LISTEN. THINK. SOLVE.®

工业控制系统（ICS) 的信息安全

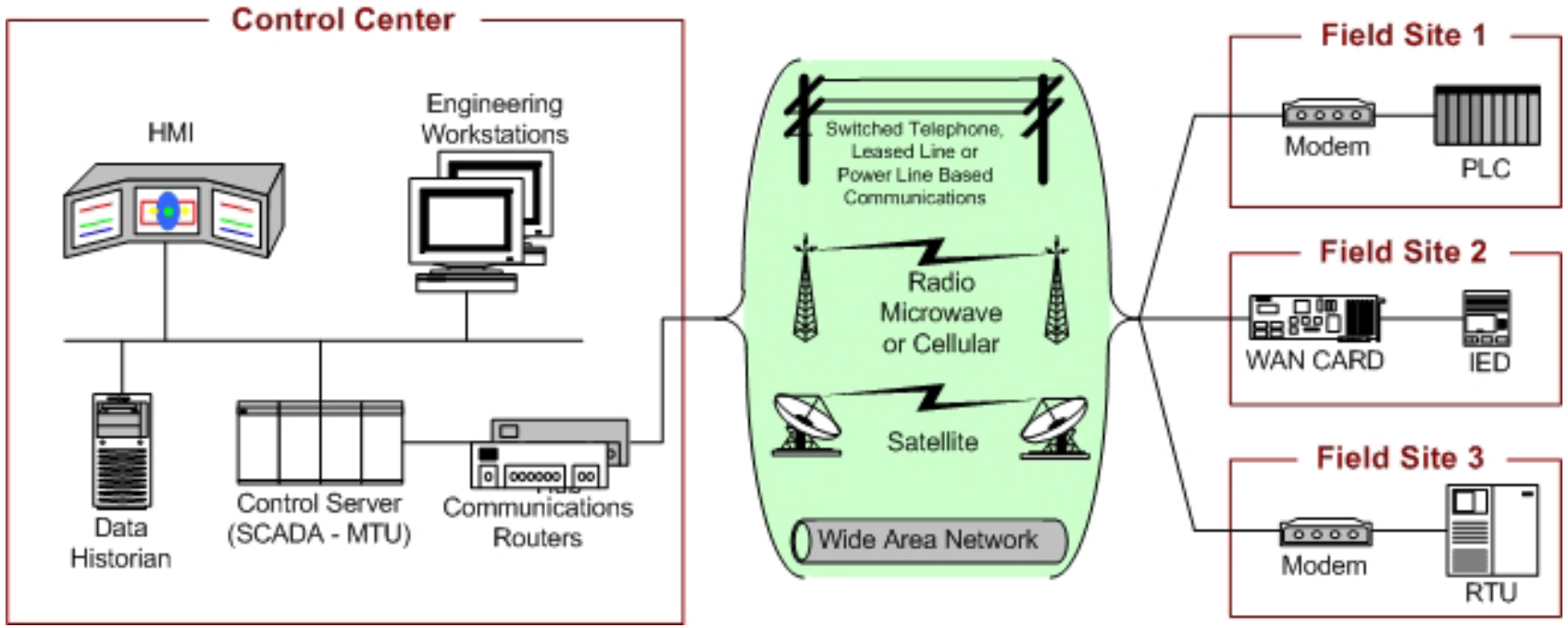
华镕
标准与贸易部中国区经理
2013年8月28日

Allen-Bradley · Rockwell Software

Rockwell Automation

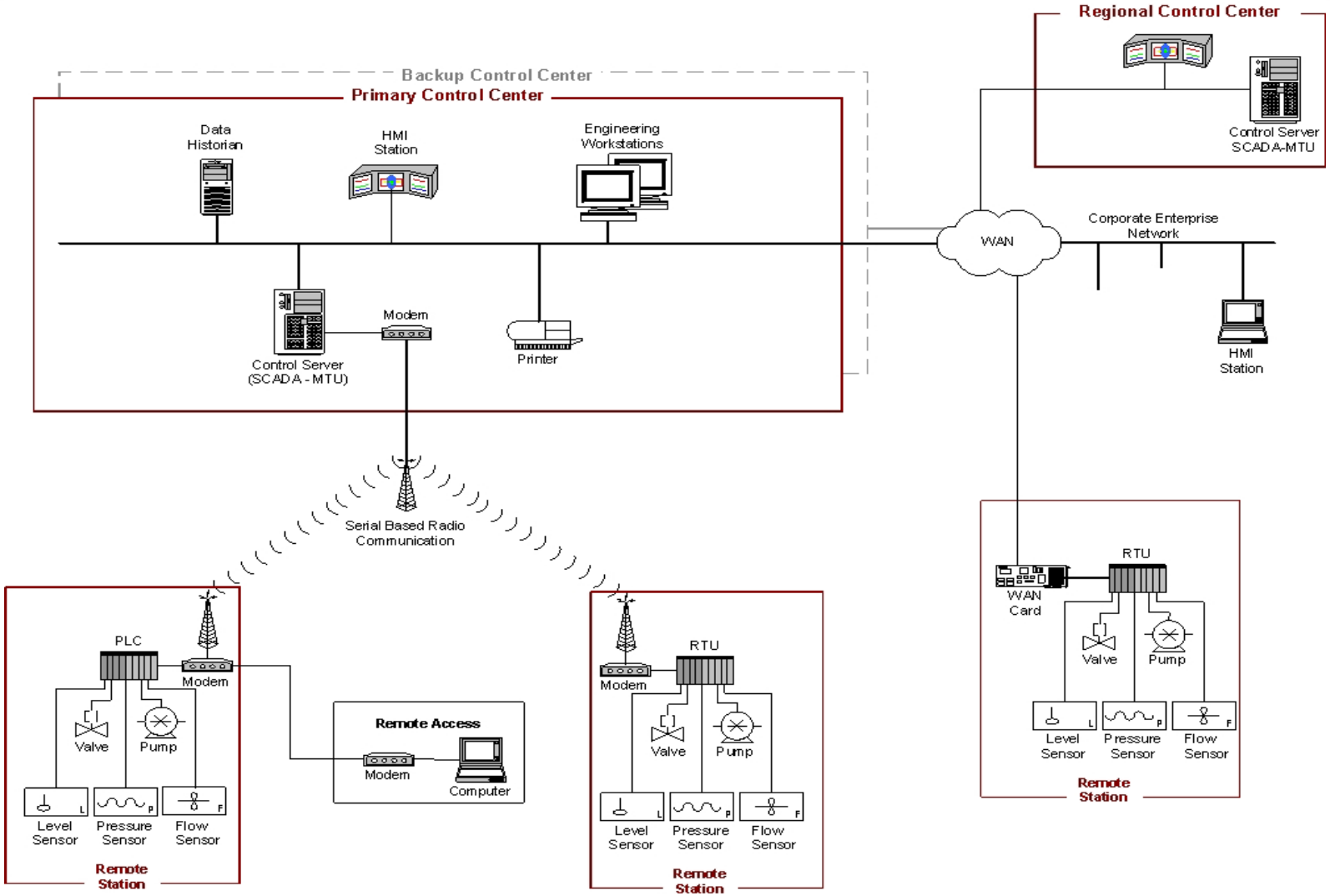
