



Nokia Network Services Platform for rail and transportation

Enhanced network visibility, security
and automation for mission-critical
communications networks



Unified network operations for the digital transportation era

Mission-critical communications networks are becoming the digital nervous system for safe and efficient transportation. Train control, signaling, operational voice, CCTV, passenger information, SCADA, ticketing, power monitoring, IoT sensors and emerging FRMCS/5G services all depend on reliable, secure and predictable network connectivity.

As rail, metro, and transport authorities modernize from purpose-built legacy networks to converged IP/MPLS, optical, 4G/5G radio, and cloud-based data center architectures, they gain greater flexibility, scalability, and operational efficiency while reducing infrastructure duplication. However, they also face growing challenges in network visibility, service assurance, automation, cybersecurity, timing, and multivendor integration.

Nokia Network Services Platform (NSP) helps rail, metro and transport authorities modernize operations by enabling unified visibility, automation and control across their mission-critical communications networks. It connects control centers, backbone networks, stations, depots, trackside assets, radio systems and data centers to create a consistent view that helps operators improve situational awareness, respond faster and reduce risk.

How rail and transportation operators benefit from NSP:

- **Protect operational continuity:** Correlated alarms, dashboards and service impact views help teams understand how network degradation may affect train movements, signaling, station systems, passenger communications and control center visibility.
- **Simplify migration and reduce change-window risk:** Intent-based provisioning, validation workflows and automation help operators move from legacy technologies to IP/MPLS, Segment Routing, optical transport and FRMCS while keeping critical services running during reduced maintenance windows.
- **Unify visibility across distributed intelligence and multilayer domains:** Topology, service path and multi-domain assurance views help operations teams plan networks and correlate issues across stations, depots, trackside sites, access networks, WAN, optical and data center domains.
- **Strengthen cybersecurity without compromising availability:** Role-based access, activity logging, secure integration and lifecycle controls help protect distributed assets, access points and operational workflows. They contribute to a zero-trust approach while supporting continuous service availability.



The importance of network management and automation

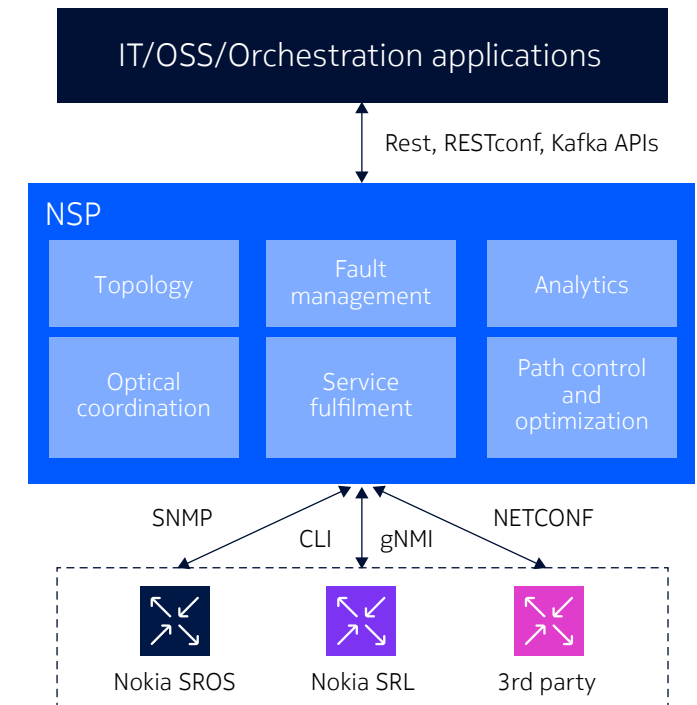
Rail, metro and transportation authorities can't efficiently manage modern communications networks with disconnected tools, manual command-line processes and reactive troubleshooting. They need a consistent operational model that connects service fulfillment, assurance, analytics, optimization and security. Nokia NSP supports this model by simplifying provisioning, control, monitoring, troubleshooting, reporting and optimization across their mission-critical communications infrastructure.

NSP abstracts network complexity across IP/MPLS, Segment Routing, trackside Ethernet and optical domains. It supports open interfaces such as REST, RESTCONF and model-driven integration approaches, helping operations teams connect the network management layer with OSS, orchestration and operational workflows. This enables them to move from device-by-device administration to intent-driven operations where services can be defined, deployed, validated, and assured through repeatable workflows. The result is greater operational efficiency, improved audit readiness, and simplified tracking of network changes to support regulatory reporting and compliance obligations.

