SIEMENS
Ingenuity for life

链接虚拟与现实

护航工业通信网络与企业 IT 系统连接安全

siemens.com/industrial-networks

概述

随着数字化的高速发展，海量数据的快速增长，工业企业正在孜孜寻求一种面向未来的可靠通信解决方案，以确保企业的竞争优势。针对企业独特需求而量身定制的自动化网络，必须在自动化层级和企业 IT 系统之间建立起可靠的连接。作为全球数字化转型的推动者，西门子在工业网络规划、设计和实施方面有着多年的丰富经验，而不仅仅是只给客户提供各种网络技术的供应商。除了提供定制化工业通信网络产品，西门子还提供全面的设计与实施支持，并确保工业通信网络与企业 IT 系统的连接能够满足未来不断变化的需求。西门子正是以这种方式在引领着发展前行之路，以实现高效的数字化流程，确保从传感器层直至管理层的端到端通信永不掉线。

1 工业通信网络对数字化的重要性

数字化为工业带来许多崭新的发展机会和前景。举例而言，智能数据分析可帮助企业提前开展生产流程规划与优化工作。数字化还助力过程工业提高了资源以及成本的利用率，为贯彻领先的能源供应理念以及实现道路和轨道交通管制提供支持。

要兑现数字化的各项承诺，就必须把不断涌现的数据采集起来，记录、存储和处理数据，并用数据进行通信。

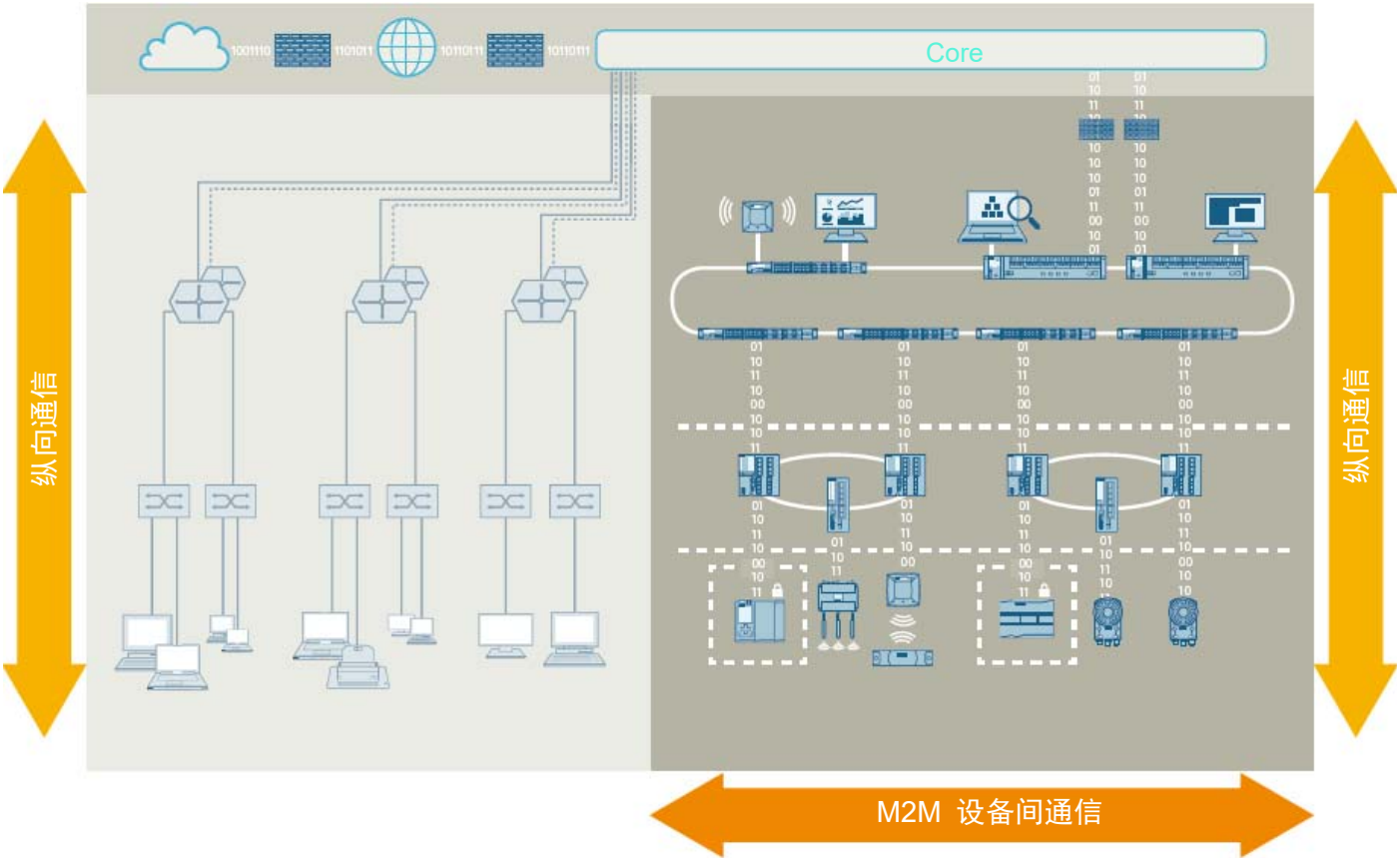
高效能的工业通信网络可以帮助整个价值链不间断地实施实时数据交换，并且在所有企业层级实现纵向数据交换。然而，这些网络必须能够满足处理数字化信息载荷的严格要求，包括具备高可用性、以及具备坚固耐用、高度灵活的组件。同时，还必须能够保证数据安全和工厂各方面的功能安全，以满足进行决定性通信的需要。

