白皮书

# 捍卫
# 工业以太网

## 如何保护您的ICS环境

HongKe
虹科

# 工业以太网 | 目录

# 绪论

在过去的30年里，工业网络发展迅速。工业以太网在新的节点安装方面已经超过了传统的现场总线技术，而工业4.0、工业物联网(IIoT)、工业控制系统(ICS)、软件定义网络(SDN)、混合云和人工智能(AI)的虚拟化和进步都对工业网络的发展产生了重大影响。

虽然数据中心虚拟化可能正在成为主流，但工业4.0运动对许多人来说仍然是新的和陌生的。以太网在工业控制系统(ICS)应用中的应用对这一演变势在必行，因为许多公司希望在保持当今需求的同时，着眼于工业4.0和工业物联网(IIoT)，使其系统面向未来。

与IT环境不同，OT领导者不能容忍哪怕是轻微的数据不一致或停机。使用PROFINET、Ethernet/IP和EtherCAT等协议，您可以确保从网络上的IIoT终端设备发送的消息以100%的可靠性传输。如果没有这些协议，您将需要在整个工业基础设施中使用多个转换解决方案和通信交换机才能实现点对点连接。

但由于有了标准化的以太网协议，您可以利用工业以太网的优势(如速度从使用RS-232的9.6kbit/s提高到1 Gbit/s和10Gbit/s)为成功的IIoT项目奠定基础，还可以选择使用光纤来增加距离和整合标准网络设备。

# 捍卫工业以太网

现场总线、串行总线和设备传统长期以来一直是工业基础设施的基石。传统设备因其在维护关键基础设施的安全和保障方面的卓越能力而持续了几十年。但是，日益增长的IT能力和OT流程之间的桥接需求导致了它们的维护问题。

以太网并不是新技术。各种规模的网络都已转向以太网连接，以跟上不断变化的互联网流量需求。另一方面，由于工业环境的不同环境，工厂设置和生产单元已经落后于以太网创新。

许多工业网络仍然以10M或100M的100BaseFX或100BaseTX布线运行，并且出于安全考虑，仍然运行在旧的操作系统，如Windows 95和Windows XP--甚至在操作系统不再支持后。由于静态生产流量受到严格管制，机器环境的任何变化都需要对工业操作进行全面的重新认证和校准，这既费时又费钱。

尽管存在这些挑战，但工业部门不能再忽视以太网连接的好处。以太网简单而有效的设计，加上相对较低的以太网硬件成本，使其成为工业网络中极具吸引力的网络设计。能源、通信和医疗保健等关键基础设施的制造商和管理者现在才开始转向采用坚固的连接器和修改的以太网协议，从而推动了工业以太网创新的崛起。

工业以太网无疑将为制造自动化和关键基础设施带来好处-但前提是正确部署和维护。随着制造商从其专有的串行端口到端口基础设施转向以太网协议，保护工业以太网将成为工业部门的主要障碍。

