

物联网

结合实际应用浅析 M2M 与物联网

文 | Peter Koldig Hansen, 丹麦 Secomea 公司的产品经理与合伙人

“Secomea 重新创造了用于 M2M、物联网或类似概念的远程通信方案。”这句描述摘录于 Secomea 在美国分销商发出的一封客户简报。

这个引用准确地描述了现实需求与流行词之间的巨大差距。本文将相关术语放在远程通信场景的方式来尝试定义 M2M（机器到机器）和物联网（Internet of Things），并为选择具有前瞻性的工业设备远程访问方案提供方向和指引（图 1）。

物联网及其延伸

让我们将 IoT 代入实际应用场景中。



图 1 丹麦 Secomea 公司的产品经理与合伙人 Peter Koldig Hansen

许多人会认为“物联网”和另外一个热门词“云”是同一概念，想象它通过因特网把万物互联的情景，可供需要的人和系统在合理的条件下使用。

IoT 起源于 M2M 和相关技术，一般而言是一个非常宽泛的概念。在较高的认知层面而言 IoT 可分为两个类别：需要人机交互的应用，即人工物联网（HIIoT）和“著名”的工业物联网（IIoT）。HIIoT 典型应用为家用温度仪表、健身记录仪或类似消费品。很容易误认为以实现交互性维护用途的远程访问工业设备方案也属于 HIIoT 范畴，特别是因为 IIoT 强调无人工介入和在此情况下运作的能力。然而下文详细说明了为什么这类 M2M 应属于 IIoT 的范畴。

IIoT 与 HIIoT 最理想的应用环境均需要 IPv6，实际上最好能解决大量已有工业设备连接 IPv6 的途径。许多 IT 从业人员都熟悉的 IIoT 的核心要素是点对点的安全体系、无单点故障、自动节点和不同应用的匹配。

将所有对技术的期望、实施条件，与现实、可预见的未来做比较，如果要很好地解决自动化行业面临的挑战与满足需求，IIoT 还有很长一段路要走。

定义 M2M

从这个角度而言，M2M 绝不仅是一个“昨日新闻”，而应是 IoT 的一个关键

组件，具有深度与实践意义。M2M 是指设备利用网络资源与远端应用进行通信，以完成监视、控制设备自身或其关联的环境（图 2）。该定义中人机交互仅仅是一个服务性附件，也可以把在人的短时间辅助下设备能完成更高级的功能认为是 M2M 定义中其中一个“M”。

因此现实中即使有人机交互环节，将 M2M 划分在 IIoT 的子集比归类在 HIIoT 更合适。

M2M 计划原则 1：从商业案例中开始

为了履行合同义务，工业设备的远程通信方案在欧洲已成为 OEM 设备厂商与系统集成商的标准配置。这不仅是为了降低员工支出和出差成本，更重要的是协议中对服务响应时间与设备在线时间的保证。随着工业设备安装的复杂程度增加，有效率地用好有限的工程师资源变得极为重要。优化服务项目和资源，要求选择合适的 M2M 解决方案，这样精力可集中放在核心业务上。

