备进行配置和编程。因此，设备的所有相关功能特性（OPC UA、应用程序和网络功能）都需要在文件中进行描述，从而替代对设备的在线访问。

相关注释：

²⁹链路层发现协议 [15]

³⁰没有可用于直通交换的标准。反对它的主要理由是帧可能损坏，它只能使用帧结尾的 FCS 检测。此外，TSN 的有些功能特性，如流量限制部分与直通并不兼容。然而，性能争论超过了缺点。

4 配置和启动

现今，几乎所有现场总线系统—无论是否基于实时以太网—都提供网络管理的机制。这些机制会启动网络设备，通过一系列状态将其转换为操作状态；启动设备检测，在运行时处理和发出错误信号；或者执行必要的程序来替换故障设备。

状态和状态转换包括网络设备识别等功能（确保设备可以在网络上到达，匹配预期的厂商/型号等）。它们也可用于执行任何必要的配置/固件更新，随后通知设备传输有效的过程数据（如果设备上的应用程序准备好这样做），并评估收到的过程数据（如果控制网络的中央网络实例决定这样做）。

在各种现场总线系统中，许多现有的网络管理实施将所有这些功能结合在一个设备中（即 PLC）。这项工作的目标明确，就是将这些功能分离和解耦成所谓的设备角色，这样理论上每个角色都可以在网络内的不同设备上实施。多实例和设备角色冗余也应解决。图 11 显示了不同角色及其通讯关系。图 12 显示了启动时通过终端设备的状态机进行漫游。状态本身是强制性的。但是，如果地址和配置进行本地存储，那么大多数状态可以快速通过。

