安全开放的过程控制解决方案

－施耐德电气PlantStruxure™协同自动化系统

施耐德电气(中国)有限公司工业事业部
陈小淙

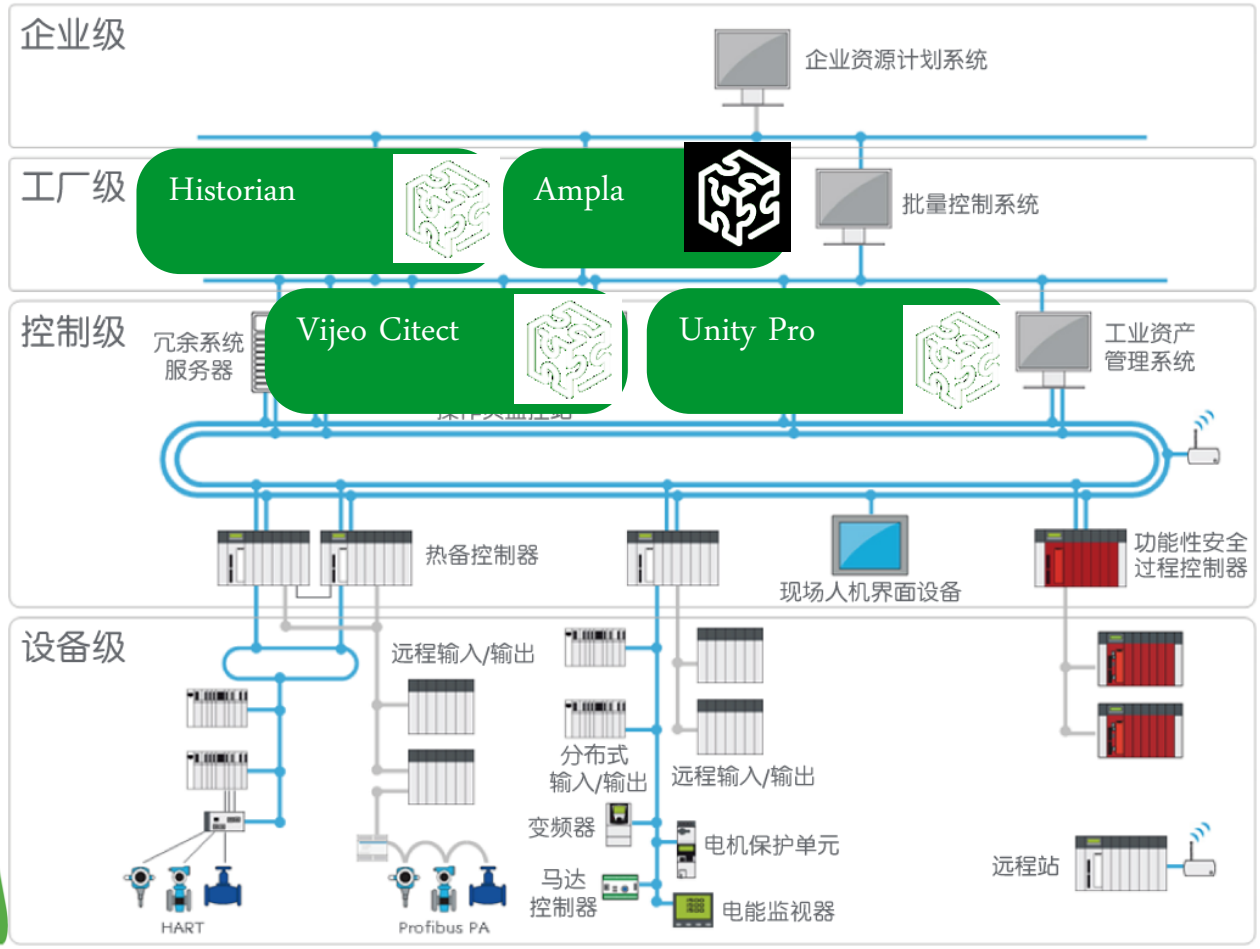
2012年11月

Schneider Electric

- 工业过程控制系统信息安全的现状
- 信息安全威胁来源及类型
- 实现工业过程控制系统信息安全的建议
- 施耐德电气的信息安全解决方案

- 工业过程控制系统信息安全的现状
-
-
- 施耐德电气的信息安全解决方案

典型工业过程控制系统



Plant Struxure™

工业控制系统发展趋势——网络化、智能化

- 从传统封闭式系统演变到开放式的网络系统
  - 开放的硬件体系
  - 开放的协议体系
- 过程控制和企业信息系统的集成
  - 供给链集成
  - 远程工作
- 无线技术的广泛应用

