The Internet of Things in Transportation

Build a secure foundation to leverage IoT for improved passenger experiences, safety and efficiency
The Internet of Things (IoT) has the potential to transform the transport industry by profoundly altering how transportation systems gather data and information by bringing together the major technical and business trends of mobility, automation and data analytics. IoT refers to the networking of physical objects through the use of embedded sensors, actuators, and other devices that can collect and transmit information about real-time activity in the network. The data gathered from these devices can then be analyzed by transportation authorities to:

- **Improve the traveler experience**, with more dependable transportation, enhanced customer services and better and more accurate communication and information.

- **Increase safety**, by better understanding transit system operations through sensor data that tracks everything from anomalies in train speeds, roadway temperatures, aircraft part condition, to the number of cars waiting at an intersection.

- **Reduce congestion and energy use**, through the use of real-time data to improve how officials scale resources to meet demand, with the agility to react quickly to fast-changing traffic patterns, or to address traffic impact on fuel use, the environment, and regional economic competitiveness.

- **Improve operational performance**, by proactively monitoring critical infrastructure and creating more efficient processes to reduce operating costs and improve system capacity.

### IoT scenarios in transportation

IoT solutions promise to make transportation organizations smarter and more successful at what they do. The IoT is at the core of forces reshaping transportation to provide greater safety, more efficient travel, improved vehicle and aircraft maintenance, and more strategic traffic management. Examples of transportation IoT include:

- **More efficient**, less costly mass transit, that employ networks of sensors, digital cameras, and communication systems to increase system capacity and enhance passenger safety and comfort while lowering costs and risks.

- **Dynamic roadside message signs** for intelligent transportation systems, which display real-time road status, toll rates, lane closures and travel times automatically relayed from sensors and cameras.

- **Autonomous vehicles**, with the ability to sense their environment, predict behavior, communicate with other vehicles and their surroundings, and react instantaneously to real-life highway scenarios.

- **Video surveillance solutions**, which feature high-resolution CCTV cameras to secure airports and rail stations, including continual monitoring of passport control checkpoints and movement of people and crowds. Intelligent video analysis software automates early detection of suspicious behavior and abandoned luggage.
Challenges of IoT deployment

The IoT brings unprecedented flows of data, presenting challenges for network and data management along with increased security risks. To address these issues, transportation authorities need to adapt traditional network designs to provide new levels of network intelligence, automation and security.

Transport organizations need a cost-effective network infrastructure that securely handles vast flows of data, and is also easy to manage and operate. The infrastructure must:

- **Provide a simple, automated process for IoT device onboarding.** Large IoT systems can contain thousands of devices or sensors, and manually provisioning and managing all of these endpoints is complex and error-prone. Automated onboarding enables the IoT platform to dynamically recognize devices and assign them to the appropriate secured network.

- **Provide a secure environment against cyberattack and data loss.** Because the many networked devices and sensors in transportation IoT networks provide a corresponding abundance of potential attack vectors, security is critical for mitigating risks of cybercrime. Security is necessary at multiple levels, including containment of the IoT networks themselves.

- **Supply the correct network resources for the IoT system to run properly and efficiently.** Many devices in the IoT system deliver mission-critical information that requires a specific level of QoS. For instance, some use cases require proper bandwidth reservations on a high performance network infrastructure to ensure service reliability.

**IT professionals are making plans for more IoT**

IT professionals in a variety of industries are already planning for increased use of IoT solutions in the near future. According to IDC’s IoT IT Infrastructure Survey, 80 percent of responding IT professionals claimed that IoT systems will have significant impact on their organization’s planning and decision-making for IT infrastructure spending and strategies in the next two years.
The growth of IoT in transportation also brings an explosion of cyber security threats, as the proliferation of sensors and connected devices greatly expands the network attack surface. IoT is especially susceptible because many IoT devices are manufactured without security in mind, or built by companies that don’t understand current security requirements. Consequently, IoT systems are increasingly the weak link in transportation network security.

