T/ZIIC 001-2021

中关村工业互联网产业联盟
团体标准

Zhongguancun industrial Internet Industry Alliance
Group standard

时间敏感网络技术在流程工业应用的应用场景及网络需求

TSN Technology Use Case in Process Automation and Network Requirements

2021-07-01 发布　　2021-07-01 实施

中关村工业互联网产业联盟　　发布

目　　次

前　　言

本标准分为4个部分：

——术语与定义

——工业自动化中的TSN

——DCS重新组态用例

——其他工业自动化用例

本标准起草单位：北京东土科技股份有限公司、北京物芯科技有限责任公司、北京星网锐捷网络技术有限公司

本标准主要起草人：黄易、邵枝晖、姚辉

本标准为首次发布。

引　　言

本标准描述了用于工业自动化的用例，这些用例应该在IEC/IEEE 60802联合标准项目中涵盖，以此来指定用于工业自动化的TSN（时间敏感网络）行规（TSN-IA）。

时间敏感网络技术在流程工业应用的应用场景及网络需求

1 术语与定义

1.1 定义

重构：
系统结构的、或者设备级内容的任何内部修改，包括任何类型的升级。参见 IEC61158 - 类型 10，动态重构；PI/PNO 提供的文档：高可用性指南。

（过程）扰动：
过程/机器的任何失灵或停顿，紧随其后的是生产损失或者是不可接受的生产质量的降级。参见：IEC61158 - 失效。参见：ODVA 非计划宕机。PI/PNO 提供的文档：诊断指导原则。

工厂（单元）/机器的运行状态：
工厂（单元）/机器的功能和生产的正常状态。

工厂（单元）/机器的维护状态：
有计划的挂起或部分挂起工厂（单元）/机器的功能的正常状态。

工厂（单元）/机器的停止状态：
工厂（单元）/机器的完全非生产模式。

趋同网络概念：
所有的局域网设备（有线的或无线的）能够通过公共基础设施交换数据，并具有定义的 QoS 参数。

设备：
终端工作站，桥接终端工作站，桥，访问点。

DCS：
分布式控制系统。

传输选择算法：
用于通信选择的一组算法，包括严格的优先级，基于信用的整性器与增强传输选择。

抢占：
可被抢占的帧的传输挂起以允许在可被抢占帧传输恢复之前允许一个或多个快速帧被传输。

调度通信的增强：
桥或终端工作站支持允许相对已知的时间尺度从每个队列被调度的传输增强。

时间敏感流：
从单个源工作站到一个或多个目标工作站的通信流，该通信对于实时传送敏感，实际上要求传输延时有界。

TSN 域：
一些公共管理的工业自动化设备；一组设备，它们的端口连接单独的使用 TSN 标准传输时间敏感流的局域网，该标准包括传输选择算法，抢占，时间同步，调度通信的增强，并且它们共享公共的管理机制。将这些设备成组化是管理的决定。

统一时间域：
用来同步统一时间的 gPTP 域。

工作时钟域：
用来同步工作时钟的 gPTP 域。

等时同步域：
具有公共设置等时同步周期实时通信类型的公共工作时钟域的工作站。

周期实时域：
具有公共设置周期实时通信类型的工作站，即使在不同的工作时钟域或者同步到本地时间尺度的。

网络周期：
包括安全边界的传输时间与包括安全边界的应用时间；对于一个 TSN 域值是特定的并且指定属于该 TSN 域的网络接口的重复行为。

绿地：
用于本标准的上下文：绿地指的是 TSN-IA 行规一致性设备，而不考虑是“旧”或“新”。

棕地：
用于本标准的上下文：棕地指的是与 TSN-IA 行规不一致的设备，而不考虑是“旧”或“新”。

流转发：
沿着流路径包括跨 TSN 域边界的流数据转发。

1.2 IEEE802 术语

优先级再生：
见 IEEE 802.1Q-2018 的 6.9.4 节，再生优先级。

入口速率限制：

见 IEEE 802.1Q-2018 的 8.6.5 节，流量分类与计量。

2 工业自动化中的 TSN

“信息-物理系统（Cyber-Physical System, CPS）”一词还没有一个公认的定义。Edward A. Lee [1]在一份报告中将 CPS 描述如下：“信息物理系统（CPS）是计算与物理过程的集成。嵌入式计算机和网络通信对物理过程进行监控和控制，通常物理过程通过反馈回路影响计算，反之亦然。”