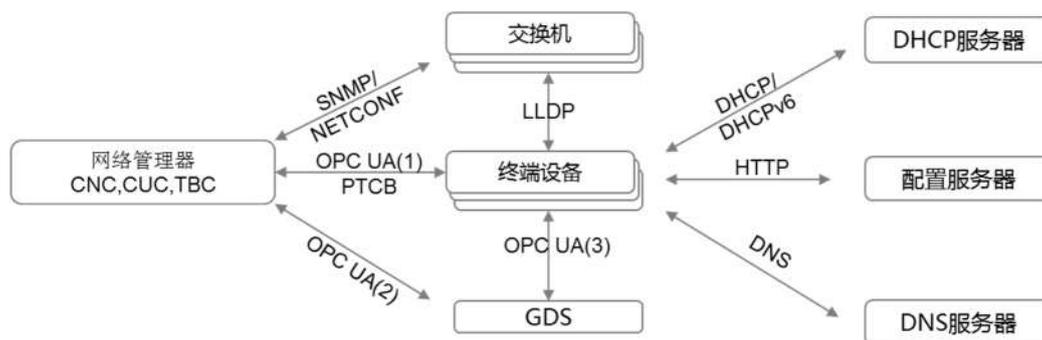


图 11 启动过程中的通讯关系

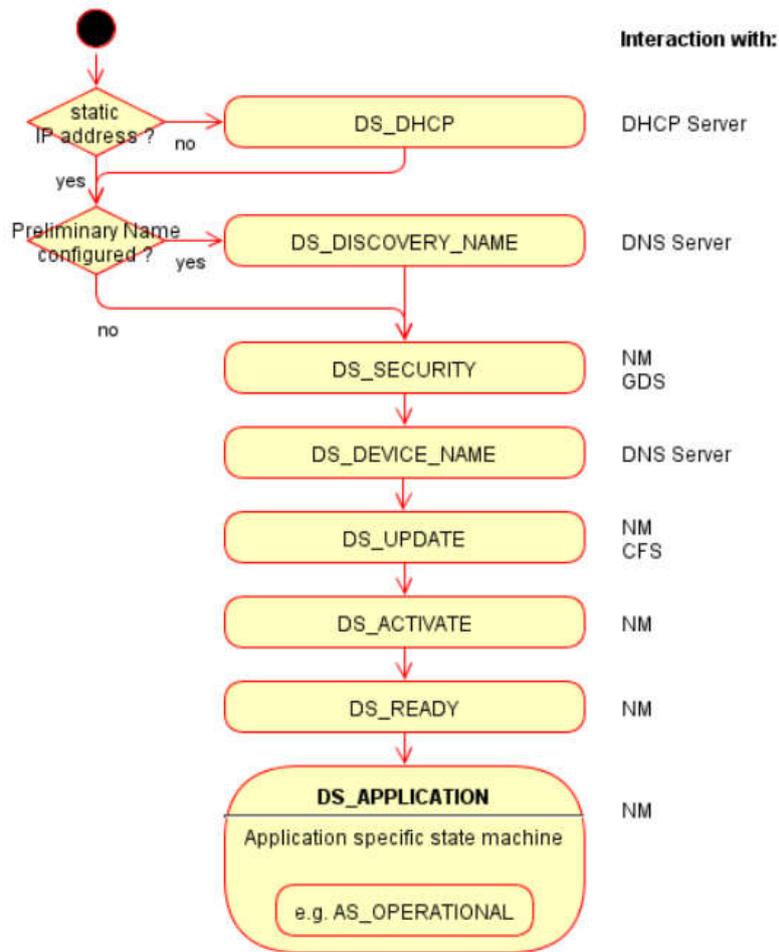


图 12 启动 OPC UA TSN 终端时的状态

5 角色管理

对于机器网络而言，需要一些网络功能，以达到启动和运行期间在网络中定义的状态。这些功能可以分组，并分配给设备角色。以下列出众所周知的针对 IT 和 OT 系统的设备角色以及针对 OPC UA TSN 的新设备角色。这部分结束时列出了用于开发和运行网络的用户角色。

5.1 当前需要的各角色

TSN 交换机：它们构成了一个 OPC UA TSN 网络的网络基础设施。多端口交换机用于从鸟瞰角度设置网络拓扑，而带两个外部（和一个内部）端口的交换机驻留在交换终端站，便于在总线型拓扑中进行有效布线。交换机的状态机添加状态以防止网络环路中的信息风暴，与图 10 所示状态相比。

DHCP（服务器）：DHCP³¹ 是一种从池中分配 IP 地址并将其分配给未配置的设备机制。此外，大多数 DHCP 服务器实施允许在第 2 层 MAC 地址和第 3 层 IP 地址之间进行静态绑定。这些功能特性的组合可以使用临时 IP 地址启动未配置的设备（具有未知的 MAC 地址），并且在成功识别后（可能是验证）- 分配预先配置的地址³²。

DNS（服务器）：DNS³³ 是解决 IP 地址描述性名称（即主机名）的机制。所有更高层协议和服务—包括工程和配置工具—随后都可以使用易于记忆的主机名。

祖时钟：该术语来自于针对精确时钟同步的 IEEE 1588 标准，已被 IEEE 802.1AS 采用。它指的是网络中具有主站功能的最精确的时钟设备。它可以通过最佳主时钟算法（BMCA）自动选择为网络的时间主站。或者在 .1AS 中，也可以预定义时钟层级。

相关链接和注释：

³¹<https://tools.ietf.org/html/rfc2131>

³²在安全情况下，强烈建议使用静态 IP 地址配置，另见^[16]。

³³<https://tools.ietf.org/html/rfc1034>, <https://tools.ietf.org/html/rfc1035>

OPC UA GDS: OPC UA 的全局发现服务器 (GDS) 负责 OPC UA 服务器的企业级管理。它通过“功能”和地址列表促进发现, 创建并分发针对安全连接的应用证书。

目录服务 (可选): 此类 IT 服务 (例如微软的活动目录) 用于企业级资产、用户和角色管理, 包括个人数据、访问权限 (对文件、程序)、证书管理等。在 OT 环境中使用这些可以在组织效率方面快速见效。

TSN CUC: 集中式用户配置 (CUC) 是一个在 IEEE 802.1Qcc 标准中定义的角色, 任务是配置终端节点 (或其应用程序-网络的用户)。这包括网络配置, 用于与 CNC 通讯。

TCB: TCB 客户端/服务器是 CUC-CNC 通讯功能加上终端站网络配置的标准化实施。TCB 服务器收到来自 CUC 的要求, 将要求转发给 CNC, 它会调度数据流并将结果报告给 TCB 服务器。最后, TCB 服务器会将如何使用调度的数据流的报告发回终端站。