这些要求对于工业通信网络与企业 IT 系统之间建立安全连接尤为重要。除非通过专门设计把这两大网络的要求纳入考虑范围，否则，这样的连接可能带来风险，危及到数据的安全和网络的稳定性。

设计、规划和实施工业通信网络并将其与企业 IT 系统相互连接，一定要具备高水平的专业技术知识与经验，还要对具体的应用有着全面的了解。如果不是由专业人员从满足具体行业需求的角度规划工业网络，是无法满足数字化工业的各项要求的。

2 标准 IT 网络与工业通信网络的区别

IT 系统与自动化网络的不同之处主要在于通信设计的目标不同。例如，IT 系统的重点是在架构传输方面，而生产则需要获得最优的正常运行时间。因此，必须同时考虑到对网络组件和拓扑结构的不同要求，才能满足对工厂可用性的各种期望值。



2.1 数据流

除了极少的例外情况，通常办公电脑都要和一台或者多台服务器进行通信。所以，与其他情形相比，在设计网络拓扑结构时，必须满足繁重的单向高带宽通信的需要。一般情况下，单个终端的故障不会对正常的业务进行造成影响，不会带来严重问题。

自动化所考虑的重点是设备与设备的通信（M2M）以及具体的应用。在所有设备上，必须实现持续不断的数据交换。如果数据丢失或者延迟，就会引发工厂停工，直接影响到业务的进行。因此，设备与设备之间的网络通信一定要在规定的响应时间内进行并通过验证。

这种确定性的通信设计是自动化网络与IT 系统的一个重要区别，是实现可靠的设备与设备间通信和工业循环控制流程的先决条件。如果网络组件不能满足这些要求，就可能出现安全应用无法可靠执行之类的问题，进而有可能造成工厂无法正常运转。

2.2 基础设施

数据流设计方面的区别也会影响工业通信网络的基础设施。

单纯为实现纵向通信设计的包括核心层、汇聚层、以及接入层的网络（最典型的当属传统IT 系统）很难保证数据流能够持续不断地流向生产层的设备。在这种情况下，有可能出现数据延迟，危及工厂的可靠运行。经验证明，在有些时候，数据流中断都是在工厂运行一段时间后才发生的，往往很难把问题准确诊断出来。

由于工业通信网络中基于以太网的通信（一种历史性的 IT 标准）不断繁衍发展，一些专用网络设计方案已经成型，这些设计全部都是为不同工业领域里的不同应用量身定制的方案。这样做的目的就是要在工业通信网络和企业 IT 系统之间建立起一种天然的、必不可少的连接。

2.3 服务

工业环境中的环境条件与数据中心和办公室里的气候条件有着巨大区别。因此，工业网络的组件还必须能在恶劣的环境条件下可靠发挥各项功能，包括在极冷、极热、靠近强电磁干扰以及存在爆炸可能的环境，甚至在剧烈振动或震动的应用中，如运输设备。

此外，办公组件的设计、维护和服务便利性，通常都不是按工业环境的各项要求量身定制的。与此相反，工业通信网络则必须具备两大易于维护的核心组件。第一，网络组件必须能得到自动化人员的访问从而对其进行维护和保养；第二，必须能够通过合适的综合诊断检测工具，快速、明白地完成故障定位，尤其是复杂的网络基础设施的故障定位。

