白皮书

# 连网再思考设计工业 IoT 网络的考量因素

**Alvis Chen**
*项目经理*

**Zig Stegner**
*技术文档撰写人*

MOXA®

如今，行业发展已呈现出全球化和数字化等新趋势。全球许多企业纷纷制定相应战略，顺应这些新趋势。由于这些趋势对企业的影响日益扩大，各企业必须应对这些趋势所引发的变革，从而保持自身的竞争力和盈利能力。然而，找到这些新兴趋势的有效应对之策并非易事。在自动化行业，大多数企业所有者都在尝试深入了解工业物联网 (IIoT)，并据此调整企业的生产和服务，确保目前甚至未来都能获得 IIoT 带来的益处。

## 重要见解

1. 向企业所有者全面介绍如何实现 IIoT 应用，并说明这类应用带来的实实在在且颇具吸引力的各种可能性。

2. 全面介绍信息技术 (IT) 与运营技术 (OT) 系统之间的连网，这被业内视为实现 IIoT 应用时面临的最重要的挑战。

3. 简要介绍多种解决方案，采用这些解决方案可以轻松、智能而高效地将 OT 和 IT 系统相连。

## IIoT – 全球趋势的创造者

在全球范围内，行业发展已呈现出全球化和数字化等趋势。这些趋势清楚地表明，企业未来发展中所面临的机遇和限制取决于企业所有者目前如何应对这些趋势。业内已涌现诸多领先举措，通过将相关的产品与系统相连寻求增加业务机会的可能，而截至 2018 年，工业物联网 (IIoT) 已经成为其中之一。设备与系统的相互融合可以大幅增加所收集的数据量，从而助力企业所有者制定更明智的决策。

大多数企业所有者已经意识到了 IIoT 的诸多益处，并已开始将 IIoT 战略纳入其业务计划之中。所有预测结果表明，到 2020 年，联网的设备将达数百亿台。如果这些设备能够有效进行通信，提高效率进而提升利润便不再是空谈，而将变为实实在在且颇具吸引力的发展前景。为实现这一目标，设备必须达到相应的智能水平，足以辨别哪些数据有用，并只将相关信息发送至 IT 系统，然后由 IT 系统对此数据进行快速解析，而无需操作员从大量未筛选数据中进行筛选。

IIoT 概念促使商业领导者思考如何制定综合性解决方案，将这些愿景变为现实。从广义上讲，IIoT 应用由四个关键部分组成：硬件、软件、服务和连网。在本白皮书中，将侧重于连网以及连网与其他组成部分之间的关联，尤其是工业自动化领域。

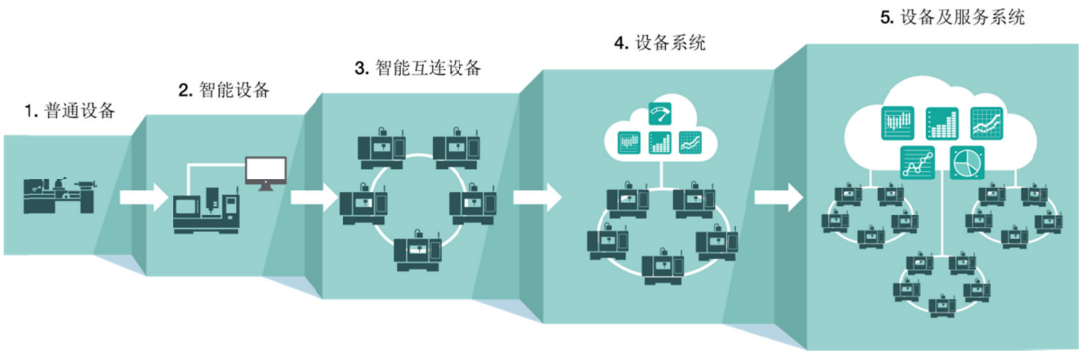
2018 年 3 月 19 日发布



Moxa 是工业自动化的领导厂商，提供完整的工业接口设备连网、工业计算机及工业网络解决方案，致力于工业互联网的共同推动与实践。Moxa 以逾 25 年的产业经验、连结全球逾 4,000 万台的工业设备，跨越 70 余国，提供全球完善的经销和服务网络；Moxa 以「可靠连网，真诚服务」的品牌承诺，协助客户打造工业通讯基础建置，提升工业自动化与通讯应用，创造长远的竞争优势及商业价值。如需获取 Moxa 解决方案的更多信息，请访问 www.moxa.com。