定义现阶段与可预见未来的需求

首先从以下类别中确定可满足您需求的远程服务类型：

1. 远程监视（Remote Monitoring）。远程监视或远程管理一般只从设备上采集特定预设信息，数据在中央服务器得以处理（图 3）。它的主要目的是进行预

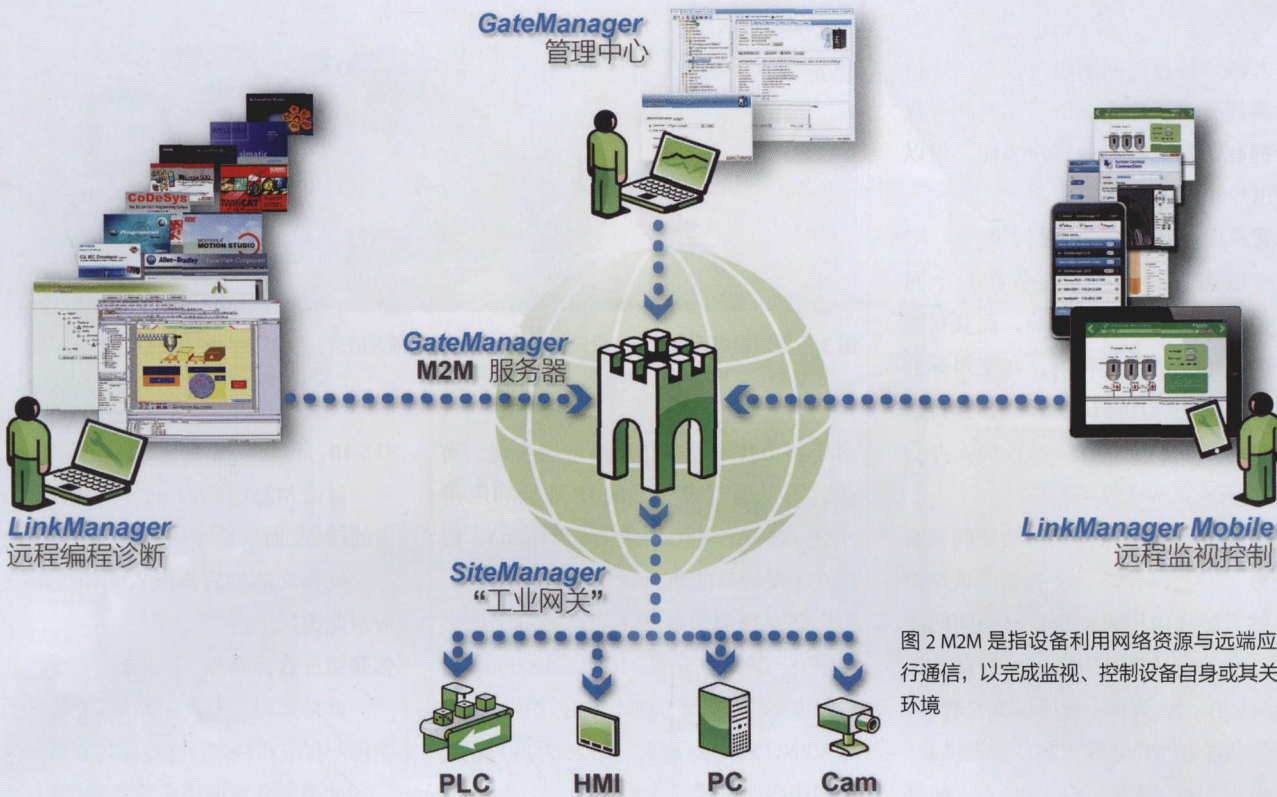


图 2 M2M 是指设备利用网络资源与远端应用进行通信，以完成监视、控制设备自身或其关联的环境

见性维护或预防性维护，如果检测出一个关键问题，技术人员将出差到现场解决。请注意这类解决方案不可通过已建立的链路远程服务设备。此类解决方案在公共事业行业应用广泛（电力、燃气、水务等）。

2. 通过远程桌面（Remote Desktop）的远程服务。许多低成本，甚至免费解决方案提供在一个局域网内设备的远程桌面访问服务。免费方案两端均需人为介入，这对工厂内的服务型 PC 而言并不现实。不需要人为介入的安全远程访问局域网设备的解决方案都不便宜。此外持续维护 Windows PC 的安全更新，再考虑在这些电脑上安装正版的 PLC 或 HMI 编程软件的成本，该方案并不是太合适。

3. 通过端口映射的远程服务。此类解决方案基于现场硬件设备充当工业设备的因特网路由器。最简单的配置方案要求在公网有一个固定 IP 地址，路由器可以路由或映射来访链路至设备上，与传统的拨号调制解调器相似。在视频监控上可常看到该类方案，将不加密的工业设备链路暴露在因特网上带来的风

险，要求固定 IP 地址，这类应用基本上为强弩之末。

4. 通过数据隧道的远程服务。这类解决方案满足大部分远程服务需求。基于 VPN 的传统 IT 方案已存在超过 10 年，近年来将 VPN 方案用于解决自动化行业的方案越来越多。绝大多数应用都是将传统 VPN 方案封装适应自动化行业的使用，可嵌入 DIN 导轨安装，使用 24 V 电源。某些厂商更进一步，打包了所有需要用户完成的复杂的 IT 设置操作和避免了防火墙设置。这类解决方案通常包括一个中央 M2M 服务器，主要作用是用户访问控制和数据转发等管理功能。至少有一个供应商，丹麦的 Secomea 完全从 VPN 方案中脱离出来，采用加密代理连接技术解决了 VPN 技术无法克服的技术瓶颈。

类别 4 是最为全面的解决方案，它们涉及到几个挑战：操作性、安全性、规模化。例如，假设如果您能以简单且安全的双向隧道方式访问设备，利用相同的设施很有可能可以满足其他远程访问需求，如数据采集。

假如类别 4 不能满足某些需求，而

需要完全不同的方案，这时请研究应用类别 4 是否会影响过程控制与资源配置。分开实施有可能会更具商业价值。

易于使用——工业安全关键环节

易于安装与设置对节省时间和让非 IT 人员实施该方案非常关键。设置防火墙、设置路由规则、安装不属于该方案的第三方软件，这类操作不是必须的。安装和初步设置可由派遣人员或现场接线的工程师完成。用户登录权限控制、设备连接设置应可由 PLC 编程工程师、OEM 项目经理或者现场负责人管理。

VPN 是一种安全与可靠的技术，用于远程连接办公室网络，也用于为远程用户提供访问总部办公室的安全链路。然而 VPN 应用在远程服务时，需求是不同用户需要访问不同现场，或者限制某些用户只访问某些设备，传统 VPN 方案在满足这类需求时是一项沉重的管理与技术任务，即使对熟练网络专家而言。请注意，安全不仅仅是加密与认证，更重要的是人的因素。因为缺乏认识，粗心以及误解造成的设置错误，就会造成安全事故。因此在方案中应尽量减少依赖熟练专家和深奥的技术文档的需求。