SCADA 系统的一般布局

Rockwell Automation



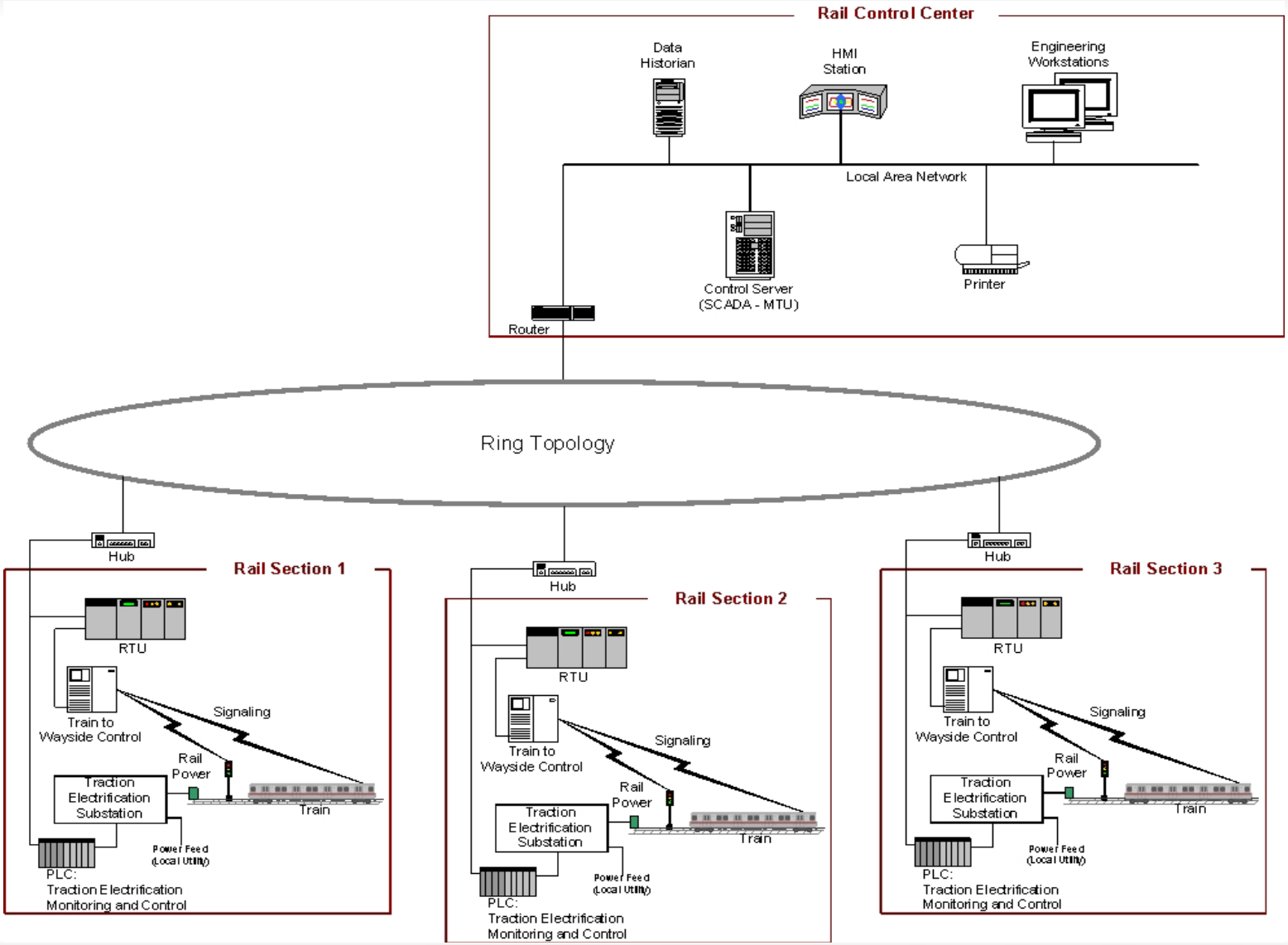
SCADA 系统举例 (分布监视与控制)

Rockwell Automation



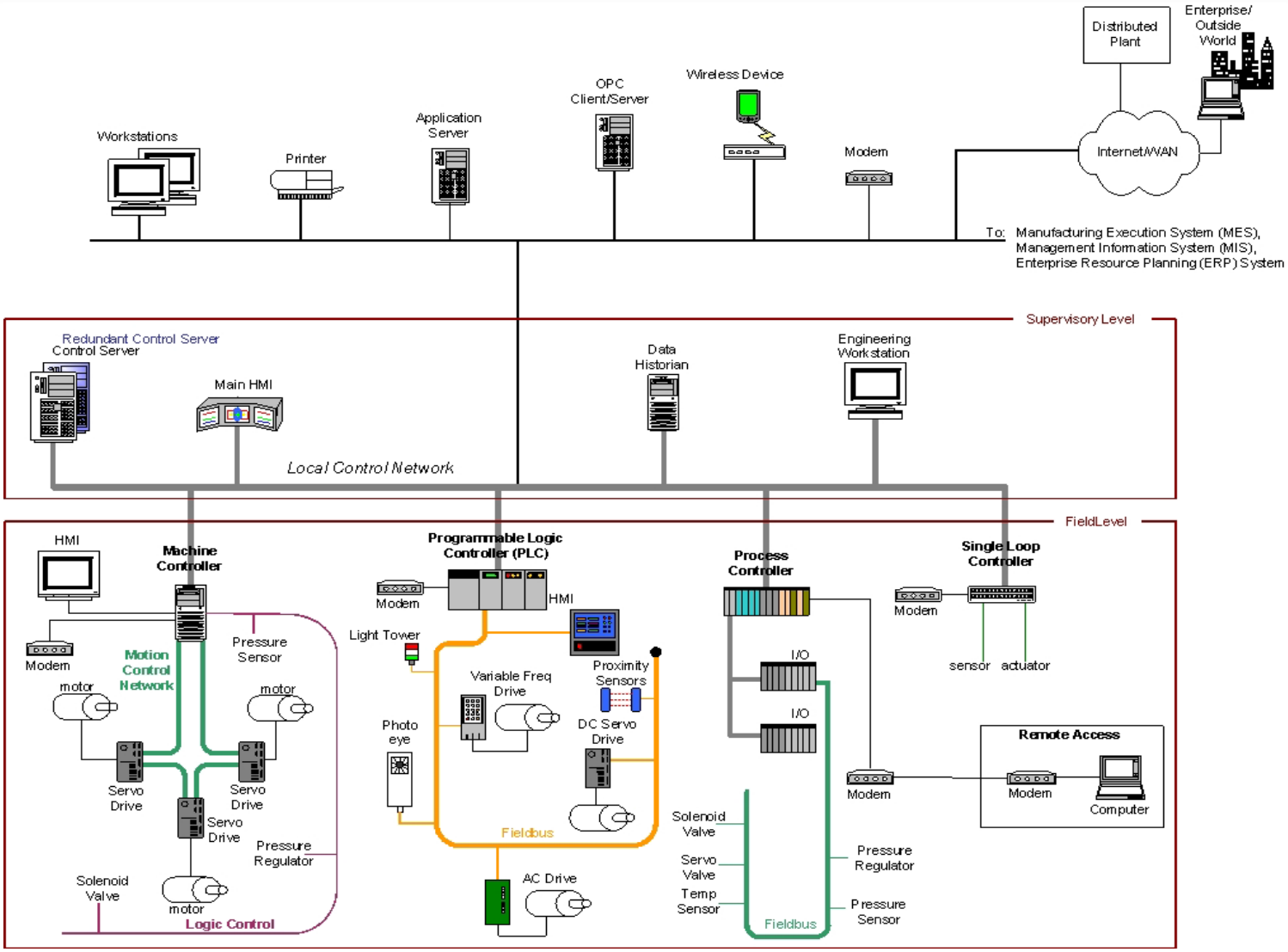
SCADA 系统举例 (铁路监视与控制)