**Moxa 联系方式**
电话： 021-52589955
传真： 021-52585505

MOXA®
Reliable Networks ▲ Sincere Service




*在 IIoT 应用成为现实之前，必须提高设备和系统的智能水平，才能促进生产率和效率的持续改进。*

## 连网对于 IIoT 的重要意义

对于工业自动化领域的企业所有者而言，他们最关注的问题是：如何将 IIoT 概念应用到业务模型中。由于信息技术 (IT) 与运营技术 (OT) 之间存在本质上的区别，连网问题通常是企业所有者面临的首要挑战。连网是最难克服的挑战之一，但带来的诸多益处证明所付出的努力是值得的。

为展示加强连网带来的益处，本文将举例说明智能、互连的产品对于提升解决方案竞争力的重要作用。以前，John Deere 只生产农用车辆。随着 IIoT 趋势的涌现，越来越多的系统和产品支持互连，为 John Deere 呈现了向多元化发展并进一步扩大的机会。现在，John Deere 能够将以往完全不同的系统相互连接，由此打造出增强型解决方案，将灌溉系统、土壤和营养源与天气信息、农作物价格和商品期货连接起来。与过去仅仅提供农用机械相比，采用这种新型连接后，John Deere 能够帮助客户优化农场整体绩效。解决方案显著提高了效率并提升了利润，最终，竞争力大大提高。此例清楚地表明，在 IIoT 应用中实现连网后，可以为企业带来巨大益处。

## 在 IIoT 网络中实现连网的考量因素

在企业开始部署 IIoT 时，需要了解 IIoT 对企业运营带来哪些影响，以及需要对其网络进行哪些变更。企业所有者需要考虑的四大关键问题如下：连接以往未连设备时发生的更改、使用不同协议的设备之间如何进行通信、如何最大程度地缩短网络停机时间以及网络安全问题。在寻找当前可用的解决方案之前，请慎重考虑以上四点。

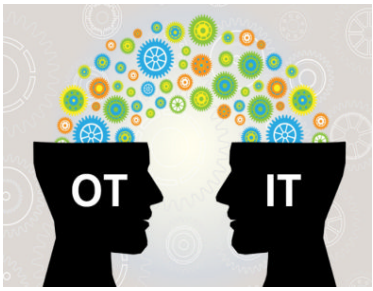
### 1. 连接未连设备时面临的问题


在自动化行业中，各公司通常会购买可以长期使用的设备。在涌现新的趋势（例如 IIoT）时，企业所有者希望在不更换现有设备的前提下，将未连网的传统设备融入现代解决方案中。总的来说，有两种方案可供选择：将传统设备直接连接到扩展网络中，或者从传统设备中提取信息并发送到其他系统。直接将传统设备连接到扩展网络很难实现；许多系统和设备使用的协议并不相同，连接时会引发通信问题，因此需要能够简化通信的解决方案。从传统设备中提取信息也变得日益困难，这是由于加入 IIoT 网络的设备越来越多，从设备中收集的数据量非常

庞大，导致操作员处理信息需要耗费大量时间。企业所有者需要寻找更智能、更高效的方法，用于从网络中部署的所有设备中提取有用数据。

## 2. 促进 OT 与 IT 系统通信时出现的问题

大多数人在日常工作、生活中通常都会使用 IT 系统，因此多多少少会了解 IT 系统的一些知识。而另一方面，人们往往并不熟悉 OT 系统。在 OT 系统内部，已开发出专有协议在现场执行具体任务。因此，OT 系统的开放性较低，不易于访问，并且不易于连接至不支持其专有协议的设备或网络。对于大多数 IT 工程师而言，将不兼容的子系统整合到 OT 环境中的需求并不常见。如果 IT 工程师不能理解遇到的各种 OT 协议，会发现将收集到的数据转换为有用信息非常困难。在工业自动化领域，经常会出现这样的情况：OT 使用现场总线协议确保实时性，而 IT 则使用 Restful API、MQTT 和 AMQP 等协议。过去，OT 和 IT 网络之间不需要直接通信，因此这些独立的协议之间也无需通信。而现在，最终目标是要确保奠定坚实的基础，使这两种网络能够支持 IIoT，从而确保企业所有者能够获得加强连网带来的益处。




