面向公用事业的瞻博网络融合工业边缘

为实现 IT-OT 融合的基于标准的开放式多供应商平台

挑战

电网基础设施现代化使管理和技术变得复杂。消除租用线路，淘汰模拟技术，采用新的流量工程控制，建立更强大的网络安全性，并引入新的应用程序，可让功能有限的孤立系统进行跨系统的数据共享。

解决方案

面向公用事业架构的融合工业边缘（包括瞻博网络路由、交换和安全、Dragos 工业控制系统威胁检测、SEL 软件定义的以太网交换机、流量控制器和 TDM 转以太网多路复用器）将最好的技术与久经考验的自动化工具相结合，扩大您的转型规模，同时消除复杂性。

优势

- *降低了提供新服务所需的总体拥有成本，同时提高安全性、态势感知能力和弹性*
- *支持在 IP 网络上使用传统的串行通信基础设施*
- *按需部署电路，无需在任何交换机中定义流量，也无需上门服务*
- *为关键基础设施保驾护航，安全看得见，并对 IT-OT 域中发生的网络攻击作出积极响应*

依靠运维技术 (OT) 网络，电力公用事业为对其业务至关重要的工业控制系统 (ICS) 提供支持。长期以来，OT/ICS 平台的管理一直独立于 IT 网络；操作模式 、刷新周期时长以及物理和网络安全考虑因素方面的差异是将 IT 和 OT 域分离的常见理由。但是，随着预算压力的增加以及电网边缘现代化业务案例的倍增 ，降低成本和简化运营的优势促使公用事业单位重新评估他们对通信基础设施融合的选择。

无论从网络安全还是互操作性的角度，OT/ICS 人员过去一直怀疑 IT 缺乏确定性、精确性和安全性。通信技术以 IT 为基础，其“尽力而为”性质不仅与电网控制和保护应用程序的亚毫秒级需求存在根本冲突，还会危及昂贵的电网资产，甚至个人安全。基于数据包的网络代表一个网络攻击面，因此，即使 OT/ICS 现代化的经济性带来了整合的优势 ，但缺乏通用、可信、安全的通信模型阻碍了它的实施及其优势的实现。

瞻博网络、SEL Inc. 和 Dragos Inc. 共同合作，构建面向公用事业参考架构的融合工业边缘。该架构直接解决了利用多供应商解决方案对 IT 和 OT 用例（在单一的端到端平台中进行保护、 控制、测试和监控）提供原生支持的过程中存在的信任、数据完整性和中介访问难题。该架构采用云原生技术，对在私有、自主、基于数据包的网络中进行的编排、控制、管理、自动化、网络安全和预测分析操作予以简化和改进，将 IT-OT 融合重新设想为私有运营云 (OC)。

挑战

IT 和 OT 的安全集成不仅对电网边缘的成功数字化至关重要，对当前和未来的业务需求也至关重要。虽然公用事业单位意识到融合带来的巨大业务价值，但必须解决对保护和控制应用程序的网络安全、安全性、可靠性和性能方面的担忧。

面向公用事业架构的融合工业边缘提供的解决方案让您可以：

- 为基于 OT-SDN 和 IEC 61850 以太网的变电站现代化做好部署准备
- 增强跨 IT-OT 边界的网络安全、合规性和态势感知
- 为公用事业运维人员配备预测分析和编排自动化平台
- 实现电路和服务的敏捷部署，无需上门服务
- 支持已安装的中继器、智能电子设备 (IED) 和远程终端单元 (RTU) 的传统通信

面向公用事业架构的融合工业边缘

瞻博网络（网络与安全领域的领导者）、SEL Inc.（电网保护与控制基础设施领域的领导者）和 Dragos Inc.（ICS 威胁检测与缓解领域的领导者）共同合作，定义了一个改变现有 IT-OT 电网通信范式的架构。该合作伙伴关系由美国能源部所拨的研究与开发专款做后盾，旨在通过面向运营环境的云原生技术增强国家能源基础设施的弹性，达成构建开放式多供应商网络架构的愿景。该架构由一个基于数据包的转发平面（从数据/控制中心扩展到变电站）、一个管理控制平面（用于端到端调配、监控和测试）以及一个网络安全平面（用于 NERC-CIP 合规性和工业控制系统威胁检测）组成。

