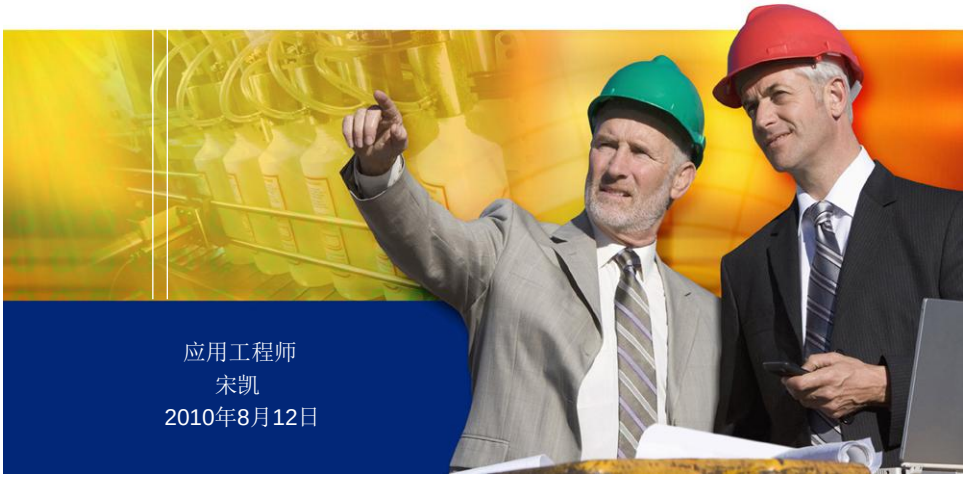
HIRSCHMANN
A BELDEN BRAND

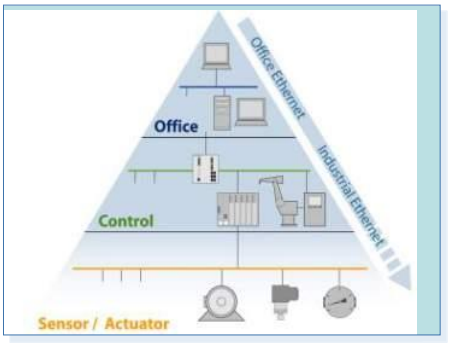
如何使控制系统网络更安全

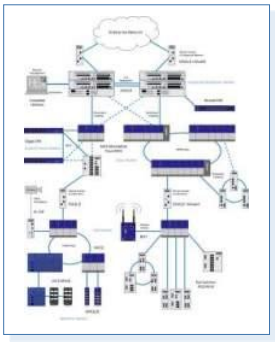


应用工程师
宋凯
2010年8月12日

关于赫思曼

- 美国百通公司旗下，提供“工业基础架构解决方案”
- 提供包括“有线网络”和“无线网络”的解决方案
- 工业领域以太网应用趋势的领导者 (PLC/ DCS, Safety, Video, VoIP Wireless)
- EAGLE Tofino™工业安全解决方案——一个独特的硬件和软件安全系统。





关于工业网络安全的典型问题

- “黑客们将永远不会攻击我的工厂”
  - 黑客不是问题。而像病毒和意外等这些日常问题才是真正的威胁。
  - 即使是一个简单的USB密钥就可以关闭整个工厂！
  - 有许多诸如设备故障，病毒，意外的设备管理信息系统配置例子。
- “为什么我不能只用Cisco？“（或其他喜爱的IT安全产品）
  - 恶劣的工业环境
  - 24x7 运行
  - 谁来配置和管理它们? 控制工程师们?
  - 成本?
  - 支持工业协议吗? (eg: Modbus Enforcer)

关于工业网络安全的典型问题

- “我永远不会把控制系统连接到互联网。那我的网络还有风险吗？”
- 我的控制系统和企业网络是使用防火墙分开的，我还需要额外的安全？“
  - 绝对 - 大多数进入系统的攻击不是从企业网络就是通过二次感染的途径，如笔记本电脑，USB钥匙，或通过虚拟专用网络（VPN）或调制解调器的远程访问。为了解决这个问题，控制系统内部的防火墙应给予额外的保护层，就像办公室电脑拥有个人防火墙和反病毒软件。这就是所谓的防御纵深战略。
- “我们并不需要防火墙 - 我们使用VLAN隔离子系统” 。
  - VLANs (eg: IEEE 802.1Q)只能使系统更易于管理，他们不添加任何数据过滤或保护。
  - 充其量，VLAN可以被认为是‘边界的保护 –在控制网络中他们不保护关键的’边界‘（PLC和RTU等）设备。