How NSP simplifies network management:

- **Fewer tools and simpler operations:** A common platform reduces operational fragmentation across network domains.
- **Faster service rollout:** Intent-based templates and workflow automation accelerate provisioning while improving consistency.
- **Lower operational risk:** Real-time auditing and configuration validation help identify drift between intended and deployed configurations.
- **Better use of network assets:** Analytics and path optimization help operations teams understand capacity, traffic behavior and service dependencies.
- **Improved service performance control:** OAM testing, telemetry and KPI-based assurance help verify that critical applications receive the required levels of network performance.

NSP provides one platform and a single pane of glass for the entire network



Accelerate provisioning with service automation

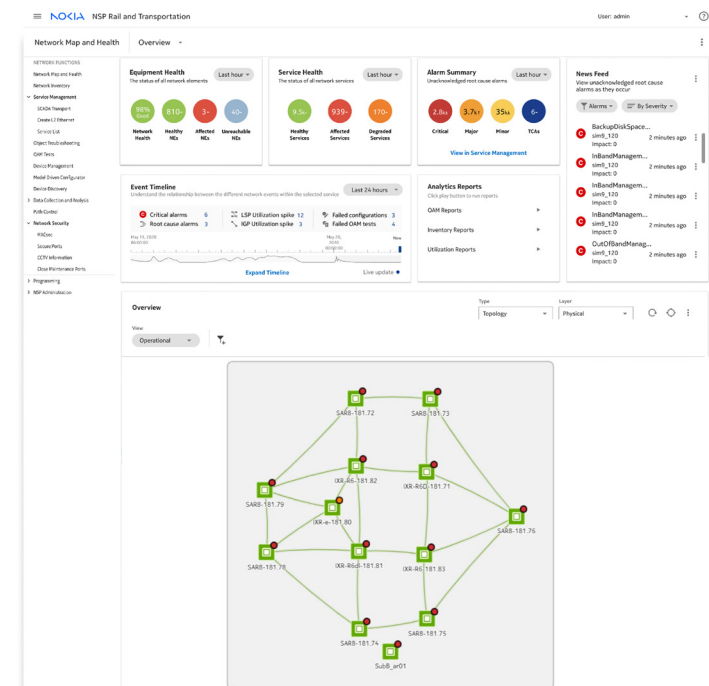
Agility is essential for transport authorities that must introduce new services, extend networks to new stations and depots, modernize trackside communications and adapt to evolving signaling and train-to-ground requirements. Manual configuration processes are slow, difficult to scale and vulnerable to error, especially when multiple vendors, technologies and operational teams are involved.

NSP helps automate the full lifecycle of network services, from onboarding and configuration to validation, maintenance, upgrades and backup. Intent-based physical and logical configuration, supported by reusable templates and software artifacts, simplifies service delivery and improves consistency. Workflow automation can perform zero-touch provisioning, pre- and post-maintenance checks, software upgrades, performance validation and device configuration backups for rollback scenarios.

How NSP simplifies service lifecycle management:

- **Intent-based service provisioning:** Translates service intent into device-specific configurations while maintaining consistency across network domains and reducing human errors.
- **Real-time configuration auditing:** Detects mismatches between the intended design and the live network before they become operational issues.
- **Workflow-driven operations:** Automates repeatable tasks such as onboarding, change validation, backups, compliance checks and maintenance procedures.
- **Automated policy consistency:** Ensures security policies and QoS rules are deployed consistently across the network while simplifying change tracking, validation and compliance management.
- **Brownfield and greenfield support:** Simplifies deployment in existing networks while providing a scalable operational model for future expansion.

