aliv business

CYBER SECURITY SUMMIT 2026

CYBER RESILIENCE
DEFENDING THE DIGITAL FRONTIER
EMPOWER, PROTECT, EVOLVE

Defending the systems that keep the world running

Securing Critical Infrastructure

Rodrigo A. Ricaurte
Cybersecurity Manager – Nokia Cloud & Network Services LAT

The systems that keep the world running

Energy & Natural Resources

- Utilities
- CSPs
- Natural Resource/ Pipeline Operators
- Mining

Transportation & Logistics

- Main Rail & Freight Rail
- Mass Transit
- Aviation
- Logistics
- Roads

Public Sector

- Defense
- Education
- Public Safety
- Smart Government
- Smart Territories

Large Enterprises

- BFSI
- Healthcare
- Manufacturing
- Real Estate & Construction
- Others

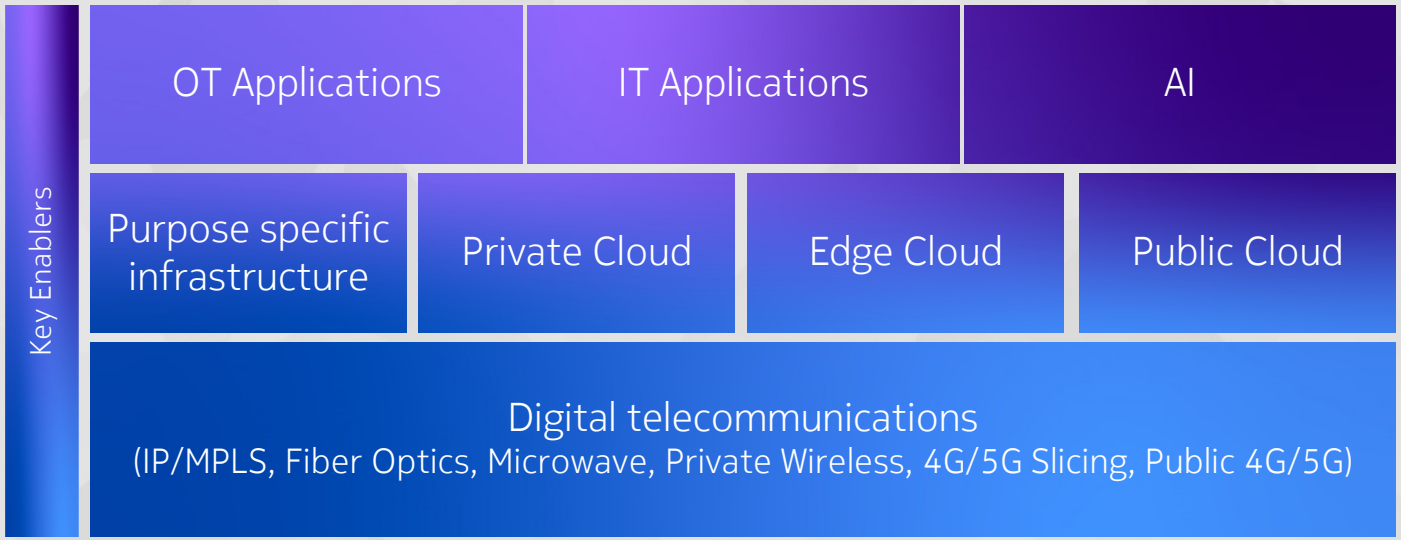
Safety Critical	Society Critical	Business Critical

Critical infrastructures are **essential systems requiring absolute reliability, resilience and security** to ensure uninterrupted services, enable intelligent automation and preserve safety of people and infrastructure

Invisible systems behind modern critical infrastructure

Downtime is no longer mechanical, it’s digital.

The resilience of critical infrastructure now depends on the resilience of its digital enablers; the failure of a single system can cascade across sectors with potentially catastrophic consequences



Threat landscape: critical infrastructures are under siege

> "Critical infrastructure whether in the hands of state, local, private, or supply chain partners; is the backbone of our daily lives, and its defense must be a shared priority to protect citizens and essential services"
>
> Madhu Gottumukkala, Acting Director of the U.S. Cybersecurity and Infrastructure Security Agency (CISA), 2025

What makes critical infrastructure security different?

In IT, security is about data.

