Railway service interruptions bring significant inconvenience to passengers, incur economic loss and affect the service level. They also lead to revenue loss as customers switch to other transport service providers. To meet these challenges, urban railway operators can embrace predictive maintenance by harnessing the agility, flexibility, security and scalability of SD-WAN to support pervasive IoT deployment. This paper explains how.
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Challenges in providing reliable railway service</td>
<td>3</td>
</tr>
<tr>
<td>Current WAN falls short</td>
<td>4</td>
</tr>
<tr>
<td>IoT connectivity everywhere</td>
<td>5</td>
</tr>
<tr>
<td>Agility and scalability for massive IoT deployment</td>
<td>5</td>
</tr>
<tr>
<td>Seamless interconnection with the cloud</td>
<td>6</td>
</tr>
<tr>
<td>Robust network security for IoT</td>
<td>6</td>
</tr>
<tr>
<td>SD-WAN bridges the gaps</td>
<td>7</td>
</tr>
<tr>
<td>The advent of SDN and SD-WAN</td>
<td>7</td>
</tr>
<tr>
<td>SD-WAN advantages</td>
<td>9</td>
</tr>
<tr>
<td>Conclusion</td>
<td>11</td>
</tr>
<tr>
<td>Abbreviations</td>
<td>12</td>
</tr>
</tbody>
</table>
Challenges in providing reliable railway service

More than two-thirds of the world population will be living in urban areas by 2050 according to the latest United Nations report. To adequately serve this growing population, urban railway operators need to increase service frequency, improve service reliability and maintain safety. More, faster and heavier trains rolling over rail tracks and higher usage of rolling stock subsystems, such as door and air conditioning systems, accelerate the deterioration of these railway assets.

Traditional preventive maintenance requires regular inspection of railway tracks and rolling stock with no awareness of their condition between scheduled inspections. While this can reduce the chance of failure, it incurs high maintenance costs, which are borne by the public in the long run. Moreover, these railway assets can fail before their next scheduled inspection because they wear out in unpredictable ways influenced by factors such as weather, age or simply frequent usage. Failures incur unscheduled outage, impacting service reliability significantly.

As a result, railway companies have shown strong interest in embracing predictive maintenance. With it, they can monitor asset conditions in real time or near-real time, so that repair works can be optimally planned ahead based on maintenance data. In this way, railway companies can optimize asset utilization and life span.

More important, the assets will not fail unexpectedly, causing unplanned outage or jeopardizing safety. For example, monitoring track geometric parameters such as deflation in real time detects rail defects before failure occurs, ensuring safe passage. Similarly, monitoring train door opening and closing cycles detects door problems in advance, preventing unplanned outage.

However, adoption of predictive maintenance has two prerequisites:

1. Broad sensor deployment throughout the railway infrastructure
2. Agile computing resources running intelligent analytics applications.

Both of these have been barriers to adoption of this new maintenance paradigm.

With digitalization and automation, railway operators are embracing the internet of things (IoT) and cloud technologies. Many are deploying IoT systems comprising multiple sensors installed along tracks and on rolling stock, collecting and sending multitudes of data to data centers for processing. At the same time, they are also migrating their data centers to a virtualized cloud model\(^1\) to improve IT efficiency and agility.

With these things in place, the conditions are now right to introduce predictive maintenance to accurately predict impending failures and forestall unscheduled failures and outages. Operators can reap the benefit of just-in-time maintenance, replacing a subsystem component well before fault occurrence but not unnecessarily early. This optimizes asset utilization and reduces maintenance costs while increasing service reliability and safety.

\(^{1}\) The cloud is a dynamic pool of on-premises (typically private data center), private virtualized compute resources and, optionally, third-party public cloud services (also known as virtual private cloud (VPC)). This model is also called hybrid cloud because it entails both private cloud and public cloud.
Current WAN falls short

As explained in the preceding section, the predictive maintenance paradigm requires pervasive IoT deployment across the railway infrastructure to collect and send data back to the cloud where intelligent analytics applications are run. Networks are essential to connect IoT everywhere and to the cloud (see Figure 1).