NSP provides tailored dashboards and operations menu for utilities



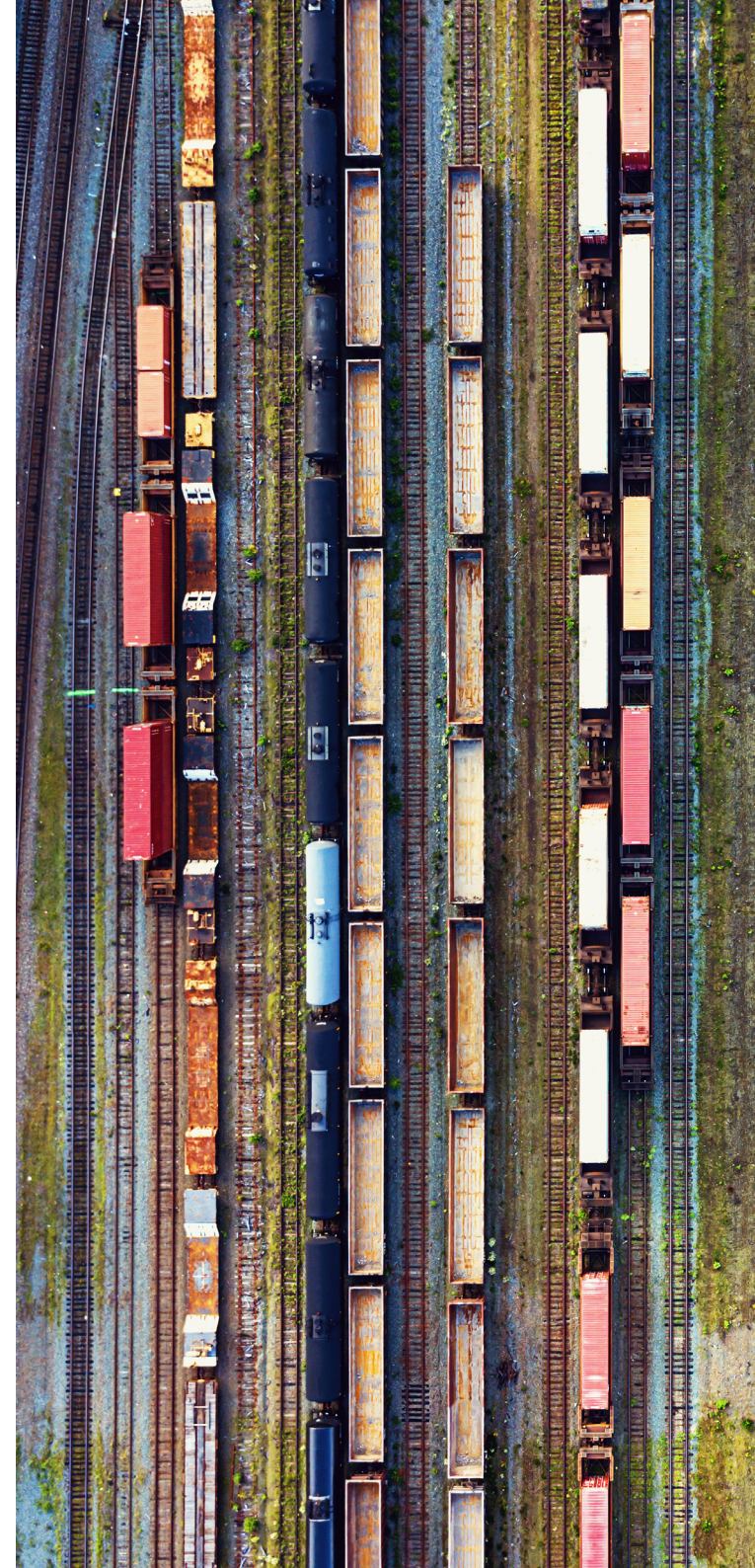
Enabling proactive service assurance for mission-critical applications

Rail and transportation applications require predictable performance and high availability. Signaling, train control, operational voice, SCADA, CCTV, passenger information and station systems can be sensitive to latency, jitter, packet loss, congestion and routing instability. As these services move onto converged IP/MPLS and Ethernet access infrastructure, operations teams need proactive, cross-domain assurance that links network conditions to service impact.

NSP provides operations, administration and maintenance (OAM) test capabilities that monitor latency, jitter and packet loss across critical services. KPI-based alarms and threshold-crossing alerts can identify degradation before applications are affected. For multicast-heavy services such as CCTV and video distribution, NSP can monitor traffic health and detect abnormal behavior that could lead to resource depletion or negative service impacts. When a fault occurs, correlated alarm views, physical and logical topology maps and service path visualization help operations teams isolate the root cause faster.