TSN CNC: 集中式网络配置 (CNC) 有两个主要任务: (1) 计算网络调度 (2) 将网络调度的参数分配给基础结构组件 (以太网交换机)。

对于后者支持互操作性, 协议的选择很关键。截止今天, NETCONF 由于其广泛的可用性、技术成熟度和操作阴影配置的可能性已成为首选技术。

5.2 新的设备角色

以下列出网络中受现今现场总线架构启发的逻辑功能。为了运行 OPC UA TSN 网络, 实施这些角色并非严格强制。但是, 没有它们, 启动和运行网络将需要频繁、大量的手动干预。所有设备角色都是跨厂商的, 因此可以实现互操作。

应用从站: 这是具有最多实例的角色。它主要通过状态机来管理其操作模式和一些远程配置功能。例如 I/O、驱动器和阀。

应用主站: 传统现场总线中的 PLC 或边缘控制器的角色。从网络基础结构的角度来看, 应用从站和应用主站没有区别。但是, 就计算性能而言, 应用功能和 TSN 功能可能差别很大。

配置服务器: 这可以看作包含版本控制以及用于固件和配置的签名二进制文件的一个 (分布式) 数据库。文件内容是厂商特定的, 可以是驻留在设备上的任何东西-从 FPGA 比特流、编译的应用程序代码和配置文件, 到图像、数据表和维护视频。

网络管理器该角色连接到工程工具, 并保存关于应用程序分发的所有信息。网络管理器通过启动过程引导所有设备, 并触发所需动作, 如地址分配和固件/配置更新。

网络管理器: 该角色连接到工程工具, 并保存有关应用程序分发的所有信息。网络管理器通过启动过程指导所有设备, 并触发所需操作, 如地址分配和固件/配置更新。

5.3 用户角色

除了设备角色 (在授权执行某些管理功能如升级设备固件的网络上代表“用户”) 之外, 一组针对人与网络交互的预定义的用户角色应该是可用的, 如管理员、用户和维护。

6 安全性和证书

安全性可能成为区别 OPC UA TSN 和传统现场总线系统的一个关键的功能特性, 因为它无法被简单地添加到系统中。用于实施电子安全工业自动化和控制系统的国际标准 IEC 62443^[17], 与针对功能安全的 IEC 61508^[18]和 IEC 61784-3^[19]一样现已被广泛接受。标准要求使用适当的硬件和软件开发过程。此外, 它定义了五个安全防护目标等级, 从 0 (无) 到 4 (防护具备高教育、高动机和高资源的攻击者)。对于每个等级, 它定义了要求, 并提出了与特定的设备实施相关的问题。

6.1 证书

证书是安全认证的一种手段。OPC UA 采用 X.509 证书。例如, 为网络管理器设备角色创建的新证书要求具备该角色的每个设备都要拥有实例证书, 以便能够配置和控制设备。所有其它设备都配有公钥网络管理器证书, 因此可以建立一条信任链。此外, 每个设备都附带它自己的实例证书, 它是从设备类型证书派生而来的, 这个证书源自厂商证书。这样就可以建立信任链, 每家厂商都可以创建其自己的设备类型系列。设备类型和网络管理器证书可以在认证过程中获得。在首次认证后, 为每个设备创建和部署应用认证, 用于进一步认证过程。

6.2 证书类型

- 网络管理器
- 网络管理器实例
- 设备类型
- 设备类型实例

- 应用程序实例
- （机器）配置

7 结果

7.1 时间同步

时间同步的准确度通常通过各种环境条件下的外部 PPS 引脚（每秒脉冲）测量^[20]。图 13 显示了 50 个贝加莱 IO 设备在总线型拓扑中使用 .1AS 的结果（实际上是第 2 部分介绍的测试设置中的一条线路）。