Figure 1. Network architecture for a cloud-based IoT deployment

Urban railway operators are no strangers to deploying and operating networks. Many already have a mission-critical WAN based on TDM technologies (SONET/SDH) and packet technologies (Ethernet, IP, and more recently, IP/MPLS). Using pseudowire, Ethernet and IP VPN connections, these networks have been reliably supporting critical operational technologies such as signaling, SCADA and land mobile radio, ensuring smooth and safe operations.

However, IoT and the cloud bring four new communications network requirements that stretch beyond the current WAN capabilities:

- IoT connectivity everywhere with seamless extension of VPN connections over wireless access
- Agility and scalability for massive IoT deployment
- Seamless interconnection with the cloud
- Robust network security for IoT

Each of these is discussed in the following sections.
IoT connectivity everywhere

Because the railway infrastructure is broad and comprises assets that include tracks, crossings and rolling stock, operators need to have versatile access options to provision connectivity wherever it is necessary. Very often, this extends beyond the reach of traditional access technologies such as fiber, copper wires and microwave. Operators need to resort to newer wireless access technologies, including 4G/LTE and low-power WAN (LPWAN), when traditional technologies may not be available or economical. This poses a challenge when extending traditional pseudowire, Ethernet and IP VPN connections over those wireless access technologies from the backbone network.

Agility and scalability for massive IoT deployment

Connecting the sheer number of IoT sensors would stretch the limits of traditional WAN agility and scalability. To deploy a new IoT sensor, a technician must be dispatched to the location, and new network connectivity must be deployed. To properly and securely connect each of these sensors, network parameters such as VLAN ID, IP address and security policy need to be configured manually. In the case of a new IoT application, a new VPN may also need to be created and configured manually. Today’s WAN network requires a labor-intensive configuration process with many integration points among different administrators (see Figure 2); this incurs significant operational cost and delay to IoT adoption. The anticipated multitude of IoT sensors that need to be deployed and activated, coupled with the massive network configuration required, make IoT adoption unfeasible in traditional WAN infrastructures.

Figure 2. IoT activation with traditional WAN
Seamless interconnection with the cloud

IoT collects and sends data to the operators’ cloud infrastructure for storage and analysis by IoT applications. This cloud infrastructure is a dynamic, flexible pool of virtualized on-premises compute resources, optionally extended to services offered by cloud service providers. Virtualized compute resources, in the form of virtual machines (VMs)\(^2\), host the IoT applications.

VMs can migrate from one data center to another or to a virtual private cloud (VPC) as part of cloud optimization and maintenance activities. To adapt to this new, dynamic cloud computing environment, many data center network fabrics have already evolved and adopted software-defined networking (SDN) technologies. SDN in data center continually tracks VM migration events to automatically adjust the fabrics. However, because there is no dynamic interworking between the data center SDN and the WAN, the WAN is not automatically notified of the new VM change in the cloud and does not reconverge to accommodate the change.

As a result, IoT sensor data is still sent to the original location even after VM migration (see Figure 3). This can be remedied only when the operator manually performs routing configuration updates every time VM migration happens. With the massive amount of IoT traffic, this process is labor-intensive, prone to errors and is not a scalable approach to support IoT.

Figure 3. Barrier to interconnecting the WAN and cloud

Robust network security for IoT

IoT devices typically bring higher security risks. First, IoT software and embedded systems are mostly developed using open-source software libraries and modules that are unlikely to have gone through rigorous security inspections. They are also typically slow to adopt the latest security patches and updates. Second, the lack of strong authentication (complex passwords, encrypted credentials, Transport Layer Security authentication) and data encryption leave the devices open to attackers. The sheer number of devices also greatly expands the attack surface.

Further complicating the security challenge is the fact that IoT applications have adopted a cloud-computing paradigm. In addition to the cloud’s dynamic nature, cloud-based applications typically adopt a modular and open architecture so they can be served from various compute locations across multiple private or public cloud services.