若要充分利用任何智能应用的 IIoT 平台，IT 和 OT 专业人员就必须密切协作。例如，在构建智能工厂时，OT 和 IT 的问题解决方案可能会截然不同，但他们都朝着共同的目标努力：优化生产。若要成功达成这一目标，这两个领域都需要访问工业数据。IT 部门负责监管企业资源规划 (ERP) 系统，有时还需要监管 MES，他们需要对此数据进行审查并形成全局概念，然后制定相应的解决方案，解决影响运营可靠性的各个问题。OT 专业人员则更密切地参与工厂车间的实际运行，需要制定出使所有不同系统（主要配备各种专有技术）协同工作的方案。企业所有者必须找到适合的解决方案，使这两组人员和两套不同的协议协同工作。

## 3. 实时数据连网的网络要求

随着不同网络开始融合，越来越多的设备变得依赖于网络运行。虽然这能够提高效率，催生出大规模定制等各种新的可能性并带来其他诸多益处，但同时意味着 IIoT 网络不再能够使用简单的逻辑将控制器与设备相连。由于融合网络承载着不同系统之间的连接，若网络发生故障，所产生的后果将更加严重。企业所有者之所以顺应 IIoT 趋势，主要驱动因素之一是，在单一网络上采用多种通信方式可实现便捷性与灵活性，而这是各个网络和系统彼此独立运行所不能比拟的。因此，企业所有者需要确保其员工充分了解使用不同协议的融合网络，避免受到可能出现的各种问题的困扰，充分利用扩展网络的优势。此外，由于越来越多的设备依赖于 IIoT 网络运行，务必要确保网络不能出现停机，一旦停机，就会使系统崩溃，几乎必然导致企业遭受经济损失。了解如何保证 IIoT 网络的正常运行对于 IIoT 获得成功至关重要。

## 4. 网络安全从以 LAN 为中心向 LAN/WAN 融合演变

由于越来越多的 OT 系统连接到 IT 网络，了解如何确保网络安全至关重要。过去，由于 OT 数据是通过现场总线或不直接连接到互联网的封闭式专有系统传输的，人们并不太重视网络安全问题。而如今，若要成功监视异质网络的安全性，需要具备 OT 和 IT 两个领域的专有知识。尽管 IT 工程师十分精通安全协议和安全策略，但也需要 OT 工程师提供与生产流程和机器部署相关的专业知识，才能确保生产系统以最佳性能运行。此

外，为最大程度地降低成本，需要在不大幅更改现有网络环境和传统设备的情况下实施此类系统，这一点非常重要。

由于目前多个设备连接在同一网络上，如果不采取适当的安全措施，网络的所有入口点都可能发生未经授权的访问。许多工业协议在设计时并未将网络安全考虑在内，进一步加剧了问题的严重性。最初设计这些协议时，人们认为设备之间以物理方式彼此互连，若要防止未经授权的访问，只需要限制对这些设备的物理访问即可。而现在，设备频繁地与互联网相连，通过互联网即可对设备进行远程访问。由于传统协议几乎不支持加密或者用户身份验证，这种操作就会产生网络安全问题。只要有权访问网络，任何人都能够轻松地对这些设备进行访问和控制。对于公共设施和其他关键基础设施而言，这个问题十分严重。企业所有者需要解决的问题是，如何确保他们的网络在目前受到安全保护，并随着网络的不断演化，在未来网络仍然安全。

## 无缝迁移到 IIoT 网络

前文已经提到企业所有者在尝试迁移到 IIoT 网络时面临的各种问题，现在介绍一些可用的解决方案以及一些可以遵循的最佳实践，确保企业所有者获得 IIoT 带来的益处。

### 1. 将传统设备连接到 IIoT 网络

IIoT 网络需要确保所有设备之间能够相互通信。面临的最大问题通常是如何将传统设备连接到 IIoT 网络。目前，基于典型运营场景，具有两种常用方案。

第一种方案是选择工业协议网关，这种网关能够在将数据传输至 IT 系统之前，采用一种统一的通信协议对传统设备进行转换和连接。例如，将传统设备使用的各种专有工业协议转换为同一个更为常用的协议（Modbus/TCP、Ethernet/IP 或 PROFINET 等）。当 OT 工程师需要从使用不同通信协议的多个传感器和机器中提取数据时，这种转换可以大大减轻 OT 工程师的工作量。

