UCS TECHNICAL FIELD GUIDE

Neeve Secure Edge Guide

Zero-trust identity and secure remote access for building OT networks

— Field-earned, not brochure-deep —

JULY 2026

Prepared for owners, facility teams, consulting engineers, IT/OT teams and project partners

NIAGARA SUPERVISION · OWNER ADVOCACY · SUPPORTABLE FIELD CONTROL

The UCS point of view

FIELD-EARNED, NOT BROCHURE-DEEP.

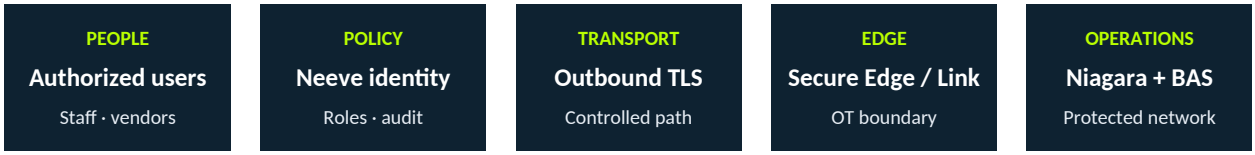
Our team has installed, programmed and serviced these systems in the field—including lines we do not represent—so we know the real strengths and trade-offs first-hand. That experience lets UCS act as an advocate for the owner, not a salesperson for a badge.

Building-automation networks increasingly carry the same risk profile as IT networks—without the same protections. Neeve puts identity, policy and audit around who and what may reach the operational-technology environment, replacing broad VPN exposure with a governed access path.

Neeve AI

Zero-trust identity, policy and secure-edge access around the operational-technology network.

Conceptual role in the architecture



Inline, behind or controlled-path placements create a stronger enforcement point than a device installed merely beside a controls network.

Value and boundaries

WHERE IT IS STRONG

- OT-focused zero-trust access model.
- Central identity, policy and audit context.
- Can reduce broad VPN exposure.
- Supports governed multi-site remote service.

DESIGN CONSIDERATIONS

- Requires early IT routing and identity coordination.
- Architecture must prevent bypass of the secure path.
- Outbound connectivity and recurring service are operating dependencies.
- Does not replace Niagara hardening, backups or network segmentation.

ROLE CLARITY

Neeve governs who and what may reach the OT environment. Niagara and Reflow still operate the building.

Manufacturer references: neeve.ai; docs.neeve.ai/docs/deployment-architecture; neeve.ai/product-selector

Deployment checklist

- Define identity, approval, routing, logging and break-glass access with the owner's IT team.
- Verify the architecture cannot be bypassed around the secure path.
- Test remote access from outside the owner network using the approved identity path.
- Document firewall rules, outbound connectivity dependencies and support contacts.
- Confirm renewal ownership for Neeve subscriptions and who administers user access over time.

Working with UCS on Neeve

- UCS deploys Neeve as the access boundary in its standard connected-building architecture.
- Niagara hardening, station backups and network segmentation remain in scope alongside Neeve—not replaced by it.
- UCS coordinates with owner IT/OT stakeholders from design through commissioning.

Manufacturer references

TOPIC	MANUFACTURER REFERENCE
Neeve platform	neeve.ai and neeve.ai/product-selector
Deployment architecture	docs.neeve.ai/docs/deployment-architecture
Tridium Niagara N4	tridium.com/us/en/products-services/niagara4

Disclaimer: This document is a conceptual planning aid, not a stamped controls design, cybersecurity plan or product-availability guarantee. Final architecture must be engineered for the specific project and approved by the owner and responsible design professionals.