



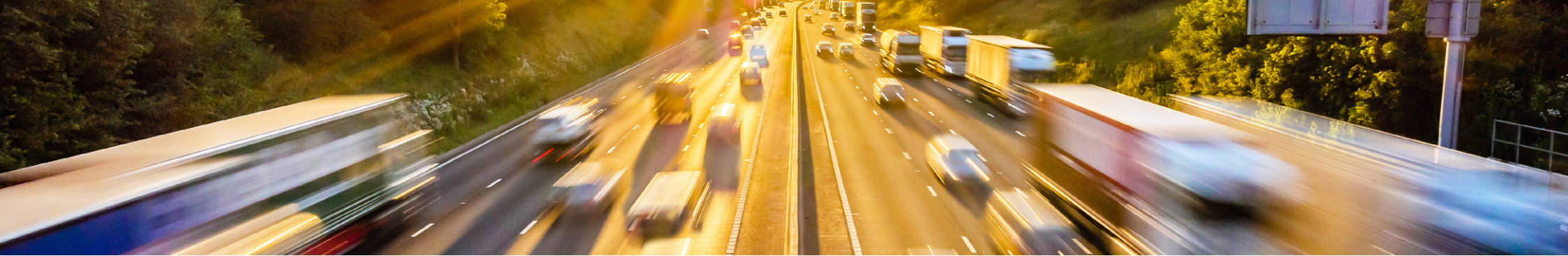
Smarter, greener, more secure transportation through digital transformation

White Paper

Alcatel·Lucent 
Enterprise

Table of contents

- | Overview
 - | Digital transformation accelerates business
 - | Digital technologies address key transportation challenges
- | Connectivity creates smarter operations
 - | Combine real-time information flows to connect people and data
 - | Transform connected operations into smart operations
- | Green from the ground up
 - | Sustainable and secure operations for digital transformation
 - | Green by design
- | Secure access to everything
 - | A zero trust network security model
 - | A step-by-step approach to zero trust
- | Conclusion



Overview

Digital transformation accelerates business

The transportation industry is extremely diverse. Some organisations are focused on moving people and goods by rail or road, while others are focused on air transport or the complex logistics of seaport operations. Each organisation has unique challenges and requirements and is at a different stage in its digital transformation.

However, despite their many differences, all organisations working in the transportation industry now face a set of common challenges that have led to a collective need: All organisations must accelerate their digital transformation.

Today, transportation operators across domains are challenged to move more people and goods faster, at lower cost, and with fewer risks. Prior to the pandemic people were travelling more, for business and for pleasure. And international commerce and trade had risen considerably, putting a huge strain on those who move goods.

For example:

- The total number of passengers carried on scheduled air services rose to 4.5 billion in 2019, which is 3.6 percent higher than in 2018.¹
- Approximately 80 percent of the volume of international trade in goods is carried by sea, and the percentage is even higher for most developing countries.²
- The number of vehicles on roads is growing rapidly, with estimates of almost 1.5 billion vehicles on earth.³

¹ [The World of Air Transport in 2019](#), International Civil Aviation Organisation, Annual Report 2019.

² [Review of maritime transport](#), United Nations Conference on Trade and Development (UNCTAD), November 18, 2021.

³ [How Many Cars Are There in the World in 2021?](#) Hedges & Company.

Digital technologies address key transportation challenges

When the global health crisis hit in March 2020, every transportation operator had to adapt their operations to take advantage of digital technologies, almost overnight. Solutions for contactless payments, virtual kiosks, and automated operations were suddenly essential to continue doing business while reducing the need for human interaction and intervention.

As pandemic restrictions ease, the pressure to digitally transform will only increase. People will yearn to travel freely throughout the world, and businesses will look to make up for missed sales opportunities. Everyone will expect to take advantage of the efficiencies that digital technologies and automation enable.

Realistically, transportation operators can't endlessly expand infrastructure to meet increased demands. It's too expensive, and they'll always be trying to catch up with demand levels. To keep pace with escalating volumes of people and goods, transportation operators must upgrade to smarter, greener, and more secure operations that:

1. Connect people, goods, and assets
2. Reduce the carbon footprint
3. Provide protection from cyberattacks

“Simply adding individual technologies in an ad-hoc way won't allow transportation organisations to achieve these goals. Instead, they must take a holistic approach that connects all systems and subsystems with real-time communications. They must consider their carbon impact. And they must protect access to every system and subsystem with the best available cybersecurity measures.”

