全厂融合以太网架构中的工业防火墙

白皮书

2016 年 12 月

罗克韦尔自动化与思科四大举措：

- 通用技术前景：
  使用开放式 Ethernet IP 标准网络技术的单一可扩展架构对于实现工业 物 联 网并在竞争激烈的制造环境中实现灵活性、可见性和效率 至关重要。

- 全厂融合以太网架构：
  由思科和罗克韦尔自动化专门技术部门开发的经测试和验证的架构集合。CPwE 的内容与运营技术 (OT) 和信息技术 (IT) 领域相关，包括已形成文档的架构、最佳范例、指导和配置设置，可帮助制造商设计和部署可扩展、可靠、安全且面向未来的全厂工业网络基础设施。

- 联合产品协同开发：
  Stratix®5950 工业防火墙、 Stratix 5100 无线接入点 / 工作组网桥以及 Stratix 5700、 Stratix 5400 和 Stratix 5410 工业以太网交换机，结合了思科和罗克韦尔自动化的最优秀成果。

- 员工与过程优化：
  通过关于运营技术 (OT) 和信息技术 (IT) 融合的培训和服务，有助于实现成功的架构部署以及高效运行，从而使关键资源能够专注于提高创新力和生产率。

文档参考编号：ENET-WP011B-ZH-P

全厂融合以太网架构中的工业防火墙

工业自动化与控制系统 (IACS) 网络的普遍趋势是技术融合，特别是 IACS 运营技术 (OT) 与信息技术 (IT) 的融合。 全厂融合以太网 (CPWE) 通过使用标准以太网和 Internet 协议 (IP) 技术来帮助实现网络技术融合，从而助力工业物联网 (IIoT) 的实现。

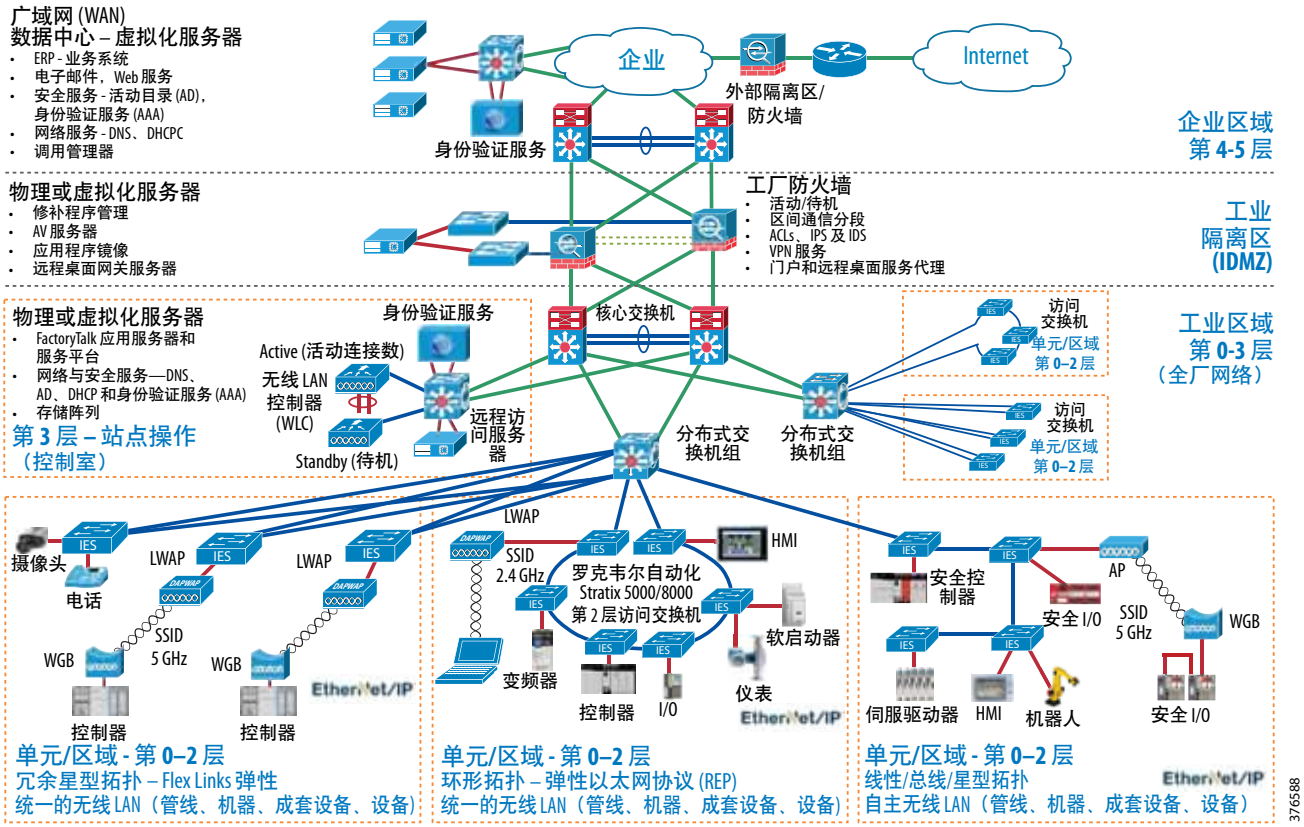
默认情况下，融合 IACS 网络通常是开放的。 开放性可实现技术共存并改善 IACS 设备互操作性，从而助于选择一流的 IACS 产品。 这种开放性还要求 IACS 网络通过配置和架构实现保护和强化。 强化的程度取决于所需的安全政策。 业务实践、企业标准、安全策略、应用要求、行业安全标准、法规合格性、风险管理策略和风险总体容忍度都是确定适当安全政策的关键因素。