以太网 – 在工业网络领域发展最快的技术

❑以透明的方式访问数据信息

- 从工厂级到企业级
- 开放的标准协议

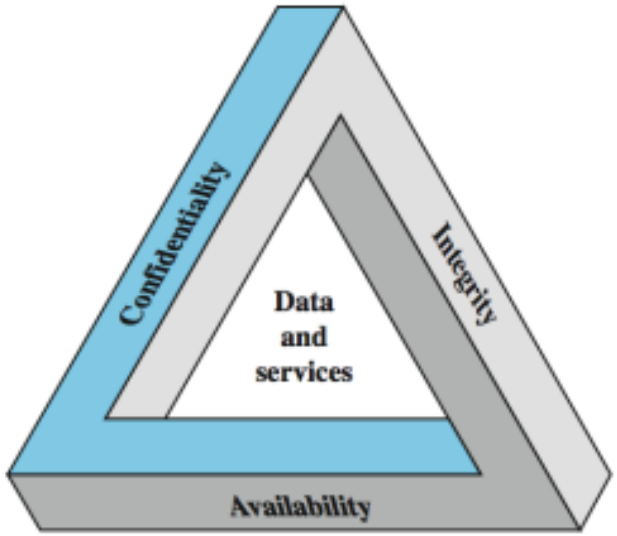
❑以太网技术的优势

- 全局互操作性
- 面向未来的投资方式
- 适用于任何应用的优化性能
- 减低最终用户总投资

❑集成其他标准网络协议

信息安全

- 通过对信息的保护实现对资产或经济活动的保护措施
- 关键的安全原则:
  - 机密性 – 防止私有信息的泄露
  - 完整性 – 未经授权不能修改数据.
  - 可用性 – 信息在需要时必须可用.



工业自动化信息安全的重要性

- 信息安全从传统IT领域快速扩展到工业控制领域

  - 2010年9月，“震网”病毒攻击伊朗核电站工控系统

  - 2011年11月，在拉斯维加斯举行的黑客大会上，演示了如何进攻中国重要基础行业正在使用的工控系统

工业自动化信息安全的重要性

❑政府及公司对工业控制系统的信息安全日益重视

- 美国是先行者
  - NERC CIP 强制能源企业信息安全否则罚款.
  - 国会议案要求关键基础设施信息安全 .
  - 石油天然气行业要求供应商Achilles 或WIB认证
  - CFATS 开始在化工厂实施.

- 中国在加速促进
  - 政府要求提高工业控制系统信息安全.
  - TC124/SC4开始起草/制定我国的工业控制系统的信息安全标准

- 其他国家
  - 澳大利亚，以色列

工业自动化信息安全的重要性

- 控制系统包含可以影响相应商业活动的有价值信息，更易受到集中的攻击
  - “FLAME” 病毒
- 控制系统中信息安全突破会带来工厂运行的负面影响
  - 费用
    - 系统停机 – 影响生产或导致服务的中断
    - 改变程序或系统配置– 导致生产中断或生产出不合格的产品
    - 丢失生产信息– 对有些需要生产记录的行业来说明严重的问题
    - 丢失维护信息
    - 增加运行成本
  - 安全
    - 非安全条件下过程处理可能导致设备、人员或环境的安全问题

工业过程控制系统信息安全现状

❑ 中国信息安全工业行业现状

- 工业控制系统信息安全研究起步较晚
- 对病毒、网络攻击等信息安全威胁重视不足
- 安全防范手段不到位
- 安全保障机制缺失
- 工业控制系统信息安全标准不健全

❑ 最终用户存在的不足

- 没有足够的信息安全职位安置及培训
- 不安全的边界防火墙
- 计算机及软件的补丁不充分
- 集团网络及工厂网络分离不充分
- 口令强度不够
- 不必要的第三方产品设备
- 企业信息安全的文档不充分