- Roch Muraine, Worldwide Sales Director for Transportation at ALE

Connectivity creates smarter operations

The need to efficiently and smoothly move data through all systems is at the core of each transportation operator's requirements — whether they're working to get the public from one location to another, or trying to get goods and materials from manufacturers and retailers to customers.

Most transportation operators have massive amounts of data, but the data is isolated within different subsystems that aren't connected to one another. There are subsystems for almost every aspect of transport operations including:

- Route and asset management
- Internal and external communications
- Electromechanical functions
- Security
- Passenger information
- Ticketing
- Business applications

Combine real-time information flows to connect people and data

Because the subsystems are not always interconnected, there's no ability to share information across systems, departments, or roles within the organisation in real-time. And there's limited ability to use data to keep passengers and customers informed.

Imagine, for example, a scenario where there's an issue with electromechanically operated doors. Think about what needs to happen when those doors don't open. Firstly, the maintenance staff need to be informed about the situation so investigations and repairs can begin as quickly as possible. Secondly, but equally important will be the ability to immediately start planning alternate arrangements for routes, asset deployment, and passenger management. Next, the travellers need to be notified about the situation and advised of any delays or cancellations. And lastly, the employees on the frontline need access to all the latest information about the status of the repairs to address passenger inquiries.

Subsystems that are not interconnected introduce delays, uncertainty, and insecurity and can have a tremendous negative impact on the situation. Subsystems that are connected can move through a pre-determined protocol to ensure repairs happen quickly and passengers are informed about what is happening at every stage.

In addition to the example provided above, there are many other opportunities to use the data within all the various transportation subsystems to work in a smarter, more efficient way. Here are just three.

- 1. Optimise route planning and asset management:** When transportation organisations can combine and analyse data from Wi-Fi and ticketing subsystems, they can reveal trends that show where people and goods need to be moved and when. They can then use this insight to meet shifting demand levels without wasting fuel, energy, or human resources. They can also align infrastructure investments with expected traffic flows to make the best possible use of their budget. The ability to share real-time data among subsystems also helps keep transport operations running smoothly and on schedule, and minimises waste.
- 2. Improve the passenger and customer experience:** With access to real-time information from multiple systems, transportation operators can provide real-time updates about the movements of vehicles and goods. For example, when CCTV cameras, sensors, weather stations, and communications systems communicate in real-time, transportation operators can provide insight into the most crowded traffic lanes, metro stations, and bus stops so people can adapt their movements accordingly. Operators can also provide advance warning about impending weather hazards to help keep people safe, and about vehicle slowdowns and movements of goods so there are no nasty surprises.

Transportation operators also can combine real-time data flows from their route management, external communications, and passenger information subsystems to help people efficiently plan their end-to-end journey. In the future, they may even be able to provide connections to other modes of transportation to further increase their value to passengers and customers.

- 3. Monetise data:** Connecting subsystems allows transportation operators to create an overall statistical view of their operations to reveal new opportunities to increase revenue. For example, when people-counting, ticketing, Wi-Fi, and other subsystems are connected, artificial intelligence (AI) and machine learning (ML) technologies can be used to gain insight into traffic patterns. That insight can then be used to offer passengers and customers discounts on nearby products and services based on where they're expected to be.

Transform connected operations into smart operations

Smarter operations require a single connectivity foundation that links all systems and subsystems.

Wireless connectivity is the most efficient, cost-effective, and environmentally friendly way to connect transportation systems and subsystems across large and small distances. The key is to choose the wireless connectivity option that makes the most sense for each location, system, and application. Wireless technologies including, 4G LTE, 5G, Wi-Fi, LoRaWAN, Zigbee, and Bluetooth® Low Energy (BLE), can all play an important role in creating a connectivity foundation for transportation operators.

In addition to newer wireless technologies, the connectivity foundation must incorporate existing wired connectivity infrastructure, such as copper and Ethernet. Leveraging this existing infrastructure simplifies deployments and ensures maximum return on previous investments. Unified management across wired and wireless environments provides seamless visibility into all systems and subsystems.