水处理事件,Harrisburg, PA

- 2006年10月一部被感染的笔记本电脑(维修用的),让黑客入侵访问了在美国宾夕法尼亚州的哈里斯堡水处理厂的计算机系统 。
- 被攻破的笔记本电脑是通过互联网，然后与一个VPN连接作为切入点用来安装病毒和间谍软件在这工厂SCADA系统的PC里。
- 虽然攻击目标并没有放在水的质量上,但此事件如果没有被发现的话,恶意软件随时可以到干扰工厂的业务。

佳士拿汽车工厂事件 - 多个地点受影响

- 2005年8月13日美国的佳士拿汽车工厂被一个简单的电脑病毒关闭了。
- 尽管公司网络与互联网之间已安装了专业防火墙，病毒依然能进入工厂的控制系统（可能是通过一台笔记本电脑）。
- 一旦进入了控制系统,病毒就能够在几秒钟之内从一个車间感染到另一个車间。
- 在这期间大约50,000流水线工人因此要暂停工作。
- 该事故的原因是什么？就是一个小小的病毒经过第二通道进入了网络。
- 估计损失影响为1,400万美元。

美国Browns Ferry核电厂的“安全”事件

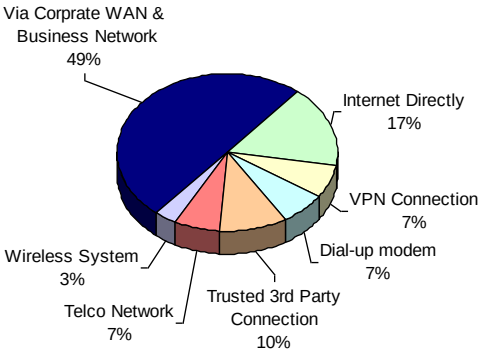
- 2006年8月因反应堆在‘高功率、低流量条件’的危险情况下，Browns Ferry核电厂所有人员不得不全部撤离。
- 控制循环水系统的冗余驱动器失效了，原因是控制网络上“过量通信”的缘故。
- 可能是两种不同供应商的控制产品产生了通讯过负荷现象。
- 该事故的原因是什么？不当和过度的通信在控制网络上。
- 核电厂因此停机2天,估计损失的费用约60万美元。

这些事件有什么共同点 ？

- **‘软’目标:**
  - 大多数控制网络中在运行的电脑，很少或没有机会安装全天候病毒防护或更新版本。
  - 控制器的设计都以优化实时的I/O功用为主，而并不提供加强的网络连接安全防护功能。
  - RTU，PLC或DCS系统都是非常容易受到攻击。任何黑客初学者都很容易获取入侵的工具。
- **多个网络端口切入点:**
  - 在多个网络安全事件中,事由都源于对多个网络端口进入点疏于防护。
  - USB钥匙，维修连接，笔记本电脑等.
- **疏露的网络分割设计:**
  - 许多控制网络都是“敞开的”,与不同的子系统之间都没有有效的隔离。
  - 问题因此通过网络迅速蔓延。

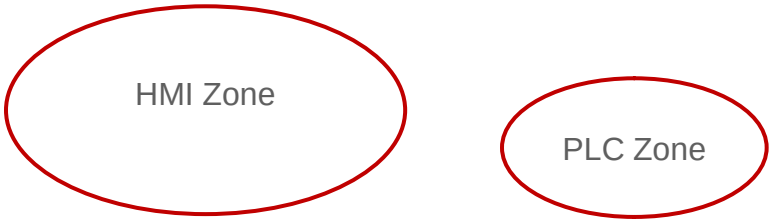
黑客如何成功入侵...