2.4 人员

故障发生或维修/服务完成后迅速恢复正常功能，是每一座工厂的工作当中的重中之重，一般没有时间等待 IT 服务商来确定问题发生的位置并将问题解决。

外包是标准 IT 应用很常见的一种做法。尽管如此，公司员工通常还要负责把与维护和故障相关的停机时间缩减到最短。然而，并非所有的企业都有全天候待命的随叫随到的 IT 专家，因此，自动化技术人员还必须熟练掌握各项网络技术。

西门子的工业网络培训部推出了培训认证项目，可以为工厂的自动化人员提供全面的工业通信网络培训。

2.5 安全与信息安全

工业环境中的功能安全是与数据安全有区别的。“安全”一词指的是与人员、设备和工厂的保护相关的各项职能。紧急情况下，必须能够有机会把某个单件设备、工厂的某个部分、或者工厂的整个综合体转移到安全状态。要想做到这一点，就必须能立即把数据直接转移到关键控制单元。无论采用何种介质，都必须把安全信号以最高优先级可靠地传送出去。

工业安全比信息安全有着更高的优先级。尽管如此，随着办公网络和自动化网络的不断增加，对工业通信网络运营商提出了更高的要求：必须密切关注数据信息的安全。事实上，信息安全是通信网络最常遇到的陷阱和风险。办公网络中那些必要的和有利的特性都可能给工业环境带来实质性的破坏。防病毒软件、更新、网络分析等，可能引发工厂停工等不可预见的问题。软件和硬件不兼容也是让人头痛的问题。

工业通信网络需要全面的交错的安全和信息安全理念，需要为工厂提供物理性的保护，还要防范来自未经授权的用户或公司外部人员的攻击。

西门子推出的“纵深防御”是一个多层次的信息安全理念，建立在工厂安全、网络安全和延伸至控制层的系统完整性保护这三大基石上。

2.6 可用性

工业厂房要想避免经济损失的发生，就必须要具备高可用性。所以，工业通信网络的连接必须采用冗余设计。设备备份、专用网络协议、以及多路径拓扑结构等机制均有助于实现相应的冗余程序。

工业骨干网

工业骨干网中，冗余是确保高可用性的重要方法。骨干网必须适于满足工业环境的各项要求，并安装在经过培训的自动化人员需要访问的工业区域内。

工业骨干网的主要任务是在企业 IT 系统和工业通信网络之间快速完成数据交换，要求工业通信网络中的单个组件以冗余的方式连接到工业骨干网。为此，通常采用环状结构。经验证明，这些结构是构建工业通信网络的非常稳定、清晰、可用性高的方法。

第 2 层冗余协议的功能是阻断环路的某条路径，并监控所有其他连接功能是否正确。如果检测到某个设备发生中断或故障，则将阻塞的路径开放并建立起一个新的连接。一旦故障得到纠正，拓扑结构便又恢复到自己的原始状态。

2.6.1 MRP 协议

MRP 是一项第二层冗余协议，是构成PROFINET标准的组成部分。该协议对设备数量不超过 50 台的环路的收敛时间短于 200 ms。MRP 帧只在环路的内部移动，不会在环与环之间传输。由于采用标准化，MRP 协议既存在于自动化设备中，也存在于网络组件中。

2.6.2 HRP 协议

与 MRP 一样，HRP 也是一项第二层冗余协议。在设备数量不超过 50 台的环路中，收敛时间短于 300 ms。HRP帧只在单个环路的内部移动，不会在单个环路之间传输。通过备用连接，多个环路可以实现冗余连接。

2.6.3 RSTP 和 MSTP

与 MRP 和 HRP 不同，RSTP 是一项点到点协议，意味着信息交换只在相邻设备之间进行。根据问题、所涉及的设备数量及故障类型的不同，收敛时间短则几毫秒，多则长达数秒。在最不顺畅的情况下，网络需要的收敛时间最长，在数秒时间内无法传输任何数据包。因此，对实时应用和需要采取确定性行为的自动化网络应用，RSTP 协议都不是首选。

MSTP 是 RSTP 协议的增强版，可支持同一物理网络中不同虚拟局域网(VLAN)的不同拓扑结构。MSTP 协议的作用与 RSTP 协议基本相同，但是，其还可将不同交换机确定为不同子网的“根网桥”（即“数据节点”），使数据载荷的分布更加完善。