- 信息安全威胁来源及类型
- 施耐德电气的信息安全解决方案

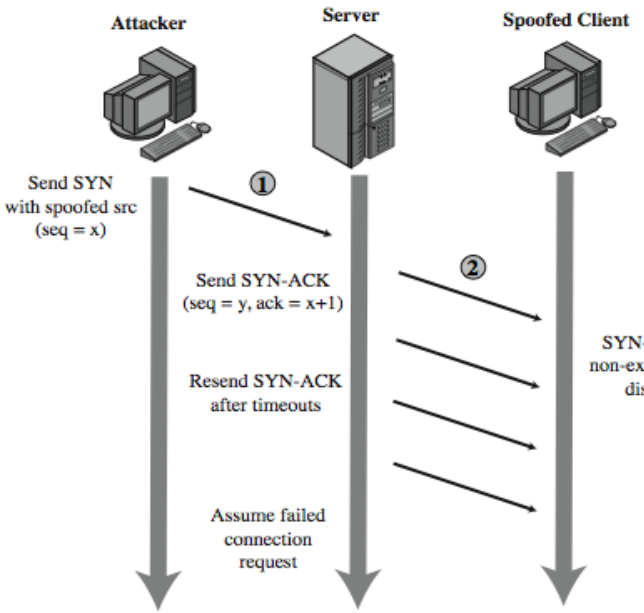
信息安全威胁的来源及类型

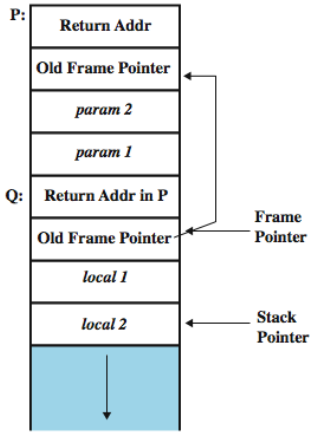
- 安全威胁可以来自外部，及内部

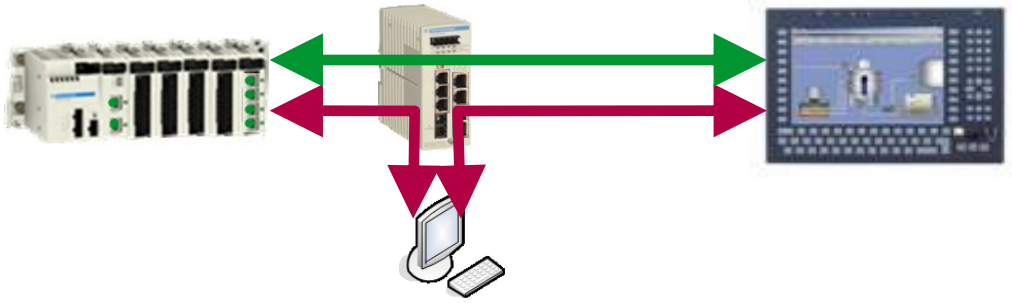
- 攻击者包括:
  - 员工
  - 激进分子/政府/勒索团伙:
  - ‘脚本小子’
  - 研究者
- 攻击原因
  - 兴趣
  - 勒索/报复
  - 商业间谍
  - 国家间谍
  - 意外

常见的攻击手段/漏洞

- 逻辑炸弹
- 拒绝服务
- 缓冲溢出
- 后门
- 口令攻击
- ‘中间人’攻击
- 重放攻击
- 网络钓鱼
- Rootkits
- DNS / Bootp / 服务扮演
- Web 跨站脚本攻击 - XSS
- Web 目录遍历
- IP地址欺骗
- MAC地址欺骗