- 透过企业广域网和商用网络
- 直接从万维网进入
- 受信任的第三方
- 受感染的笔记本电脑连接到这个电脑网络上。



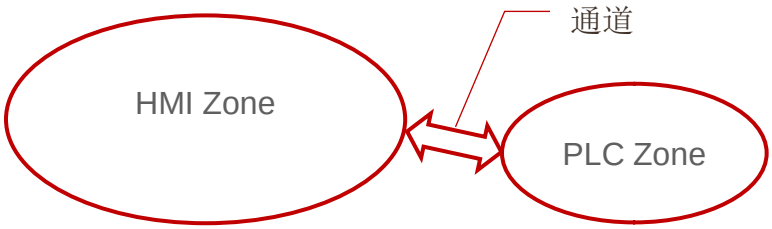
ANSI/ISA-99: 控制系统划分

- 新ANSI/ISA-99安全标准的核心理念是“区域和通道”
- 在控制系统内部采用水平分割和传输控制。
- 根据控制功能将网络分层或区域。
- 多个独立区域有助于提供“深度防御”。



ANSI/ISA-99：区域的连接

- 通道是两个区域之间的数据流路径，安全控制如下：
  - 进入区域的控制
  - 采用抵御拒绝服务（DoS）防范攻击或恶意软件的转移。
  - 屏蔽其他网络系统
  - 保护网络流量的完整性和保密性。

