case study



Bringing a Niagara Network Back to Life after a Period of Abandonment

Since shifting to a fully remote role in 2018, my engineering world has largely existed behind 3 LED monitors. I support, troubleshoot, and manage complex Tridium Niagara building automation systems across the country, entirely comfortable at my desk.

But a few months ago, I got a call that required me to dust off my physical tool bag, step away from the remote comfort zone, and catch a flight.

The mission? Walk onto a sprawling, decades-old institutional campus facing a massive ownership transition. The underlying nervous system of the facility: a large-scale Building Automation System (BAS) encompassing 21 JACE-8000 controllers and over 800 downstream BACnet MS/TP devices. It had completely gone dark.

CHALLENGE

The property had been sold in mid-2025, and by summer of that year, the departing corporate IT department executed standard de-provisioning protocols to reclaim their enterprise assets. When they pulled their managed network switches, the physical link layer for the facility's independent building automation platform was completely severed. The Niagara Supervisor itself, hosted in the previous owner's private cloud, became unreachable along with it.

The industry expectation for a recovery of this scale normally dictates a multi-week on-site discovery and deployment window. But scheduling constraints heavily compressed the deployment into the week of Memorial Day, leaving me a razor-thin, four-day window to either completely resurrect the infrastructure or fly home defeated. Working completely solo, with only the local O&M contractor helping me unlock the doors to the mechanical and electrical rooms, I wrapped it up in less than 72 hours.

Here is the engineering framework of how I did it, and why "old-school" IT discipline is the ultimate secret weapon for modern OT recovery.

1. The Principle of the "Known Good."

When you walk onto an undocumented institutional site alone, the sheer volume of variables will drown you if you let them. Is it a dead controller? A smashed fiber line? A bad IP routing table?

To defeat the chaos, you must establish a baseline of absolute certainty before your boots ever hit the mud.

"For nearly a year, 21 JACE controllers sat orphaned with no supervisor to report to and no path to recovery. Faced with a dark campus, the new ownership group was met with incredibly expensive, standard industry quotes to rebuild the network and front-end from scratch. But, the existing Niagara platform wasn't lost. It was waiting. I recovered it in less than 72 hours"

Rodrigo Garcia
Building Automation Architect

FAST FACTS

Customer: Commercial real estate investment and development firm

Project Type: OT Network Recovery

Project Scope:

- Rebuild central enterprise BAS gateway
- Reinstate Niagara Supervisor
- Bring JACE 8000 Controllers (21) back online, reporting to supervisor
- Verify communication with downstream BACnet MS/TP devices (approx .800)
- Map physical network including core fiber aggregation layer

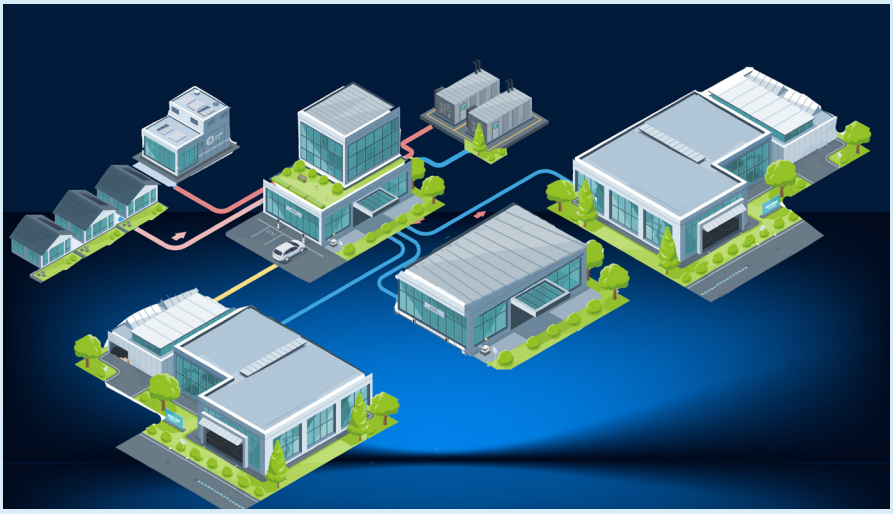
Key Technologies:

- Vykon Pro Tools

VYKON

Before flying out, I built a miniature replica of the entire campus network on a test bench in my office. I pre-configured and pre-labeled a centralized enterprise gateway, a core fiber aggregation layer, and a small army of localized edge switches, going as far as slapping physical "BAS - DO NOT UNPLUG!" labels onto every single AC power adapter.

Furthermore, I knew I was walking into a historical, multi-generational facility. Over decades, these sites accumulate physical remnants from original installations before they were ever absorbed into a corporate IT backbone: things like legacy Ethernet-to-fiber media converters, undocumented splices, and a wildcard mix of both legacy multi-mode and modern single-mode fiber cabling.