Rockwell Automation



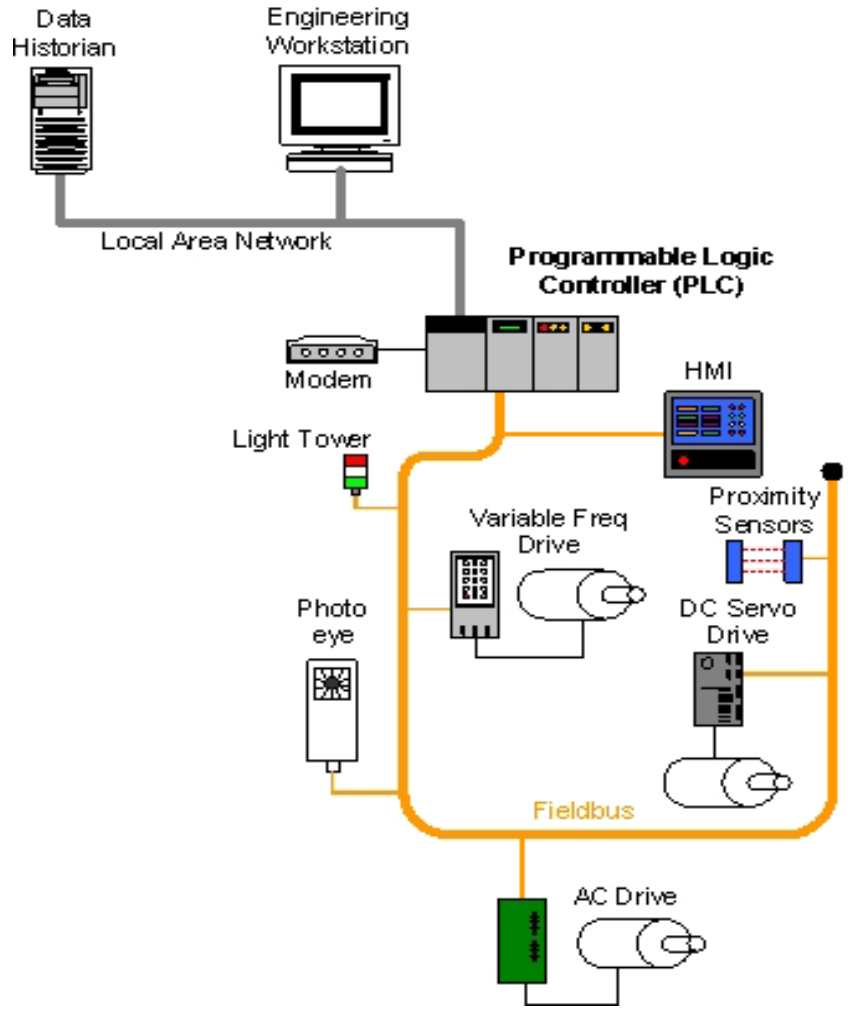
DCS 系统举例

Rockwell Automation



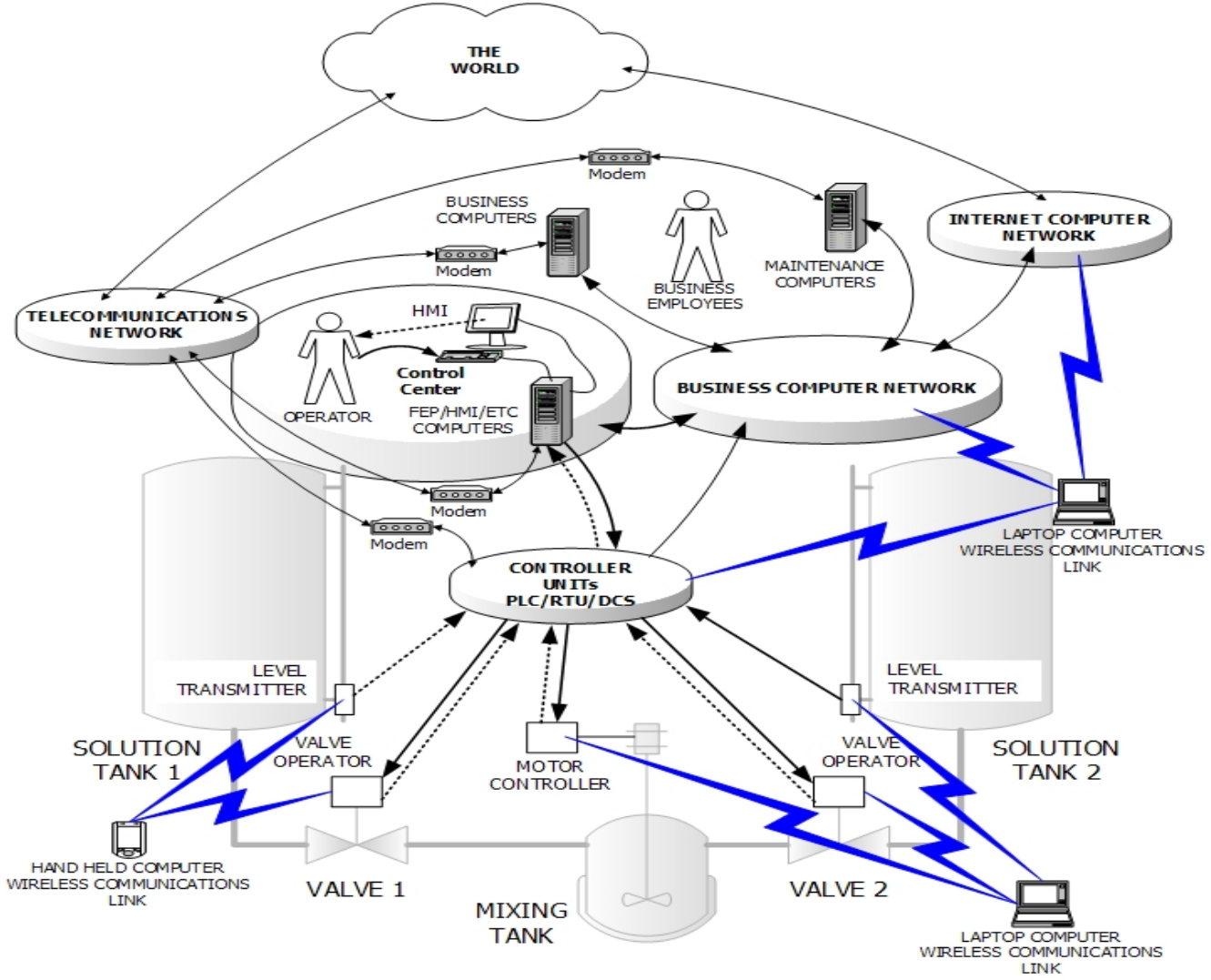
PLC 控制系统举例

Rockwell Automation



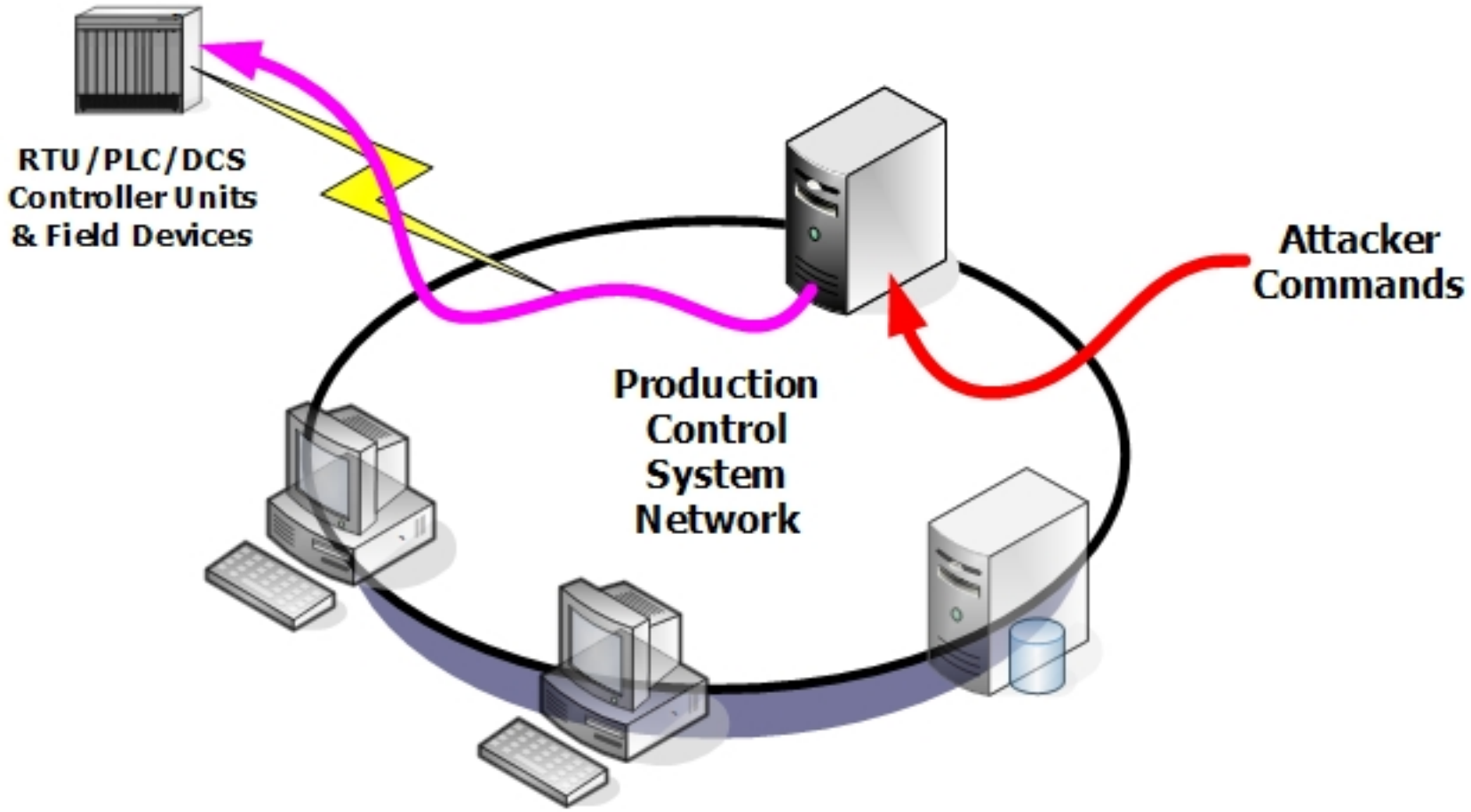
工业控制系统之间的通信

Rockwell Automation



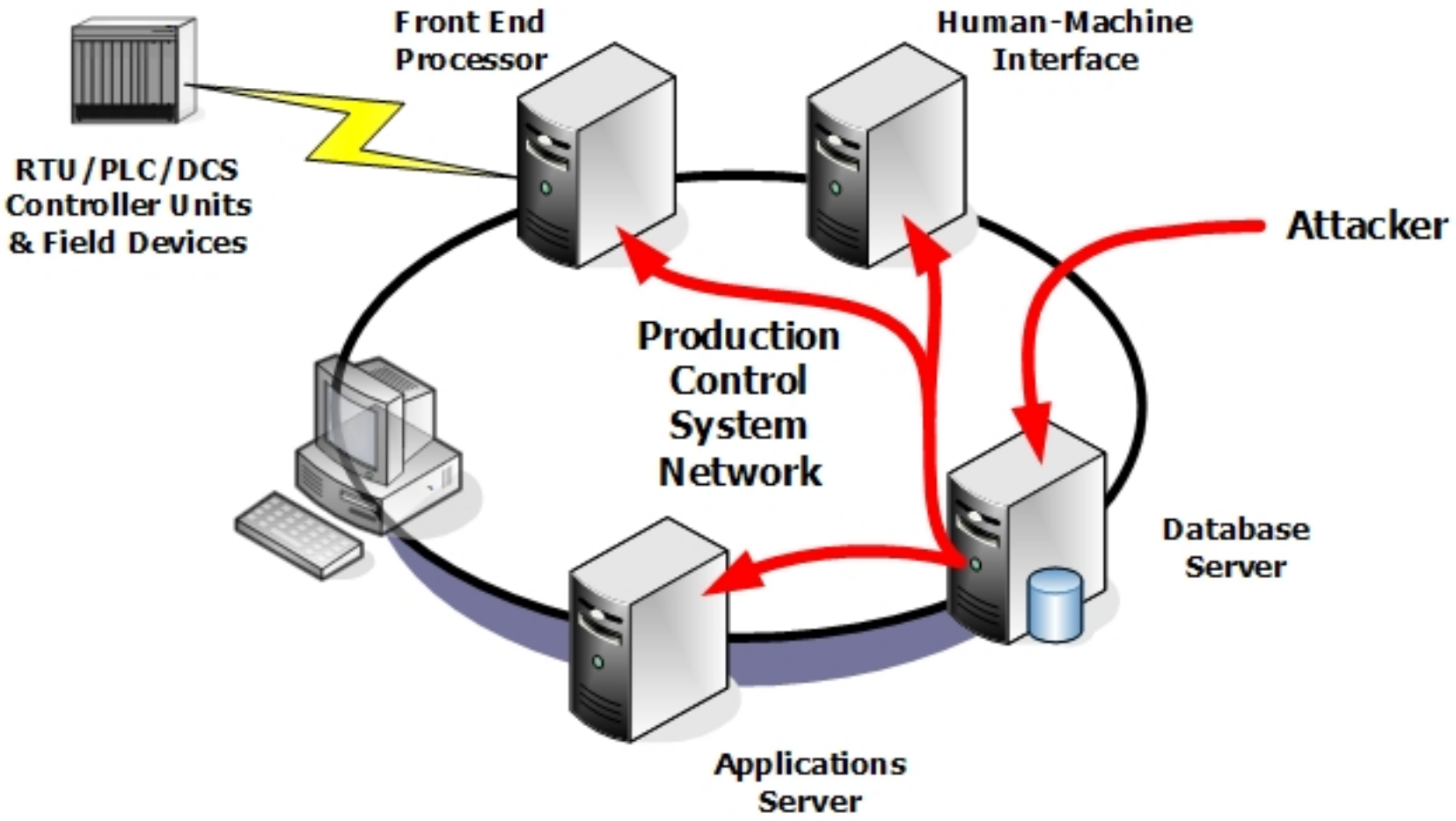
攻击举例 1

Rockwell Automation



攻击举例 2

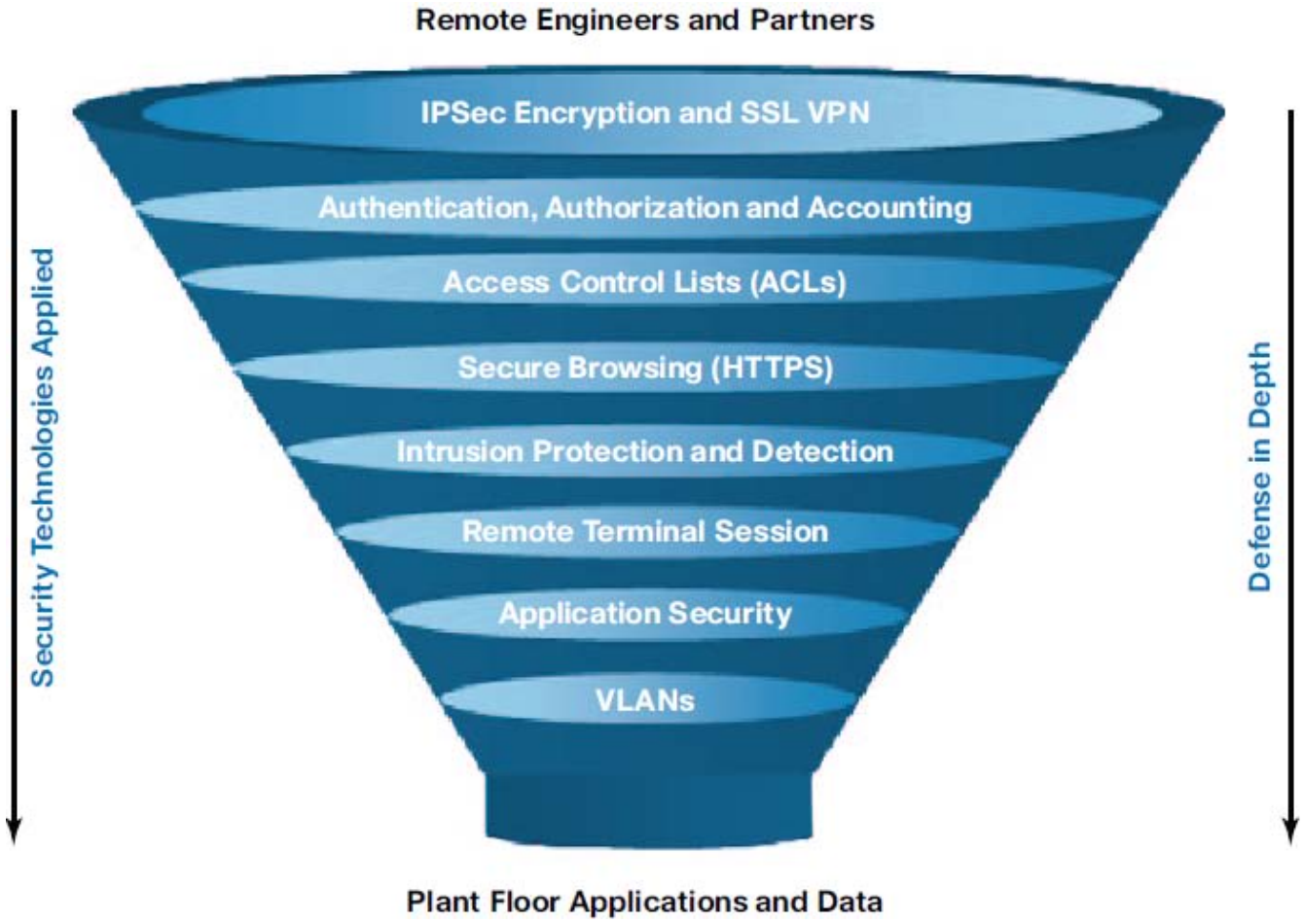
Rockwell Automation



信息安全的实施