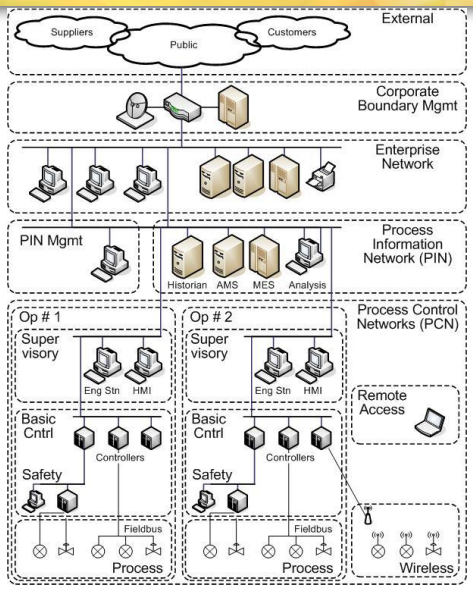


采用区域及通道来保护网络

- 每一个服务通道，防火墙只允许设备正确操作所必需的数据流经过。

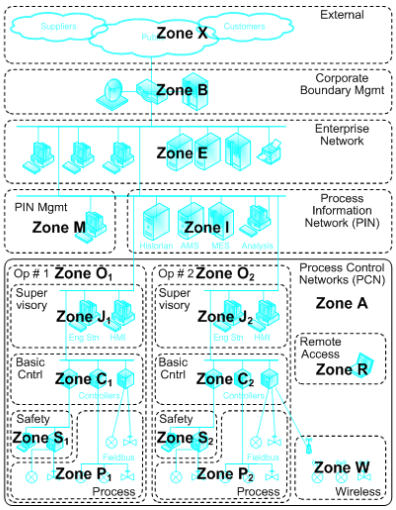
HIRSCHMANN
A BELDEN BRAND

区域的设计：以一座炼油厂为例

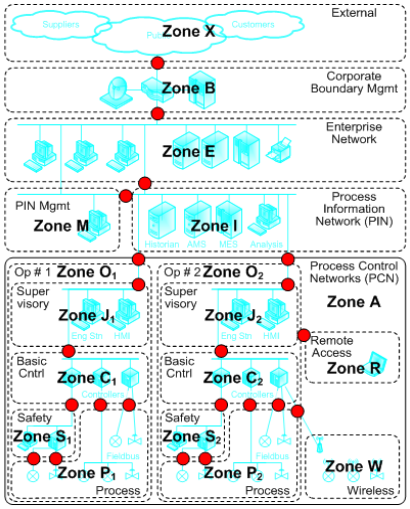


HIRSCHMANN
A BELDEN BRAND

区域的划分

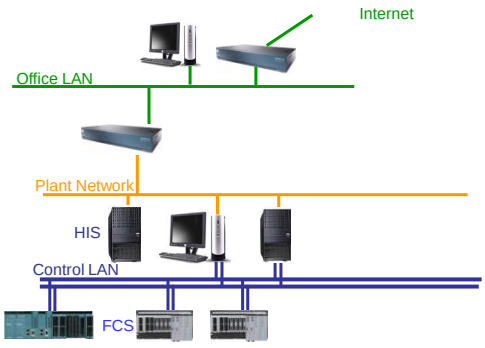


通道的设定



典型控制网络

- 多层结构 – ‘Purdue’ 模型（5层结构）



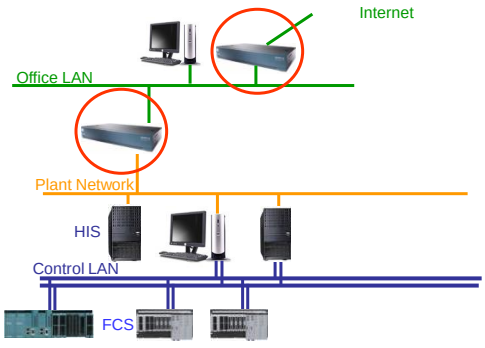
分层防御

- 网络边界安全
- 内部网络安全
- 终端安全

Yokogawa Security Standard of System
TI 33Y01B30-01E

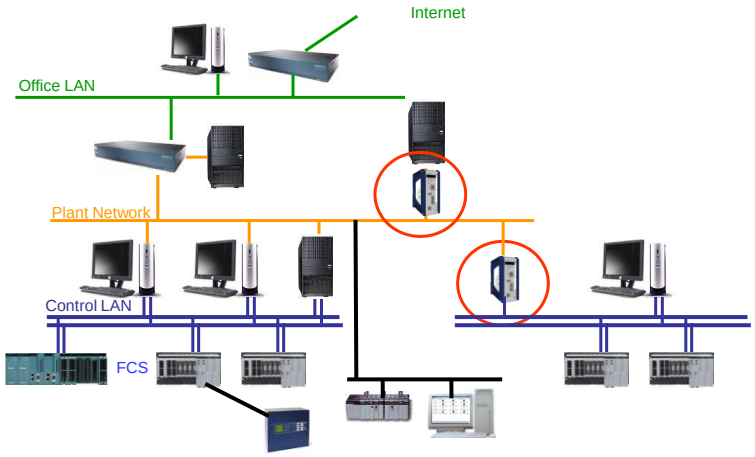
网络边界安全

- 在主接入点放置大型IT式防火墙
- 在第二层接入放置工业防火墙



内部网络安全

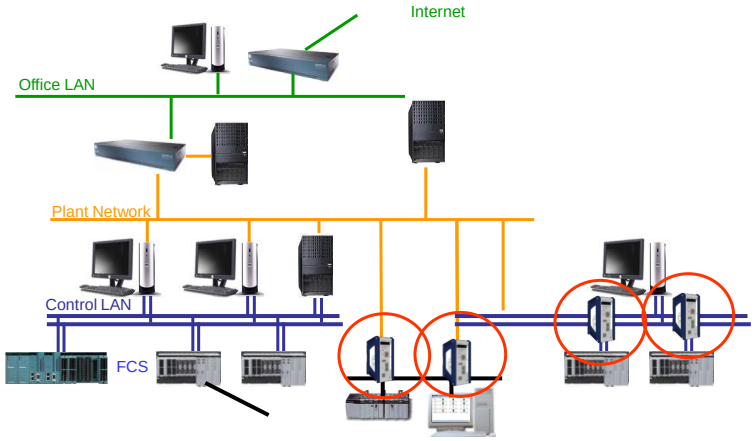
- 各个子系统间的工业防火墙



终端安全

- 个人终端出现任何问题都可以添加安全软件：
  - 补丁
  - 个人防火墙 (like ZoneAlarm)
  - 防病毒软件
  - 加密 (VPN Client or PGP)
- “*我们建议在个人电脑上使用下列个人防火墙策略组件*.”
- 但是你不能添加防火墙软件到PLC或RTU …

