软件

电力设施网络的“保护伞”

电力行业网络安全面临的一个长期挑战是集成操作、信息技术团队以及功能，尤其在它们涉及远程或第三方系统时，有一个新的军事等级安全方法将确保工业控制系统安全性，同时又不影响日常操作。

文 | David Mattes

发电公司和波音公司有什么共同点？那就是需要保护工业数字控制系统，同时不妨碍这些系统的日常运行，并保持远程设备和系统的必要通信。

虽然有很多保护工业控制系统（ICS）资产的办法，但找到一个能轻松地集成所有遗留系统、设备和接口的通用方法却是一个重大挑战。确保网络安全的关键资产绝不只是一个“单步”过程。ICS 和网络软件系统补丁应能系统地确保最高安全水平，员工安全意识培训是一项长期的任务。但对今天的行业来说，随着至关重要的数字系统数量的增加和多样性的提高，“保护伞”解决方案可以显著提高维护运行环境安全的可能性。

确保默认值

人们越来越依赖计算机自动化来优化电力生产，电力设施的攻击面也在增加。运营团队（OT）面临着优化这些分布式设施的关键任务系统，但资源和信息技术（IT）安全专家人数通常有限。Tempered Networks 解决方案在 OT 和 IT 团队日益提高的运行完整性的需求与要求组织关键基础设施信息的可用性之间架起了一座桥梁。它的解决方案专门帮助发电设施明显提高分散资产的整体安全态势，同时增强分布式控制系统（DCS）网络的稳健性。

图 1 Tempered Networks 系统，HIPswitch Conductor 是一个可伸缩的协调编引擎，它管理 SimpleConnect Web 管理界面和分布式 HIPswitches 之间的配置、安全策略、信任关系、监视以及分析

Tempered Networks 提供了一个集中管理的安全设备解决方案，它包括加强型内置硬件和软件组件，利用客户现有网络基础设施有效地确保工业连接的安全性。虽然没有银弹安全解决方案，Tempered Networks 系统在设计上采用默认方式，使用简单且极具成本效益。

公司的解决方案包括三个紧密集成在一起的组件：HIPswitch Conductor、HIPswitch Securty Appliance 和 SimpleConnect Web Management Interface。HIPswitch Conductor 是一个可伸缩的协调编引擎，它管理 SimpleConnect Web 管理界面和分布式 HIPswitches 之间的配置、安全策略、信任关系、监视和分析。

Tempered Networks 保护工业控制系

统和设备的方法涉及三个主要组件：分段、安全的连接和远程监控，以及管理第三方连接。

电力设施关键基础设施和 DCS 网络保护的行业最佳实践是分段网络。Tempered Networks 的解决方案使组织能将生产设施之间的连接进行分段，并在段与段之间相互隔离。然而，与传统防火墙或虚拟专用网络（VPN）不同的是，Tempered Networks 解决方案并不是简单的检查，它遍历网络控制系统，同时增加了授权证书、数据机密性、完整性和可用性保护。它在实质上提供了一个“作为服务设备的 VPN”，因此你能以无限的规模维持管理下的单个覆盖网络。

另一个区别是，解决方案专门由 OT 团队部署和管理，而防火墙和 VPN 要求先进的安全技术，属于资源密集型，尤其对于大规模设施。

协调 / 控制概述

在设计解决方案时，符合行业标准是一个关键要素，客户始终看重这一点。Tempered Networks 基于可信计算组织（TCG）、互联网工程任务组（IETF）和国际社会自动化（ISA）标准提供了一个专用 ICS 和关键基础设施解决方案。协调基于可信计算组织的 IF-MAP 协议进行，遵循专用工业控制系统网络安全规范。

协调遵循一个网络概念“控制平台”，它仅用于控制和监测 HIPswitches 部署。这是一个极有效的方法，因为它会避免 Tempered Networks 陷入系统瓶颈。HIPswitches 独立处理数据平面，无须协调。因此在无法使用协调服务时，它们能继续依靠当前配置运行。

无论任何组织，始终要考虑管理方面的人为因素，当采用协调服务来管理安全和连通性时，这个问题就会出现。Tempered Networks 已采用措施来管理这种风险，包括角色授权、粒度日志和通过强调合作来提高可见性。