How NSP automation streamlines service assurance:

- **Service-based monitoring:** Provides an abstracted per-service view of the network assets that support applications such as signaling. This helps operations teams quickly determine whether an issue is network-related or application-related, which reduces time to restore.
- **KPI-based performance assurance:** Tracks latency, jitter, packet loss, availability and other service-quality indicators using alarms, thresholds and analytics to detect degradation before it affects services.
- **Multicast and video service assurance:** Monitors multicast flows that support CCTV and other video services across stations, depots and trackside locations to detect abnormal traffic behavior or resource-impacting conditions.
- **Impact-aware fault isolation:** Correlates IP, Ethernet, optical and service-layer alarms with service impact views and operational dashboards, helping network operations center (NOC) teams reduce alert noise, identify affected sites and accelerate root-cause analysis.



Enhancing network planning, visibility and analytics

Rail and transportation network operations teams need greater control over how critical services are routed across increasingly dynamic communications networks. As service demands evolve, they need the ability to steer traffic based on service intent, real-time network conditions and operational constraints. NSP can be expanded with path computation and optimization capabilities that help place traffic-engineered paths or Segment Routing policies according to network state, service requirements and engineering policies.

For transportation applications, these capabilities can support latency-aware routing, congestion avoidance, route diversity and maintenance-window planning. Operations teams can visualize paths, simulate changes and apply policies that help keep critical services aligned with operational requirements.

These capabilities improve communications network availability by helping services remain on resilient, diverse and performance-aware routes. They also reduce the risk of disruption during congestion, failures or planned maintenance. They further support planned network evolution by enabling traffic migration during maintenance activities and automated path optimization as network elements are added, removed or reconfigured.

How NSP helps improve network performance:

- **Policy-based path computation:** Places critical rail and transportation services on paths that align with service intent, network conditions and operational policies.
- **Latency-aware path placement:** Supports signaling, train control, operational voice and other applications that require predictable end-to-end performance.
- **Route diversity:** Reduces correlated failure risk by separating primary and backup paths across diverse transport routes.
- **Congestion avoidance:** Uses network state and telemetry to identify more suitable paths for traffic.
- **Maintenance planning and service continuity:** Simulates planned work and supports make-before-break traffic migration during fiber maintenance and network upgrades, helping keep critical rail services operational while changes are performed.
- **Dynamic topology adaptation:** Supports the seamless addition or removal of network elements through automated path optimization based on network policies and constraints.

Strengthening security for mission-critical transportation networks

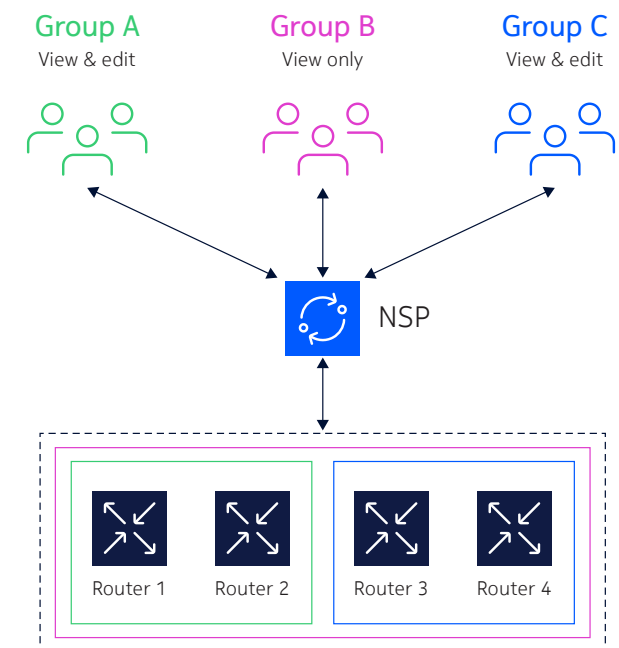
Communications networks play a critical role in maintaining safety, continuity and public trust in transportation systems. Securing these networks against cyber threats is a top priority. NSP is designed with a defense-in-depth approach that helps operations teams protect network access, control user privileges, maintain auditability and support secure operations across the network lifecycle. Security requirements span the platform, users, devices, services and integrations.

In transportation environments, many critical edge Ethernet devices may not support 802.1X authentication, including legacy signaling equipment, CCTV cameras, ticketing devices, passenger information displays, sensors, controllers and other operational technology (OT) assets in stations, depots and trackside cabinets. These devices still need network access, but they can increase exposure to threats if ports are left open or device changes are not controlled.