# 构建工业控制系统(ICS)环境的可见性

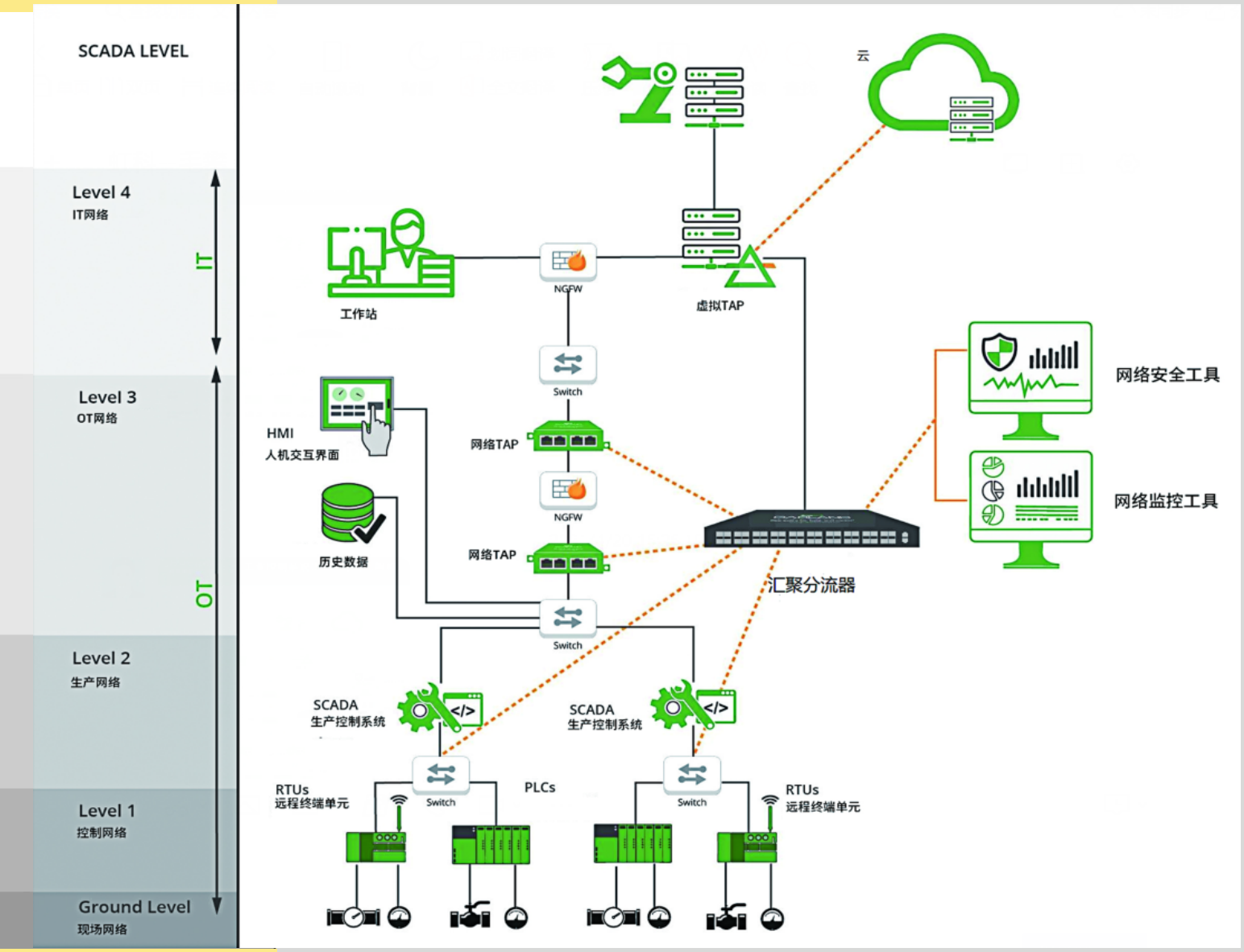
工业控制系统(ICS)基础设施以及运营技术(OT)与信息技术(IT)的融合，为该行业带来了许多挑战，包括增加网络攻击和网络盲点的脆弱性。许多公司并不像他们的IT基础设施那样，对其OT系统具有可视性。

工业控制系统(ICS)描述了工业环境中软硬件集成的关键基础设施网络连接。ICS包括监控和数据采集(SCADA)和分布式控制系统(DCS)、工业自动化和控制系统(IACS)、可编程逻辑控制器(PLC)、可编程自动化控制器(PAC)、远程终端单元(RTU)、控制服务器、智能电子设备(IED)和传感器。本地操作通常由从远程站接收监控命令的现场设备控制。ICS系统广泛应用于化工加工、制造、发电、油气加工和电信等行业。

在这些ICS环境中，工业自动化中数据的可用性至关重要。优化的安全性和性能始于100%的网络流量可视性，包括虚拟和物理环境。而可视性从数据包开始。网络可视性结构包括网络TAP和数据包代理，提供完整的网络可视性和链路优化，可以降低网络复杂性，使基础设施升级更容易，帮助满足特定的法规，促进流量增长，提高工具和网络性能的有效性。