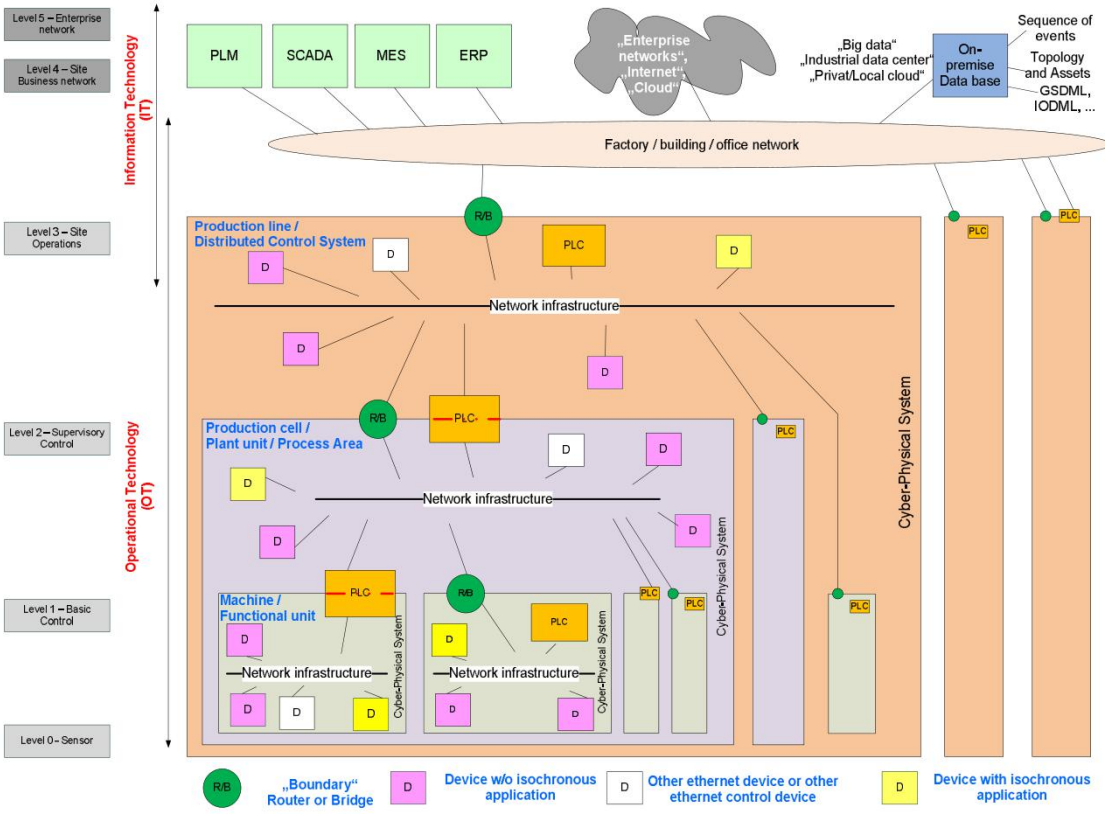

图 1 — 工业自动化的层次结构

信息物理系统是“智能工厂”和工业 4.0 的基石，IEEE 802 LAN 技术提供了操作技术控制层通过趋同网络连接到时间关键型工业应用的机制（例如 TSN 功能）。

具有 TSN 功能的 IEEE 802 LAN 可以被用于工业自动化：

- 信息物理系统（CPS）内部的实时通信
- 信息物理系统之间的实时通信

一个信息物理系统（CPS）包括：

- 控制设备（通常为 1 台 PLC）
- I/O 设备（传感器，执行器）
- 驱动器
- 人机界面（HMI）
- 上层接口：
  - ✧ PLC(作为网关)
  - ✧ 路由器
  - ✧ 网桥
- 其他以太网设备：
  - ✧ 服务器或任何其他计算机，可以是实体机或虚拟机
  - ✧ 诊断设备
  - ✧ 网络连接设备