将传统 OT 设备数据传入 IIoT 网络的第二种方案是，采用传统的 OPC（用于过程控制的 OLE）解决方案进行工业自动化远程通信。OPC 架构采用轮询模型（拉取式）从 PLC、RTU、电机驱动器和远程 I/O 等设备中获取设备数据，并与 SCADA（数据采集与监控系统）服务器和设备交换数据和命令。然而，随着 IIoT 应用中的设备/传感器数量日益增加，这种轮询方法将导致网络所需的带宽大幅增加。为解决这一问题，OPC 基金会对一种新的方法 OPC 统一架构（简称 OPC UA）进行了标准化，该方法额外提供“订阅与监控项”和“异常报告”推送式模型，只有在通信数据发生变更时才会发送数据。该方法能够提高运行效率，并能最大程度地减少所需的网络带宽。


## 2. 利用 IIoT 网关提高设备智能水平

IIoT 网关常用作 OT 和 IT 系统中的设备之间进行数据传输的桥梁。由于几乎所有 IIoT 网络当前并未采用一套通用协议，在可预见的未来，IIoT 网关将在 IIoT 网络中发挥重要作用。在此类网络中，直接跨网络传输大量数据会导致网络出现延迟，并且 IT 人员需要花费大量精力识别有用数据，从而导致数据分析延迟。为解决此问题，网关应能够支持如下一些功能，帮助提高过程效率。

**智能处理能力：**由于网关部署在许多不同的应用中，每个网关都应该有特定的规则，确保只将对应用有用的数据传输至云端，然后在云端对数据进行分析。例如，如果可接受温度范围为 -40 到 70°C，则只有当传感器记录的温度超出此范围时，才将数据传输至云端进行进一步分析。

**安全远程通信：**网关能够支持的最实用的功能之一是远程监视。IIoT 网络通常需要多个网关，因此支持远程监视至关重要，如果出现问题后可以远程纠正，则无需到现场解决。为防止存储在网关中的数据遭到篡改，应使用 TPM（可信平台模块）等文件保护系统加以保护。对于远程连接，应采用 VPN（虚拟专用网络）连接控制中心与网关。

**简化数据采集：**操作员发现非常实用的另一项功能是网关支持多种协议的功能，因为此功能有助于减少操作员的工作量。OT 和 IT 领域的工程师通常只擅长各自的领域，而此功能能够帮助弥合 OT 和 IT 领域之间的鸿沟。例如，如果设备能够自动转换 OT 工程师常用的 Modbus/TCP 和 EtherNet/IP 等协议，以及 IT 工程师常用的 SNMP 和 RESTful API 等协议，就能简化具有不同接口的设备之间的通信。此外，如果协议能够自动转换，工程师也无需掌握并不熟悉的各种协议。

## 3. 带宽充足、可用性高的网络能够避免网络中断、停机和故障

与传统网络相比，IIoT 网络中的设备更多，因此提高 IIoT 网络的可靠性显得更为重要。虽然将多个网络融合成单一 IIoT 网络会带来诸多益处，但对于企业所有者而言，网络中断、停机或故障都是特别棘手的问题，因为这意味着整个系统都将停止运行，而融合之前只有一小部分系统无法正常运行。提高 IIoT 网络可靠性的一种方法是确保网络可用性并提高带宽。高可用性意味着网络设计支持冗余功能，能够防止出现单点故障，确保网络持续正常运行。此外，这种冗余网络设计还可以最大限度地缩短修复网络问题所需的停机时间。随着加入 IIoT 网络的设备越来越多，务必确保这些设备和应用运行时不会发生延时，不会使网络过载从而导致网络崩溃。

**网络带宽：**对于使用无线技术的 IIoT 网络，802.11ac 和 4G LTE 标准提供的吞吐量和传输速度明显优于先前的标准，因此这些标准非常适合用于融合工业网络。为确保可用带宽充足，强烈建议有线以太网网络使用 10G 带宽。尽管在大多数情况下 5G 带宽可能足够，但发生网络停机的可能性会高得多。就整个网络生命周期而言，选择 5G 网络的成本几乎必然高于选择 10G 网络的成本。

**网络冗余：**随着网络扩展，其中包含的设备和应用越来越多，网络冗余会被频繁应用，这是因为网络冗余能够在发生单点故障时，避免数据包丢失。网络冗余能够确保在网络中发生单点故障时，通过当前处于活动状态的点重新路由数据，从而避免数据丢失和网络停机。