- 实现工业过程控制系统信息安全的建议

施耐德电气的信息安全解决方案

实现过程控制系统的信息安全

❑供应商的责任

- 设计或提供具有信息安全特性的产品或解决方案
- 确保他们能使客户遵守相应的信息安全标准
- 提供实施安全的指导建议及方法

❑最终用户的责任

- 制定信息安全制度（组织架构的信息安全性保证）
- 指定相应的责任人(人员的信息安全保证)
- 确保遵守相应的信息安全标准

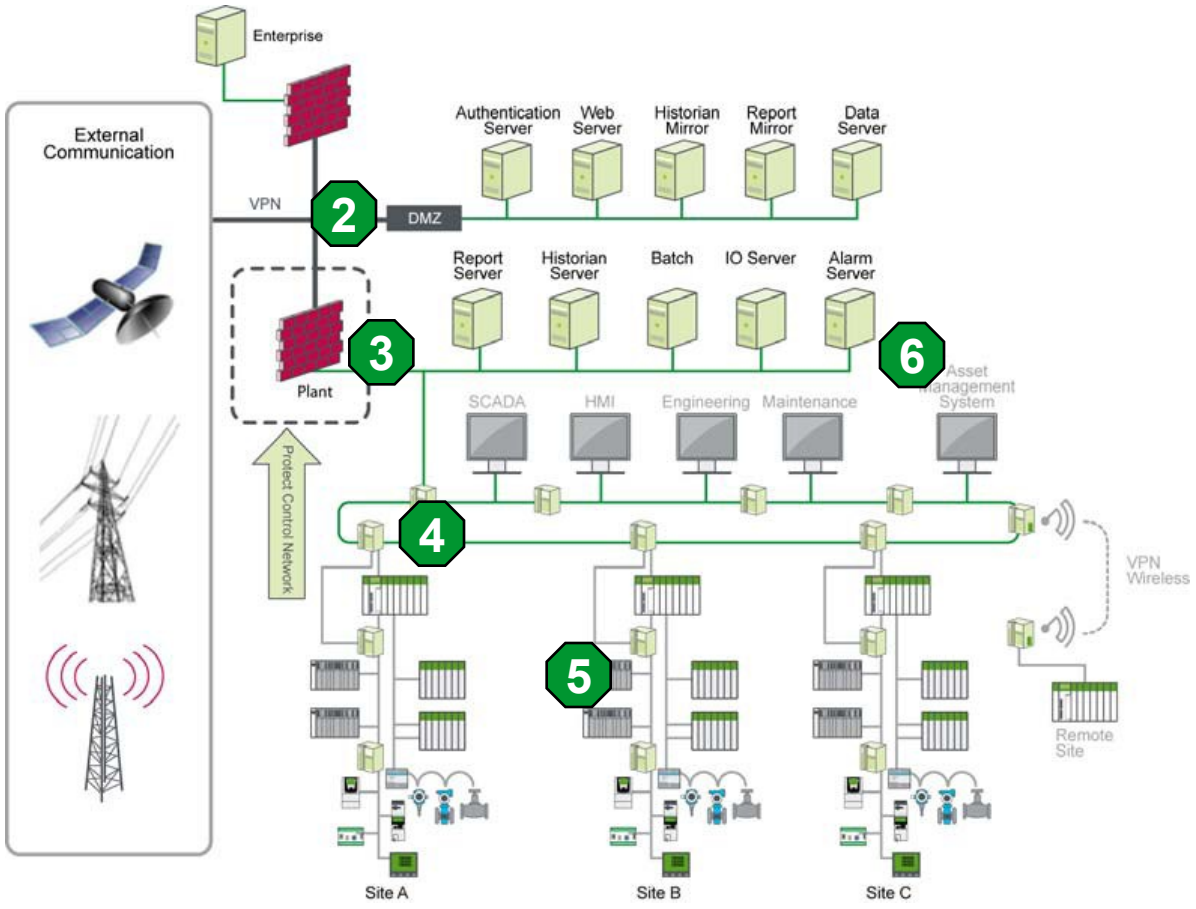
❑实现安全需要一套方案而不是仅仅与产品相关

- 人员，制度，系统结构，产品

❑实现工业过程控制系统信息安全需要多层保护

- 信息安全计划，网络分离……

实现过程控制系统信息安全的最佳办法– 纵深防御

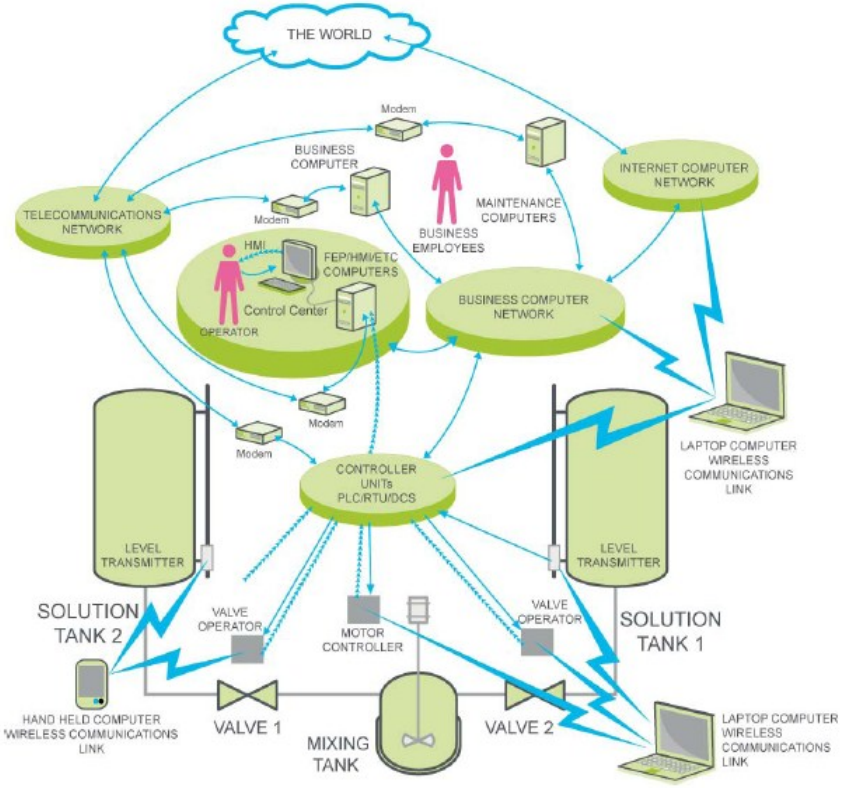


6 关键步骤：

1. 安全计划
2. 网络分隔
3. 边界保护
4. 网段分离
5. 设备加固
6. 监视与更新

纵深防御 第一步：安全计划

- 定义：
  - 角色和职责
  - 许可的行为，操作，方法
  - 不遵守的后果
- 全网络的评估
  - 通讯路径.
  - 所有设备的稽核.
  - 安全设置.
  - 网络图.
- 安全漏洞评估：
  - 潜在的威胁.
  - 后果.
  - 风险评估及缓解措施