NSP helps strengthen security across mission-critical transportation environments by supporting access-layer policies that enforce port-level controls, limit unauthorized connectivity, detect unexpected changes and contain unauthorized access attempts at the network edge. This helps operations teams reduce risk in distributed environments exposed to maintenance activity, third-party access or harsh field conditions.

NSP supports role-based access control (RBAC), which allows permissions to be aligned with operational responsibilities. It also supports essential security capabilities such as local account management, identity brokering from remote sources, multi-factor authentication, configurable password and session policies, and comprehensive logging of user activity for troubleshooting and security auditing.

NSP strengthens security with role-based access control



Use case:

Unified WAN and Ethernet access management

Transportation communications networks often combine a mission-critical wide area network (WAN) with station, depot and trackside Ethernet access in a daisy chain or ring topology. Traditional ring-based approaches can become difficult to operate when each ring is managed in isolation, especially as services traverse multiple domains. NSP enables operations teams to manage the WAN and Ethernet ring environment as one operational domain. This improves visibility into services, ring status, protection paths and mission-critical traffic.

NSP can manage G.8032 Ethernet Ring Protection Switching (ERPS) environments, which helps operations teams maintain loop-free resiliency and fast recovery for trackside and station rings. When combined with IP/MPLS or Segment Routing in the backbone, this approach provides a resilient and efficient alternative to traditional spanning-tree-based designs. It supports scalable service automation, integrated OAM and centralized assurance across the WAN and ring domains.

With NSP, operations teams can manage ERPS rings across trackside, station and depot environments while maintaining visibility between backbone services and access rings. This makes it easier to understand how WAN and Ethernet edge domains interact, support rapid loop-free recovery for critical access connectivity, and reduce reliance on multiple tools or manual correlation. By applying OAM and KPI-based monitoring to services that span the WAN and Ethernet edge, NSP helps operations teams improve assurance across ring-based environments and keep mission-critical transportation services aligned with operational requirements.



Use case:

Network time synchronization management

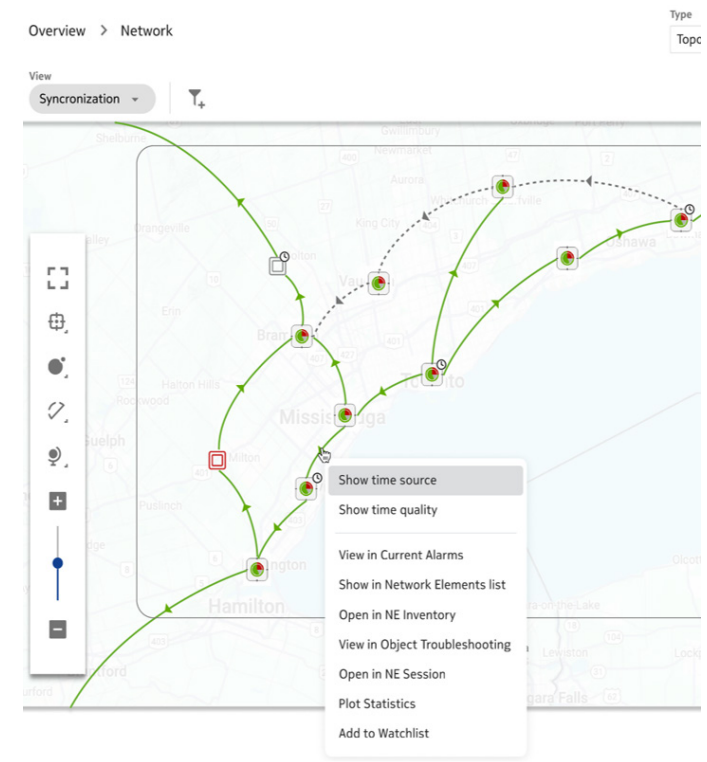
Network time synchronization remains essential across legacy and next-generation communications networks. For legacy TDM, SDH/SONET and circuit-emulated services, accurate frequency synchronization helps prevent slips, jitter-buffer issues and service degradation. For FRMCS/5G deployments, network time synchronization becomes even more critical because radio and packet-based services require precise frequency, phase and time alignment to support reliable train-to-ground communications and coordinated operations. IEEE 1588v2 Precision Time Protocol (PTP) enables precise time distribution over packet networks, which allows timing data to be delivered through the communications infrastructure rather than through separate, difficult-to-scale timing architectures.