---

\(^2\) Container is another feasible technology to implement virtualized compute resources. While equally applicable to both technologies, this paper uses only VM to simplify the discussion.
For example, a temperature-sensing application comprises an authentication module, a telemetry module and a device management module. Each of these modules runs from different tiers of the server that are assigned and allocated dynamically from different physical locations (typically data centers) across the enterprise network or in the virtual private cloud hosted by a cloud service provider. To strengthen security, only predefined traffic flows should be entitled to specific network resources so that each IoT device can only communicate with the application module using a predefined set of protocols. (For example, Message Queuing Telemetry Transport (MQTT) and OMA Lightweight M2M could be predefined as the protocol for use towards the telemetry server and management server; all other protocol traffic is filtered).

With a traditional WAN, the default security solution is to apply a heavy-handed network segregation technique such as IP VPN (also known as network segmentation) to isolate the traffic of each IoT application within its own domain. This approach frustrates hackers’ attempts to move laterally across the network from the compromised IoT device to other, more critical, systems. Although this approach is very effective as a defence perimeter to thwart outside attackers from penetrating into the domain, it is not compatible with cloud-based IoT architecture due to the following shortcomings:

- It does not adapt to the changing of compute resources that are dynamically assigned to optimize network resources and meet application SLAs.
- It has no visibility of application or context to limit the data flow between endpoints inside a domain (for example, it cannot limit communication between a sensor and the telemetry server to only the MQTT protocol).
- It does not have room to scale to cater to a plethora of IoT devices.
- It is highly dependent on manual and static configurations, which are prone to error.

**SD-WAN bridges the gaps**

The preceding section explained the four capability gaps that restrict traditional WANs from becoming the communications foundation for predictive maintenance. This section explores how software-defined WAN (SD-WAN), the natural WAN extension to SDN, can overcome these shortcomings. First, we provide an overview of SDN and SD-WAN; then we explain how SD-WAN can bridge the gaps.

**The advent of SDN and SD-WAN**

SDN is a new way of building and operating communications networks that enable better end-to-end control, automation and service agility. Evolved from the traditional network model, in which the control and data planes were integrated in the network equipment (also known as the network element), SDN decouples these two planes. With SDN, the data plane continues to reside in the network element. The control plane migrates from the network element to a centralized platform called the SDN controller.

The SDN controller communicates with all network elements to instruct them how to build the overlay networking paths across the network. In addition, a policy control engine provides an interface used by the network operator to program the network, ensuring that applications receive the performance and security they require. This policy control engine is equipped with an open, northbound application programming
interface (API), which can be easily integrated into operations support systems (OSSs) and business support systems (BSSs). As a result, the network is now programmable (software-defined), allowing other OSSs/BSSs or applications to control the network and intelligently provision network services with scalability through the policy engine in a programmatic manner (see Figure 4).

Figure 4. Evolution to the SDN network model

While SDN has been fully embraced by IT technologies and carrier network operators, urban railway operators who have used WAN to reliably carry mission-critical data are understandably wary of transforming their WANs to support SDN. However, with today’s innovative networking technology, there is a flexible SDN deployment model that can provision SDN connections as overlay paths across existing WANs without any changes or upgrades required. This overlay SDN model is commonly known as software-defined WAN (SD-WAN).

SD-WAN extends the network edge with SD-WAN gateways (commonly known as network services gateways3 [NSG] connecting to IoT endpoints through a local LAN, Wi-Fi or LPWAN. Essentially, the SD-WAN is a collection of these NSGs managed by an SDN controller. Through the SDN controller, the operator can program the network as required over their existing WAN and can even extend it to carrier VPN services as well as cellular data services (see Figure 5).

As an overlay network, SD-WAN does not disrupt the present mode of network operations and the critical applications carried. At the same time, SD-WAN brings SDN agility, scalability and programmability to transport specific IoT data in the field. In addition, SD-WAN is a natural extension of the data center SDN because it is controlled by the same SDN controller.

---

3 For more information about the NSGs, visit https://www.nuagenetworks.net/products/virtualized-network-services/
SD-WAN advantages

Any access medium
As indicated earlier, SD-WAN can be provisioned across any network transport, including WAN, carrier VPN services and cellular data services. This extreme flexibility enables operators to select the most optimal medium and connectivity solutions to provide IoT connectivity everywhere, extending and complementing the reach of an operator’s WAN with wireless access and carrier services.

Support for agile IoT deployment
Operators can harness the capability of SD-WAN’s open API to speed IoT deployment. By coupling the SDN policy engine with an IoT management platform, there is an opportunity to automate network service provisioning to bring connectivity whenever a new IoT is installed.

