Optergy

AXON CYBER SECURITY

V1.2

20 OCTOBER 2026

Table of Contents

01 **The Axon**
Summary
What the Axon is
Network position

02 **Secure Connectivity**
Connectivity requirements
How NovaQ Connect works

03 **Security architecture**
Hardware-rooted identity
Transport and identity
Access control enforcement
Revocation and audit
Firmware updates

04 **Data and assurance**
Data
Local operation and resilience
Certifications and assurance
Specifications and installation





Optergy

01 The Axon

What is the Axon?

An edge compute appliance running Optergy software in a comms or plant room. It runs no user workloads. It has no field inputs or outputs - its terminals are power and serial only, which constrains what the device can be made to do.

On nomenclature: the UL listing (E507611) describes the Axon as a Network Energy Management Controller. That is the classification under which the device is listed; it is the same device described throughout this document.

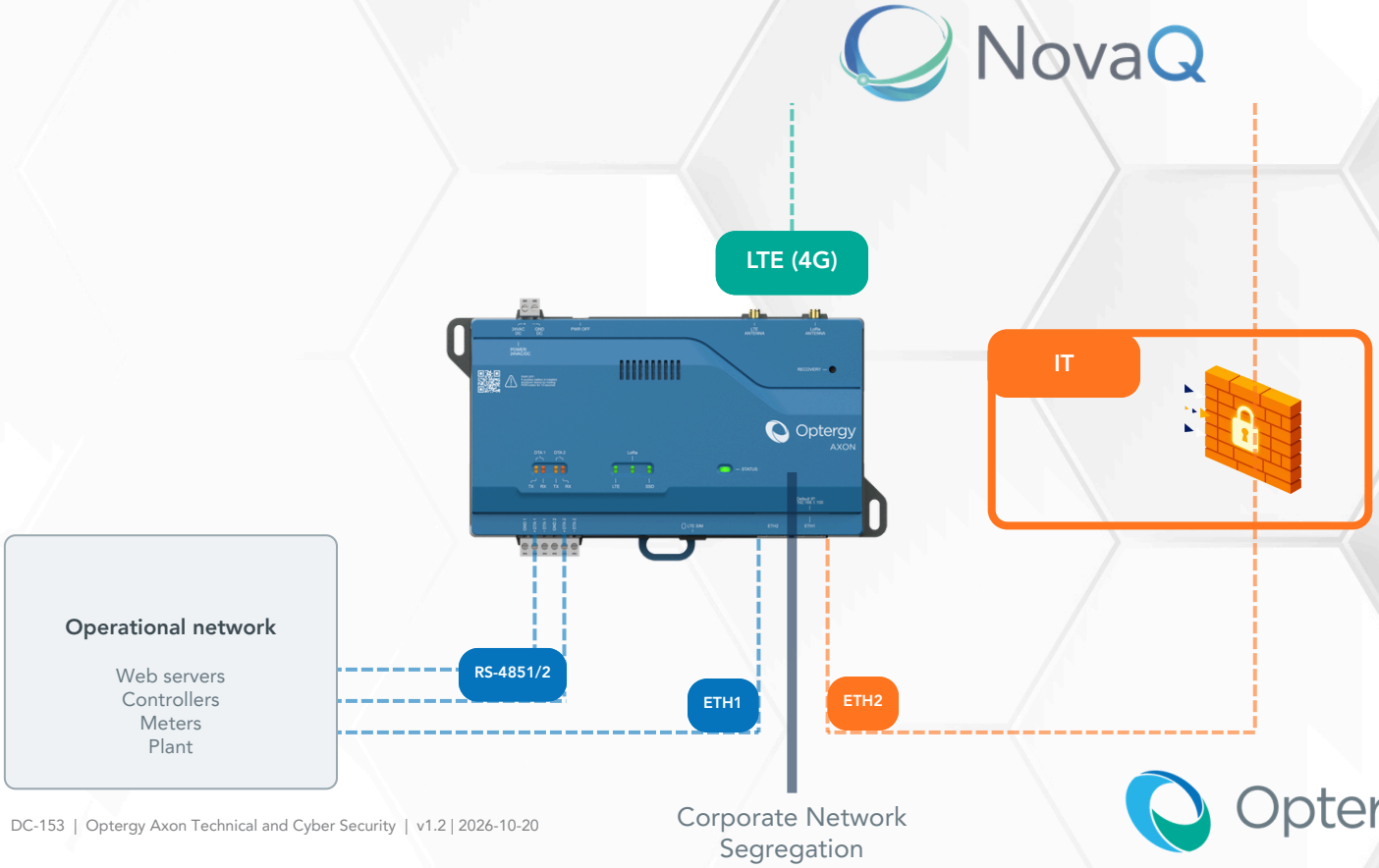
What does it do?