工业防火墙 (IFW) 的全厂部署是全面纵深防御的工业安全政策的一部分，有助于强化 IACS 网络基础设施，并创建更小的信任区域。 工业防火墙有能力限制和检查全厂范围的 IACS 网络中的通信流。 OT 人员通常应用工业防火墙来保护其早期 IACS 应用 - 设备、机器或成套设备。 原始设备制造商 (OEM) 将工业防火墙作为其产品的一部分，这种做法变得越来越普遍。 为了支持 OT 和 IT 的融合，现代工业防火墙具有使用本地或集中管理的多种不同用法进行部署和管理的能力。 本地管理对于 OT 工厂人员和 OEM 应用较为常见。 而集中管理对 IT 来说则较为常见。

有关在全厂融合以太网架构 CVD （思科和罗克韦尔自动化验证设计）中部署工业防火墙的信息记录于 Deploying Industrial Firewalls within a CPwE Architecture Design and Implementation Guide (DIG) 中，该信息列出了在全厂 IACS 网络中设计、部署和管理工业防火墙的几个使用案例。 CPwE 工业防火墙 CVD 通过思科和罗克韦尔自动化间的战略联盟而投入市场。

CPwE 作为一种基础架构，可为现代 IACS 应用所采用的控制和信息策略、装置和设备提供标准网络服务。 CPw E架构 (图 1) 通过思科和罗克韦尔自动化的测试和验证，可提供设计和实施指导、测试结果和记录的配置设置，从而帮助实现现代 IACS 应用对实时通信、可靠性、可扩展性、安全性和弹性的要求。

图 1　　CPwE 架构



注意　这一版本的 CPwE 架构侧重于 EtherNet/IP™，而该网络采用 ODVA 通用工业协议 (CIP™)，可实现工业物联网 (IIoT)。有关 EtherNet/IP 的详细信息，请参见 odva.org，网址如下：http：//www.odva.org/Technology-Standards/EtherNet-IP/Overview

整体工业安全

没有任何一种产品、技术或方法能够完全保护 IACS 应用的安全。保护 IACS 资产需要采用能够应对内部和外部安全威胁的纵深防御安全方案。此方法利用多层防御（管理的、技术的和物理的），在各个 IACS 级别应对不同类型的威胁。CPwE 工业网络安全框架 (图 2) 采用纵深防御方案，符合工业安全标准，例如 IEC-62443（原 ISA-99）工业自动化和控制系统 (IACS) 安全和 NIST 800-82 工业控制系统 (ICS) 安全。