纵深防御 第二步：网络分隔

❑将工业控制系统与外部隔离

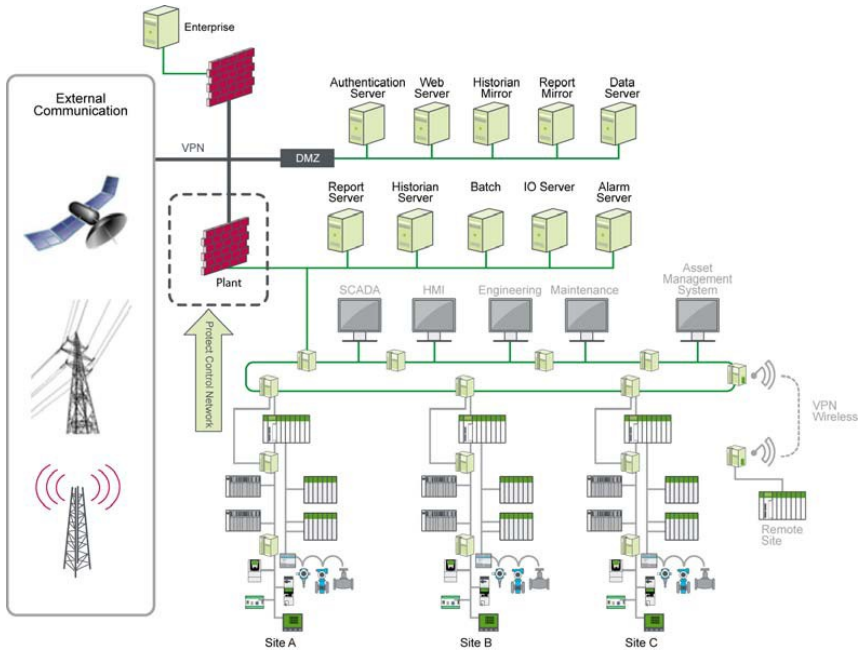
- 建立缓冲区 (DMZ).
- 所有进入信息经过DMZ区
- 限止外出信息仅保留必要的通信 .

❑DMZ区-服务器：

- Vijeo Historian 镜像点.
- Web 服务器.
- 鉴定服务器 .
- 远程接入服务器 server.
- 防病毒服务器 .
- 无线接入点 .

Router

Firewall



纵深防御 第三步： 边界保护

- 用防火墙保护工业控制系统的边界 ：
  - 状态检测防火墙
  - 验证数据包及协议
  - 对特的数据包作授权管理
  - 限止IP地址或用户的进入

Firewall

- 过程处理关键部分用额外的防火墙保护

- 保护远程进入
  - 采用路由器或防火墙的VPN技术
  - 选择基于IPsec协议的VPN 技术.
  - 使用最新的鉴别及授权技术

Router

纵深防御 第四步： 网段分离

❑采用管理型 交换机

- VLAN:
  - ➢ 正确分隔网段.
  - ➢ 防止未确认的或错误的连接
- 减少组播或广播.
- 降低信息风暴的威胁： （DoS-类攻击）.

❑选择环型网络拓扑结构替代总线型结构

- 提高可用性及可靠性

❑SNMP V3

- 实现每个站点的网络管理 .
- V3 加密密码

纵深防御 第五步： 设备加固

❑针对所有设备：

- 用“强“密码替换默认的密码
- 关闭未用的端口，通讯服务及硬件接口
- 设置网络风暴限制功能 .
- 采用组播过滤.
- 采用进入控制功能 .