The IoT management platform can generate installation orders to dispatch a field technician for installation. The old way of coordinating with multiple administrators to get the IP address, VLAN and firewall rules configured is replaced. Instead, the IoT management platform can program the SD-WAN through the SDN controller and the API to automatically provision a new SD-WAN connection, along with the necessary network attributes, to the network services gateway connected to the new IoT device. This automation capability greatly increases onboarding speed and reduces IoT deployment cost (see Figure 6).
Figure 6. Interlocking SDN with IoT platform for rapid IoT rollout

Seamless interconnection with the cloud
Many data centers have adopted SDN in their network fabric to create a dynamic cloud-based computing environment. The SDN can automatically adapt to creation, deletion and migration of VMs without any human intervention. As a result, network connectivity is never disrupted. Managed by the same SDN controller, the SD-WAN deployed in the field connects to the data center SDN network fabric, providing seamless interconnection that links the IoT sensor to the IoT application running over a VM inside the cloud.

Any VM changes in the cloud are now advertised to all NSGs to ensure automatic network convergence. Figure 7 shows how this is attained:

1. The VM running the IoT application is moved to another server in another data center for maintenance.
2. The SDN fabric in the second data center detects the change and notifies the SDN controller.
3. The SDN controller updates the IP forwarding table in the NSGs.
4. The NSGs now forward IoT traffic to the new data center.
Strengthened IoT security through micro-segmentation

Micro-segmentation is the ability to apply fine-grained security policies to individual IP flows. SD-WAN supports micro-segmentation to further virtually segment a set of network resources into many distinct sets. Only specific applications or protocols are allowed in specific network segments, thereby protecting the rest of the network from within the perimeter. This approach enforces security policies to limit data flows at a very granular, application-specific level.

For example, for all IP flows between IoT devices and the MQTT server, only TCP port 1883, the port reserved with IANA for use with MQTT, is allowed. This policy prevents a compromised IoT device from contacting the command center for the associated malware and spreading it to the MQTT server, which could otherwise be used as a bridgehead to propagate the malware further in the organization.

Furthermore, micro-segmentation policy configurations can be fully automated through the API of the SDN controller, which subsequently distributes policy creation or updates to all NSGs. As VMs migrate to another tier of the server, another data center or even the virtual private cloud in the hosting data center, the policy adapts to the migration, ensuring continued control of data flows.

Conclusion

Railway service interruptions bring significant inconvenience to passengers, incur economic loss and affect the service level. They also lead to revenue loss as customers switch to other transport service providers. To meet these challenges, urban railway operators can embrace predictive maintenance by harnessing the agility, flexibility, security and scalability of SD-WAN to support pervasive IoT deployment and provide seamless connection to a dynamic cloud compute environment. This improves service reliability so that the urban population can have dependable transport to work, play and socialize.

To learn more about Nokia solutions for railways, visit our [Railways web page](https://www.nokia.com/collaboration-and-chevron/solutions/railways).
Abbreviations

IP  Internet Protocol
LAN  local area network
LPWAN low power wide area network
LTE  long term evolution
OSS  operations support system
MPLS Multiprotocol Label Switching
MQTT Message Queuing Telemetry Transport
NSG  Network Services Gateway
PCEP  Path Computation Element Communication Protocol
SCADA  supervisory control and data acquisition
SDH  synchronous digital hierarchy
SDN  software-defined network/networking
SD-WAN software-defined wide area network
SLA  Service Level Agreement
VPN  virtual private network
WAN  wide area network

About Nokia

We create the technology to connect the world. Powered by the research and innovation of Nokia Bell Labs, we serve communications service providers, governments, large enterprises and consumers, with the industry’s most complete, end-to-end portfolio of products, services and licensing.

From the enabling infrastructure for 5G and the Internet of Things, to emerging applications in digital health, we are shaping the future of technology to transform the human experience. networks.nokia.com

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.

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.

© 2019 Nokia
Nokia Oyj
Karaportti 3
FI-02610 Espoo, Finland
Tel. +358 (0) 10 44 88 000

Document code: SR1905035207EN (May) CID206423