Traditional synchronization management is often performed device by device, which becomes difficult as networks expand across corridors, radio sites, stations, depots and control centers. NSP provides a network-based approach to synchronization management, which gives operations teams visibility into synchronization topology, master and slave clock relationships, source-to-node timing paths, clock status and timing-related alarms.

This approach simplifies network synchronization troubleshooting by using a network map with an overlay of IEEE 1588v2 PTP packet flows. It allows operations teams to see how timing is distributed, which paths timing packets follow and where the synchronization chain may be degraded or interrupted. Instead of troubleshooting clock issues node by node, teams can analyze the end-to-end timing flow, isolate timing faults faster, validate grandmaster and boundary clock relationships, and understand the service impact of synchronization events.

- **Network time synchronization visibility:** Visualizes IEEE 1588v2 PTP packet flows on the network map to understand timing distribution and identify potential fault locations.
- **Source tracing:** Identifies the upstream timing source for a specific node or site.
- **Faster troubleshooting:** Correlates timing alarms with topology, timing paths and service impact.
- **What-if analysis:** Assesses the impact of timing topology changes before implementation.
- **Legacy and FRMCS/5G readiness:** Improves timing resiliency for existing TDM-based services while providing the synchronization foundation needed for future FRMCS/5G train-to-ground deployments.

Visualizing synchronization packet flows with NSP



Use case:

Multilayer and multivendor network operations

Communications networks increasingly combine IP/MPLS routing, Segment Routing, Ethernet switching, coherent optics, packet optical transport and third-party devices. Managing each domain separately makes it harder to understand service impact, diagnose root causes and optimize resources. NSP provides converged visibility and control across multiple technologies and vendors, helping operations teams manage the network as an integrated transport fabric.

With IP/optical coordination, NSP can correlate alarms between routing and optical layers, which improves fault isolation and reduces time spent determining whether a service issue is caused by an IP, optical or physical-layer condition. Support for coherent optics and IP over DWDM helps operators converge transport layers while maintaining visibility into the service and infrastructure relationship. SNMP-based integration of third-party Ethernet switches in trackside cabinets or stations allows operations teams to monitor nodes, ports, alarms and statistics from non-Nokia equipment in the same operational environment.

How NSP enables multilayer and multivendor network management:

- **IP/optical alarm correlation:** Identifies root causes across routing and optical domains.
- **Coherent optics support:** Improves visibility into IP-over-DWDM and high-capacity transport designs.
- **Third-party device monitoring:** Integrates multivendor devices using SNMP to monitor availability, port status, alarms and statistics.
- **Open integration:** Uses northbound APIs to integrate with OSS, orchestration and operational systems.
- **Integrated lifecycle management:** Enables teams to manage discovery, inventory, provisioning, assurance, upgrades and backups in a consistent operational environment.