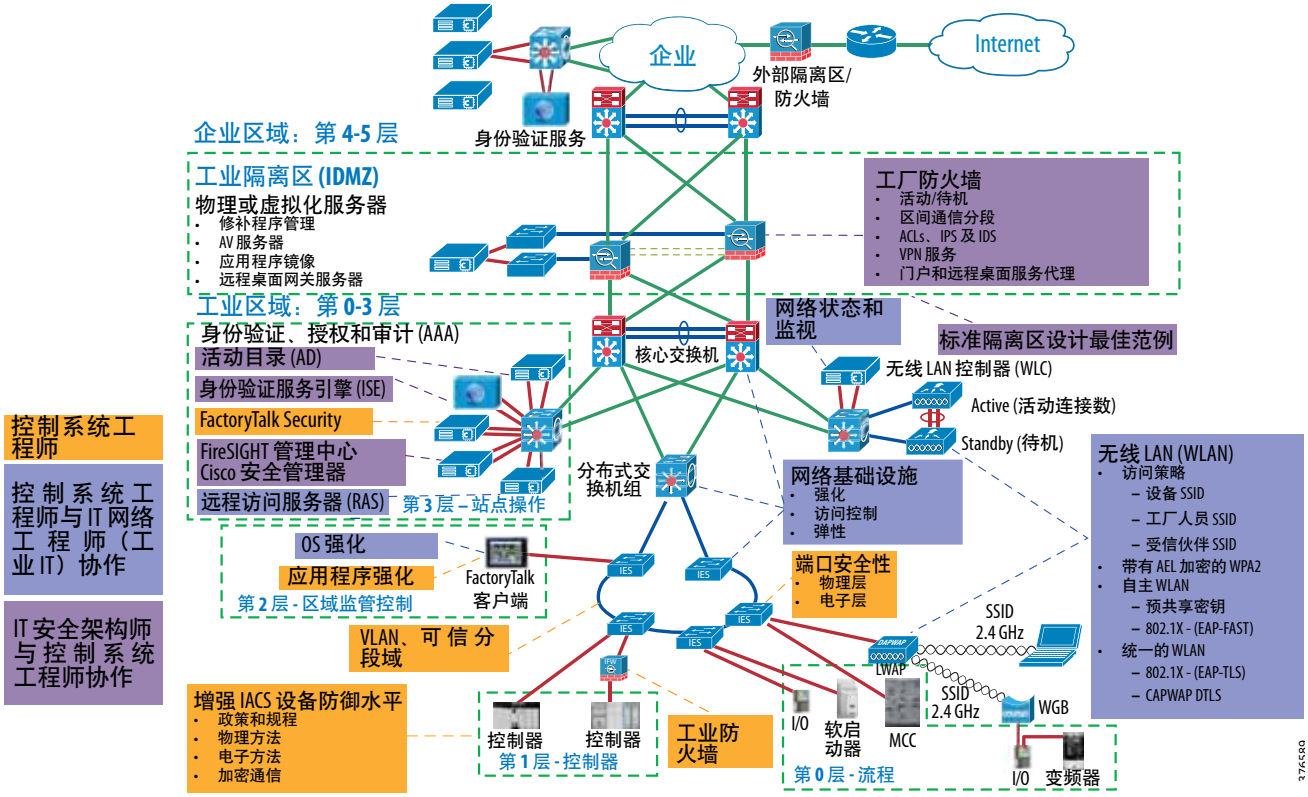
设计和实施全面的 IACS 网络安全框架应该是 IACS 应用的自然延伸。网络安全不应作为事后补充来实施；工业网络安全框架应该在 IACS 中普及并成为其核心，不过对于现有的 IACS 部署，可逐渐增加相同纵深防御层的使用，以改善 IACS 的安全政策。

CPwE 纵深防御层 (图 2) 包括：

- 控制系统工程师（以棕色突出显示）— 增强 IACS 设备防御水平（例如，物理和电子防御）、增强基础设施设备防御水平（例如，端口安全）、网络分段（信任分区）、在 IACS 应用边缘的工业防火墙（带检测）、IACS 应用认证、授权和审计 (AAA)
- 控制系统工程师与 IT 网络工程师协作（以蓝色突出显示） — 增强计算机防御水平（OS 修补、应用程序白名单）、增强网络设备防御水平（例如，访问控制、弹性）、无线 LAN 访问策略

- IT 安全架构师与控制系统工程师协作（以紫色突出显示）— 身份验证服务（有线和无线）、活动目录 (AD)、远程访问服务器、工厂防火墙、工业隔离区 (IDMZ) 设计最佳实践