The Optergy Axon is an edge compute appliance whose purpose is to operate operational technology software securely on site, and to securely move that data as required to cloud platform service/s without exposing the site to the internet.

Four claims define its security posture.

It **does not** accept inbound connections except those authorised by NovaQ.
It **does** connect via outbound connections only.
It **does** root its core identity in a Trusted Platform Module (TPM) hardware chip.
It **does** continue to operate standalone when internet is lost so your building keeps operating because no control logic depends on internet connectivity.

Where does it sit in a network



Optergy

02 Secure Connectivity

Outbound Connectivity Requirements

Every connection below is initiated by the Axon, **outbound only**. No inbound firewall rule or port forwarding is required.

Port/s	Protocol	Destination and purpose	Requirement
443	TCP	Optergy cloud service — Site Connect and Remote Connect	Required
53	UDP and TCP	Site DNS resolver, or a public resolver — name resolution	Required
123	UDP	Site time source, or a public NTP server — time synchronisation	Required
49152–65535	UDP	Optergy NovaQ VPN service endpoints — Secure Connect, relay mode.	Required
1024–65535	UDP	Any destination — Secure Connect peer-to-peer optimisation	**Optional**
N/A	ICMP	Google Public DNS (8.8.8.8) - Latency and jitter diagnostics	**Optional**

Additional Ports, and Whose Decision They Are

The table above is what the appliance itself requires. Additional outbound access arises from configuration choices made by the system integrator who installed and manages the system, not from the device. Outbound mail for email notifications is the common example.

Where such a feature has been configured, the integrator is responsible for identifying it and raising it with the network team. Optergy states what the appliance requires; the integrator states what the configuration requires.

What the Axon Does Not Do

- Accepts no inbound connections from the internet or from the corporate network.
- Requires no inbound firewall rule, no port forwarding, no static IP address and no dynamic DNS.
- Exposes no listening service to the corporate network.
- Does not route traffic between the operational and corporate networks.
- Does not require internet connectivity for the building to keep operating — control and metering continue locally.

Optergy

02 Secure Connectivity

How NovaQ Connect works, and why that is secure?

The three access paths

Site Connect
Exposes the web interface of an on-premise device into an authenticated NovaQ browser session. No VPN, no client software, and no network-level access granted.

Remote Connect
SSH, RDP and VNC delivered through the same authenticated browser session.

Secure Connect
A WireGuard-based VPN, established peer-to-peer where possible and mediated through the NovaQ service where not.

All three paths run through one Zero Trust identity, one authentication and one audit trail. No connection to a site gets established without a verified user login whose confirmed there identify via multi-factor authentication before they press connect. There is no separate credential set, no shared account, and no path that bypasses the others.

Why the direction of connection matters

A device that only initiates outbound has no listening service — no port bound, no process waiting for a request, nothing that answers an unsolicited packet. A scan of the site's public address finds nothing belonging to the Axon, because there is nothing there to find. The session exists only because the Axon created it, and only for as long as the Axon maintains it.

This is why no inbound firewall rule, port forward, static IP or dynamic DNS is required. Those measures exist to let something outside reach something inside. Nothing outside needs to reach the Axon.

The comparison to your existing system

The arrangement this replaces is a onsite router port forwarding a public static IP to local devices, or a VPN service. Both work. Both also mean an OT network carries a permanent inbound door, reachable by anyone who finds it, open whether or not anyone is using it.



An outbound-initiated session is not a smaller version of that door. **There is no door.**

When no session is running there is no inbound path at all.
Peer to peer does not weaken this. It is still outbound-initiated and still accepts no inbound rule. What it asks for is a broader outbound egress permission, which is a network-policy question rather than an exposure question. A network that declines it loses no capability: Secure Connect falls back to the relayed path, and that fallback is what makes the no-port-forwarding claim hold without exception.

No inbound rule. No port forward. No static IP. No dynamic DNS. No exception.

Optergy

03 Security Architecture

Hardware-rooted identity and integrity

The claim in one sentence: a device that has been tampered with cannot attest, and a device that cannot attest cannot join the service. The mechanisms below are what make that true.

Device attestation on connection

The NovaQ service evaluates the device's attested state before admitting it. The behaviour is fail-closed: a device that cannot attest does not connect and each attempted connection is logged and audited.

Firmware signing

Firmware is signed and validated manufacturer, firmware is validated during startup and prior to each update being implemented.

Provenance

Designed, built and coded by Optergy in its own facilities in Australia and Malaysia. Country of origin for an individual unit appears on the unit label and on the shipping documentation.

Transport and identity

Mutual TLS between the Axon and the NovaQ service. Both ends present a certificate and each verifies the other, so neither is trusted on the strength of its network location alone.

Multi-factor authentication is required on all NovaQ logins.