Stylistic rendering of a network infrastructure that runs around and through an institutional campus slated for rejuvenation and development.

Because I deployed a "Zero-Failure" prep strategy, I packed for every single physical layer contingency. I didn't just bring switches; I brought a massive arsenal of varied transceivers and specialized fiber patch cables: SC-to-LC, SC-to-ST, multi-mode, and single-mode.

When I arrived on-site and things inevitably went sideways on Day 1, I didn't have to wonder if my core hardware, transceivers, patch cables, or configurations were the problem. I knew they were flawless. That allowed me to treat the physical campus yard as an isolated variable.

Spending extra money on redundant single-strand BiDi transceivers, varied glass adapters, and clean patch cables before you cross the tarmac is infinitely cheaper than a return flight because you were short of a single link-layer variable.

2. Network Archaeology at Layer 1 & 2

The legacy network diagrams showed that the campus's original routing core (a corporate Cisco managed network) was anchored inside a centralized telecommunications hub out in the yard. But with that tenant infrastructure decommissioned and uninstalled, the underlying routing logic was gone. The original plan was to house the new security gateway and the core fiber aggregation switch together in the same location.

However, field reality required a fast pivot: the incoming ISP gateway landed at a separate perimeter service structure.

Finding the Fun in Reviving Fiber Network

To establish a clean baseline without sacrificing performance, I adjusted the architecture on the fly. I installed the security gateway directly in this perimeter structure at the ISP handoff. Because the gateway features native SFP+ ports, I used the existing campus fiber to link it directly to the core fiber aggregation switch in the central hub. This strategic realignment dropped the need for an intermediate fiber switch at this building. That let me optimize the campus fiber paths, remove an extra hardware hop, and hand over a fully pre-configured, plug-and-play edge switch to the client as a valuable cold spare.

From there, the physical network archaeology began. I was not just clicking buttons; I was dealing with the raw physics of old glass. I spent hours hunting down dusty, uncapped LC bulkheads, deploying fiber click-cleaners, shooting lasers with a Visual Fault Locator (VFL) to catch hidden light leaks, and measuring raw optical power metrics.

The physical infrastructure threw everything it had at me, including a critical long-haul backbone link holding onto a thread with a brutal -23dBm signal drop buried somewhere deep out in the campus yard.

The Buzzing Enemy at the Gate

And then there was the literal layer-1 physical security: an active, aggressive hornet's nest built right at a roof hatch entrance. Climbing up a vertical ladder only to find a swarm defending the roof access hatch is a quick reminder that fieldwork in Operational Technology (OT) requires a physical tool bag, safety gear, and a canister of wasp spray, not just a command-line interface.

By cleanly decoupling the physical constraints from my logical layout, I bypassed the dead runs, cleared the perimeter, and re-routed the core backbone trunk across verified glass paths. Even the localized desktop hookup felt like an excavation; the front-end workstation line was running over a legacy CAT-5e trunk. Someone had hidden an inline plastic barrel coupler inside a hallway ceiling panel just to stretch the path.

To keep things resilient and fast under a tight deadline, I made the conscious tactical decision to deploy a completely flat network subnet. When you are fighting the clock on a legacy campus solo, trying to force deep layer-3 VLAN segmentation onto unfamiliar, decades-old controllers is a trap. A flat layout allowed my enterprise gateway's DHCP tables to dynamically provision and rebuild the entire 20+ switch topology within minutes of the cutover.

My focus on getting the main front-end PC, the security gateway, and the core aggregation switch online on Day 1 payed off on Day 2. With these foundational elements established, a rolling cutover building to building, plugging in the edge switches one by one, could begin the next morning. The legacy network documentation had mapped the infrastructure as a massive, fragile 7-switch daisy chain in the survivor wing—a layout notoriously prone to single-point-of-failure collapses.

But as the hardware energized and checked in, the controller's centralized topology mapping engine revealed an entirely different reality on my phone's mobile app. The physical plant wasn't a fragile chain at all; it was a highly resilient, 3-branch star network. Standing out on the pavement on Day 2, watching that dynamic network visualization map itself out in real time as the downstream buildings woke up, populated, and flashed green right in the palm of my hand, was an unforgettable engineering payoff.

3. Waking the Tridium Ghosts

Once the network highways were open, I had to systematically awaken 21 JACE-8000s that had been isolated for months. In an OT environment, a network outage doesn't just mean "no Internet." It means localized controllers are blindly screaming data into a void until their internal routing tables lock up.

I faced standard transition hurdles right out of the gate: a previous contractor had reset all the platform credentials sometime before my arrival. I happened to notice it when provisioning backups failed for a large cluster of JACE-8000s. After the appropriate verified authorization and the required credential-recovery process, the access was securely restored..