图 2 CPwE 工业网络安全框架



工业防火墙使用案例

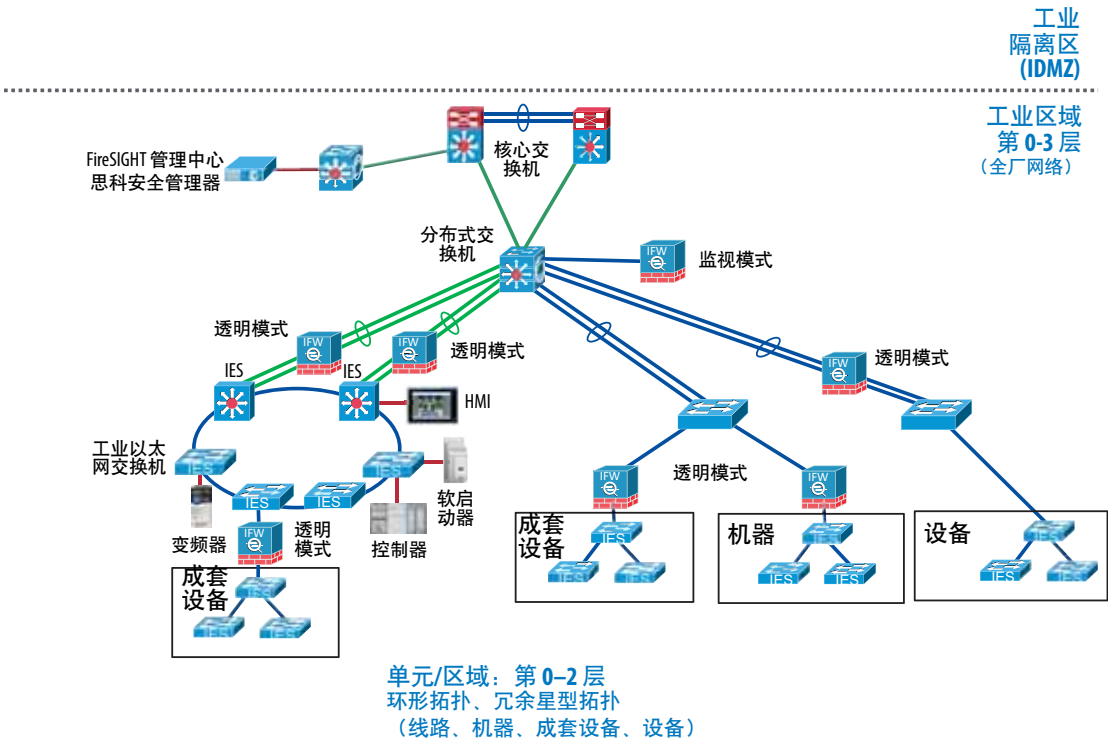
IACS 部署在各种离散和过程制造行业，如汽车、制药、消费品、纸浆和纸张、石油和天然气、采矿和能源。 IACS 应用由多个控制和信息领域组成，如连续过程、批次、离散和混合组合。 对标准以太网和 IP 融合 IACS 网络技术进行工业强化，从而利用与工业物联网 (IIoT) 相关的业务优势，这是制造商面临的挑战之一。

Deploying Industrial Firewalls within a CPwE Architecture DIG 概述了用于经过思科和罗克韦尔自动化测试、验证和记录的应用案例的概念、要求和技术解决方案，为强化和融合后的全厂 EtherNet/IP™ IACS 架构提供支持和帮助。 以下是 CPwE IFW CVD 使用案例的总结：

- 工业防火墙技术概述：
  - 工作模式：
    - 在线透明模式
    - 在线路由模式
    - 无源监视 - 仅模式
  - 网络防护（思科自适应安全设备）
  - 入侵防护和检测（思科 FireSIGHT® 管理系统）、通用工业协议 (CIP) 的深度包检测 (DPI)
  - 工业防火墙 (IFW)：

  - Allen-Bradley® Stratix® 5950 工业网络安全设备
  - 思科工业网络安全设备 3000
- 应用案例 (图 3)：
  - 设备/机器/成套设备保护
  - 单元/区域保护：
    - 冗余星型拓扑、环形拓扑
  - 单元/区域监视
- 管理使用案例：
  - 本地管理：
    - 命令行接口 (CLI)、自适应安全设备管理器
  - 集中管理：
    - 思科 FireSIGHT 管理中心、思科安全管理器
  - 工业防火墙从本地管理改为集中管理