In critical infrastructure, security is about keeping critical services running

	IT security	Critical Infrastructure security
What's top of mind	Critical data protection	Operational continuity, safety, service availability. 99.999% uptime
Network scope	Enterprise IT networks, cloud, endpoints	Highly distributed IT + OT + industrial control systems + telecom environments
Infrastructure and protocols	Standard IT systems (TCP/IP, HTTP, SaaS, APIs)	Legacy systems, ICS/SCADA, industrial protocols, real-time systems
Skillsets	IT security analysts, SOC teams, cloud security	IT + OT engineers, control system specialists, safety experts
Tools and technology	Homogenous security tools like IT SIEM, IAM, EDR, and laptop antivirus	PAM, Non-intrusive monitoring, OT-aware detection, segmentation, safety-aligned controls
Insider threats	Credential misuse, privilege escalation	Operational access abuse, vendor misuse, safety override risks
Regulatory landscape	Governed by standards like HIPAA, PCI, and GDPR	Sector-specific mandates (energy, telecom, water), national resilience regulations
Economic impact	Financial loss, lawsuits, brand damage	Service disruption, public safety risk, cascading national impact

Five strategic pillars for critical infrastructure protection

Industry-Aligned security architecture

Controls should be tailored to sector-specific risks; energy grids, telecom cores, manufacturing systems, healthcare networks, supported by advanced cybersecurity consulting expertise.

Controlled and transparent access

Human and machine identities must be authenticated, authorized, and properly governed, with access tightly controlled, continuously monitored, and lifecycle-managed.

Deep visibility without disrupting operations

Deep visibility without disrupting operations through transparent, purpose-built monitoring that avoids interference with industrial and mission-critical environments.

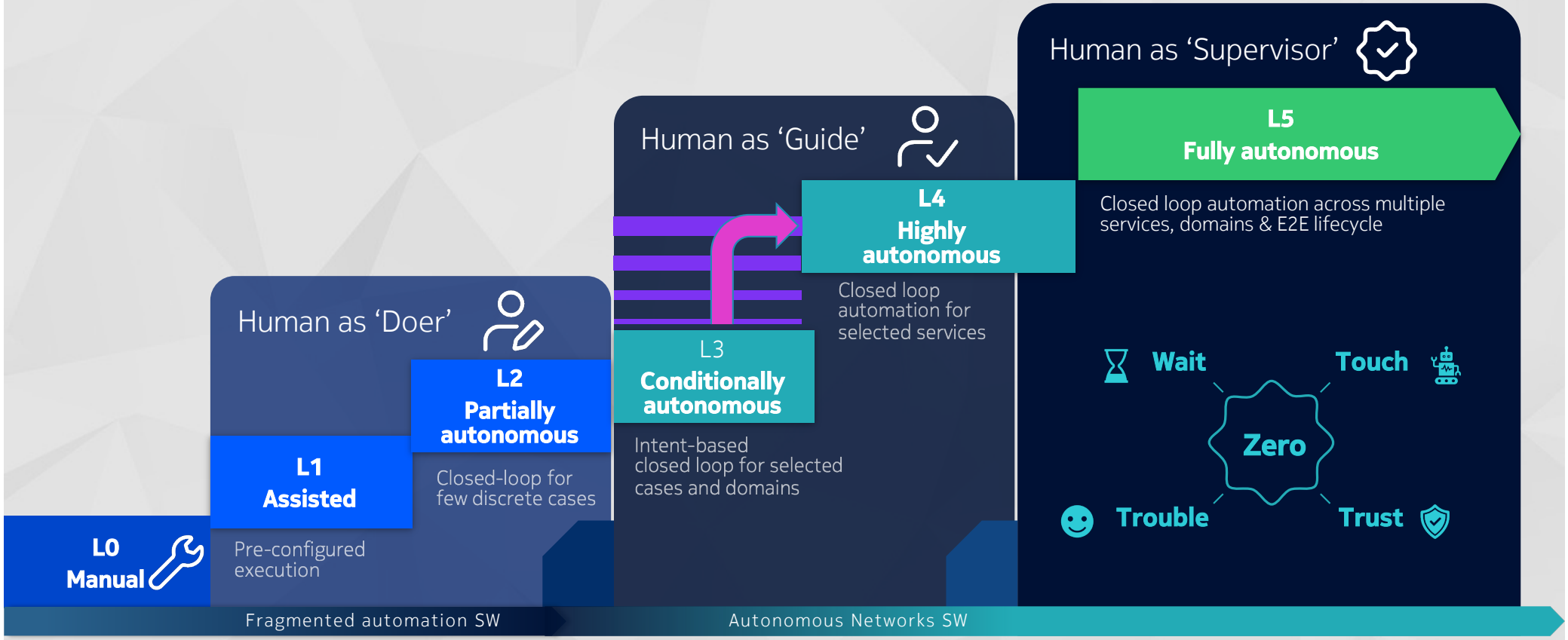
Secure and trusted communications

Secure every layer. Robust encryption across core networks, signaling, cloud workloads, and OT environments, combined with strong key management to ensure integrity.