终端安全



EAGLE Tofino™ System

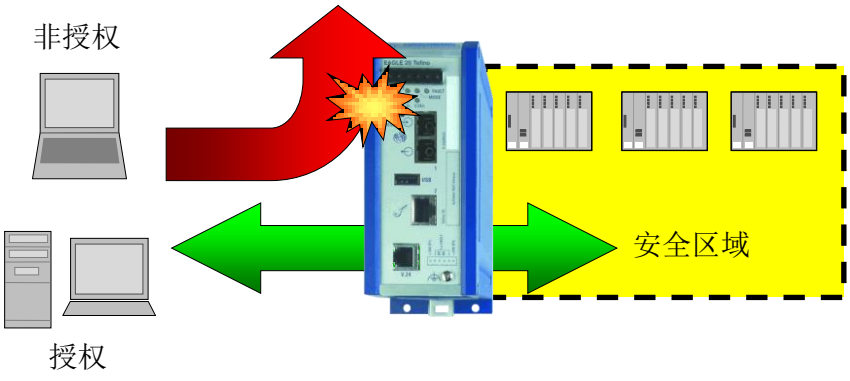
EAGLE Tofino™是什么?

- 一个专为工业自动化设计的网络安全系统
- 配置或操作无需IT知识要求
- 预定义的模板：
  - > 50 个工业通信协议
  - > 25 个厂家的工业控制器
- 提供“深度防御”
  - 内部网络的安全区

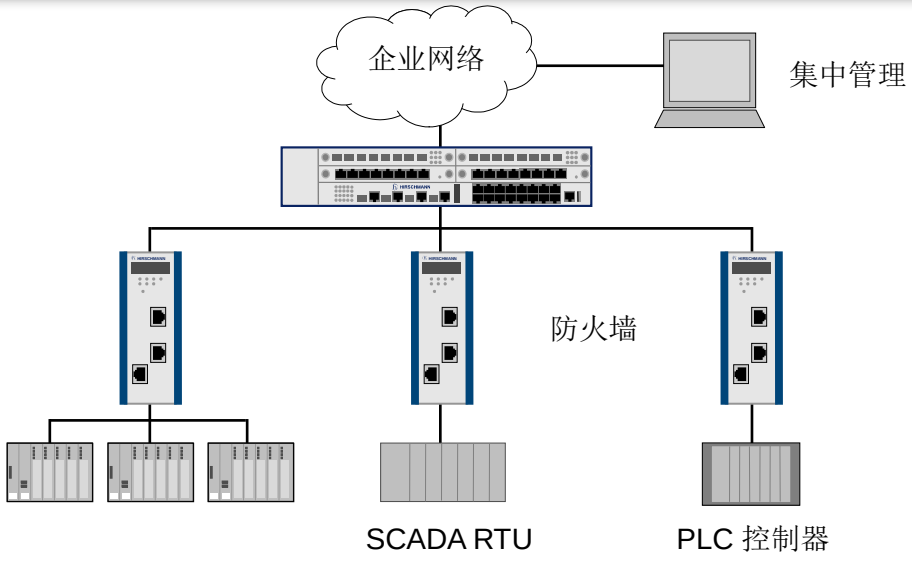
为什么要使用EAGLE Tofino™?

- 传统的防火墙并非专为控制系统或工业环境而设计的，这样会把一切工厂设备和系统都暴露在黑客威嚇之下。
- 每年网络攻击事件和主要基础设施被破坏的损失高达数十亿美元。
- EAGLE Tofino™为你提供贴身制定的防火墙，提供对设备的保护区-区级安全™。安全保护超越一般传统的防火墙。

区域级安全



EAGLE Tofino™架构

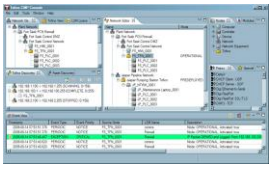


EAGLE Tofino™关键组件

- Tofino™ Security Appliance
  Tofino™安全设备模块

- Tofino™ Loadable Security Modules (LSM)
  Tofino™可装载的安全插件 (LSM)