2.1 互操作性

互操作性可以在不同的层次上实现。图 2 和图 3 显示了需要覆盖的三个区域：

- 网络配置（根据 IEEE 定义的管理对象）
- 流配置和建立
- 应用配置

三个区域间是相互影响的（如图 2 所示）。

应用配置不被期望成为行规的一部分，但其他两个区域是行规的一部分。

TSN-IA 行规做出的选择涵盖了 IEEE 802 定义的第 2 层和用来配置第 2 层的选定协议。

应用也使用上层，但是这些超出了行规的范围。

流建立是由应用初始化的，用于允许应用之间的数据交换。应用请求资源，通过网络配置、流配置和建立来得以实现。

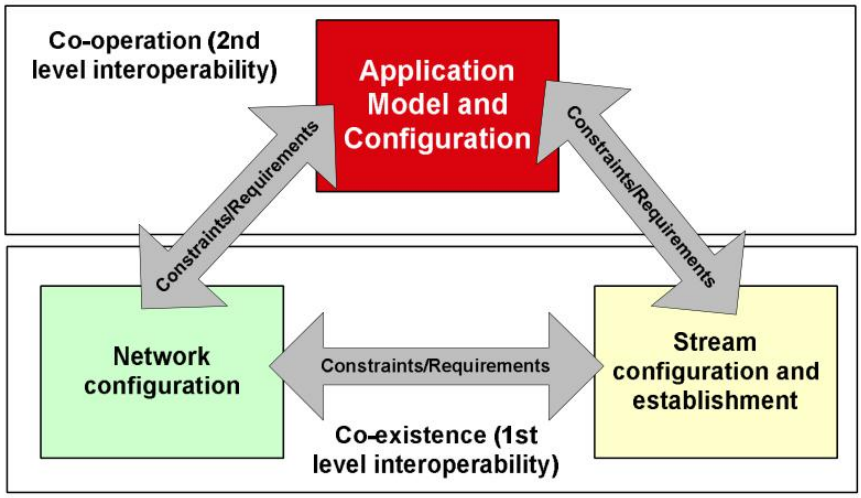

图 2 — 互操作原理

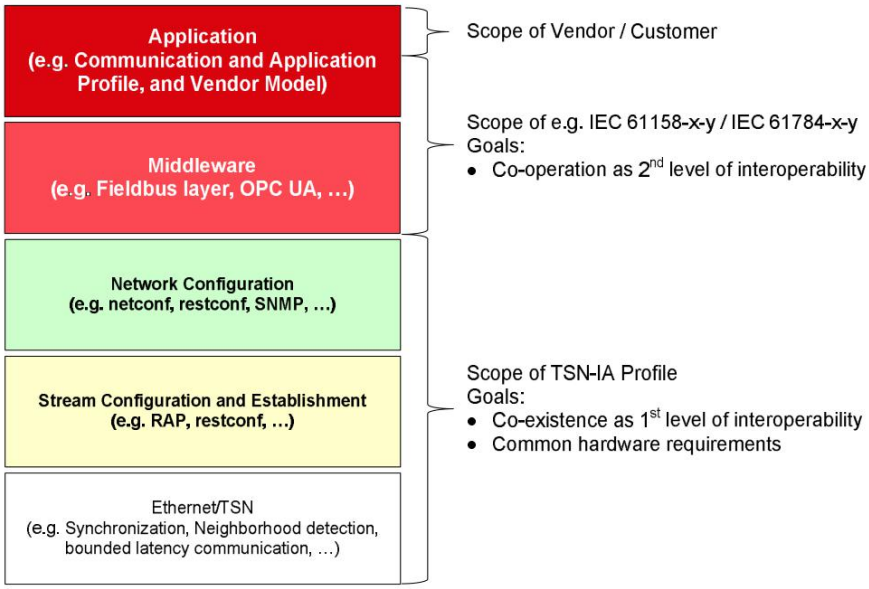

图 3 — 工作范围

2.2 TSN 域

2.2.1 通用

TSN 域被定义为一定数量的通常可被管理的工业自动化设备；成组这些设备是管理的决定。

TSN 域特性：

- 一个或多个 TSN 域可以存在于单个第 2 层广播域中
- 一个 TSN 域可以不被多个第 2 层广播域共享

- 多个 TSN 域可以共享一个公共的统一时间域
- 两个相邻的 TSN 域可以实现相同的请求，但保持分离
- 多个 TSN 域通常在一个网桥中实现（参见 2.2.2.2）
- 多个 TSN 域通常在一台路由器上实现（参见 2.2.2.3）
- 多个 TSN 域通常在一个网关中实现（参见 2.2.2.4）