客户通常舍得花钱投资其他 IT 安全解决方案，例如防火墙、深层数据包检测（DPI）、安全事件和事件管理（SIEM）系统、数据二极管和网络入侵检测系统（NIDS）。Tempered Networks 网络解决方案用于任何这些现有系统，有效保护客户投资。Tempered Networks 解决方案不仅为保护措施构建一个安全的周边环境，而且还通过隐藏关键基础设施的足迹来提供一个额外的安全层。所以，即使攻击者获得原有虚拟局域网（VLAN）或 VPN，客户的关键基础设施和信息仍受到保护，因为对于黑客来说，它是隐匿的、无形的。

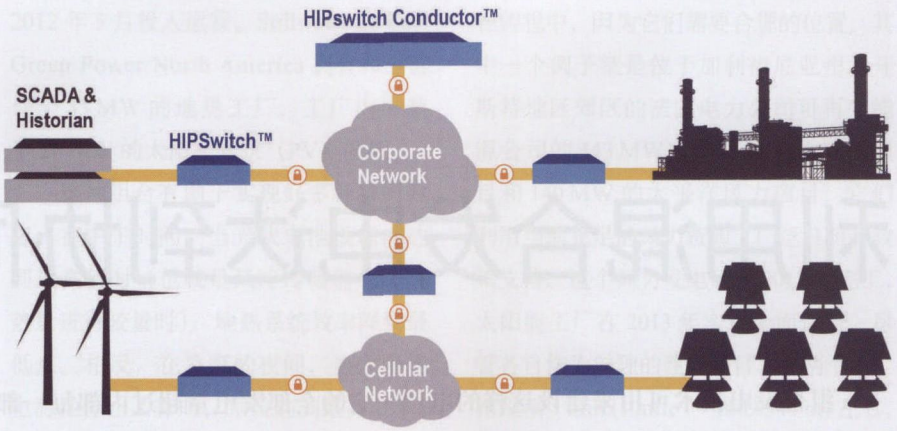

图 2 分布式设备和多元化系统的安全连接，Tempered Networks 的 HIPswitch 安全设备与运输和拓扑无关，支持任何 Cellular、WiFi、有线以太网或卫星通信网络

网络资源显示一种趋势，企业中多个业务用户共享资源，模糊了传统的“一网一用户”模型。此外，公司没有那么多钱来建立多重独立网络。

ICS 和企业 IT 网络面临越来越明显的连通性和收敛性的趋势使安全问题更加复杂。由于工业设备是联网的，他们实质上面临着网络安全威胁，使安全成为各个企业的主要问题。因此，许多行业的 IT 部门在保护他们产生收入的关键基础设施方面的负担越来越重。

Tempered Networks 解决方案增加了额外的保护措施，以确保 ICS 设备顺利通过补丁更新周期。即使当前威胁环境升级，但 ICS 供应商仍不着急发布适用于当前支持产品的补丁。供应商的延误会使关键 ICS 组件暴露在风险中。而且，在供货商支持结束后，许多设施仍继续使用 ICS 产品。

Tempered Networks 现处于早期部署阶段，正在接受几家北美发电设施，包括燃煤、燃气和风力发电设施的评估，主要应用程序是为了确保能量管理系统（EMS）/ SCADA 系统能远程连接和远程访问用户。除了军用安全等级外，客户对这个解决方案也很满意，因为它易于部署和维护。从它还在波音公司的制造车间里，设计要求的一个原则就是提供一个透明的救援方案。客户不能容忍现有业务中断，这可能包括在现有的设备上安装软件、对现有设备进行配置修改和安装系统时，出现任何部件停机。为了避免运行中断，Tempered Networks 的 HIPswitches 能运送预配置和在网络上快速部署。

符合标准 超越期望

相对于为了满足监管要求而产生的成本，电力企业正在权衡越来越多的各级设施互联网协议（IP）连接的好处。符合北美电力可靠性公司（NERC）的关键基础设施保护（CIP）标准可不是一件容易的事，无论从执行、验证，还是从潜在处罚来说。在未来，电力基础设施所有者必须部署满足法规遵从性的网络架构。

该解决方案是为了部署在监管下的电力公用事业环境，以实现通常与提高连通性有关的业务目标，同时有助于符合法规和减少符合 NERC-CIP 标准产生的成本。MM