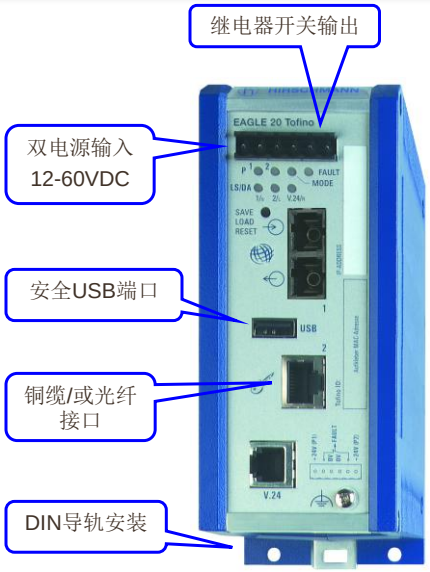
- Tofino™ Central Management Platform (CMP)
  Tofino™中央管理平台(CMP)



Eagle 20 Tofino

硬件规格：

- 外形类似普通的I/O模块和隔离器
- 温度0℃到60 ℃
- 双电源输入12-60VDC
- 继电器开关输出
- 铜缆/或光纤网络接口
- MUSIC安全认证



零配置安装模式

- 现场技术人员只需要做的：
  - 安装防火墙到导轨上
  - 连接电源
  - 插入网络电缆
  - 离开…
- Eagle Tofino™在启动过程中对网络系统是完全透明的。
- 二层（以太网）桥接指无需更改网络架构或现有设备无需做地址的处理。

EAGLE Tofino™可装载安全软插件(LSM)

- LSM是软件插件，提供的安全服务诸如：
  - 防火墙
  - 稳固资产管理
  - 内容检测
  - VPN加密
- 每个LSM插件是可下载到EAGLE Tofino™安全设备模块(TSA)里，使它能够提供可定制的安全功能，这取决于控制系统的要求。