❑对PC及HMI:

- 禁止或严格限止外部存储器的应用

❑对Unity Pro及 Vijeo Citect

- 设置所有的安全特性：口令，用户配置文件，操作员日志
- 保持操作系统的更新提高对病毒及恶意软件的保护
- Unity：关闭程序上传功能，采用静态IP地址及进入控制功能

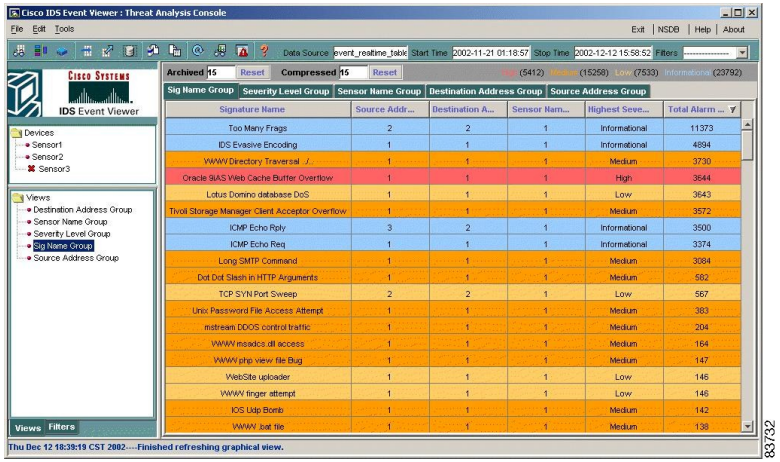
❑对 ConneXium 交换机:

- 端口的进入仅限于分配的地址

纵深防御 第六步： 监视与更新

❑方法:

- 日志.
- 认证陷阱.
- 入侵检测系统(IDS)
  - ➢ 网络
  - ➢ 主机



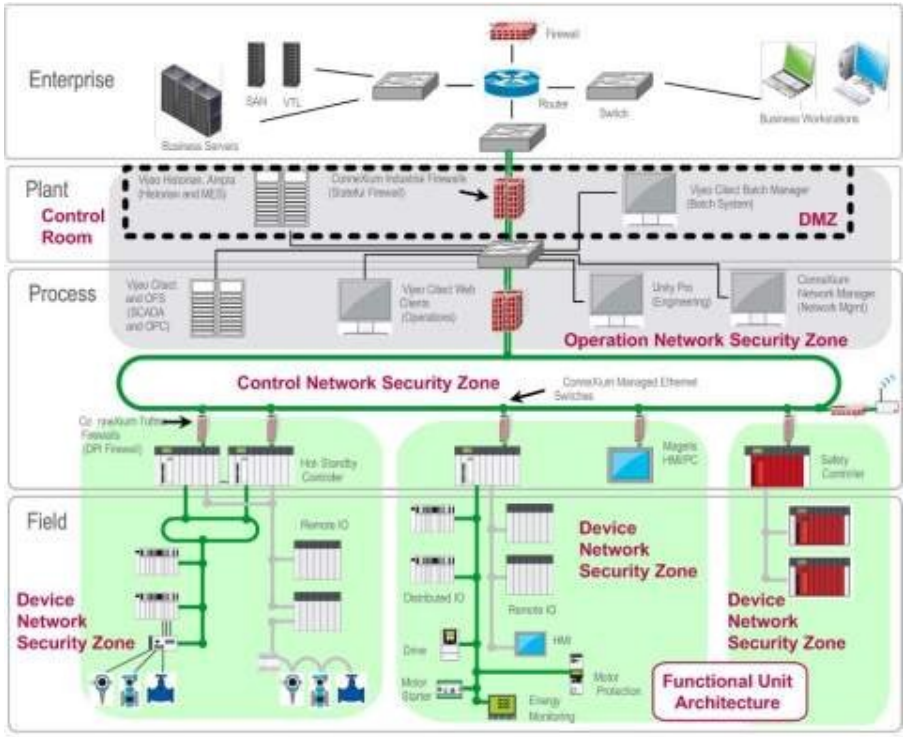
❑监视:

- 未授权的登录企图 .
- 不寻常的活动
- Windows事件查看器 .
- 网络的负荷
- 设备的日志文件

实现“安全”的系统

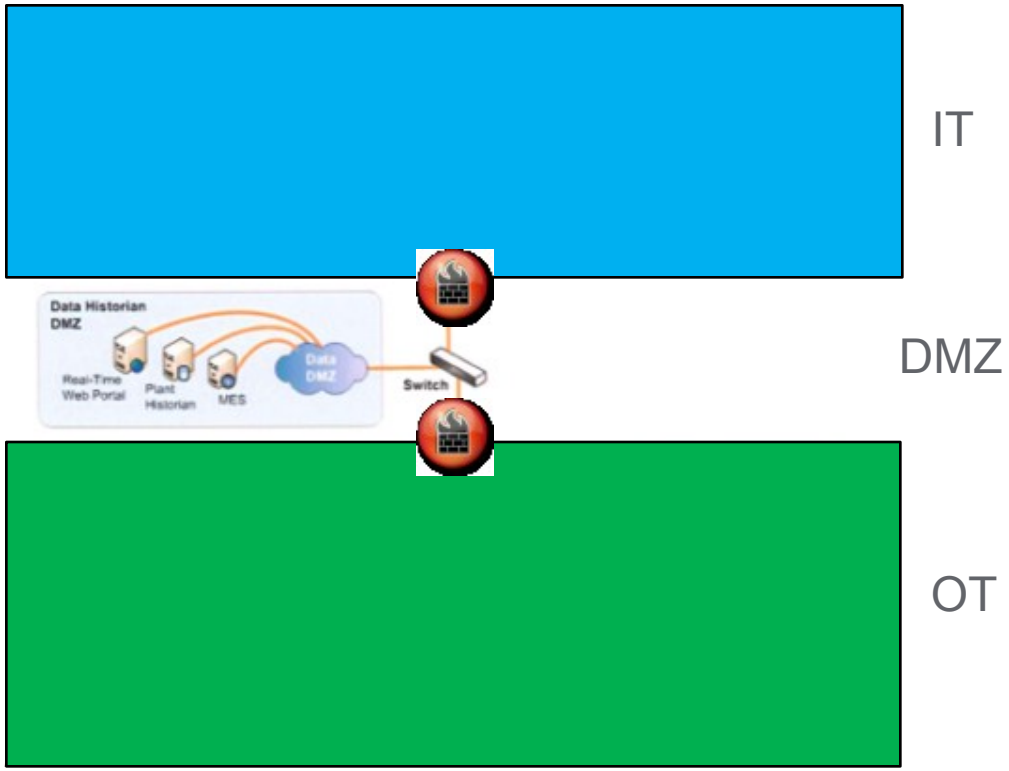
政策制度，　人员培训，　安全的系统架构

- 边界保护
  - 路由器，防火墙，VPN，
- 网络分段
  - DMZ 区
  - 信任区分段
- 计算机的保护
  - 防病毒，进入控制，
- 控制器/设备的加固
  - 设备安全，额外保护
- 监视与反馈
  - 日志，通讯监视，报警
  - 未授权事件响应



“管理” 安全系统

- 持续的计算机保护
  - 防病毒
  - ‘白名单’应用
  - 进入控制
- 监视设备加固
  - 设备设置
  - 外部设备
- 流量, 用户日志, 事件日志等的监视
- 未授权事件的响应
- 补丁！补丁！补丁！



工业过程控制系统信息安全的现状

- 施耐德电气的信息安全解决方案

施耐德电气信息安全解决方案

❑提供给客户的信息-----信息安全指导及漏洞信息的发布站点

http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

- 白皮书
- 产品安全漏洞数据
  - ➢漏洞清单
  - ➢缓解/解决方案
  - ➢补丁及固件更新
- 信息安全漏洞报告
- 信息安全新闻
  - 产品发布及更新
  - 行业新闻
- RSS 订阅