# ICS可见性架构

大多数工业安全和网络监控工具都是基于数据包的。以数据包的形式获取网络流量是至关重要的。不过这种基础架构中存在一些固有的挑战。 SPAN端口在OT交换机上是可用的，但容易出现丢包、重复，或者可能已经在使用。甚至一些老旧的传统交换机，可能连SPAN端口选项都没有。




该图说明了网络TAP和SPAN流量的可视性结构如何在ICS系统中集成，为第2-4层提供全面的可视性， 在网络数据包代理中聚合，过滤并与安全和网络监控工具共享流量。

# 网络可见性为您的工业基础设施提供了许多好处：

- **改善网络安全：**高级攻击者在网络盲区茁壮成长。他们创造的威胁载体能够通过混入您的正常流量，溜过您的防御系统。当您无法看到每一个位、字节和数据包时，您就有可能错过恶意活动。最大限度地提高网络可见性可确保您的安全工具能够看到所有必要的数据，以便就潜在威胁向您发出警报。

- **更高效的性能：**即使是应用程序性能的轻微延迟也会显著影响员工的生产力和您的底线。您防止这些延迟的能力取决于积极主动地解决性能异常问题。如果没有适当的网络可视性，您可能在问题已经影响到员工之前都不会发现。适当的网络可视性可以提高监控工具的效率，从而使您在网络管理中更加积极主动。

- **提高工具利用率：**网络可见性包括您有效平衡负载的能力。这意味着根据安全和监控工具真正需要的数据来进行流量的转移。当您拥有全面的可视性时，您可以确保不浪费带宽，并确保您的安全和监控工具得到充分的利用。

- **最小化解决问题的平均时间：**知道有一个网络问题要解决，只是成功了一半。最小化解决问题的平均时间对业务性能至关重要。当您对100%的数据包具有网络可视性时，您就可以利用日志数据来快速识别问题的根本原因并有效地进行故障排除。

构建网络监控和安全，同时管理ICS应用的性能，与传统的网络可视性结构大同小异。利用整个流水线应用和工厂网络的兴趣点，增强监控和诊断能力。在此基础上，需要对连接性、环境和安全性进行一些周密的考虑。

# 连接

## 奠定工业以太网框架

确保工业以太网的安全始于正确的采购和部署流程。事先建立正确的框架，有助于减轻未来的网络攻击。在基本设备方面，部署工业以太网需要正确的电缆和连接器。

当我们谈到工业以太网时，很容易超前于我们自己。你看到工业物联网不断增长的现实，以及对这些网络安全的长期担忧，你会开始认为这种级别的连接是理所当然的。

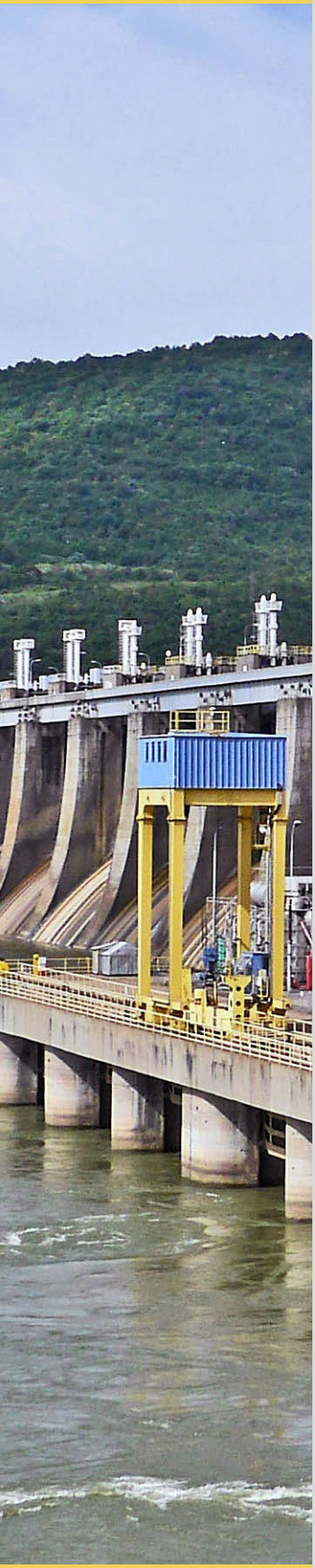
在升级网络时，选择正确的框架对于确保在升级过程中不会中断流量至关重要。为标准设置选择电缆、连接器和安装可能非常困难，但当您在工业环境中升级到以太网时，请牢记以下7点：