典型的机器/功能单元（见图 1）被当作单独的 TSN 域。生产单元和生产线也可以设置为 TSN 域。设备可以并行地成为多个 TSN 域的成员。

图 4 显示了在公共广播域和公共统一时间域内的两个示例 TSN 域。TSN 域 1 是一个纯周期实时域，而 TSN 域 2 另外还包括了三个重叠的等时同步域。

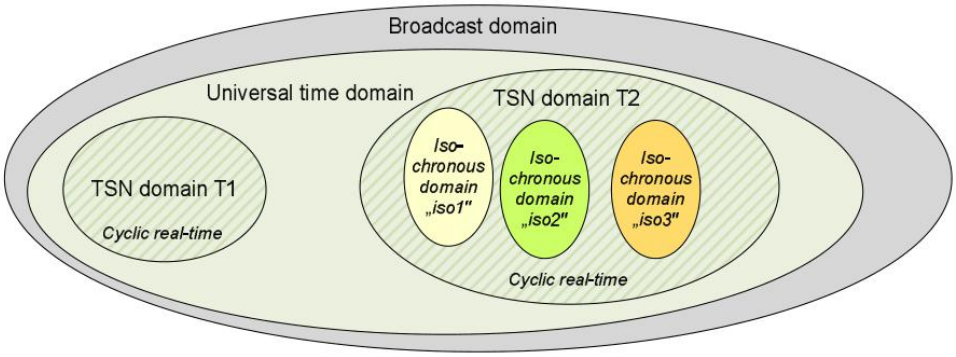

图 4 — 不同类型的域

TSN 域之间的互联在 2.2.2 和 2.6.1 中进行描述。

2.2.2 TSN 域的互联

2.2.2.1 通用

TSN 域可以通过以下方式进行连接：

- 桥接（2 层）
- 路由（3 层）
- 应用网关（7 层）

无线接入点或 5G 基站也可以用来连接 TSN 域。

2.2.2.2 桥接（2 层）

当一个网桥是多个 TSN 域的成员时，一个网桥端口只能是一个 TSN 域的成员。

图 5 给出了一个包含两个网桥的例子，每个网桥分别是两个 TSN 域的成员。网桥 B1 在 TSN 域生产单元 1 和 TSN 域机器 1 之间提供端口和连接，网桥 B2 为生产线 1 和生产单元 1 提供端口和连接。

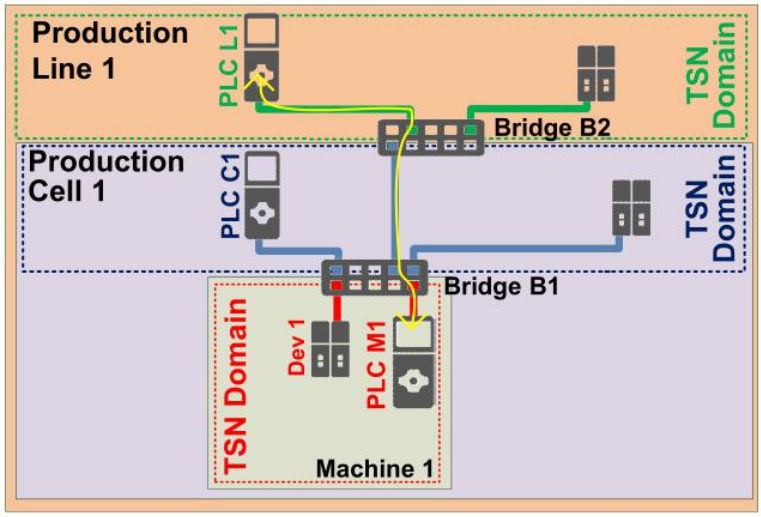

图 5 — 由网桥连接的三个 TSN 域

为了支持多个 TSN 域之间的连接（例如，PLC L1 与 PLC M1 ），需要指定一种在多 TSN 域上预留时间敏感流的方法，包括：

- 找到通信伙伴
- 标识参与的 TSN 域
- 标识独立于配置模型（集中式，混合式，全分布式）的参与的管理实体
- 确保所需要的资源
- 如果需要，参数化 TSN 域连接点以此来允许流转发

2.2.2.3 路由（3 层）

与路由器一起，可以构建内部联网和互联网。然而，在本规范中，只涉及内部联网用例。

当路由器是多个 TSN 域的成员时，一个路由器的接口/端口只能是一个 TSN 域的成员。图 6 给出了一个包含两台路由器的示例，每台路由器都分别是两个 TSN 域的成员。路由器 R1 在 TSN 域生产单元 1 和 TSN 域机器 1 中提供端口和连接，路由器 R2 为生产线 1 和生产单元 1 提供端口和连接。