Coordinated and automated response

Detect, contain, and recover before disruption escalates. Integrated detection and response across OT infrastructure ensures operational continuity and minimizes impact.

Redefining security for autonomous operations



Nokia's layered approach to critical infrastructure cybersecurity

NOKIA

Design and standards

Standards-based security architecture

- ✓ 3GPP security framework (authentication, encryption)
- ✓ Standardization guidelines (Security baselines, compliance)
- ✓ Zero-Trust principles (identity-based access, segmentation)
- ✓ API security standards

Build and deploy

Secure development and deployment

- ✓ Threat and risk analysis per network element
- ✓ Network security architecture
- ✓ Secure coding, security testing, hardening and patching
- ✓ Supply chain security (SBOM, firmware integrity, image assurance)
- ✓ Vulnerability monitoring and remediation

Operate and assure

Operational security and continuous assurance

- ✓ Access control (IAM, PAM)
- ✓ Runtime protection (EDR, NDR, network function integrity)
- ✓ Monitoring and incident response (SIEM, SOAR, XDR, anomaly detection)
- ✓ Certificate management (issuance, renewal, revocation)
- ✓ Compliance and auditing (regulation mandates)
- ✓ Resilience and recovery (backup, failover strategies)

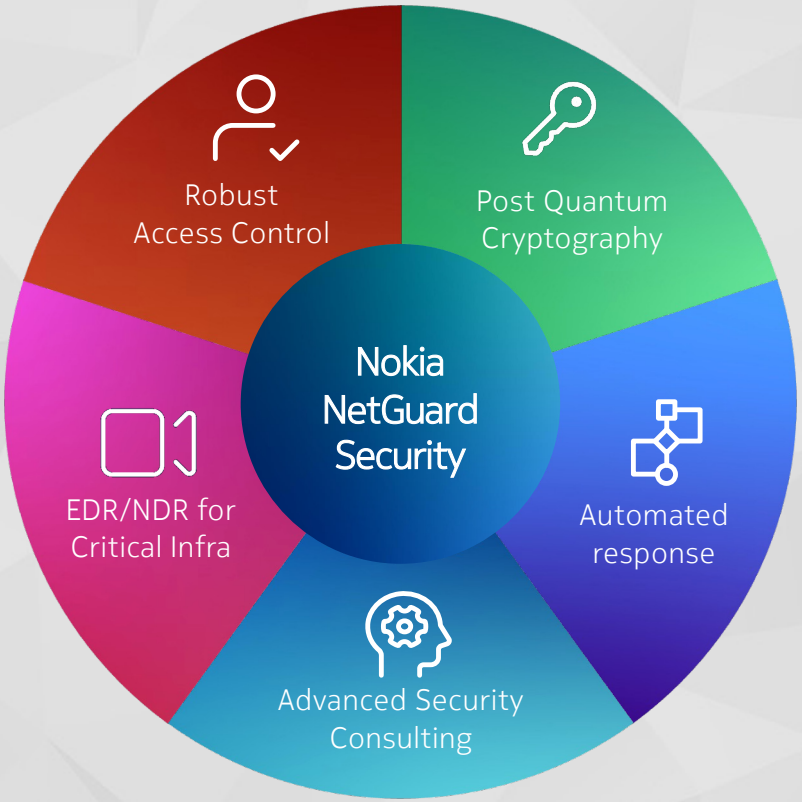
Regulations

Nokia's security for critical infrastructure

Granular access controls, strong authentication, privileged access management, and monitoring to protect critical infrastructure

Comprehensive non-intrusive endpoint and network detection and response solution deployed throughout critical infrastructure

Study case:
Securing a Utility's Networks



Implementation of post-quantum cryptographic standards to protect critical networks against emerging quantum computing threats

Integrated detection and automated containment in critical infrastructure reducing mitigation times and preventing disruption

Comprehensive risk assessments, security architecture reviews, and governance frameworks tailored to critical infrastructure resilience.


aliv business
CYBER SECURITY SUMMIT 2026
CYBER RESILIENCE
DEFENDING THE DIGITAL FRONTIER
EMPOWER, PROTECT, EVOLVE