### 1) 你的数据速率需求是多少？

工业企业在切换到以太网协议时，必须遵守IEEE802.3标准。公司必须应对的最大争议是对布线长度的限制。虽然铜缆和光纤都支持，但铜缆设备到设备的连接不能超过100米。光纤2000米连接限制则要宽松得多，但根据环境的不同，光纤并不总是一种选择。在设计新的工业以太网部署时，请牢记这些限制。

**确定应用数据速率：** 你的网络需求可能是100M以太网，一直到1G、10G以及更高的速率。这时您需要权衡您的光纤/铜缆选项，并考虑各种电缆类别（100M或1G的Cat 5e，10G的Cat 7）。一个最好的做法是避免混合和匹配电缆类型，选择适合环境的电缆，并尽可能普遍地部署。

**2对电缆 vs 4对电缆：**如果只需要普通的10/100BaseT应用，2对电缆是可以接受的。然而，当工业环境正在向千兆、10G及更高的水平发展时，4对布线要高效得多。四对电缆还支持更强大的 "以太网供电（PoE）"功能。



## 2) 你的环境到底有多恶劣？

在标准的IT网络中，你可以根据业务应用需求来选择线缆。但当你在谈论工厂车间的OT网络时，环境就是一切。

您的许多考虑因素都归结为特定电缆选择的坚固性。无论您评估的是哪种电缆，您都需要了解以下所有类别的性能：

- 磨损
- 冷弯曲
- 冷冲击
- 压碎
- 穿透
- 高温
- 耐油性
- UV照射
- 水浸式

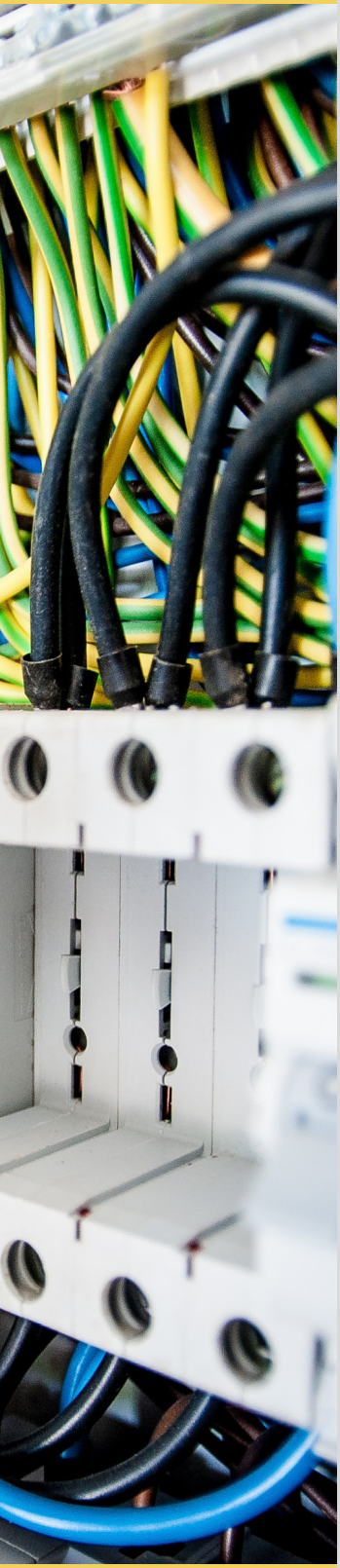
考虑电缆必须承受的振动水平。你会把电缆保护在特定的控制室中吗？在这种情况下，你可能不需要找到这样的易损电缆，因为振动将被最小化。