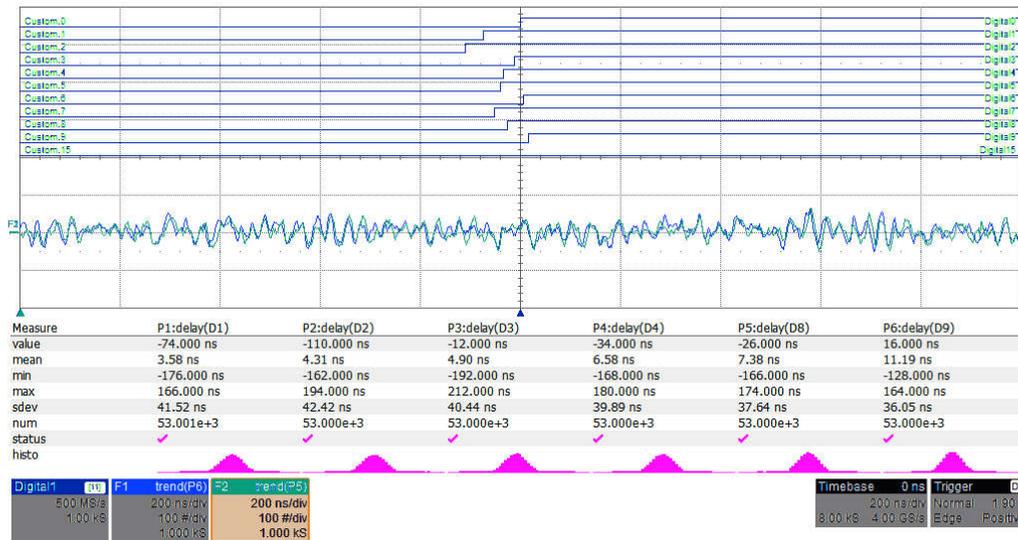


图 13 使用 IEEE 802.1AS 进行时间同步测量的结果

图 13 在 50 个设备的总线中使用 IEEE 802.1AS 进行时间同步的结果。每 10 个设备进行测量。在实验室条件下，PPS 精度³⁴的标准偏差远低于 50 ns。

相关注释：

³⁴在 .1AS 中的精确度是网络中两个时钟间的绝对差值。在我们的实例中，我们时钟对照祖时钟。

7.2 实时性能

根据工程工具的能力，对 OPC UA TSN 系统的大小和复杂性没有真正的限制。我们预计，中期将会出现多达 10,000 个设备的系统。

对于单个设备，所实现的最小循环周期完全取决于所使用的硬件和软件。我们期待设备很快具备 10 μs 循环周期。贝加莱的原型 I/O 站可在外部和背板总线上实现 50 μs。假定有一个强大的 PLC，其中 200 个可以在一根电线上运行 50 μs。

7.3 用户体验

用户体验的主要因素可以在设备或系统供应商的工程工具中看到。通常在机械自动化中，客户的工程工具来自于 PLC 供应商。但是，将 IT 和 OT 无缝融合到现场总线项目中可以实现比以往更高层次的自动化配置，独立于厂商，从而导致更少的人为干预³⁵。此外，由于 OPC UA 和 TSN 并非紧密地绑定在一个特定厂商上，因此我们期待周围的生态系统要比过去不同的现场总线大得多。

相关注释：

³⁵例如，基础结构交换机的静态配置可以通过工程工具自动计算，并由 PLC 分配。

8 结论与展望

OPC UA TSN 正在到来。它将在许多应用中取代今天基于以太网的现场总线。文中概述的主要原因是：

- 跨厂商
- 在其它领域广泛应用
- 融合网络
- 大而灵活的拓扑
- 完整的 IIoT 功能

- 无与伦比的性能
- 集成安全和
- 现代数据建模。

针对工业应用的相关 OPC UA 标准和 TSN 标准已经完成，少数未发布的标准将会在 2018 年年初发布。这些标准已经由众多国际市场参与者在国际试验台如 IIC 上得到实施和测试，并取得了可喜的成果。目前，主要的芯片制造商正在制造适用于现场设备互联的产品，以便很快就能与今天产品的成本相匹配。标准的以太网卡可用于单端口设备，因此无论如何无需讨论成本。对于双端口设备，预期边际硬件成本为 0 欧元，因为 TSN 将在不久的将来成为任何具有竞争力的工业级 SoC 的组成部分。因此，OPC UA TSN 将变得很平常—就像以前的 CAN 一样。