大部分远程访问解决方案都会宣传安全靠加密, 这种情况下请花时间寻找一个拥有友好可视化的用户界面, 用以管理用户和现场权限。

使用客户现场网络的安全性讨论

一般而言, 工厂或设备在一个网络与企业办公网络是独立的, 而且只有办公网络可以访问因特网。在使用标准VPN 功能路由器访问设备网络的时候, 您需要将该路由器的WAN 口接入办公网络, LAN 口接入设备网络。

IT 部门此时会不高兴网络之间装有一个第三方的设备, 即使您重申该路由器内置了防火墙用来抵御在网络间的非授权访问。而且您必须精准地解释该设备如何运作, 它为何不会降低安全程度。这类信息将由远程通信方案厂商提供。

此外, 这类解决方案必须能在一般都开放的端口上建立加密隧道链路。这可以是web 端口80 (Http), 443 (https)。别希望IT 部门会根据您的意愿来开放端口。

某些情况下, 企业政策不允许任何第三方设备通过企业网络获得因特网连接, 与IT 部门争取也许不明智, 最好寻找其他途径或妥协。可以要求客户为设备建立独立的网络, 或者选择带有无线模块的远程通信设备。

网络冲突

也许连接多个用户和网络时最常见的问题是网络冲突。在通过路由器或VPN 静态连接多个网络时, 所有网络必须有不同的IP 子网。这在未来的IPv6 不是一个问题, 但在应用IPv4 的今天以及未来很多年中都肯定是。

典型例子是两个工厂可能使用完全相同的IP 子网。大部分工业远程访问设备解决该问题是通过动态建立按需连接, 完成后再关闭。唯一限制是2 个服务工程师不能同时连接到一个工厂, 当然这种情况也不多。

更麻烦的任务是工程师所在网络与工厂网络一样的情况下(例如, 工程师子网为192.168.0.10/24, 他尝试通过VPN 连接一个拥有相同子网的工厂)。



图3 远程监视或远程管理一般只从设备上采集特定预设信息, 数据在中央服务器得以处理

对于路由技术而言, 这不可能实现。当然这可以通过设置别的IP 地址和应用NAT (Network Access Translation), 但这个不是轻易能完成的。

您必须确保远程访问产品对于此类情景有一种解决方案。例如, Secomea 的解决方案则是基于加密代理连接技术而不是VPN, 对此类子网冲突是天生免疫的。

双因子权鉴登录

典型的VPN 方案静态连接办公网络是基于x.509 证书, 在建立VPN 初始连接时手动进行交换。近年来基于SSL/TLS 的VPN 方案因为防火墙友好型和自动双向认证变得流行。对于此类用于工业访问的解决方案的担忧是最初的连接仅仅是基于用户名和密码。

双因子权鉴登录意味着您拥有额外的权鉴, 例如, 安装在PC 上的个人证书文件或者一个具有时效的手机短信。

因此请确保您选择的远程访问方案拥有双因子权鉴登录功能。

可追溯的日志查询

日志文档可查看何人、何时访问了何物。主要目的不仅是记录某个远程用户对设备做的变动造成的影响, 更是确保服务工程师是否完成其服务任务。

确认是否存在日志, 以及如何访问日志。

查看安全标准

在自动化行业, 设备安全与系统安全同等重要。运动的设备安全事宜甚至被提上政府规章制度, 确保OEM 厂商在远程服务时必须合理提示现场操作人员正在进行远程操作。(欧洲标准如EN

415-10, 包装机械的安全标准)

讨论M2M 和IoT 的专家有忽视该需求的趋势, 而只关注系统安全和互动性。

确保您的供应商嵌入了相关方案来应对此类规定。

依赖第三方云服务

此前提到, 中央M2M 服务器对于控制用户权限和数据转接链路越来越关键。

此类服务可能免费或者有维护费用。详细了解其规模化后的成本并为此制定预算方案。

最重要的是您需要研究M2M 服务器只有由厂商托管的云服务器, 或者可自建M2M 服务器上。大型OEM 厂商通常不喜欢受限于某个厂商的服务以及服务器在线时间以及执行的安全措施(一般远程访问厂商可以看到根目录下的所有设备)。

总结

由于远程通信厂商采用因特网作为链路基础, IT 行业新技术和潮流的快速发展现在成为自动化行业中讨论的热门话题。这些由工业解决方案厂商开始引用的新词为自动化行业的决策者们造成了疑惑和不确定性。

首要原则: 理性地看待, 不要让IoT 和IPv6 的蓝图主导了决策, 确认您偏好的服务提供商是否符合技术演变的潮流。

首先且着重需要考虑什么方案可以在目前以及在预期优化您的业务, 以及这些优化如何让您的客户受益。使用以上所列的方法来协助您选择最合适的解决方案。**MM**