

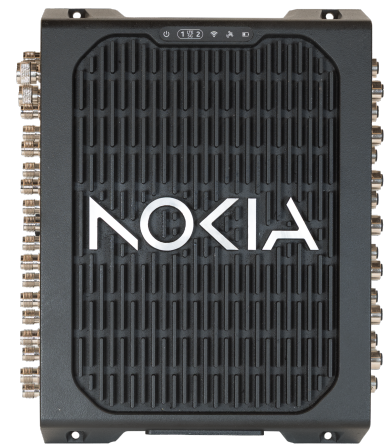
Cognitive Edge Node

Release 26

The Cognitive Edge Node (CEN) portfolio comprises rugged multi-access edge platforms for Nokia Cognitive Operations (NCO), bringing intelligence closer to mission-critical assets through on-site processing, resilient multi-radio connectivity and AI-driven action — keeping operations connected, aware and in control.

Overview

Designed by Nokia Bell Labs from the ground up for extreme environments, CEN is a family of platforms available in three configurations: Compact, Essential, and Extended. It scales from a connectivity focused edge node to a fully ruggedized, multi radio, AI accelerated edge system, supporting a wide range of deployment requirements. It combines 5G/LTE, Wi-Fi with mesh networking, satellite connectivity and LoRa with local edge computing, vehicle telemetry, routing, security, SLA-aware traffic steering, and multi-access bandwidth aggregation, turning mobile and remote assets into intelligent, connected systems. This enables application-aware connectivity, real-time visibility and autonomous decision-making in harsh environments.



Within Nokia Cognitive Operations (NCO), the CEN family serves as the field-deployed intelligence layer that connects assets, hosts local applications and enables autonomous action close to where operational decisions are made. NCO extends this edge foundation into a unified operational platform for mission-critical industries, helping operators maintain situational awareness, automate critical workflows and sustain operations when network conditions are degraded, disconnected or rapidly changing.

For more details on the Nokia Cognitive Operations (NCO) platform, refer to the [brochure](#).

Operational resilience and intelligence

Operational resilience starts with keeping mobile and remote assets connected, observable and responsive as field conditions change. CEN combines adaptive connectivity, end-to-end telemetry, SLA-aware assurance and local intelligence so operations teams can sustain critical workflows across remote, obstructed and rapidly changing environments.



Always-on connectivity for moving operations

CEN maintains operational continuity with up to three 5G/LTE modems, redundant RF channels and simultaneous public/private wireless connectivity. It adapts to changing field conditions by switching automatically based on signal quality, latency or congestion. Multi-technology link diversity across 5G, LTE, Wi-Fi, satellite and LoRa extends reliable reach across harsh or remote environments. Seamless Wi-Fi and cellular handover keeps mobile assets connected as they move between coverage zones, while intelligent Wi-Fi access point handover reduces application disruption. Non-terrestrial network (NTN) satellite communication and self-healing mesh networking across CEN nodes further strengthen resilience in remote or obstructed areas.

End-to-end visibility for faster decisions

CEN provides real-time telemetry across the full data path, from the asset and gateway through the RAN, core and transport network to the application and control center. This end-to-end visibility enables unified monitoring and faster diagnostics across the operational environment. Context-aware alerting correlates anomalies in asset behavior with network and application performance. With better visibility and faster troubleshooting, operational teams can make more informed decisions and respond more effectively.

AI-driven assurance for predictive operations

CEN supports application-level SLA management for critical workflows, including latency, jitter, throughput, availability and packet loss. On-device machine learning, anomaly detection and predictive analytics help anticipate failures or performance degradation before they affect operations. Built-in automated root-cause analysis accelerates incident response and helps prevent SLA violations. This shifts maintenance from reactive response to predictive action.

Edge intelligence that adapts as operations evolve

CEN operates autonomously on site, with no dependency on cloud connectivity. Its modular architecture supports Docker-based containerized applications, enabling custom logic and third-party applications to be deployed at the edge. On Extended configurations, GPU acceleration supports demanding workloads such as AI inference and real-time video compression, enabling applications such as fatigue and collision detection. An internal battery option maintains operation during power loss, and the platform restarts in 30 to 45 seconds. A software-defined design with remote update capabilities enables the platform to adapt as operational needs evolve.

Defense-in-depth security

For mission-critical operations, resilience and security must work together across the device, network, application and operational layers. CEN implements a defense-in-depth cybersecurity architecture spanning hardware, operating system, networking, applications and operations. This layered approach helps protect the platform, the data it carries and the services it supports across private, public and hybrid wireless environments.