三个独特功能使得该联合解决方案有别于竞争对手：

1. **端到端、基于数据包的数据平面：**数据包转发平面由瞻博网络路由器、交换机和防火墙组成，针对两种用例进行了架构优化：a) 安全的云就绪数据/控制中心，b) WAN 传输核心、聚合和边缘。基于数据包的转发平面利用 SEL Inc. 的 OT-SDN 以太网解决方案扩展到变电站。端到端电路调配以及遥测聚合和可视化提供了服务等级 (CoS)、计时以及同步和控制平面的灵活性，可解决要求毫秒级分辨率的确定性应用程序。

   优势：可在该基础设施中创建、测试、监控和拆除端到端标签交换路径 (LSP)、第 2 层/第 3 层 VPN 和逻辑流。使用以下所述的管理和控制平面创建端到端电路调配以及遥测聚合和可视化。

2. **管理和控制平面：**管理和控制平面由独立的软件应用程序组成，例如 WAN 和 LAN 控制器、遥测聚合器、整理器和元素管理器，所有这些都在一个现代 Kubernetes 软件平台上实现安全互操作，从而将用例、服务和应用程序部署为工作流程。软件组件集成在针对本地私有网络部署进行了优化的物理服务器上。

   优势：管理和控制平面利用 Kubernetes 群集微服务架构来部署和控制通过标准 API 公开的多供应商应用程序，以确保互操作性。事件驱动型基础设施提供应用程序间的通信，而工作流程引擎将操作者的意图与企业网络安全策略和网络库存连接在一起。用例以自动工作流程交付，在有限的人力干预下触发调配、监控和测试。

3. **网络安全平面：**网络安全平面由位于数据/控制中心内部和整个 IT-OT 环境中的 Juniper Networks® SRX 系列服务网关以及面向 OT ICS 环境的 Dragos Inc. 威胁保护和事件响应产品与服务组成。瞻博网络和 Dragos 通过已建立的 REST API 进行互操作。

   优势：行业内对 OT 事件安全源的首次积极响应由 Junos Space® 策略实施器引擎提取摘要，以积极响应运营域内的攻击。

借助私有 OC，公用事业单位可以安全地加快以下方面的部署：

- 时分多路复用 (TDM) 到 IP 传输的转换
- OT-SDN 和 IEC 61850 变电站数字化二次系统 (DSS) 的现代化
- 数据或控制中心的现代化
- 在不影响 OT 系统性能的情况下安全地引入 VoIP 和视频流等新服务

面向公用事业架构的融合工业边缘以自动工作流程交付用例。对用户意图、网络安全策略和网络库存进行建模和模板化，使用户错误和一次性网络需求成为离群值。由此产生的效率增益降低了提交新服务和改进安全性、态势感知以及弹性所需的总体拥有成本。

工作原理

面向公用事业架构的融合工业边缘利用来自每个公司各自专业领域的组件提供完整的端到端融合解决方案：

- 瞻博网络 MX 系列 5G 通用路由平台提供安全传输 OT-SDN、IEC 61850 和 TDM 转 IP 流量所需的可扩展、弹性和自动化就绪的 MPLS 主干，以及 VoIP、视频和企业 IT 应用程序。
- 瞻博网络 QFX 系列交换机和 EX 系列以太网交换机提供一个现代的基于第 3 层 IP 的底层（也称为 Clos 网络），以及一个用于网络虚拟化的以太网 VPN (EVPN) - 虚拟可扩展 LAN (VXLAN) 叠加网络。
- 瞻博网络基于微服务的管理和编排工具建立了一个自动化背板，能将独立的软件系统（例如，故障单系统、SDN 控制器和元素管理系统）与可配置的工作流程融合在一起，创造更高的业务价值和成本效益。
- Dragos Inc. 面向 OT ICS 环境的威胁保护与事件响应产品和服务使 ICS/OT 资产以及公用事业和其他关键基础设施面临的威胁完全可见，在发生重大损失之前提供最佳实践的响应建议。
- 针对变电站进行了强化的 SEL 2740S 软件定义交换机和 SEL 5056 软件定义流量控制器为变电站的现代化提供了 OT-SDN 和 IEC 61850 以太网交换矩阵。
- SEL 集成通信光纤网络 (ICON) TDM 转以太网多路复用器与 MPLS 网络集成，同时保持了线路电流差动保护和直接传输脱扣应用程序的毫秒级精度，从而为传统电路需求提供支持。