3 连接工业通信网络与企业 IT 系统

在考虑自动化网络和标准 IT 系统的区别时，有一个问题：如果说可靠的端到端数据传输是实现高效率数字化流程的先决条件，那么组织应对如何做，才能把这两个环境结合到一起？

对这个问题的回答是：不要把这两个环境结合到一起，而是要把二者分隔开。关键的一点就是把工业通信网络从企业网络中分隔并隔离出来。第三层隔离可以为工业骨干网和核心系统提供一个安全而设计清晰的连接，从而防止企业网络和工业通信网络之间发生相互影响。

在把工业骨干网连接到核心系统时，一定要注意以下几个方面：

- 仅有维护数据交换和通讯关系方面的工业应用才允许网络间的相互访问
- 确保为数据中心、办公室和自动化网络提供足够到位的保护
- 确保可用性和端到端通信的连续性
- 有机会监测和控制数据交换的情况

3.1 访问规则

如上所述，在把工业骨干网连接到数据中心的核心系统时，可以不通过办公网络而直接通信。

这样，MES 系统（制造执行系统）就可以和 ERP 系统（企业资源规划系统）直接通过自动化层进行数据交换，而无需从办公网络绕行。

但是，在这种情况下，建立工业通信网络架构和管控数据交换是有意义的，通常是把工业通信网从逻辑上划分为几个互不相连的部分，也就是所说的“虚拟局域网”（VLANs）。

通过这种功能上的网络分隔，可以针对每一个子网实施专用的访问规则，从而防止未经授权的访问。如果不允许单个子网（VLANs）之间相互通信，则须通过适当的工业防火墙或访问控制名单（ACL）来防止子网间相互通信的发生。

3.2. 连接类型

要在工业通信网络和企业网络之间建立安全连接，可以采用不同的方法，一种方法是静态路径选择，还有一种方法是动态路径选择。在非常罕见的情况下，还可采用第二层连接直接接入核心系统。下面分别对这三种连接方法进行详细的介绍。

3.2.1 静态路径选择

静态路径选择用的是骨干网和核心系统之间的双向路径，由人工输入。这种方法的优点是：只有被网络期待的连接才会被路由器选择。尽管如此，对于庞大而又复杂的网络而言，静态路径选择的管理工作可能会耗费非常多的时间。

静态路径选择采用虚拟路径选择冗余协议（VRRP）。VRRP协议允许在虚拟IP（互联网协议）和 MAC（介质访问控制）地址下将多个路由器合并成一个逻辑冗余路由器。

其中一个路由器会激活并使用虚拟 IP 地址和 MAC 地址工作，作为主机发挥作用。辅助路由器（从站 ）负责监测主路由器的状态。如果辅助路由器监测到主路由器不再做出响应，就会把虚拟 IP 地址和 MAC 地址接管过来，以确保网络和网关保持正常的功能。

3.2.2 动态路由选择

单个网络之间的动态路径选择是自动获知的，这是建立庞大而复杂的网络时的一个优点。如果单个连接发生故障，则会自动将替代路径搜索出来，或由已知的路径发挥作用。西门子的 SCALANCE XM-400 和 XR-500 系列产品支持用来创建动态路径选择表的 RIP 工业标准协议以及 OSPF 工业标准协议。

RIP 是一个“距离矢量”协议，特点就是简单易用、实施方便。RIP协议会和邻近的路由器自动交换路径选择表。实现这一点的方法就是：每隔 30 秒，就进行一次“宣告”。但是，由于时间的跨度太大，路径选择变更传达到网络的速度会非常慢。因此，RIP 协议通常因为兼容性考虑而被使用。

OSPF 不同于 RIP 协议。OSPF 是一个“链接状态”协议。其特点是扩展性极强，而在发生故障时，切换时间非常短。每个参与到OSPF 协议的路由器都会自动为自己的区域建立一个网络拓扑数据库，并与临近的路由器同步。变更则是以递增方式实现同步。以这种拓扑数据库为基础，每个路由器都可以独立计算出通过网络的最优路径。

经过良好规划，还可以用 OSPF 协议建立庞大而复杂的网络。这点使该协议成为把工业通信网络与企业网络相连接的最佳选择。

3.2.3 第二层连接

特殊情况下，还可在工业通信网络和企业网络之间实施第二层连接。但是，这样做之前需要进行周密的考虑和构想，因为这会带来风险，也就是企业网络和工业通信网络之间会产生相互影响，从而危及到网络的稳定性。