Platform and device protection

CEN strengthens platform integrity with a hardened operating system, service minimization, secure boot, read-only system partitions, file system integrity controls and package signing verification. Non-root application execution and application sandboxing isolate applications and reduce the



attack surface. ECC-protected memory, hardware watchdog protection and device identity management add resilience at the hardware and device level.

Tamper detection and logging, secure recovery procedures, GNSS position logging during security events and secure firmware upgrades help protect the device through its full operational lifecycle.

Data and credential protection

CEN protects sensitive information through encrypted communications, encrypted configuration storage, encrypted credentials storage and secure key storage. Role-based access control ensures that users and administrators have the appropriate level of access. Audit logging and secure remote administration provide the visibility and control needed to manage security events and operational changes. Together, these capabilities help safeguard data, credentials and management access across the deployment.

Network protection and secure connectivity

CEN provides a built-in stateful, zone-based firewall to protect traffic across operational domains. Secure networking capabilities include IPsec, WireGuard, MPLS VPN, VXLAN overlays, VRF isolation, multi-APN segmentation, WAN bonding security and SLA-aware traffic steering. These capabilities help isolate traffic, secure overlays and support dynamic path selection across available access technologies. As a result, CEN enables resilient and secure operations across 5G/LTE, Wi-Fi, satellite and private network infrastructures.

Technical specifications

The Cognitive Edge Node portfolio includes multiple configurations designed to address different deployment environments, connectivity densities and edge compute requirements: Compact, Essential and Extended.

Table 1: Cognitive Edge Node platform specifications

Specification	Compact	Essential	Extended
Fixed interfaces	• 4 × RJ-45 1000 Mb/s, two SFP 1000 Mb/s (optional) • optional CAN bus connector • optional 2 × DI, 2 × DO interfaces	• 6 × M12 X-coded 1000 Mb/s • optional CAN bus connector over M12 X-coded connector • optional 2 × DI, 2 × DO interfaces over M12 X-coded connector	• 8 × M12 X-coded 1000 Mb/s • optional 4 additional M12 X-coded ports with 100 W shared PoE • optional CAN bus connector over M12 X-coded connector • optional 2 × DI, 2 × DO interfaces over M12 X-coded connector
Cellular interface	• See Table 2 • Up to 3 modems (2x 4FF nano SIM per modem + eSIM)	• See Table 2 • Up to 3 modems (2x 4FF nano SIM + eSIM)	• See Table 2 • Up to 4 modems (2x 4FF nano SIM + eSIM)
Wi-Fi interface	• See Table 3 • 1 Wi-Fi module • 1 additional optional Wi-Fi module	• See Table 3 • 1 Wi-Fi module • 1 additional optional Wi-Fi module	• See Table 3 • 1 Wi-Fi module • 2 additional optional Wi-Fi modules
Non-Terrestrial Networks (NTN)	• See Table 4 • Optional LTE Cat M1 and NB-IoT (3GPP Rel-14) with support for NTN Rel-17 with 1 dedicated 4FF nano SIM	• See Table 4 • Optional LTE Cat M1 and NB-IoT (3GPP Rel-14) with support for NTN Rel-17 with 1 dedicated 4FF nano SIM	• See Table 4 • Optional LTE Cat M1 and NB-IoT (3GPP Rel-14) with support for NTN Rel-17 with 1 dedicated 4FF nano SIM



Specification	Compact	Essential	Extended
GNSS port	GPS, Galileo, QZSS, GLONASS, BeiDou and SBAS. RTK L1, L2, L5 frequency module optional		
Central processing unit (CPU)	Quad-core, 64-bit Arm Cortex-A53 1.6 GHz	Quad-core, 64-bit Arm Cortex-A53 1.6 GHz	Quad-core, 64-bit Arm Cortex-A72 1.8 GHz
Graphics processing unit (GPU)	-	-	NVIDIA Jetson Orin NX 16 GB ¹
Tensor processing unit (TPU)	Optional 30 TOPS TPU module via mPCIe expansion	Optional 30 TOPS TPU module via mPCIe expansion	Optional 30 TOPS TPU module via mPCIe expansion
Indicators	Power, Wi-Fi, LTE/5G, NTN	Power, Wi-Fi, LTE/5G, NTN	Power, Wi-Fi, LTE/5G, NTN
RAM memory	4 GB with ECC	4 GB with ECC	4 GB with ECC (8 GB optional)
Local storage	64 GB eMMC with external SD card up to 1 TB		
IP rating	IP67		
Power	+12 V to +36 V DC	+12 V to +36 V DC	+12 V to +36 V DC Built-in battery option ²
Power consumption	Typical 15 W	Typical 15 W	Typical 25 W (max. 100 W with PoE module)
Cooling	Fanless, passively cooled		
Physical dimensions	Height: 48.8 mm (1.92 in) Width: 150 mm (5.9 in) Depth: 200 mm (7.87 in) Weight: 2.1 kg (4.63 lb)	Height: 68.8 mm (2.7 in) Width: 150 mm (5.9 in) Depth: 200 mm (7.87 in) Weight: 2.3 kg (5.07 lb)	Height: 78.8 mm (3.1 in) Width: 179.7 mm (7.07 in) Depth: 234 mm (9.21 in) Weight: 4 kg (8.81 lb)
Operating temperature range	-40 °C to +75 °C (-40 °F to +167 °F)		