Once the connectivity foundation is in place, the next step is to deploy technologies that enable smart operations. Key technologies to consider include:

- **Virtualisation and automation** technologies that simplify infrastructure, reduce the need for hardware, and minimise maintenance requirements
- **Cloud** technologies that enable smarter automation and increase sustainability
- **Artificial intelligence and machine learning** technologies that provide the insight needed to make informed decisions
- **Convergence** technologies that bring operational and IT systems and subsystems together to simplify infrastructure and minimise environmental impact
- **Data anonymisation** technologies that ensure data sovereignty and privacy regulations are respected end-to-end

“Real-time information flows can only occur when all subsystems are interconnected. The earlier that warnings about issues, delays, and hazards can be provided and acted upon, the better for everyone involved. Staff can work more efficiently and effectively. And the safety and security of people and goods can be better protected.”

- Roch Muraine

White Paper

Smarter, greener, more secure transportation through digital transformation



Green from the ground up

Sustainable and secure solutions for digital transformation

Alcatel-Lucent Enterprise understands how digital transformation helps transportation organisations involved in railways, air transport, intelligent transport systems (ITS), and seaports evolve to smarter, greener operations.

Over the years, ALE have partnered closely with hundreds of customers across these transportation domains to understand their unique requirements and address their specific challenges with secure, end-to-end solutions that reduce their carbon footprint.

Green by design

ALE solutions for smarter, greener transportation are designed from the ground up to increase efficiency and minimise impact on the environment before, during, and after deployment.

To achieve these goals, ALE has:

- Created energy-conscious product designs that require less power, manage power better, and reduce heat dissipation
- Reduced the size of hardware, miniaturise components, and densify ports to reduce materials and space requirements
- Used virtualisation technologies to eliminate the need for some hardware altogether
- Shifted solutions from on premises to the cloud to reduce space and energy requirements and leverage sustainable data centres
- Optimised architectures and product life cycles for maximum longevity to reduce waste
- Used eco-friendly packaging materials that can be easily recycled
- Complied with environmental directives for product end-of-life and disposal, including Waste Electrical and Electronic Equipment (WEEE), Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), and Restriction of Hazardous Substances Directive (RoHS)

“ALE has developed a Go Green program that combines our efforts with those of our supplier, partner, and customer organisations and ecosystems to reduce digital pollution, improve waste management, and decrease energy consumption across the entire value chain.” - Roch Muraine

White Paper

Smarter, greener, more secure transportation through digital transformation



Alcatel-Lucent Enterprise Recognised as an Eco-Friendly Communications Provider

In 2021, Alcatel-Lucent Enterprise received an EcoVadis Silver Medal rating in the manufacturer of communications equipment category, ranking in the top 10 percent of participants across the industry.

EcoVadis is a performance rating agency focused on environmental issues, social issues, and governance. The agency rates organisations' efforts towards creating a sustainable planet based on 21 criteria.

Secure access to everything

Connecting all systems and subsystems and bringing more technologies into the network increases the need for robust cybersecurity measures. However, cybersecurity risks should not stop organisations in the transportation industry from taking full advantage of faster, smarter, and greener operations that use automation, cloud, AI, and other technologies.

Understanding the new methods for securing access to their systems and subsystems can alleviate concerns and let operators reap the benefits of new innovative solutions.

A zero trust network security model

A zero trust approach to network security protects the organisation's resources, rather than the network itself. That means the focus is on protecting access to those resources.

Multiple layers of security are applied to protect resources in a way that assumes attackers are already present and always ready to strike. There is no implicit trust. The same high levels of security protection are applied equally to every internal and external person, system, subsystem, application, and device that attempts to access the network. Access is strictly limited to only the resources that are needed when the request is made, and all network resources are continuously scanned for unusual or malicious activities.

To adopt a zero trust network security model, organisations must change the way they segment security to fit the way people work today. Traditionally, security measures were applied based on organisational structure and departments such as finance, sales, R&D, and human resources. Today, this type of segmentation no longer makes sense. People are much more mobile. They may be working from home, from a hotel room, or from a customer or partner site. People are no longer trusted simply because they're an employee. And no departmental system is considered safer than another.

In addition to changing the way they segment; transportation operators must switch from multiple management systems for network resources to a single system that provides a cohesive view across all wired and wireless network resources. This is the only way to gain rationalised and standardised visibility, and control over all network resources.

"Transportation operators are specialists in their industry focus area, however, they may not be experts in a zero trust approach to network security. An experienced partner can offer this vital expertise to develop and deploy the right zero trust network for each operator's unique situation."