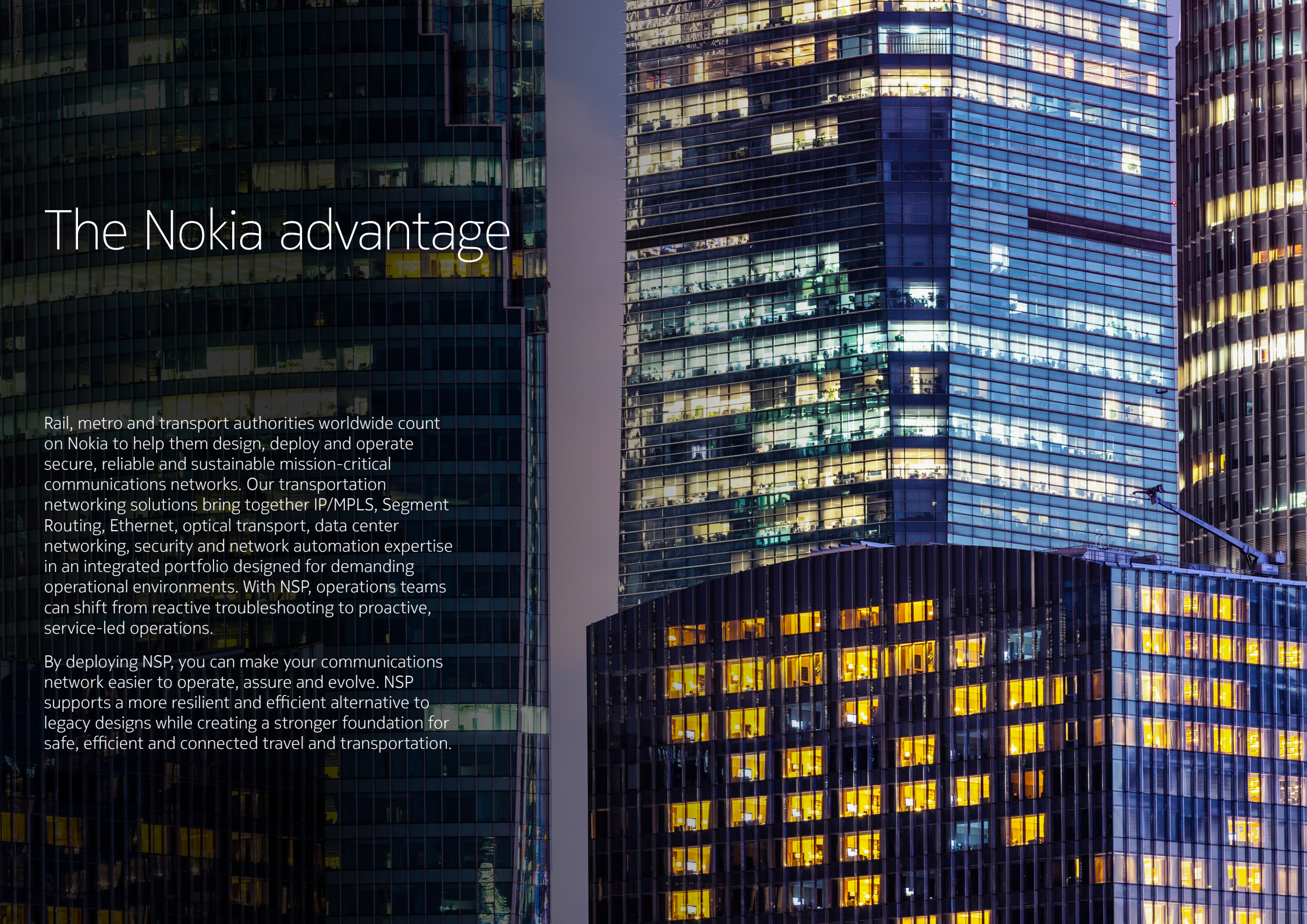


Evolving with Nokia

Nokia has a long tradition of leadership in mission-critical IP, optical and network management solutions. NSP incorporates this experience into an extensible platform that helps rail, metro and transport authorities simplify operations, reduce maintenance windows, improve resilience and prepare for the next phase of digital transformation. Its modular architecture can help your operations teams address today's challenges while building a foundation for FRMCS/5G evolution, cloud-based operations, AI-assisted assurance and increasingly automated network lifecycle management.

Why choose NSP for your communications network?

- Streamline migration from legacy transport technologies to IP/MPLS and Segment Routing.
- Reduce human error and accelerate service delivery through repeatable, validated provisioning workflows.
- Proactively assure mission-critical services and improve fault resolution.
- Improve visibility from the backbone to stations, depots and trackside assets.
- Reduce maintenance windows with pre-tested scenarios and automated workflows.



The Nokia advantage

Rail, metro and transport authorities worldwide count on Nokia to help them design, deploy and operate secure, reliable and sustainable mission-critical communications networks. Our transportation networking solutions bring together IP/MPLS, Segment Routing, Ethernet, optical transport, data center networking, security and network automation expertise in an integrated portfolio designed for demanding operational environments. With NSP, operations teams can shift from reactive troubleshooting to proactive, service-led operations.

By deploying NSP, you can make your communications network easier to operate, assure and evolve. NSP supports a more resilient and efficient alternative to legacy designs while creating a stronger foundation for safe, efficient and connected travel and transportation.

Nokia OYJ
Karakaari 7
02610 Espoo
Finland

Tel. +358 (0) 10 44 88 000

CID:215534

nokia.com

NOKIA

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 is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

© 2026 Nokia