总而言之，企业所有者应部署支持充足带宽和智能冗余的网络，确保网络不会发生任何中断、停机或故障，从而使网络满足未来发展需求。

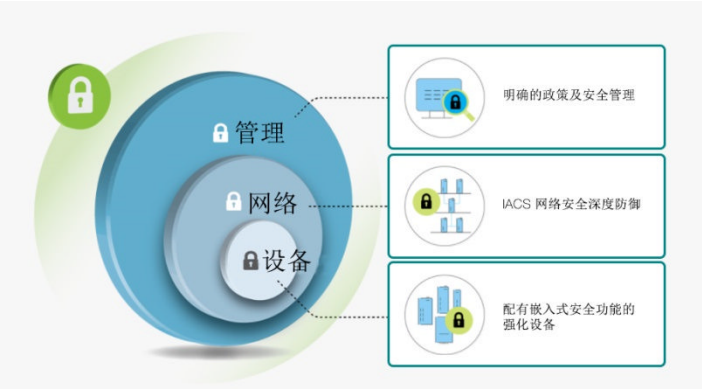
## 4. 确保目前及未来的网络安全

许多系统操作员都表示，采用深度防御安全架构是确保网络免受网络攻击的最佳方式，这种架构的设计能够保护各个独立的区域和单元。对于需要跨这些区域或单元进行的通信，必须通过防火墙或 VPN 完成。部署这种架构能够降低整个网络因遭受攻击而出现故障的可能性，因为每一层都能够应对不同的安全威胁。此外，这种架构还能降低整个网络的风险；如果网络的某一部分发生问题，该问题很可能只保留在该层，而不会向其他层蔓延。

解决网络安全问题后，需要考虑的下一步是如何避免用户无意或有意地对设置作出产生不良后果的更改。操作和管理网络的用户、第三方系统集成商以及要求执行网络维护操作的承包商都可能造成这种问题。保护网络免受这种威胁的最佳方式是增强网络设备的网络安全，确保它们的设置不会以危及设备或网络安全的方式进行更改。许多网络安全专家将 IEC 62443 标准视为对如何保护工业网络中的设备具有重大意义的出版物。此标准中包含一系列指南、报告和其他相关文件，定义了实施电子安全 IACS（工业自动化与控制系统）网络的相关程序。

在自动化系统的整个生命周期中，都需要由当地工程师或系统集成商执行维护。随着网络，特别是 IIoT 网络的不断发展和变化，需要对网络及其中的所有设备进行持续监视，确保它们受到适当保护，能够抵御网络安全威胁。由于负责监视和维护网络中不同设备的维修人员往往人数众多，让所有维修人员基于自身的知识或经验

执行安全设置并不妥当。因此，应制定良好的标准操作程序，明确定义如何配置设备设置，而所有维修人员应始终遵循这种程序。为避免发生错误，并保护网络免受所有安全威胁，务必对网络进行持续监视。




## 结论

很显然，对于企业所有者而言，部署支持 IIoT 发展趋势的解决方案和产品具有诸多益处。但是，仍然需要克服一些障碍。在这些障碍中，OT 与 IT 系统之间的连网被认为是最为重要的问题。因此，企业所有者必须特别关注他们当前的连网解决方案是否适用于 IIoT 应用。企业所有者在制定 IIoT 连网开发方案时，应将以下四大应对之策考虑在内。

1. 选择智能、高效的解决方案收集未连网传统设备中的数据，并将数据传输至 IIoT 网络的系统。
2. 为加速 OT 和 IT 系统之间的融合，部署有助于提升设备智能水平的 IIoT 网关。
3. 确保网络设计具有充足的带宽，并支持网络冗余，以便目前及未来都能够无延迟地传输数据。
4. 确保在 OT 和 IT 系统之间传输数据时网络具有充分的安全性。

企业所有者实施以上四条建议后，就能够踏上正确轨道，从而成功迁移至 IIoT 应用。

过去几年间，Moxa 因应 IIoT 趋势，开发出了边缘到云端连网解决方案支持全面工业连网，此外，还开发出计算解决方案，帮助企业所有者轻松、快速且智能地部署 IIoT 应用。

有关部署边缘到云端连网解决方案的详细信息，请访问：
http://www.moxa.com.cn/support/IIoT-Flyer.htm