- Roch Muraine

White Paper

Smarter, greener, more secure transportation through digital transformation

Trusted by leading transportation organisations

ALE is involved in some of the most innovative digital transformation initiatives in the transportation industry globally. Following are a few examples of our enduring commitment to our customers' success:

- The **Nevada Department of Transportation (NDOT)** has established a strong, long-term partnership with us to lay the foundation for its next-generation intelligent transportation system. With our ruggedised switches in the backbone network, stackable switches at the network core, and SPB technology, NDOT can securely support the increasing number of sensors, cameras, and other IoT devices along 8,000 kilometers (5,000 miles) of state-maintained roads and highways.

- **Grand Paris Express** is the major public rail initiative in Europe, that will take place in several phases over the next 10 years, from 2020 to 2030. It will transform the Paris region public transportation services with 200 km of automated lines, 69 stations, and 7 operations centres.

ALE was selected for this multi-service network project based on its robust network solutions, including switches for data centres and stations, and reliable long-term support. ALE was also recognised for its established relationships with powerful industry consortiums and Nokia alliance.

The secure, mission-critical multi-service network will support video monitoring in stations, and air quality monitoring through thousands of IoTs at the new circle line around Paris.

Inauguration of this significant project will take place at the 2024 Summer Olympics in Paris, with the new Orly airport station demonstrating cutting-edge multi-modal transport solutions.

- The **Saint Gotthard Tunnel**, the longest and deepest traffic tunnel in the world, uses 1,000 of our hardened network switches to connect the tunnel's 70,000 data access points. The tunnel's specialised network ensures passenger and vehicle safety in an extremely challenging environment where temperatures can exceed 40 °C (104 °F) and humidity levels can exceed 70 percent.



A step-by-step approach to zero trust

Every transportation operator's cybersecurity requirements are unique to their industry focus area, systems, technologies, staffing strategy, physical and virtual presence, and other factors. However, they can all follow the same five-step methodology to assess and implement the zero trust security measures that make the most sense for their organisation:

- 1. Monitor:** Identify all data types, applications, assets, and network services that need to be protected.
- 2. Validate:** Assess the way data flows onto, through, and off the network, including cloud environments as well as the way network resources interact.
- 3. Plan:** Architect and segment the zero trust network around the data types, applications, assets, and network services that need to be protected.
- 4. Simulate:** Develop and test the zero trust policy to verify it appropriately considers and protects all network resources.
- 5. Enforce:** Continuously monitor the zero trust environment to detect policy violations, apply remediation, and discover opportunities to strengthen the policy.

Conclusion

Challenges unleashed by the global health crisis have catapulted transportation operators into a world of digital technologies almost overnight. Solutions that might have taken months or years to rollout became essential to business continuity as the need to reduce human contact and intervention accelerated.

Despite the industry's diversity, and their many different stages of digital adoption, it's clear that digital transformation accelerates business and is key to a robust future. Transportation operators that adopt smarter, greener, and more secure strategies, to connect people, goods, and assets; reduce their carbon footprint; and ensure protection from cyberattacks will prosper.

www.al-enterprise.com The Alcatel-Lucent name and logo are trademarks of Nokia used under license by ALE. To view other trademarks used by affiliated companies of ALE Holding, visit: www.al-enterprise.com/en/legal/trademarks-copyright. All other trademarks are the property of their respective owners. The information presented is subject to change without notice. Neither ALE Holding nor any of its affiliates assumes any responsibility for inaccuracies contained herein. © Copyright 2022 ALE International, ALE USA Inc. All rights reserved in all countries. DID22011401EN (February 2022)



ALE delivers end-to-end cybersecurity

Alcatel-Lucent Enterprise is ISO 27001 certified for information security management. All our hardware and software solutions for the transportation industry incorporate security measures that support zero trust network strategies and multilayer security frameworks. For example, our:

- Ruggedised network switches are security-hardened and include advanced security technologies verified and validated by third-party organisations
- Single, secure operating system reduces the organisation's attack surface, simplifies risk mitigation, and enables targeted remediation
- Solutions include key security technologies such as Wi-Fi Protected Access 3 (WPA3), Shortest Path Bridging (SPB), MACsec encryption, Address Space Layout Randomisation (ASLR), and role-based network access control.

Learn more

To learn more about how we can help you optimise your digital transformation experience [contact us today](#).

www.al-enterprise.com/en/industries/transportation