PROVISION INFOTECH

CASE STUDY: IDENTIFYING AND ELIMINATING ROGUE WIRELESS ACCESS IN A CRITICAL OT ENVIRONMENT

What We Did

A major gas processing facility began experiencing sporadic HMI latency and delayed alarms. Although internal IT teams found no anomalies through standard tools, concerns over operational risk led the company to engage Provision Infotech for an on-site OT network assessment.

Using PacketProof™ capture tools and a structured walkdown, our team quickly identified irregular broadcast traffic and latency spikes within the control VLAN. Tracing the signal path, we discovered several unauthorized cellular modems and wireless access points installed by a third-party vendor—devices with open outbound internet access and no firewall segmentation from SCADA or HMI servers.

These rogue devices introduced uncontrolled remote access to critical systems, violating corporate policies and bypassing all network protections. Provision isolated and decommissioned the devices, then redesigned the vendor-access structure with a secured DMZ, VLAN isolation, firewall rules, and multi-factor authentication.

The root cause of the latency issue was resolved, but the impact extended further. Our findings triggered a company-wide review of OT segmentation, resulting in stronger zoning policies, updated architecture diagrams, and improved alignment between IT protocols and plant-floor practices. The engagement mitigated immediate risk while delivering long-term improvements in cyber hygiene, vendor oversight, and operational reliability.

Highlights

Rogue Devices Found on Control Network

Unauthorized modems and wireless access points were discovered with open internet access - posing a serious cybersecurity risk.

Root Cause Resolved with PacketProof™ Tools

Broadcast traffic and latency spikes were traced to unapproved devices, resolving HMI delays and alarm issues.

Vendor Access Re-Engineered for Security

Provision implemented a dedicated DMZ, VLAN isolation, MFA, and firewall controls to secure third-party connections.

Triggered Company-Wide OT Network Overhaul

The incident led to improved segmentation policies, architecture updates, and better alignment between IT and operations.

Ready to see these results for your business?

Contact Us

info@provisioninfotech.com

provisioninfotech.com

PROVISION INFOTECH

Empowering the **Energy Industry Through IT & OT Excellence**

We bridge the gap between corporate IT and front-line operational technology (OT), delivering reliable, hands-on, facility based secure technology solutions that keep Western Canada's energy infrastructure operating safely and efficiently.

Who We Are

Provision Infotech has supported energy producers across Alberta, British Columbia, and Saskatchewan since 2015. Our team brings together corporate IT engineers and deep OT expertise, safety-certified field technicians, making us equally effective in head offices, control rooms, and remote well sites.

What We Deliver

OT & IT Specialists
One team that speaks both languages.

Certified On-Site Support
Our COR-certified, ISNetworld & ComplyWorks-verified field technicians are embedded onsite in remote field locations, providing consistent, boots-on-the-ground support

Cybersecurity & Risk Management
Threat hunting, patching, and compliance for industrial networks assessments.

Control & Industrial Networks
Design, build and maintenance for SCADA, PLC, and HMI.

Secure Remote HMI Access
Encrypted, role-based connectivity for dispersed operations.

Why Choose Us

Purpose-built IT & OT team
A uniquely blended skill-set designed expressly to support both corporate offices and field operations for Western Canadian energy producers

Aligned with your production goals
We plan and act to minimize downtime, control costs, and respond rapidly to critical field issues and emergencies.

Deep dual-domain expertise
Seasoned in enterprise servers, networks, and cybersecurity and in SCADA, PLC, and control-system environments - bridging the gaps between IT & OT.

Proven Field Experience
Delivering real-world and hands-on reliability across 300+ Western Canadian sites.

Safety you can Trust
Comprehensive HSE program, COR certification and full ComplyWorks & ISNetworld registration; every technician holds H2S, First Air, CSO, WHIMIS, and more.

Contact Us

 info@provisioninfotech.com

 provisioninfotech.com