图 3　　全厂工业防火墙部署



总结

CPwE 是由思科和罗克韦尔自动化的专门技术部门，按照思科验证设计 (CVD) 方案而开发的经过测试和验证的架构集合。 CPwE 的内容与运营技术 (OT) 和信息技术 (IT) 领域相关，包括已形成文档的架构、最佳范例、指导和配置设置，可帮助制造商设计和部署可扩展、可靠、安全且面向未来的全厂工业网络基础设施。 CPwE 还可通过久经考验的设计，帮助制造商降低成本，从而在部署新技术时，加快部署速度，降低部署风险。

Deploying Industrial Firewalls within a Converged Plantwide Ethernet Architecture Design and Implementation Guide (DIG) 列出了在全厂工业自动化和控制系统 (IACS) 网络基础架构中设计、部署和管理工业防火墙的多种使用案例。 该 DIG 强调了 IACS 应用要求、技术和支持设计考虑因素，以帮助在 CPwE 框架内成功设计和部署这些具体使用案例。

有关 CPwE 设计和实施指南的更多信息，请访问以下 URL：

- 罗克韦尔自动化网站：
  - http://www.rockwellautomation.com/global/products-technologies/network-technology/architectures.page?
- 思科网站：
  - http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/landing_ettf.html

注意

本文档将 FireSIGHT 管理中心作为 IFW FirePOWER™ 模块集中管理软件。 该软件从版本 6.0 开始，更名为 Firepower 管理中心。 这两个版本都能够管理执行 CIP 检查的 IFW FirePOWER 模块。 有关此名称更改的更多信息，请参阅 Cisco Firepower Compatibility Guide，其 URL 如下：
http://www.cisco.com/c/en/us/td/docs/security/firepower/compatibility/firepower-compatibility.html

思科是网络领域的全球领导者，推动了人们联系、交流和合作方式的转变。 有关思科的信息，请访问：www.cisco.com。 欲了解最新动态信息，请访问 http://newsroom.cisco.com。 欧洲地区使用的思科设备由 Cisco Systems International BV 提供，该公司是 Cisco Systems, Inc. 的全资子公司。

www.cisco.com

美洲地区总部
Cisco Systems, Inc.
美国加利福尼亚州圣何塞

亚太地区总部
Cisco Systems (USA) Pte. Ltd.
新加坡

欧洲地区总部
Cisco Systems International BV
荷兰阿姆斯特丹

思科在全球范围内有 200 多个办事处。 各办事处的地址、电话号码和传真号码均已列在思科网站上，网址为 www.cisco.com/go/offices。

Cisco 和 Cisco 徽标是思科和或其附属公司在美国和其他国家或地区的商标或注册商标。 要访问思科商标列表，请访问此链接：www.cisco.com/go/trademarks。 所提及的第三方商标为其各所有公司的资产。 合作伙伴一词的使用并不表示思科与任何其它公司之间存在合作伙伴关系。 (1110R)

罗克韦尔自动化是电力、控制和信息解决方案的领先供应商，致力于提高客户生产率，促进世界可持续发展。 为了支持智能制造的概念，罗克韦尔自动化通过建立互联企业，帮助客户实现价值最大化，并帮助其对未来做好准备。

www.rockwellautomation.com

美洲地区：
罗克韦尔自动化
1201 South Second Street
Milwaukee, WI 53204-2496 USA
电话：(1) 414.382.2000
传真：(1) 414.382.4444

亚太地区：
罗克韦尔自动化
香港数码港道 100 号
数码港 3 座 F 区 14 楼
电话：(852) 2887 4788
传真：(852) 2508 1846

欧洲/中东/非洲地区：
罗克韦尔自动化
NV, Pegasus Park, De Kleetlaan 12a
1831 Diegem, Belgium
电话：(32) 2 663 0600
传真：(32) 2 663 0640

Allen-Bradley、FactoryTalk、Rockwell Automation、Rockwell Software 和 Stratix 是罗克韦尔自动化公司的商标。 不属于罗克韦尔自动化的商标是其各自所属公司的财产。

EtherNet/IP 和 CIP 是 ODVA 的商标。

© 2016 Cisco Systems, Inc. 和 Rockwell Automation, Inc.，并保留所有权利。 出版号 ENET-WP011B-ZH-P 2016 年 12 月