Access control, and how it is enforced

Access policy is enforced at the moment data is retrieved, rather than by keeping data in separate places, and it is enforced in two independent layers.

Enforced at query time

Every request — browser session, REST API or machine interface — is evaluated against the caller's entitlements at the moment it is answered.

Row-level access control

Row-level access control within the tenancy database, enforced by the database itself as well as by the application. Defence in depth: the application filters, and the database refuses regardless. A query issued outside the application cannot return rows the caller is not entitled to.

Fail closed

An unresolved or ambiguous identity returns nothing, and is logged and audited.

Denials are logged

Denials are logged as well as accesses, so attempted boundary crossings are visible rather than merely prevented.

Tested adversarially, every release

A test suite attempts cross-boundary retrieval through every interface, including deliberately hostile queries. A failure blocks the release.

03 Security Architecture

Revocation and audit

A single administrative action blocks a user across every site.

- There is no per-site cleanup and nothing to remember: an engineer who leaves the business loses access to every building at once in NovaQ.
- Cloud webpages will stop serving the blocked user after the next page load, logging the user out of all sessions.
- Site/Host webpage streaming will stop serving the blocked user after the next page load, logging the user out of all sessions.
- Secure Connect tunnels are typically torn down within seconds however may take up to a maximum of 15 minutes to expire in some circumstances.

What is logged: system logs, and user navigation and action tracking.

Software and firmware updates

Updates are signed.

Patch currency is a shared responsibility between Optergy, the integrator and the customer.

Core AxonOS firmware and security updates occur automatically so long as the Axon is able to reach **fleet.optergy.com**, this may require manual patching by the integrator or customer from portal.optergy.com if the Axon is offline for a significant amount of time or if access to **fleet.optergy.com** is not provided.

Additional software and services running on the Axon outside of core updates will require patching from the integrator or customer either manually or via NovaQ (scheduled)

Optergy

04 Data and Assurance

Data

Common questions your team will have.

What leaves the site, and what stays on it

Device and system health information (uptime, Axon monitoring) is sent to NovaQ. Only point/trend data that is selected to display in NovaQ is sent to the cloud.

Where it is stored

Hosting is AWS, with separate regional instances. The AP instance is live on ap-southeast-2.

Encryption

Encrypted in transit and at rest.

Retention

Data is stored at different retention periods according to the data type and to your contract with Optergy.

- Audit records for user access and action tracking are retained for **1 year.**
- Time-series and trend data is retained **2 years**, unless contract ended or data retention extended via contract.

Local operation and resilience

Control and metering continue when the connection to the NovaQ service is lost. No control logic depends on internet connectivity, and only remote access is affected.

The Axon buffers data during an outage and forwards it on reconnection. Storage is managed first in, first out: as retained data approaches the capacity of the disk the oldest data is deleted to preserve function, and warnings are raised at both the device and the service before deletion begins.

The device's connectivity and control responsibilities take priority over any analytics or retrieval activity.

Optergy

04 Data and Assurance

Certifications, standards and independent assurance

Certifications

CE, FCC and UL standard across all products with specific regional certifications product dependent, see individual datasheets.

Organisational

ISO 27001 for information security
ISO 9001, ISO 14001 and ISO 45001 for organization management.

Independent testing

Penetration testing and security assessment by CyberCX.

HARDWARE SPECIFICATIONS

Model	Axon-V1
Processor	ARM Cortex-A76 2.4GHz + Cortex-A55 1.8GHz (8 Cores Total)
Ethernet	2 * Gigabit Ethernet Port supporting different IP subnets
Storage	512GB NVME SSD + 2nd optional NVME Slot
RAM	8GB LPDDR4x
Terminals	1x Power Terminal, 1x Serial Port Terminal
RS-485 Ports	2xRS-485 Ports (9.6K, 19.2K, 38.4K, 76.8K, 115.2K)
Power	2-Pin Terminal, 24VAC (1/2 wave) or 24VDC (Class 2) Max load: 40 VA with 24 VAC or 40 W with 24 VDC
Operating Temp	-4°F (-20°C) to +140°F (+60°C)
Storage Temp	-40°F (-40°C) to +185°F (+85°C)
Humidity	0 to 95% RH (non-condensing)
LTE (Optional)	1 * 4G LTE Cat 4 (Nano-Sim), LTE-FDD: B1/22 /3/4/5/7/8/28; LTE-TDD: B40; WCDMA: B1/2/4/5/8 ; GSM: B2/3/5/8
Lora (Optional)	Semtech Network's SX1302 LoRaWAN® Supporting NA/AU/AS (915MHz) or EU (868MHz)
RTC	Real Time Clock supported via Super Capacitor for up to 5 days
Battery Add-on	Supports optional 18650 Lithium-Ion Battery for Battery Backup
Country of Origin	Australia

HARDWARE DIMENSIONS