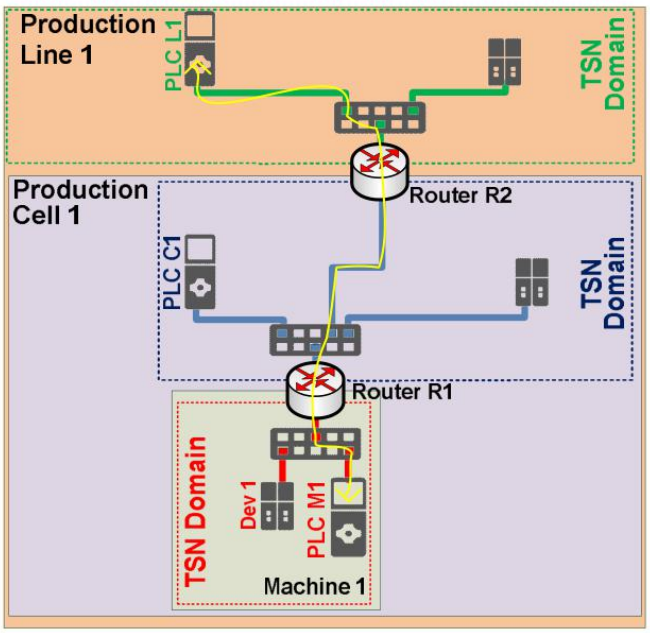

图 6 — 由路由连接的三个 TSN 域

为了支持多个 TSN 域之间的连接（例如，PLC L1 与 PLC M1 ），需要指定一种在多 TSN 域上预留时间敏感流的方法，包括：

- 找到通信的伙伴
- 标识参与的 TSN 域
- 标识独立于配置模式（集中式，混合式，完全分布式）的参与的管理实体
- 确保所需要的资源
- 如果需要，参数化 TSN 域连接点以此来允许流转发

2.2.2.4 应用网关（7 层）

当一个应用网关是多个 TSN 域的成员时，一个网关的接口/端口只能是一个 TSN 域的成员。

图 7 给出了一个包含两个应用网关的例子：

- 网关 CM1 是 TSN 域生产单元 1 和机器 1 的成员
- 网关 CF1 是 TSN 域生产单元 1 和现场总线 1 的成员

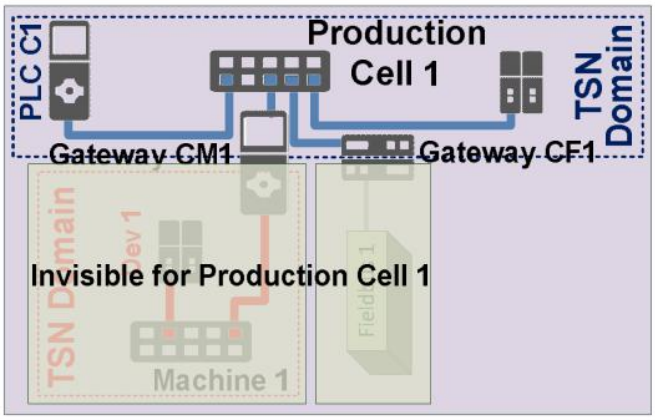

图 7 — 由网关连接的两个 TSN 域与接入的现场总线

应用层网关不提供不同 TSN 域设备之间的直接访问，而是作为 TSN 域出口和入口通信的终端。

可以在应用层网关中实现控制和数据的专用转换应用以访问相邻的 TSN 域，从而实现 TSN 域互连。 这种转换可能涉及数据和控制的缓冲、收集与重排。 因此，应用层网关将 TSN 域解耦，以至于相邻 TSN 域的内部结构和配置是分别不可见的。

应用层网关还将用于基于非以太网或以太网的现场总线连接到 TSN 域（请参见图 7 中的网关 CF1，另请参见用例 11：现场总线网关）。

3 DCS 重新组态

3.1 DCS 重新组态用例的挑战

这些用例带来的挑战是重构对现有通信的影响：所有的事情都必须不干扰生产的情况下发生。

我们认为，重要的是，我们可以连接系统中任何位置的任何新设备，并且它们通过支持 TSN 功能的现有基础设施获得连接，而不改变系统的运行模式。

3.2 用例 1：DCS 设备级重新组态

适用图 1 所示的结构。图 8 提供了逻辑站视图。

- 对设备的软件修改
  - ✧ 应更改该设备的软件/软件应用程序，这不需要更改其他设备上运行的软件/软件应用程序（包括固件更新）
- 设备更换/替代
  - ✧ 由于维护原因，过程设备被另一个装置替换，例如非过程校准或设备有缺陷（注：有缺陷