Table 2. Cognitive Edge Node cellular radio specifications

Feature	All configurations
Market	Latin America, North America, EMEA and APAC
5G FR1 bands	n1, n2, n3, n5, n7, n8, n12, n13, n14, n18, n20, n25, n26, n28, n29, n30, n38, n40, n41, n48, n66, n71, n75, n76, n77, n78, n79
5G FR1 bandwidth	120 MHz, 2CC CA DL
LTE bands – 4G fallback	B1, B2(B25), B3, B4(B66), B26(B5, B18, B19), B7, B8, B12(B17), B13, B14, B20, B28, B29(DL), B30, B32(DL), B34, B38, B39, B40, B41, B42, B43, B46(LAA), B48(CBRS), B66, B71
WCDMA bands – 3G fallback	B1, B2, B4, B5(B6, B19), B8
Modem approvals	Anatel, FCC, IC, RED, NCC, JATE/TELEC, KC, CCC, RCM, GCF, PTCRB, AT&T, FirstNet, KDDI, KT, Telstra, T-Mobile US, VzW, various MNOs

¹ Optional, to be supported in future releases

² To be supported in future releases

Table 3. Cognitive Edge Node Wi-Fi interface options

Feature	Standard	Option 1: High-power 2.4 GHz Wi-Fi 6	Option 2: High-power 5 GHz Wi-Fi 6	Option 3: Dual-band Wi-Fi 6, single- concurrent	Option 4: Dual-band Wi-Fi 7, dual- concurrent
WLAN	802.11a/b/g/n/ac/ax (2.4 GHz and 5 GHz) 20 MHz, 40 MHz, 80 MHz	802.11ax (2.4 GHz only)	802.11a/n/ac/ax (5 GHz only)	802.11a/b/g/n/ac/ax (2.4 GHz and 5 GHz)	802.11b/g/n/ac/be ³ (2.4 GHz) 20, 40 MHz 802.11a/n/ac/ax/be ³ (5 GHz) 20 MHz, 40 MHz, 80 MHz, 160 MHz, 240 MHz
Spatial streams	2×2 MIMO	2×2 MIMO	4×4 MIMO	4×4 MIMO	2×2 MIMO
Host interface	PCIe 1.1	Mini-PCIe PCIe 3.0	Mini-PCIe PCIe 3.0	Mini-PCIe PCIe 3.0	Mini-PCIe PCIe 3.0
Bluetooth	SIG v5.2 Compliant	Not integrated	Not integrated	Not integrated	Not integrated
Modes	STA, AP	STA only	STA only	STA, AP	STA, AP
Wi-Fi transmit power	19 dBm @2.4 GHz 8 dBm @5 GHz	30 dBm @2.4 GHz	30 dBm @5 GHz	20 dBm per chain	Up to 20 dBm @2.4 GHz Up to 18 dBm @5 GHz (per chain)
Security	WPA/WPA2 (personal) WPA3 (personal/ enterprise)	WPA2/3, AES	WPA/WPA2- Personal/WPA2- Enterprise and WPA3 Personal	WPA/WPA2/3, Enterprise-grade	WPA/WPA2/3, Enterprise-grade

Table 4. Cognitive Edge Node NTN radio specification

Feature	All configurations
Market	Latin America, North America, EMEA and APAC
5G FR1 bands	n1, n2, n3, n5, n7, n8, n12, n13, n14, n18, n20, n25, n26, n28, n29, n30, n38, n40, n41, n48, n66, n71, n75, n76, n77, n78, n79
5G FR1 bandwidth	120 MHz, 2CC CA DL
Bands	LTE: B5, B8, B12, B13, B17, B18, B19, B20, B26, B28 NTN: B23/255/256
Baud rate	115.2 kb/s
Modem approvals	FCC/IC, ETSI, TELEC, PTCRB, GCF

³ 802.11be (Wi-Fi 7) to be supported in future releases

Software features

The Nokia Cognitive Edge Node portfolio supports a broad set of networking, routing, security and service capabilities, including the following.