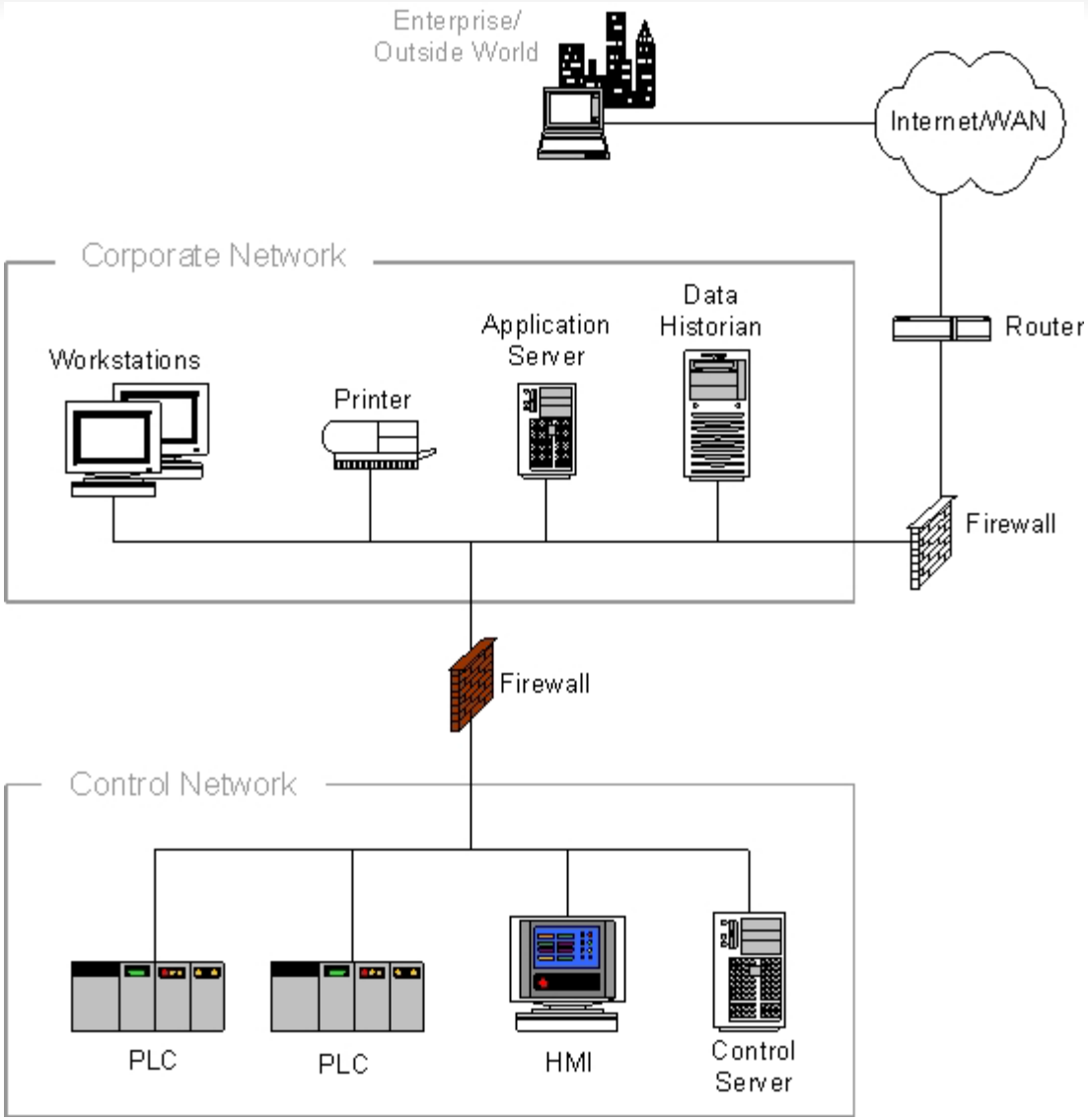
Rockwell Automation

- 使用按纵深防御的方法



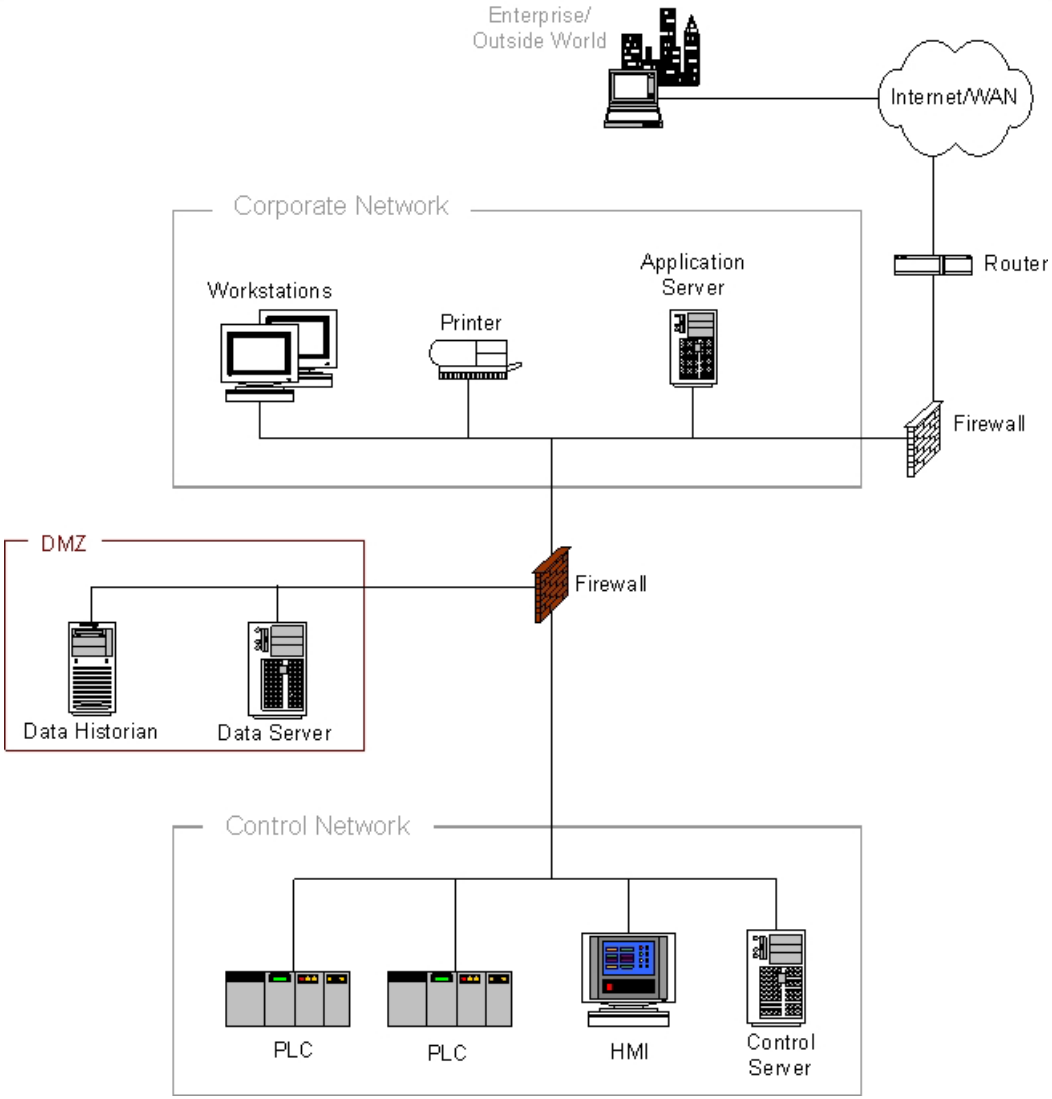
在企业网与控制网之间加防火墙

Rockwell Automation

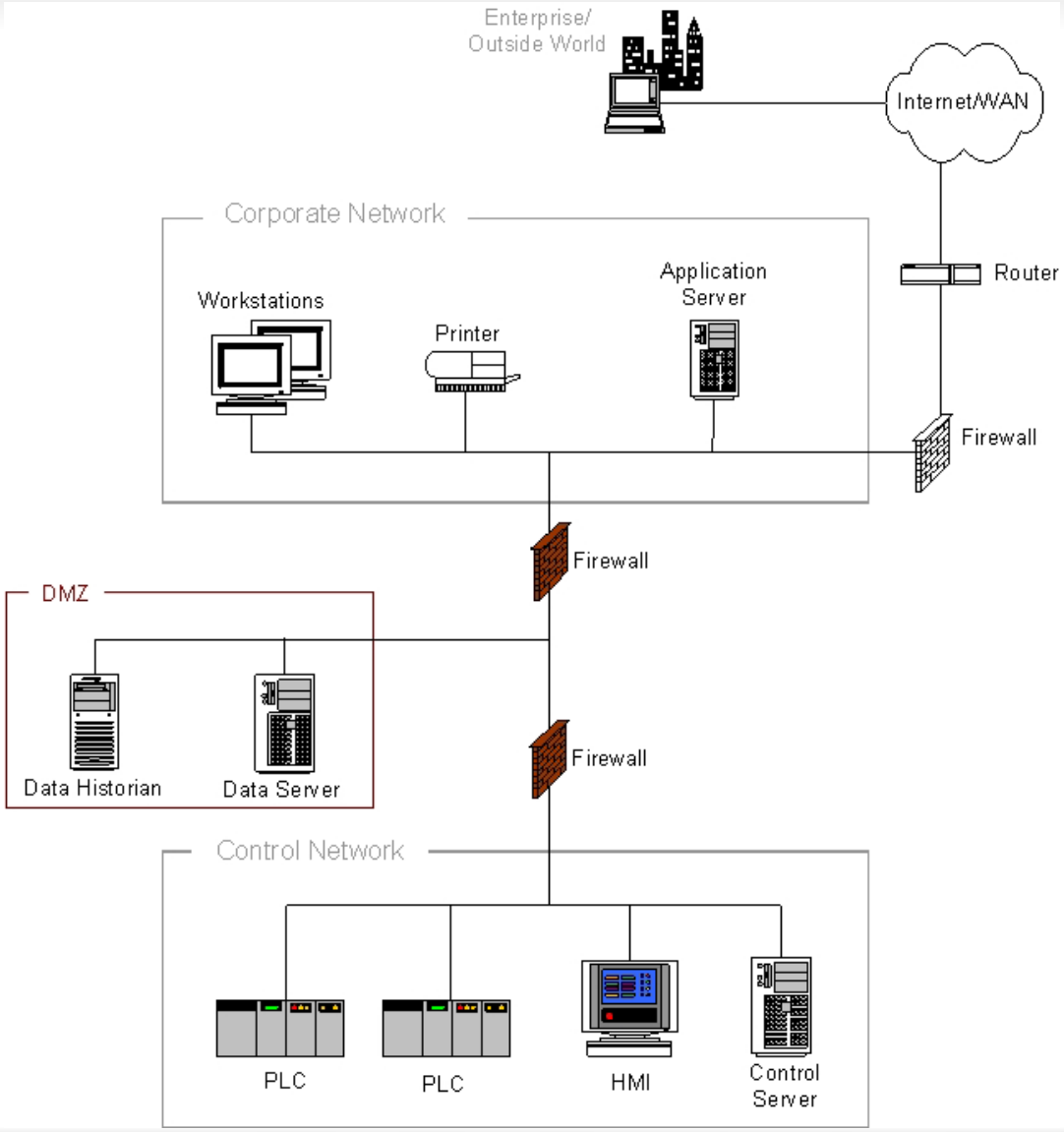


在企业网与控制网之间加带隔离区防火墙

Rockwell Automation

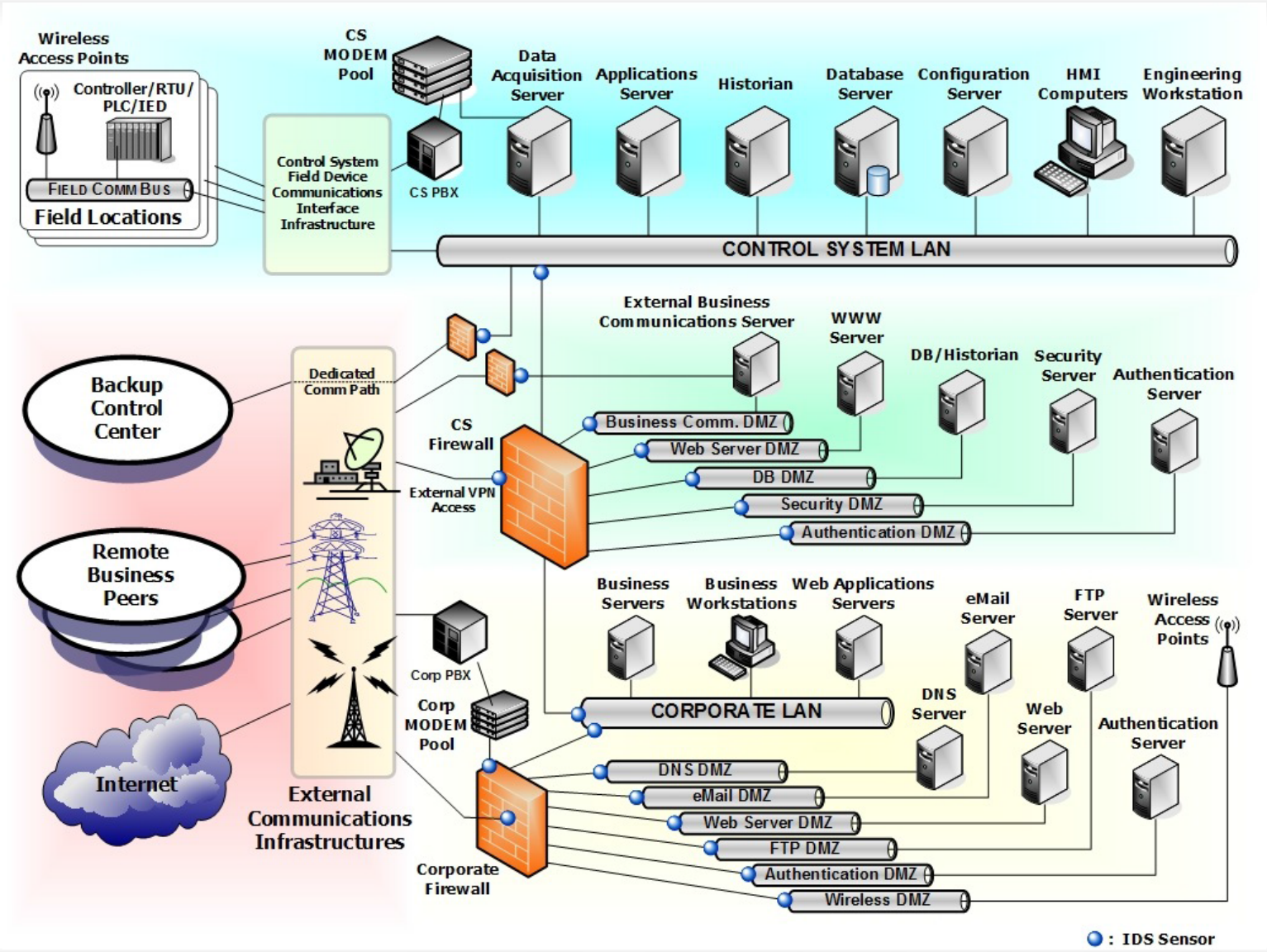


在企业网与控制网之间加双防火墙



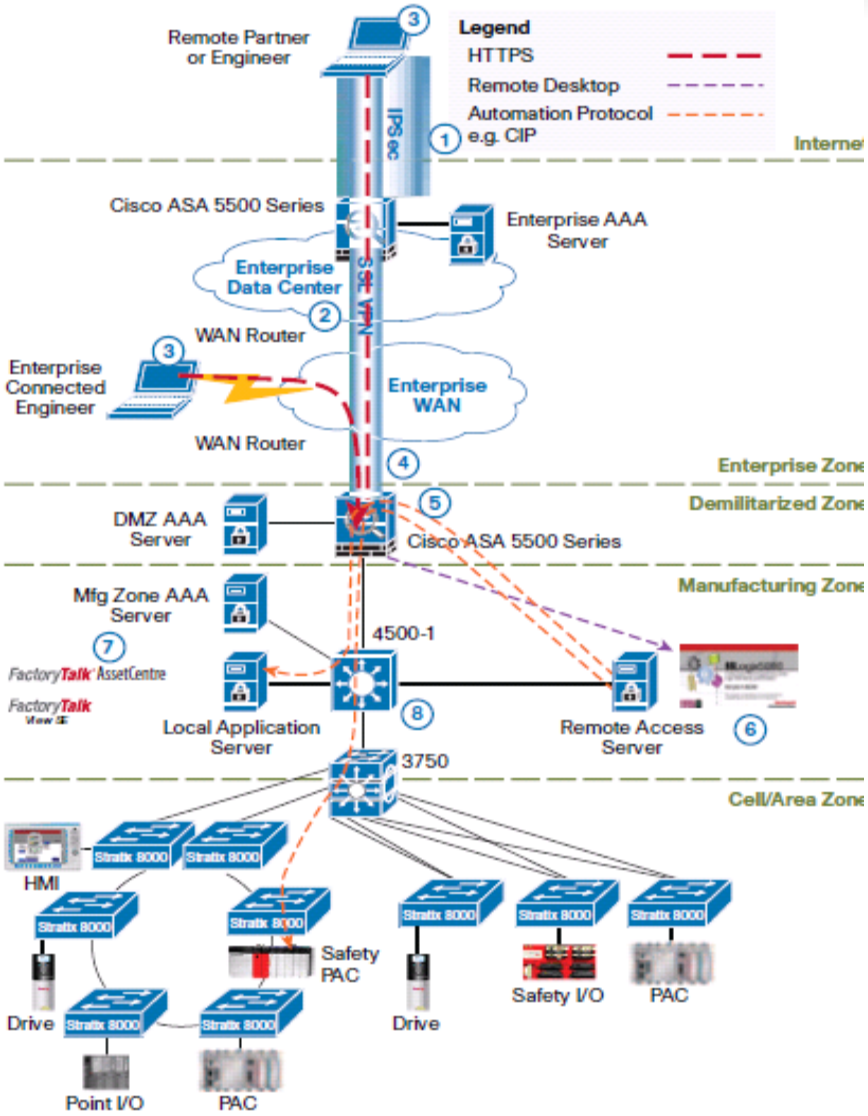
按用户要求定制信息安全方案

Rockwell Automation



罗克韦尔自动化的推荐方案

Rockwell Automation