参考文献

- [1] J. Jasperneite, M. Schumacher, and K. Weber. "Limits of increasing the performance of industrial ethernet protocols," in 2007 IEEE Conference on Emerging Technologies and Factory Automation (EFTA 2007), Sept 2007, pp. 17–24.
- [2] J. Robert, J.-P. Georges, Éric Rondeau, and T. Divoux. "Minimum cycle time analysis of ethernet-based real-time protocols," International Journal of Computers, Communications and Control, vol. 7, no. 4, pp. 743–757, 2012.
- [3] S. Zuponic, R. Klecka, M. Hantel, and P. Didier. "TSN Influences on ODVA Technologies: IEEE - 802.1, AVnu, IETF," ODVA, Tech. Rep., 022017.
- [4] E. Gardiner. "Theory of Operation for TSN-enabled Systems," AVnu Alliance, Tech. Rep., 02 2017.
- [5] R. Hummen, S. Kehrer, and O. Kleineberg. "White paper: TSN – Time Sensitive Networking," Belden, Tech. Rep., 02 2017.
- [6] "IEEE Std 802.1AS-2011: Standard for local and metropolitan area networks - timing and synchronization for time-sensitive applications in bridged local area networks," IEEE, New York, USA, Standard, Mar. 2011.
- [7] "IEEE Std 802.1AS-Rev-2018: Standard for local and metropolitan area networks - timing and synchronization for time-sensitive applications," IEEE, New York, USA, Standard.
- [8] "IEEE Std 802.1Qbv-2016: Standard for local and metropolitan area networks-media access control (mac) bridges and virtual bridged local area networks amendment: Enhancements for scheduled traffic," IEEE, New York, USA, Standard, Mar. 2016.
- [9] "IEEE Std 802.1Qav-2010: Standard for local and metropolitan area networks—virtual bridged local area networks - amendment: Forwarding and queuing enhancements for time-sensitive streams," IEEE, New York, USA, Standard, Jan. 2010.
- [10] "IEEE Std 802.1Qcc-2018: Standard for local and metropolitan area networks-media access control (mac) bridges and virtual bridged local area networks amendment: Stream reservation protocol (srp) enhancements and performance improvements," IEEE, New York, USA, Standard.
- [11] "IEEE Std 802.1CB-2018: Standard for local and metropolitan area networks - timing and synchronization for time-sensitive applications," IEEE, New York, USA, Standard.
- [12] "IEEE Std 802.1Qbu-2016: Standard for local and metropolitan area networks - media access control (mac) bridges and virtual bridged local area networks - amendment: Frame preemption," IEEE, New York, USA, Standard, Aug. 2016.
- [13] "IEEE Std 802.3br-2016: Standard for local and metropolitan area networks- media access control (mac) bridges and virtual bridged local area networks- amendment: Specification and management parameters for interspersing express traffic," IEEE, New York, USA, Standard, 2016.
- [14] "CiA 301-2007: CANopen application layer and communication profile," CAN in Automation (CiA) e. V., Nuremberg, DE, Standard, Jul. 2007.
- [15] "IEEE Std 802.1AB-2009: Standard for local and metropolitan area networks - station and media access control connectivity discovery," IEEE, New York, USA, Standard, Sep. 2009.
- [16] "NIST Special Publication 800-82 : Guide to Industrial Control Systems(ICS) Security," NIST, Gaithersburg, USA, Standard, May 2015.
- [17] "IEC Std 62443-2017: Security for industrial automation and control systems," IEC, Geneva, Switzerland, Standard, 2017.
- [18] "IEC Std 61508-2010: Functional safety of electrical/electronic/programmable electronic safety-related systems," IEC, Geneva, Switzerland, Standard, 2010.
- [19] "IEC Std 61784-3-2016: Industrial communication networks - Profiles -Part 3: Functional safety fieldbuses - General rules and profile definitions," IEC, Geneva, Switzerland, Standard, 2016.
- [20] S. Schriegel and J. Jasperneite. "Investigation of industrial environmental influences on clock sources and their effect on the synchronization accuracy of ieee 1588," in 2007 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control and Communication, Oct 2007, pp. 50–55.