的设备可能仍然完全正确地参与网络和通信，例如，如果只是传感器不再正常工作）

- ✧ 用例：修复

- 添加/删除其他设备
  - ✧ 一个新的设备将被添加到一个现有的系统或功能中，这些系统或功能将在应用中使用，并被添加到一个正在运行的设备中，例如通过启用一个软件功能或插入一个新的硬件模块。即使变更的范围不限于单个设备，因为其他设备也参与相同的应用
  - ✧ 对于进程设备、服务器：BIOS、操作系统和应用程序更新、新虚拟机、工作站
  - ✧ 使用案例：用现有设备的升级/降级进行替换，只需添加新设备，删除设备，添加设备之间的连接
- 与通信相关的影响因素
  - ✧ 新增设备通信要求（新增时）
  - ✧ 现有 QoS 参数（即协议特定参数，如超时或重试）
  - ✧ 设备冗余
  - ✧ 网络/媒体冗余
  - ✧ 虚拟化
  - ✧ 对于服务器：内部或云
  - ✧ 所涉及的过程设备中的时钟类型
  - ✧ 统一时间和工作时钟域
  - ✧ 新设备所需的周期时间
  - ✧ 可用带宽
  - ✧ 现有安全策略

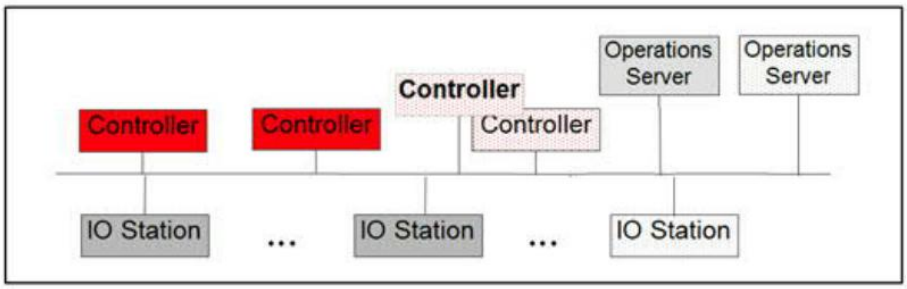

图 8 — 设备级重构用例

3.3 用例 2：DCS 系统级重新组态

适用图 1 所示的结构。图 9 提供了一个逻辑站视图。

- 扩建现有工厂
  - ✧ 向现有网络添加新的网络段
    - 现有非 TSN/新增为 TSN
    - 现有 TSN/新增 TSN
- 更新系统安全策略
  - ✧ 新密钥长度、新安全区、新安全策略
  - ✧ 确定如何处理和由谁处理
- 影响因素
  - ✧ 与“设备级别”相同

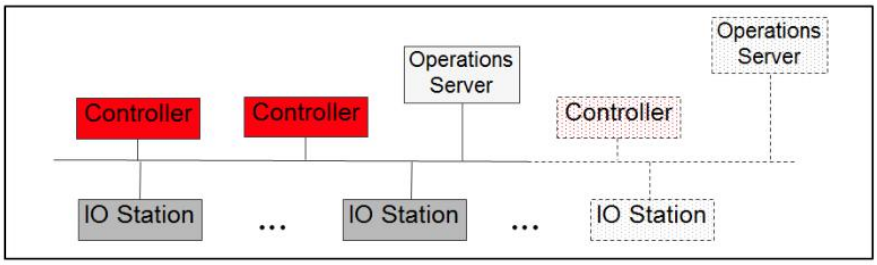

图 9 — 系统级重构用例

4 其他工业自动化用例

4.1 用例 3：网络监视与诊断

诊断在系统和设备的管理中起着重要的作用。工业自动化需要一种对故障作出快速反应的方法。出现错误的反应应限制错误造成的损害，并尽量减少机器停机时间。

应在几个周期内进行错误检测（准确值取决于应用），并在出现错误的情况下精确规定反应。机器停止并不总是对错误的正确反应。这种反应可能发生在说话者和听话者身上。

维修由现场服务人员进行，他们没有具体的沟通知识。必须被修理的部件的指示应在几秒钟内出现。

修理期间机器断电。典型的维修时间目标是 15 分钟以下。这包括重新启动机器和指示问题已解决。

一般来说，在这种情况下使用的机制是非循环的或具有大的周期时间，因此从网络的角度来看，它们可能被认为是偶发的。大多数与诊断相关的用例都将包含在这个类别中。

快速识别错误位置对于最小化生产中的停机时间非常重要（另请参见用例 01：事件序列）。

监视网络性能是一种预测问题的方法，这样即使在出现错误和停机时间之前，也可以计划安排并付诸实施。

工业以太网上的设备识别应以通用的、可互操作的方式进行，以便在聚合的 TSN 网络上实现互操作。这个标识既需要显示设备的类型，也需要显示网络的拓扑结构。IEEE 802.1AB，链路层发现协议（LLDP）提供了一种可能的机制，可以在第二层完成这项工作，但在实现中提供了很大程度的可变性。