然而，如果您的电缆暴露在油污、中度振动、化学物质和更多的工厂地板上，您将需要一个更耐用的选择。在极端情况下，由于腐蚀和振动增加，机器上存在的任何电缆都需要最高级别的灵活性。

## 3) 合适的保护外壳

在考虑您的环境之后，您需要决定为网络中的电缆选择正确的保护壳。有4个主要选项需要考虑：

- PVC：万能保护外壳价格合理，在大多数情况下都能很好地工作。
- 阻燃非腐蚀性 (FRNC)：如果消防是你的环境的一个关键问题，多付一点钱买这个保护外壳可能是你最好的选择。
- 热塑性弹性体 (TPE)：这种塑料和橡胶的组合在冷却情况下具有最佳性能，并具有出色的灵活性。然而，性能较高的同时，价格也高于FRNC或PVC。
- 聚氨酯(PUR)：极其耐用，适用于高磨损情况或电缆暴露在化学品、油类和其他溶剂中的环境。



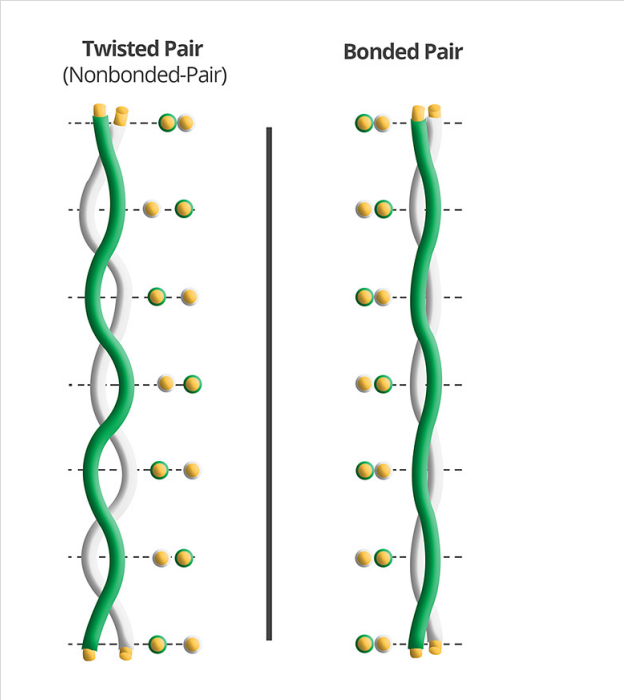
## 4) 屏蔽还是非屏蔽

许多环境使用非屏蔽双绞线是安全的，但有些工业部署需要更多的保护。如果电缆暴露在阀门或其他加工元件的噪音中，可能需要使用屏蔽电缆。

## 5) 绞合 vs. 粘合 通过振动

当你不必担心环境中的振动时，实心导体就能正常工作。然而，当振动挑战需要绞线时，你需要在绞合和粘合对之间做选择。

绞合导线可能会节省您的费用，但它们在实施过程中容易收到损坏，并且可能会因网络不匹配而带来更大的挑战。粘合对导线可能更适合严格的环境。




## 6) 工业以太网连接器

工业以太网设计者必须为其特定环境选择适当的连接器。污染和干扰在工业网络中很常见，但正确的连接器可以保护电缆免受潜在的问题。密封式连接器可使电缆免受灰尘和化学品的影响，而螺钉式连接器可提供更好的防震保护。工业以太网连接器的决定往往归结为两个选项 - RJ45和M12。


- **RJ45连接器**：这些连接器经常出现在标准的办公环境中，但对于工业以太网来说，会有一些变化。锁定机制和8针组件布局支持Cat5和Cat6布线。然而，这些大型连接器往往会引起设计问题。

- **M12连接器**：随着网络架构师倾向于更紧凑的设计，M12连接器找到了自己的位置。M12连接器比RJ45小，但提供了同样恶劣条件下的坚固保护。

## 7) DIN导轨 - 在工业环境中的安装

与工程师在数据中心环境中看到的标准19英寸机架不同，许多工业网络使用带有DIN导轨支架的工业控制面板。DIN导轨是用于将电气设备固定或安装到网络的安装系统。此环境中的目标是尽可能少地移动部件，以最大限度地降低电缆拔掉插头或中断网络的风险。