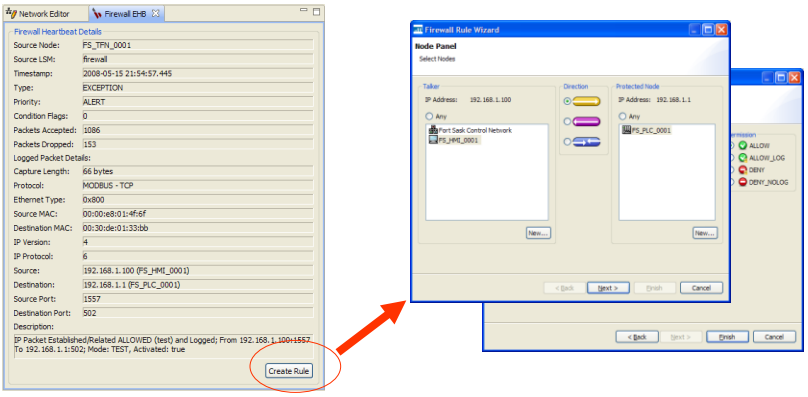
EAGLE Tofino™防火墙功能

- 控制工程师可制定通讯规则。
- 自动阻止并报告任何不匹配规则的数据流。
- 可使用图形拖放来编辑简单的规则定义。

EAGLE Tofino™ 安全资产管理功能

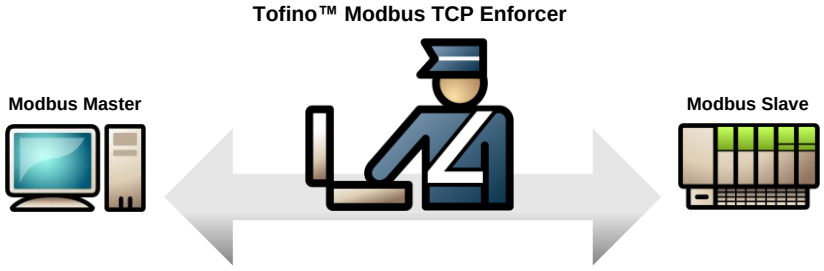
遗漏了一些规则？没问题

- 安全资产管理（SAM）插件会执行一个向导，指导用户从防火墙报警列表中建立用户新的防火墙规则。



EAGLE Tofino™ Modbus TCP协议执行器功能

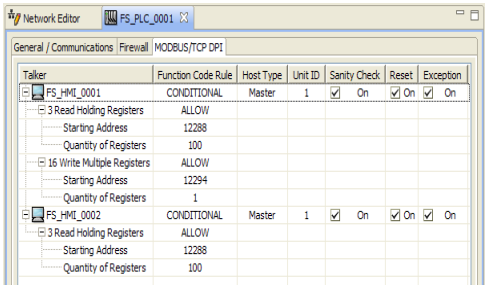
- 控制工程师可定义允许的Modbus指令列表。
- 自动阻止并报告任何不匹配规则的数据流。
- 协议要通过‘完整性检查‘, 这可阻挡任何不符合Modbus标准的数据流。



EAGLE Tofino™ Modbus TCP协议执行器

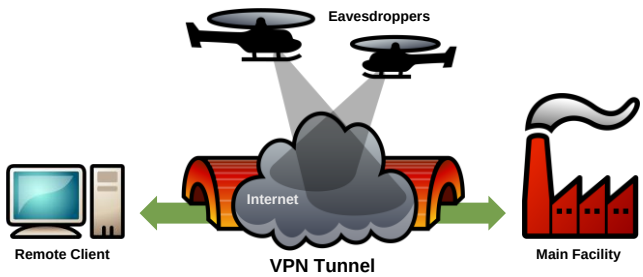
例如：2台HMI对 PLC的访问

- 人机界面＃1允许具有完全的读/写访问
- 人机界面＃2只允许读访问
- 所有非必要功能码都被封锁



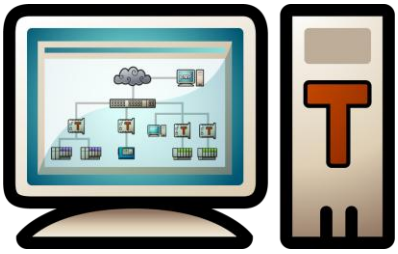
EAGLE Tofino™ VPN功能

- 建立安全可靠的连接: Tofino™模块之间、 Tofino™模块与个人电脑之间，以及Tofino™与支持的第三方设备之间。
- 简单的设置和管理
- 可与其他Tofino™ LSM (如防火墙，Modbus TCP数据执行机器）的安全功能相结合相互操作。



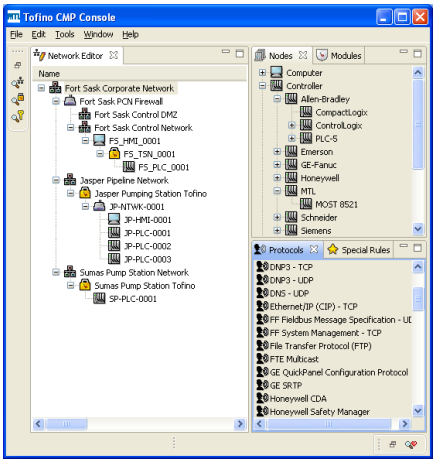
EAGLE Tofino™中央管理平台（CMP）：集中式安全管理

- 组态，从一个工作站上管理和监测所有EAGLE 20 Tofino。
- 内置的网络编辑器可让你快速的组态你的控制网络。
- 图形拖放的编辑器，让你快速制定网络安全规则与配置。



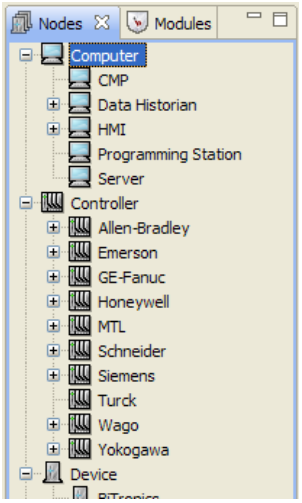
EAGLE Tofino™中央管理平台（CMP）：操作简单

- 在整个系统里很容易查找EAGLE 20 Tofino，控制器和个人电脑
- 网络拓扑
- 使用可拖放模块、通讯协议等来制定你的网络规则。
- 测试
- 部署
- 监控和管理