施耐德电气信息安全解决方案

❑ 安全的产品

- 新产品的开发将依据工业信息安全标准

  Achilles 认证, ISA安全认证

- 老产品

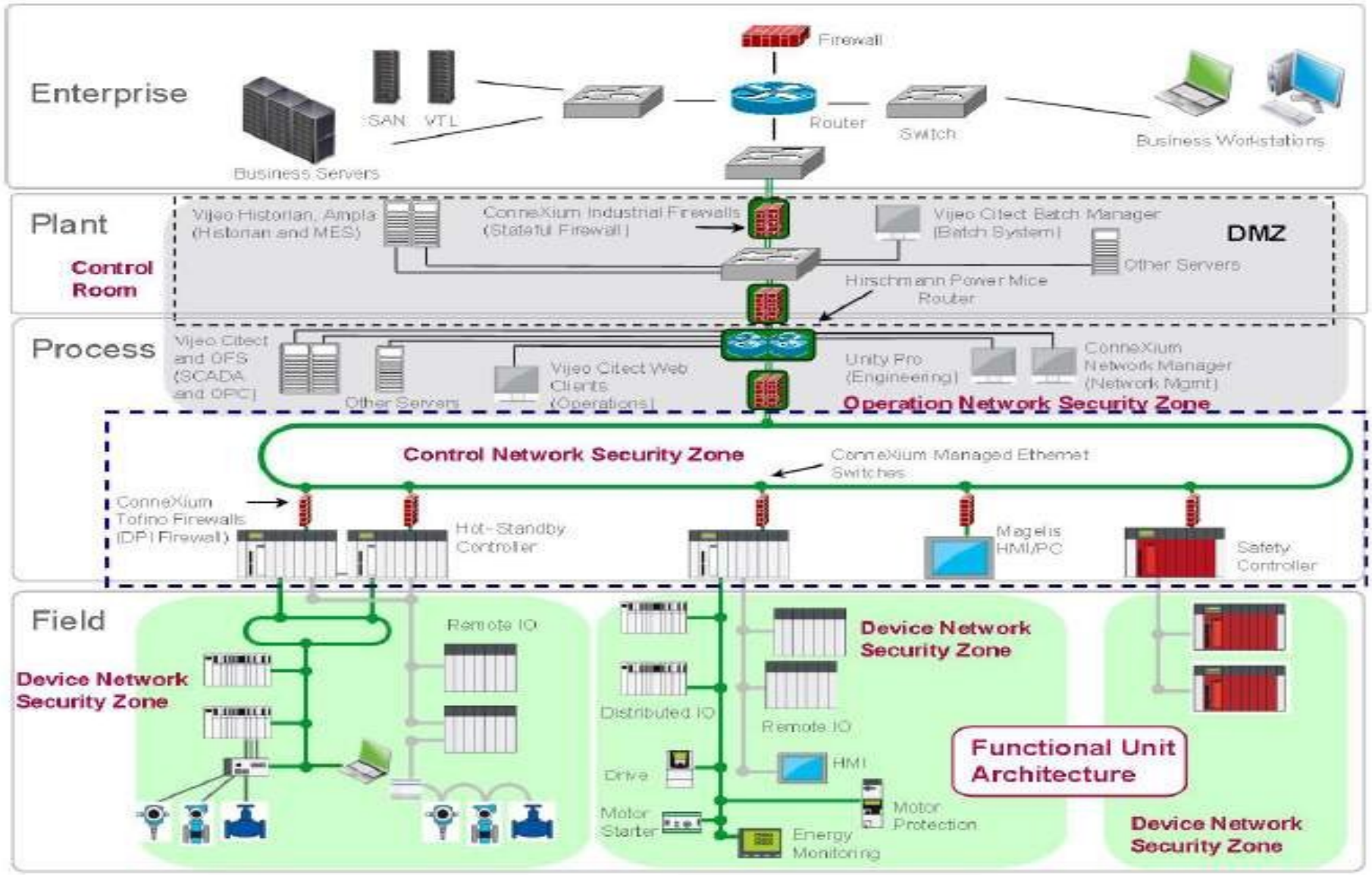
  应用ConneXium Tofino防火墙保护 .

  - ➢低成本 .
  - ➢可深入数据帧保护

- 安全网络基础设备
  - ➢ConneXium 系列产品 .
  - ➢包括Connexium Eagle 及 Tofino 防火墙.

- 信息安全认证实验室

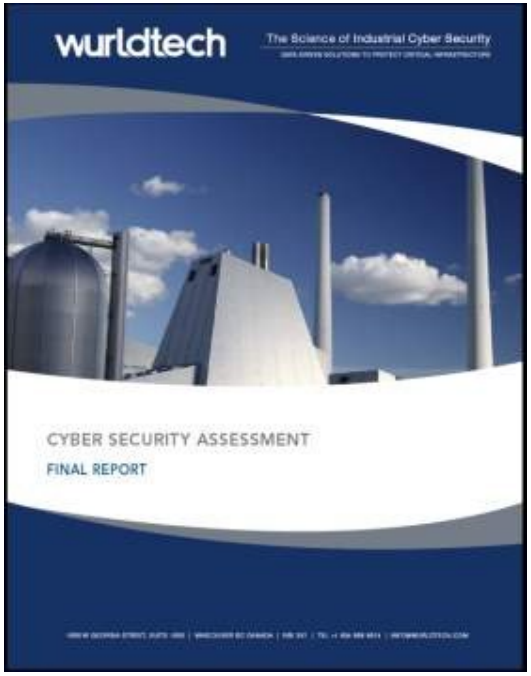
施耐德电气信息安全解决方案



施耐德电气信息安全解决方案

❑ 评估及设计服务

- 确认客户系统中存在漏洞
- 根据确认的漏洞及威胁评估系统的风险
- 提供建议
  - ➢架构
  - ➢设备加固
  - ➢培训
  - ➢处理
- 与Wurldtech 及SiS合作
  - 安全评估的领导者
  - 主要的安全标准提供者



总结:

- 信息安全在工业控制系统的日益重要
- 纵深防御是实现工业控制系统信息安全的最佳方法:
  - 降低风险 .
  - 提高系统可靠性 .
- 施耐德电气的信息安全解决方案
  - 提供信息
  - 评估及设计服务
  - 安全的产品
  - 推荐的安全协同自动化架构