为了将路由器、交换机、防火墙和监控设备等电气元件固定在DIN导轨上，该元件本身必须有一个DIN导轨支架。

# 克服工业以太网中的连接挑战

由于有如此多的连接选项、法规和操作系统，以及将传统设备与安全和性能监测工具相结合，许多工程师遇到了挑战。你如何连接各种连接器或媒体类型？如果你的网络分析仪是铜千兆接口，而你需要连接100Base-FX的链路，你该怎么办？你的安全或性能监测设备没有100Base-FX的网卡。

在构建你的可视性结构时，专门的网络TAP，如Garland Technology提供的媒体转换可以解决这些问题，同时通过100BASE-FX/LX、LC、ST光纤连接提供全双工的流量副本。

Garland Technology还拥有各种基于工业的TAP配件，包括网络TAP的DIN导轨支架、DC-DC电源转换器和螺钉式电源锁连接器，为保持连接的电源提供额外保证，以帮助克服你可能面临的连接和环境挑战。

当工业以太网框架就位后，公司必须使网络做好准备，以应对从串行到以太网转变所带来的一连串安全挑战。如果采取了正确的安全措施，网络攻击的担忧就不会如此令人望而生畏。

# 确保工业以太网的安全

针对关键基础设施的网络攻击比典型的IT网络的风险要高得多。这就是为什么运营技术团队对技术如此谨慎的原因。但你不可能永远在传统的操作系统上运行封闭的网络。

关键基础设施的安全是最重要的，随着近年来高频率的攻击，世界经济论坛正在敲响警钟。他们的《2020年全球风险报告》强调："对关键基础设施的网络攻击被我们的专家网络评为2020年的第四大风险，已经成为能源、医疗保健和交通等部门的新常态。

据估计，全球有210亿台物联网设备，到2025年将翻一番，《全球风险报告》承认，"2019年上半年，对物联网设备的攻击增加了300%以上，而在2019年9月，物联网被用来通过经典的分布式拒绝服务（DDoS）攻击来攻陷维基百科，预计物联网设备被用作中介的风险将增加。2021年，网络犯罪的损失可能达到6万亿美元，这相当于世界第三大经济体的国内生产总值。

# 需要更好的安全评估

在最近的SANS ICS安全调查中，最令人担忧的统计数据之一是大多数受访者认为他们75%的网络连接是不合规的。随着IT和OT的融合，缺乏网络意识只会增加事故指挥系统（ICS）对危险网络攻击的脆弱性。

为了帮助改善认识状态，建议对关键基础设施公司的安全评估采取六方面的方法：

- **资产盘点：**发现任何未记录的设备
- **网络流量基线：**ICS流量的闭环意味着有一个流量的基线，可以更容易地识别恶意的异常情况。
- **安全漏洞检测：**攻击者可以在网络中持续数周、数月甚至数年--定期的安全评估可以帮助你识别漏洞
- **漏洞识别：**了解最新的安全威胁，从而找到自己的漏洞所在。
- **确认补救措施：**你应该记录你已经解决的每个漏洞，以及你是如何加固你的ICS的。
- **安全态势的洞察力：**适当的文件可以进行分析，为高管提供必要的指标来批准资源分配。

所有这些步骤可以帮助ICS安全专业人员走上改善关键基础设施安全的正确道路。然而，捍卫工业以太网需要的不仅仅是安全评估。

实施可见性基础可加快安全事件检测，提高正常运行时间和服务性能，减少安全事件和违规事件。

# 改善工业安全的六个小技巧

在许多情况下，保护工业以太网看起来与保护标准网络没有太大区别。然而，对工业部门来说，这是一个新的世界，所有潜在的问题都必须通过全面的安全准备来覆盖。以下是一些需要考虑的标准工业安全实践。