如果网络发生错误，第二层连接会给故障排除工作带来更多的困难，因为不能清楚地判定故障所在的位置。网络中的所有区域都有可能受到影响。因此，对于工厂可用性，第二层连接不应当是第一选择，而应在认真规划之后再行考虑。

4 西门子助您实现企业网络与工业通信网络的安全连接

工业通信网络的重要性今非昔比，对实现数字化进程和在不断变化的市场保持竞争力必不可少。这些网络的作用并不只是所有组成部分的叠加，而是必须开展详细的规划与分析、通过定制化的设计方案确保与企业的信息环境实现安全和可靠的连接。

这里面包括为实现安全可靠灵活的通信而开展的领先的以太网解决方案的具体实施。另外，还要提供有资质的支持服务，才能建立起当今大部分非常复杂的工业通信网络。

作为工业领域的合作伙伴，西门子可提供完善的网络产品组合、完善的服务和经过认证的培训项目。西门子是解决方案提供商，拥有多年积累的丰富经验和深厚的专业技术知识，可帮助客户设计并实施能满足未来发展需要的工业网络解决方案，并已在全球范围内获得经过认证的西门子工业领域知名合作伙伴的支持。

西门子为您提供：

量身定制的产品

西门子凭借丰富的自动化领域工作经验，非常清楚企业对工业骨干网和企业网络之间的连接提出的要求。针对与企业网络的连接，西门子推出了 SCALANCE XR-500 工业以太网交换机。这些高性能产品可以满足商用交换机的需求以及工业设备的特殊需要。

www.siemens.com/x-500

专业化服务

西门子针对工业网络提供专业化的服务，包括各种服务与支持，内容非常全面，可帮助客户规划并实施工业通信网络；还可提供与网络设计有关的各种咨询服务、现场详细分析服务、以及确保迅速完成调试实施的服务和高质量的培训课程。西门子专业服务团队将帮助客户稳步完成各项工作的具体实施。

www.siemens.com/industrial-networks-services

培训与认证服务

西门子“工业网络教育”培训认证项目可以帮助企业培训工业通信网络工作人员。该培训项目覆盖面广，包含交换、路由、安全、甚至无线网在内，内容丰富全面。“工业网络教育”项目可以提供涵盖各相关领域的专家级的专业知识。自动化人员将会受到把工业通信网络作为自动化技术与 IT 接口的全方位培训。

www.siemens.com/industrial-networks-education

SCALANCE XR-500 可以为客户带来以下几方面获益：

- 由于全部采用模块化设计，网络的扩展和修改变得非常灵活，没有任何限制条件；
- 即使在运行过程中也可以经由组合端口实现电气设备联网和光纤联网（SCALANCE XR524-8C/XR526-8C)（热插拔）；
- 由于全部采用模块化设计，降低了不同型号设备的现货库存成本；
- 采用 KEY-PLUG 方式，无需更换硬件，即可选择实施第三层功能改造；
- 由于提供冗余电源供应、C-PLUG 可插拔介质和冗余功能，可用性大幅提高；
- 各种各样的衍生型号，通过不同的可选冗余供电（交流电/直流电）满足全部要求；
- 设备性能得到提高，经由 10 Gbps 端口实现海量数据传输；
- SCALANCE XR-528 和 XR-552 这两款模块化交换机的连接密度更高，针对不同传输介质，灵活性也更强。

西门子股份公司

过程工业与驱动技术集团
2017 年出版
邮箱：48 48
德国纽伦堡，90026

安全信息

为了保护工厂、系统、设备以及网络免于受到来自网络的威胁，有必要采取一套整体性的先进工业安全理念，并不断维护更新。西门子的产品和解决方案只是这一理念的组成部分。

客户应负责保护自己的工厂、系统、设备以及网络免于受到未经授权的访问。系统、设备以及部件都只能与企业网或采取了某种程度上适当而且必要的安全措施的（如采用防火墙和网络分隔等方法）互联网连接。

此外，还应将西门子的适当安全措施指南纳入考虑范围。如果您还需了解关于工业信息安全的其他信息，请登录：www.siemens.com/industrialsecurity。

西门子的产品和解决方案始终在进一步开发过程中，以便提高其安全性能。西门子强烈建议在产品更新推出时就立即采用，并始终使用最新版本的产品。使用不再受到支持的产品版本或者不采用最新的更新，都会使客户暴露于来自网络的威胁之下。

如需及时收到产品更新信息，敬请登录

www.siemens.com/industrialsecurity，订阅西门子《工业安全 RSS 讯息汇编》。