要求：

- 减少停机时间
- 应提供监测和诊断数据，包括使用的 TSN 特征，例如已建立的流、失败的流、流类型、带宽消耗等…
- 应利用诸如 IEEE 802.1AB 之类的发现协议来满足 TSN IA 的需要
- 应支持报告 TSN 特性的详细诊断信息

使用的 802.1（ietf）机制：

- MIBs (SNMP)
- YANG (NETCONF/RESTCONF)
- …

4.2 用例 4：信息安全

工业自动化设备可能成为蓄意破坏或间谍活动的目标。
因此，信息安全的各个方面也可以在工业自动化中找到：

- 保密性是指不向未经授权的个人、实体或过程提供或披露信息的属性
- 完整性意味着维护和保证数据的准确性和完整性
- 可用性意味着所有资源和功能单元都可用，并在需要时正常运行。可用性包括防止拒绝服务攻击
- 真实性是指数据源和数据汇的可验证性和可靠性

要求：

- 可选的保密性、完整性、可用性和真实性支持
- 安全不应限制实时通信
- 针对在经过身份验证的工作站上运行的恶意应用程序的保护超出了本范围

使用的机制：

- 802.1X
- IEC62443 标准
- …

4.3 用例 5：固件升级

固件更新是在正常操作期间进行的，以确保机器（例如 1000 台设备）能够在几乎没有停机时间的情况下进行更新。

带扰：单独加载（需要 2 个 FW 版本的空间）和协调激活，以尽量减少停机时间
无扰：具有无扰切换的冗余站 - 单个设备可能会失去连接（变得有扰）。

要求：

- 站点应能够在不受干扰的情况下接收和存储额外的固件版本。

使用的 802.1 机制：

- …

4.4 用例 6：虚拟化

工作负载整合是通过虚拟化硬件接口来完成的。即使在这种环境中，根据 TSN-IA 行规的 TSN 特性也应可用并工作。

虚拟化交换机/虚拟化网桥
图 10 和图 11 显示了以太网通信概念的两种主要设置，允许两者通信，即虚拟机到以太网和虚拟机到虚拟机。虚拟机内的应用程序不应看到它们是否与另一个虚拟机或以太网节点通信。

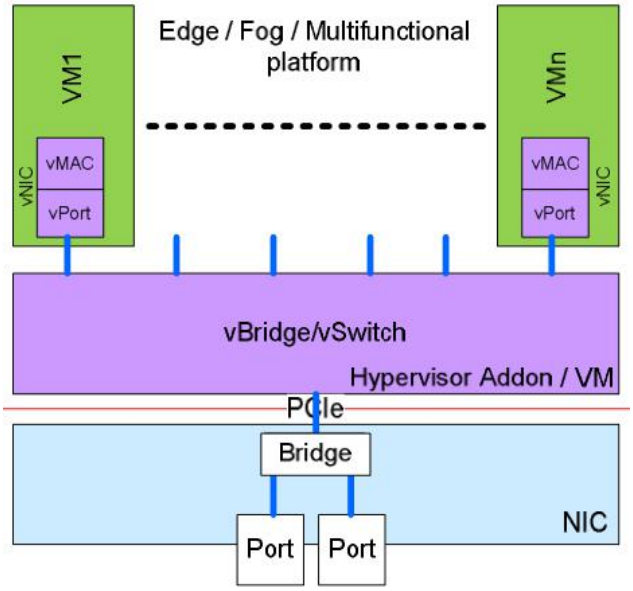

图 10 — 与基于 VM 的虚拟网桥的以太网互联

图 10 针对几乎无限数量的虚拟机进行缩放，因为 vMAC/vPort 和 vSwitch/vBridge 虚拟机的内存带宽和计算能力远远高于 NIC 的 PCIe 带宽。