## 1 确保物理网络的安全

工业环境中的流量不能被篡改。当涉及到未经授权的访问时，网络架构师不能有任何侥幸心理，必须实施端口安全以防止流量被操纵。要采取的另一项预防措施是禁用未使用的端口，消除未经授权的用户操纵流量的机会。

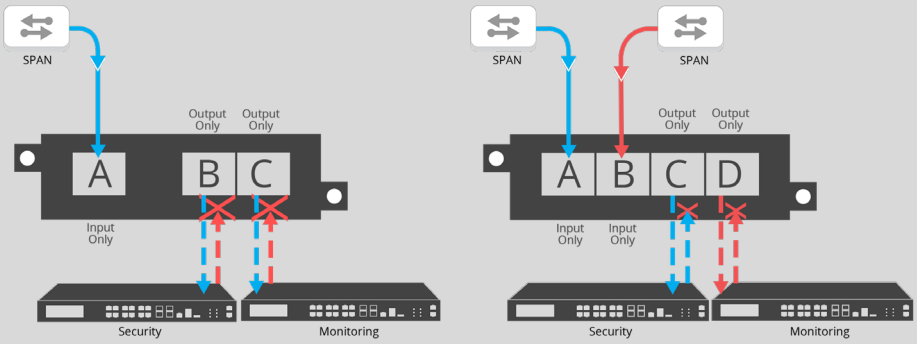
基于端口的MAC地址管理可以帮助防止未经授权的访问。访问控制列表可以由系统管理员创建，只允许限定的MAC硬件地址连接到网络。这些名单应该保持简短，并且只限于那些必须为关键业务应用连接其工作站的人。

# 2 单向网关

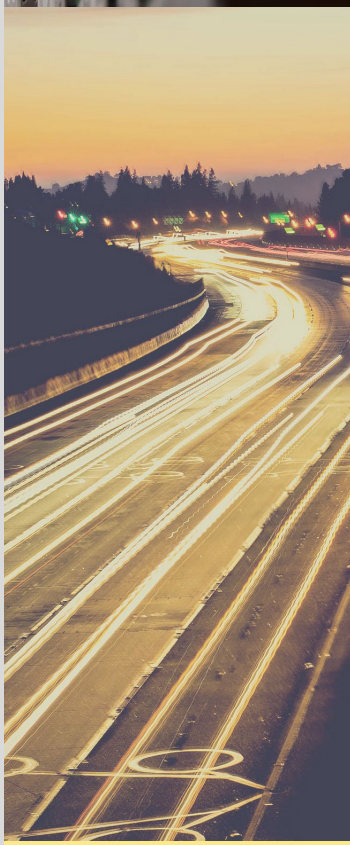
对于特定的行业，新的法规强制执行物理单向性，加上复制数据库和模拟协议服务器的软件来处理双向通信，并包含广泛的网络安全功能，如安全启动、证书管理、数据完整性、前向纠错（FEC）和通过TLS的安全通信。

根据ANSSI关于管理信息系统的工业控制系统的网络安全标准，“ 互连应是单向的，面向企业网络。单向性应在物理上得到保证(例如，使用数据二极管)。应使用经过认证的设备进行互联。”

在这些网络部署中，使用SPAN是根本无法接受的。SPAN或网络交换机的端口镜像是双向的，这就为部署监控或安全的设备创造了黑客入侵的机会。数据二极管提供了一个单向的连接，提供了所需的安全性。




这些图显示了为单向网关提供数据二极管解决方案的单一和双重选择。



数据二极管是一种网络设备或装置，类似于网络TAP，它只允许原始数据在一个方向上传输，用于保证信息安全或保护关键数字系统，如工业控制系统，免受入站网络攻击。Garland Technology的数据二极管TAP为10/100/1000M铜缆网络提供了 "无注入 "的分路聚合功能。这些产品将帮助您创建单向监控解决方案，捕获每一个比特、字节和数据包，并确保复制的数据包不会再进入并扰乱工业网络--所有这些都在一个专门设计的、不可破解的包装中。