From there, I needed a fast, comprehensive way to audit the health of the entire campus layout without manually clicking through 21 separate stations. I relied heavily on the VykonPro module as part of my toolkit. Using components of that module, I executed bulk database audits via RemoteBQLReport queries across the entire architecture simultaneously. Within minutes, I was able to map out the exact status of all 800+ downstream BACnet elements. The data revealed that most of my "offline" flags weren't network faults at all; they were specialized process exhaust systems that had been safely decoupled by decommissioning crews.

With the foundational telemetry clear, I leveraged the power of the Niagara Provisioning service to execute a massive, automated cleanup. Because these controllers had been isolated from an external clock source for nearly a year, their internal time clocks had drifted by more than an hour, a fatal issue for scheduling and trend histories. I executed a batch job to push proper NTP synchronization settings across all 21 units simultaneously, snapping the system time back to precision accuracy. Through the same provisioning engine, I sanitized the user directories on the fly: deleting legacy user accounts, adding the new ownership's profiles, and hardening the platform credentials.

To wrap up the station recovery, I ran a final round of automated provisioning backup jobs. This captured a pristine, post-remediation backup snapshot of every single JACE I touched, archiving a perfectly clean slate right at the device level.

I also navigated known platform software issues that had been found and fixed since Niagara 4.6. I applied available patches and updated all platform licenses to give the client a clean upgrade path to version 4.15. I also sniffed out undocumented "shadow IT" elements, like a rogue point-to-point industrial wireless bridge hidden on a pump room switch.

4. Leaving a True Clean Slate

A project isn't finished just because the graphics turn green on your laptop screen. True engineering is about how smoothly the next person inherits your work.

Before packing up, I optimized the user profiles down to native HTML5 views, tested secure encrypted remote access tunnels straight to the local O&M contractor's phone, and verified he could command setpoints and acknowledge alarms from anywhere.

I fell back on my old-school IT systems background to build an airtight recovery strategy. First, I created a custom, bootable bare-metal recovery ISO and left it on-site on a physical 16GB thumb drive inside the server cabinet for immediate emergency access.

Next, I pulled a full, block-level system backup using Veeam Agent. Because I successfully restored the historical database, preserving nearly 100 GB of continuous trend data right up until the moment the network went dark, the final archive was far too massive for standard thumb drives. That full image is being delivered securely via a cloud drive, alongside a comprehensive close-out report detailing every sanitized credential, verified MAC address, and physical port mapping. If that drive fails tomorrow, the incoming team won't just have a functioning system; they will have its entire operational history completely intact.

5. Engineering for the Demolition Clock

One last detail shaped every architectural decision on this project: this campus has a demolition clock running in the background. The new ownership group isn't preserving the full historical footprint indefinitely; portions of the property are slated for long-term redevelopment.

Knowing that, I deliberately engineered the network topology to die gracefully on a modular schedule. The core infrastructure for the active, occupied survivor wing is fully self-contained. When the bulldozers eventually reach the outlying buildings, the local operations team won't face a complex network redesign or an infrastructure collapse. They will simply unplug the decommissioned paths and keep right on running. Building for long-term reliability and building for a planned teardown aren't opposites. Done right, they are the exact same discipline.

The Takeaway: IT Roots in an OT World

Before I ever touched an HVAC controls loop or a Tridium station, I was an IT guy. We are talking the Windows NT 4.0 and Windows 2000 days, working as an international student managing instructional technology infrastructure for a community college campus.

Back then, you couldn't rely on cloud orchestration or automated setup wizards. If a loop crashed, you had to understand manual routing tables, broadcast boundaries, packet behavior, and physical link layer constraints.

That old-school IT discipline is exactly what allowed me to walk onto a blind, silent facility and bring it completely back to life in 72 hours. Modern smart buildings don't just live in the cloud; they are anchored to physical switch ports, legacy copper buses, and dust-covered mechanical rooms.

Sometimes, to move an infrastructure forward, you must look at it through the lens of how we used to build things to last.

ABOUT TRIDIUM

Tridium is a global leader in business application frameworks that facilitate open environments for automation and control. Founded in 1996, Tridium revolutionized the industry with the introduction of the Niagara Framework®, a universal software platform that integrates diverse systems and devices, regardless of manufacturer or communication protocol. Tridium's commitment to innovation and excellence has established it as a trusted partner for system integrators, OEMs, and end-users worldwide. With a robust global community and a network of certified professionals, Tridium continues to drive advancements in building automation, IoT integration, and smart infrastructure solution. Additional information about Tridium is available at www.tridium.com.

TRIDIUM
tridium.com

Americas: support@tridium.com
EMEA: ordersEMEA@tridium.com
Asia-Pacific: tsupportAP@tridium.com

© 2026-0014

This case study is provided for informational purposes only. Results may vary by customers.