信息安全的实施 1

Rockwell Automation

- 实施步骤

1.使用标准企业远程访问方案，基于客户机的形式，使用IP安保（IPsec）加密的虚拟个人网络（VPN）技术，通过因特网安全地连接企业的边界。VPN的建立需要对远程个人进行远程验证拨入用户服务（RADIUS），这通常是由IT部门组织实施和管理。

2.使用隔离区（DMZ）/防火墙中的访问控制列表（ACL），限制远程伙伴通过IPsec到工厂现场的访问。通过隔离区连接到工厂现场，只能使用一种安全浏览器（HTTPS）。

3.访问一个安全浏览器（HTTPS）门户应用，它运行于隔离区/防火墙上。这要求再次登录/验证。

4.在远程客户机和工厂的隔离区防火墙之间，使用一种安全套接字层（SSL）的虚拟个人网络（VPN）会话，并且限制通过HTTPS使用远程终端会话（比如，远程桌面协议）。

信息安全的实施 2

Rockwell Automation

- 实施步骤

5. 利用在防火墙上的侵入保护和检测系统（IPS/IDS），检查进出远程访问服务器的数据流，防止攻击和威胁，并适当地给予阻截。这对防止来自远程设备穿越防火墙和影响远程访问服务器的病毒和其他威胁是非常重要的。

6. 允许远程用户执行终端会话，访问驻留在远程访问服务器中的自动化和控制应用。需要应用级的登录/验证。

7. 执行应用安保功能，对访问远程访问服务器的用户，限制其应用功能（诸如只读，非在线功能）。

8. 把远程访问服务器分配到不同的虚拟局域网（VLAN），并且让所有在远程访问服务器到制造区域之间的数据流通过防火墙。对这个数据流使用侵入检测和保护服务，保护制造区域免受攻击、蠕虫和病毒的破坏。

信息安全的实施 3

Rockwell Automation

- 相关责任的划分

步骤	IT	生产
1. 在企业中 VPN 网络，包括安装 VPN 客户机软件和企业授权	✓	
2. 对生产防火墙有限访问	✓	