3

## 被动、只监听的TAP将传统的设备带入工业以太网

传统设备的设计并不能超越其孤立的系统进行通信。当您开始推动传统设备将数据传输到这些专有系统之外时，就会使工业网络面临安全漏洞。

在被传统设备困扰的工业以太网环境中，对被动实时监控的需求比以往更加强烈。被动网络TAP是工业以太网环境中一个重要的连接解决方案，有被动光纤和被动10/100M铜缆两种类型。安全和监控设备必须接收100%的流量，而不向数据流引入新的或被操纵的流量。

## 4 Air-gapping网络

Air-gapping将设备和应用与外部网络和互联网物理隔离，以确保攻击者无法渗透或破坏你的IT/OT基础设施的关键组件。随着物联网设备、人工智能和虚拟化的性能要求和创新的工业 4.0用例的兴起，增加一个Air-Gapped的解决方案变得至关重要，同样具有挑战性。Garland Prisms在云环境中提供air-gapped流量镜像和TLS解密，使你的虚拟化迁移成为可能。

## 5 标准安全措施仍然适用

捍卫工业以太网仍然需要典型数据中心和IT环境中的标准安全设备。

将以太网引入工业部门时，带外安全分析工具(如入侵检测、网络检测和响应)都是必需的。数据包通过网络TAP或SPAN传送到带外解决方案，然后可以与网络数据包代理(NPB)结合，为带外解决方案聚合和整理数据包数据。

在线安全设备--新一代防火墙、入侵防御系统和数据泄漏保护也可以在工业IT基础设施中得到利用。由于在线设备放置在入站和出站流量中，确保故障不会导致停机是至关重要的。虽然一些安全设备可能有内部旁路功能，但外部旁路设备的可靠性和性能被认为是最佳做法，这使得旁路TAP对内联安全至关重要。

在工业环境和典型环境中，这些设备之间的主要区别是生产流量是标准化的。当数据中心处理来自外部用户的不同流量需求时，生产流量被设置为重复运行相同的完全相同的环路。安全设备引入的这些流量模式的任何变化都可能对网络造成严重破坏，并造成重大安全漏洞。

6

# 可见性对于确保工业以太网的安全至关重要

确保工业环境安全的最后一个也可以说是最重要的提示是网络可见性。如果在设计网络时没有考虑到可视性，那么将昂贵的安全和监控设备安装到位，并在员工培训方面投资数百万美元，都无助于保护工业以太网。当涉及到关键的基础设施时，公司无法承受盲点、丢包、流量瓶颈或遭受网络停机。在整个工业以太网框架中部署网络TAP可确保正常运行时间，并消除SPAN/镜像端口不可避免地带来的数据包交付问题。

根据SANS 2019年OT/ICS网络安全状况调查，"可见性对于管理OT/ICS系统至关重要。根据调查对象的说法，提高控制系统网络资产和配置的可见性是组织在未来18个月内预算的首要举措。"

Garland Technology 开发了一系列专为工业以太网连接设计的网络分路器，因为我们知道，保护工业以太网需要 100%的流量可见性，而无需处理或引入新数据包。

# 为实现工业网络可视化的成功最好准备

如果您想更多地了解如何弥合您的传统设备与向工业以太网和IIoT的转变之间的差距，我们很乐意为您提供帮助。请立即联系我们，了解有关可见性对您的工业以太网的重要性的更多信息。

Garland Technology 是一家为全球企业、服务提供商和政府机构提供网络产品和解决方案的行业领导者。自2011年以来，Garland Technology开发了业界最可靠的测试接入点(TAP)、网络包代理(NPB)和云可见性解决方案，使数据中心能够解决IT挑战并获得完整的网络可见性。

**虹科电子**是Garland Technology在中国的合作伙伴，虹科网络可视化与安全事业部提供网络流量可视化，网络流量采集，分析，网络安全等解决方案。

HongKe 虹科

更多详细咨询？请联系我们：network@hkaco.com

电话：400-999-3848

广州丨上海丨北京丨深圳丨武汉丨成都丨西安丨香港丨台湾

关注我们

联系我们