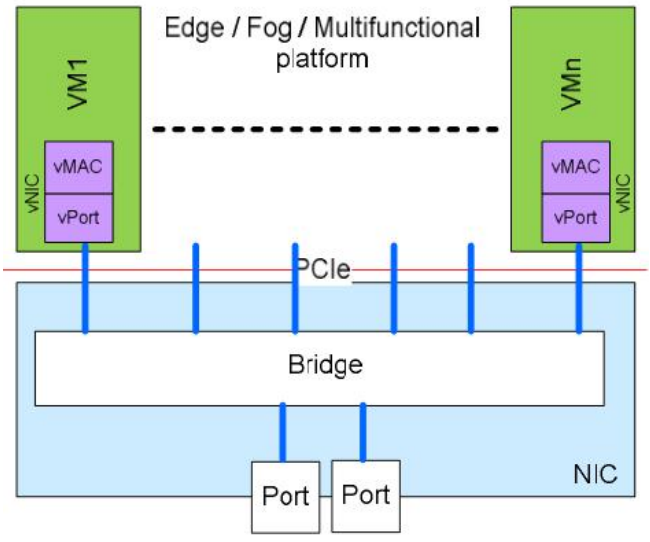

图 11 — 与 PCIe 连接的网桥的以太网互连

图 11 适用于数量有限的虚拟机，因为它节省了额外的 vSwitch/vBridge 虚拟机。对于给定数量的虚拟机，例如 PCIe Gen3 x4 或 Gen4 x4，似乎就足够了。

要求：

- vBridge 和 vPort 应该表现为实时网桥和实时端口：数据平面、控制平面…
- vBridge 和 vPort 可以成为 TSN 域的成员
- 应该像用例“多个应用程序”一样工作

使用的 802.1 机制：

- …

4.5 用例 7：离线配置

机器的配置通常在机器实际制造之前完成。这对于检查所有部件的可用性以及作为机器编程的输入是必要的。这需要现场设备的电子数据表。桥接组件和说话者听话者行为应在这些文件中描述。说话者和听话者的参数是从应用配置以及通信间隔中推导出来的。网桥描述可以包括端口属性和为各个目的支持的流的数量。设置系统还需要性能参数。基于 XML 的文本描述目前被用来描述机器中使用的现场设备的功能。将各个元素组合起来，并定义其他参数，从而生成另一个描述机器配置的文件。该文件在机器设置后提供给机器控制单元，用于验证调试。需要协议来比较真实的机器单元和配置的单元。拓扑发现是一项重要特征，也是访问网桥以读取和写入管理数据的重要功能。

延迟要求限制可用拓扑，反之亦然。一些应用可以用延迟上限的描述来处理。在这种情况下，配置可以不使用网桥描述中的累计延迟，而是在设置期间必须检查的限制。

实时通信的另一个参数是时间同步的质量，它取决于同步路径中使用的组件的几个参数。IEEE 802 组件的 YANG 模型可以适合于作为单个网桥组件和 IEEE 802 网络的离线数据库的目的。机器配置程序不必处理与 YANG 相关的协议，而需要使用模型。YANG 模型使用的一种完全不同的语言，它意味着两个数据库以及两个描述性单元之间的一些转换和一致性问题。因此，建议提供 XML 和 YANG 之间的映射。

要求：

- IEC/IEEE 60802 组件的设备类型说明，包括所有必要的管理组件需要定义对象
- 以文本形式（如 XML）离线存储机器配置的方法
- 支持离线-在线比较机器的配置

有用的 802.1 机制：

- IEEE802.1YANG 模型；

4.6 用例 8：数字双胞胎

机器的虚拟预调试可以节省大量的时间和金钱。

由于数字孪生技术的实施和使用，提高了工程效率，预计开发新机器可节省 30%的时间。应能在客户所在地更快地开发、交付和调试新机器。

数字孪生在尽可能多的细节显示真实的机器，并允许其操作模拟。借助数字孪生，机器可以逐渐地、虚拟地开发出来，与客户所在地机器的实际生产和调试过程并行。

要求：

- 应能可靠地规划、开发、测试、方针和优化结果

使用的 802.1 机制：

- …

4.7 用例 9：无需工程化的设备更换

工厂中的任何设备，即终端、桥接终端或网桥，最终都可能损坏。如果发生这种情况，则需要快速简单地更换损坏的设备，将生产干扰降至最低。

无需任何工程努力（即无需工程工具）就用新设备“机械地”更换故障设备是将维修停机时间降至最低的先决条件。

要求：

- 在维修的情况下，应能够更换终端、桥接终端或网桥，而无需工程工具。

使用的 802.1 机制：

- …