3. 安全浏览器	✓	
4. 建立到工厂防火墙的 SSL VPN	✓	✓
5. 在工厂的防火墙上建立 IPS/IDS	✓	✓
6. 建立和配置远程访问服务器		✓
7. 自动化和控制应用安保		✓
8. 分段远程访问服务器		✓

信息安全的标准

Rockwell Automation

- IEC62443 1-2 主要用语和缩写词汇
- IEC62443 1-3 系统信息安全遵从指标
- IEC62443 2-2 运行IACS信息安全程序
- IEC62443 2-3 IACS环境中的补丁管理
- IEC62443 3-2 对区域和线槽的信息安全确保等级
- IEC62443 3-3 系统信息安全需要和信息安全确保等级
- IEC62443 4-1 产品开发需求
- IEC62443 4-2 对IACS产品的技术信息安全需求

结束语

Rockwell Automation

- 工业控制系统的信息安全及应用是工业安全的大事，为此国家和工信部已经发出了相关文件，责令工业企业以及关键性基础设施要对信息安全给予高度重视，所以这次会议对大家提高安全意识、防止事故发生于未然具有重要意义。
- 罗克韦尔自动化会遵从国家的法律法规，积极参与信息安全国家标准的制定和宣贯，帮助企业实现信息安全的咨询、评估、方案提供和方案实施。
- 希望在座的同仁能够一起努力，确保国民经济的平稳增长，确保我们的人身健康、企业资产、自然环境能够可持续、和谐地发展。

LISTEN. THINK. SOLVE.®

感谢您的参与!

Follow ROKAutomation on Facebook & Twitter.
Connect with us on LinkedIn.

www.rockwellautomation.com

Allen-Bradley • Rockwell Software

Rockwell Automation