借助自动化的强大功能，瞻博网络、SEL 和 Dragos 可以帮助我们的共同客户做到以下几点：

- 加快部署基于策略的新架构，同时降低人为错误的风险
- 创造一个规范化设计的网络环境，安全地对数据流进行实例化、测试、监控和停用
- 借助传统与现代混合的变电站架构，实现从传统 IED、RTU，再到中继器的过渡
- 将协议、网络流量、历史数据、主机日志、资产特征和异常作为数据源，为 ICS/OT 环境提供出色的可见性

总结 - 通过健全工程实现电网现代化

电网基础设施现代化可能会导致管理和技术过于复杂。当今的公用事业单位需要进行适当的工程简化。

过去 30 年来，IT 领域以惊人的速度不断演化。但是，这种演化带来了巨大的复杂性，使 IT 系统的管理更难、安全性更低。OT 领域对变化速度和不稳定性持谨慎态度，避免在关键基础设施中采用 IT 技术，这是可以理解的。

面对这些挑战，IT 组织进行了大规模创新，以扩展其产品/服务和功能。云原生技术创造了当今世界上规模最大的企业所使用的软件定义网络功能、编排、自动化以及新型网络安全，为他们最重要的运营提供支持。

通过应用健全的工程原则，可以及时地在关键基础设施中部署基于以太网/IP 的数据包技术，满足公用事业单位的需求，为新一代边缘配电网现代化和工业物联网应用程序提供支持。通过引入自动化，可以填补年龄偏大和即将退休的 OT 员工的职位，并安全地停用或更换已达到使用寿命的机电设备。

IT 在与复杂性的战斗中生存了下来，拥有了简化工程的全新使命。面向公用事业架构的融合工业边缘自动执行复杂任务（例如跨多个网络交换矩阵和操作系统对电路进行端到端调配），充分利用了这些久经考验的创新技术。它采用软件定义的模型，将物理组件提取到从控制中心到终端设备的转发平面中。它还针对本地和私有网络应用程序进行了优化，保持了集中管理和控制安全性、态势感知以及网络敏捷性的能力。

后续举措

要了解有关此联合解决方案的更多信息，请联系您的瞻博网络客户代表 (Juniper-SEL-OT-SDN@juniper.net)，或访问 www.juniper.net/cn/zh/solutions/industrial/utility/

关于瞻博网络

瞻博网络将简单性融入到全球互联的产品、解决方案和服务之中。通过工程创新，我们消除了云时代网络的限制和复杂性，可应对我们的客户和合作伙伴日常面临的严苛挑战。在瞻博网络，我们坚信：网络是分享知识和实现人类进步的资源，它将改变这个世界。我们致力于开创具有突破性的方式，提供以业务速度发展的自动化、可扩展且安全的网络。

关于 Dragos Inc.

Dragos 是工业网络安全专家，一如既往地肩负着保护文明的使命。在网络安全威胁不断增加的世界中，Dragos 为最关键的基础设施提供保护，正是这些基础设施为我们提供了现代文明的基本原则，因此即便对手日益强大、蓄意破坏，也无法构成威胁。Dragos 专注于编撰和分享我们对 ICS/OT 系统的深度行业知识，为全球的工业防御者提供他们所需的知识和工具，尽可能有效、高效地保护他们的系统。要了解更多信息，请访问 www.dragos.com/#Dragos

关于 SEL Inc.

SEL 发明、设计和构建为全球电网提供保护的数字产品和系统。该技术可防止停电，使客户能够在降低成本的同时提高电力系统的可靠性和安全性。SEL 是一家 100% 员工所有制公司，其总部位于华盛顿州普尔曼，自 1984 年起在美国制造产品，目前服务于全球客户。我们的使命很简单：让电力更安全、更可靠、更经济。访问 www.selinc.com 了解更多信息

公司和销售总部
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
电话：888.JUNIPER (888.586.4737)
或 +1.408.745.2000
传真：+1.408.745.2100
www.juniper.net

亚太地区及欧洲、中东和非洲地区总部
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
电话：+31.0.207.125.700
传真：+31.0.207.125.701

JUNIPER NETWORKS | Engineering Simplicity