L1/L2 networking

- 802.1Q VLANs
- Q-in-Q encapsulation
- Layer 2 Tunneling Protocol (L2TP)
- Wireless mesh networking

IPv4 and IPv6 routing protocols

- IPv4 and IPv6 forwarding
- Policy and interface-based routing
- Source routing for multi-APNs
- Static IPv4 and IPv6 routes
- Open Shortest Path First (OSPF) v2, v3
- Intermediate System to Intermediate System (IS-IS)
- Border Gateway Protocol v4 (BGP4) and Multiprotocol BGP (MP-BGP)
- Routing Information Protocol version 2 (RIPv2) and Routing Information Protocol next generation (RIPng)
- Babel routing protocol (babeld)
- Point-to-Point Protocol over Ethernet (PPPoE)
- Equal-cost multipath (ECMP)
- Segment Routing over MPLS (SR-MPLS)
 - SR-IS-IS and SR-OSPF
 - Traffic engineering (SR-TE) for IPv4 and IPv6
- Segment Routing over IPv6 (SRv6)
 - SRv6 IS-IS shortest path tunnel support in MT=0 and MT=2
- MPLS label edge router (LER) and label switching router (LSR) functions
 - Label Distribution Protocol (LDP)
 - Resource Reservation Protocol with traffic engineering (RSVP-TE)

OAM and security

- Bidirectional Forwarding Detection (BFD)
- Secure Network Time Protocol (NTP)
- Network address translation (NAT)
- IPsec for GRE and VXLAN tunnels
- OpenVPN and Wireguard VPN
- User profile management, strict login controls and scope of command/control
- Remote Authentication Dial-In User Service (RADIUS) client
- Secure Shell v2 (SSHv2)
- OAuth2 / OpenID Connect
- HTTPS management interface with TLS 1.2 / TLS 1.3
- Message Queuing Telemetry Transport (MQTT) over TLS
- Public Key Infrastructure (PKI) supporting X.509 certificates
- Stateful firewall and zone-based firewall policies
- IPv4 and IPv6 filters using access control lists (ACLs)
- Port-based and protocol-based filtering and policing

Layer 2 and Layer 3 services

- Virtual Private Wire Service (VPWS) and Virtual Private LAN Service (VPLS):
 - Signaled by BGP
 - Signaled by T-LDP using MPLS, GRE, or L2TPv3 transport
 - Static LDP for VPWS
- Protocol-Independent Multicast (PIM)
- Ethernet VPN (EVPN)
- Layer 3 Virtual Private Routed Network (VPRN) and VRF-Lite
- IP-in-IP and GRE IP tunnelling
- Simple Internet Transition (SIT)
- Virtual Extensible LAN (VXLAN) overlay
- WireGuard and WireGuard routed services for VXLAN tunnels and VRF
- Internet Group Management Protocol (IGMP) proxy
- Multicast Listener Discovery (MLD) proxy
- BGP Prefix Independent Convergence (PIC)



Standards compliance⁴

Environmental specifications

MIL-STD-1275 Rev. E for 28V systems

Electromagnetic compatibility

ETSI TS 102 514

Radiated emissions CISPR 32 Class A

Directives, regional approvals and certifications

ANATEL Ato Nº 3152/2020

3GPP TS 36.521-1 V17.6.1 (2023-07)

3GPP TS 38.521-1 V17.7.0 (2023-02)

3GPP TS 38.521-3 V17.7.0 (2023-02)

3GPP TS 36.523-1

ANATEL Ato Nº 7971/2023

ANATEL Ato Nº 14448/2017

ANATEL Ato Nº 1120/2018, Resolution No. 772 and Resolution No. 773

ANATEL Ato Nº 16539/2023

ANATEL Ato Nº 915/2024

ENACOM Resolution No. 1064/2025

ENACOM Resolution No. 57/2026

About Nokia

Nokia is a global leader in connectivity for the AI era. With expertise across fixed, mobile, and transport networks, we're advancing connectivity to secure a brighter world.

Nokia operates a policy of ongoing development and has made all reasonable efforts to ensure that the content of this document is adequate and free of material errors and omissions. Nokia assumes no responsibility for any inaccuracies in this document and reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

© 2026 Nokia

Nokia OYJ

Karakaari 7

02610 Espoo

Finland

Tel. +358 (0) 10 44 88 000

Document code: (September) CID215508

⁴ System design intent is according to the listed standards.
Refer to product documentation for detailed compliance status.