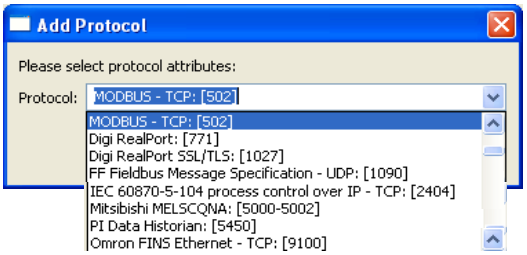
控制器模板预定义

- 超过25个预定义的控制器模板
  - 定义通讯协议
  - 在必要时，可制定特殊规则以堵塞漏洞。
- 在网络编辑器里，可采用拖放手段操作。
- 每个新版本都自动更新。



工业通信协议

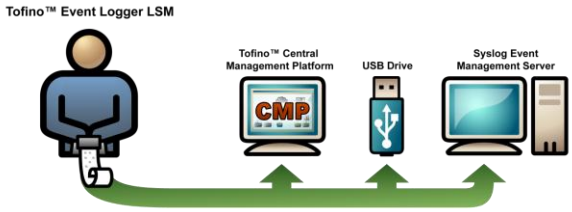
- EAGLE Tofino™支持的主要工业通信协议：
  - MODBUS/TCP
  - Ethernet/IP (Rockwell)
  - GE-Fanuc
  - Honeywell
  - Yokogawa
  - Emerson
  - Mitsubishi
  - PI
  - OPC
  - 还有更多！（超过50种）



- 含有内建的协议向导，能很容易地添加新的协议。

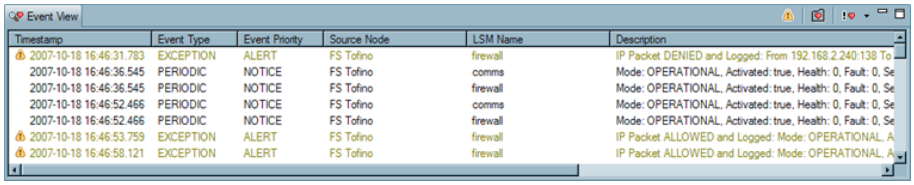
EAGLE Tofino™事件记录器：对事件日志记录的三重保护

- EAGLE Tofino™安全设备模块(TSA)可同时记录事件到下列任何一项：
  - 系统日志服务器
  - EAGLE Tofino™ CMP工作站
  - 本地存储 - 通过USB卸载



测试模式

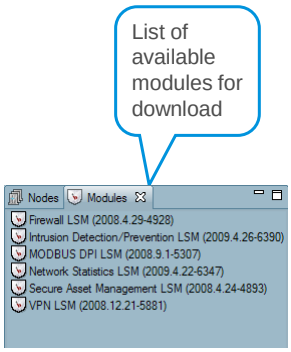
- EAGLE Tofino™有三种工作模式：
  - 被动模式 - 允许任何的连接，历史记录关闭
  - 测试模式 - 允许任何的连接，历史记录启动
  - 操作模式 - 防火墙规则启用
- 在操作模式时， EAGLE Tofino™将阻止任何没有‘允许规则’许可的传输与连接。
- 测试模式允许任何的连接，但会报告被删除的传输与连接。



不仅仅只是一个防火墙

可加载的安全插件（LSM）使得在同一台设备上可以添加多种安全功能：

- 支持安全功能有：
  - 防火墙
  - 安全资产管理
  - Modbus执行器
  - VPN/加密客户端和服务器
  - 事件记录
- 未来的安全功能有：
  - OPC 执行器
- 随时可以加入新的安全模块（TSA）



EAGLE Tofino™的关键特点和优点

- 专为工业应用设计
  - 特别为恶劣的工业环境而设计。
  - 不需系统停顿就可以安装，配置，操作和版本更新。
  - 测试防火墙规则时，也不会阻塞正常的传输和连接。
- 优点
  - 工厂风险最小
  - 投资成本最低
- 专为控制工程师而设计
  - 通用控制器和协议都是预先设定的。
  - 简单容易的操作可实现快速的部署和减少配置错误的几率。
- 优点
  - 部署成本最低
  - 增强的安全性

HIRSCHMANN
A BELDEN BRAND