- The distributed denial-of-service attack on Dyn in October 2016 that brought down much of the internet was perpetrated through hacked networked devices such as security cameras and digital video recorders.¹
- Hackers attacked the San Francisco Muni public transit system network in November 2016, rendering ticket machines and other computing infrastructure inoperable as part of a ransomware scheme.²
- In 2016, Chinese security researchers took remote control of a Tesla Model S from a distance of 12 miles, interfering with the car’s brakes, door locks, dashboard computer screen and other electronically controlled features in the electric car.³ The following year, the same group of hackers again took control of the car, despite Tesla’s patching of the initial vulnerability.⁴
Building a secure IoT network infrastructure

Protecting IoT traffic and devices is a challenge that can’t be solved by any single security technology. It requires a strategic approach that takes advantage of multiple security safeguards.

To help organizations take advantage of the benefits and reduce the risks of IoT, Alcatel Lucent Enterprise (ALE) provides a multi-level security strategy. ALE’s strategy delivers protection at every layer of the infrastructure, from the individual user and device out to the network layer itself. It also provides an IoT containment strategy to simplify device onboarding and deliver the right network resources to run the system properly and efficiently, all in a secure environment to safeguard transportation systems from cyberattack.

IoT containment

To enable IoT containment, all users, devices and applications within the ALE network are assigned profiles. These profiles, which define roles, access authorizations, QoS levels, and other policy information, are relayed to all switches and access points in the network.

- Devices are placed in “virtual containers” using network virtualization techniques that allow multiple devices and networks to use the same physical infrastructure, while remaining isolated from the rest of the network.
- In these virtual containers, QoS and security rules are applied.
- By segregating the network with virtual containers, if a breach does occur in one part of the virtual network, it does not affect other applications.
- When a new IoT device is connected, the network automatically recognizes its profile and assigns the device to the appropriate virtual environment.
- Communication is limited to the devices within that environment and to the application in the data center that controls these devices.
- Because all users also have profiles within the ALE network, access to the IoT virtual containers can be limited to authorized individuals and groups.

In-depth security

In addition to IoT containment, ALE networking technologies provide layered security across multiple levels of the network.

- Secure diversified code protects networks from intrinsic vulnerabilities, code exploits, embedded malware, and potential back doors that could compromise switches, routers and other mission-critical middle- and hardware.
- At the user level, profiles ensure users are authenticated and authorized with the appropriate access rights.
- At the device level, the network ensures that devices are authenticated and compliant with established security rules.
- At the application level, the network establishes rules regarding access to specific applications, including blocking, limiting bandwidth and controlling who can access what.
- At the network level, ALE switches and access points offer smart analytics capabilities that provide visibility and detailed information about the network, users, devices and applications being used on the network.
- ALE smart analytics also provide deep packet inspection capabilities, which can detect the type of data and applications moving through the network, making it possible to identify unusual network traffic patterns and unauthorized activity and network intrusions.

IoT devices pose risks to assets across the entire network. By establishing containers via virtual network segmentation, IoT devices and the applications that control them are isolated, thereby reducing threats without the cost or complexity of separate networks.
End-to-end operational and network management

ALE network solutions also provide significant operational and management advantages.

- **ALE enables multiple separate virtual networks to operate on a single infrastructure**, saving CAPEX investment in multiple physical networks.

- **ALE networking solutions have a single management system for all elements of the infrastructure**, including unified management of both wired LAN and wireless WLAN networks. The Alcatel-Lucent OmniVista® 2500 management suite provides a single pane of glass to manage virtual environments, switches, access points and all other components of the network.

- **The ALE Unified Access solution allows wired and wireless technologies to work together** as a single, robust network, with a common set of network services, a policy framework, a common authentication scheme and a single authentication database.

**A high performance network portfolio**

ALE switches, access points and controllers support the latest generation of high bandwidth and low latency capabilities and manages large numbers of devices in high-density environments. ALE networking products and solutions are able to address the networking needs for organizations of all sizes. **ALE also provides a selection of ruggedized switches, access points and routers for transportation network deployments in harsh environments.**

**Secure transportation IoT networks and strategies are here today**

ALE products and solutions build a secure network foundation to help organizations deploy IoT systems that can increase the capacity, safety and comfort of transportation systems while decreasing costs and risk. ALE’s IoT containment and layered security strategies reduce the risks and simplify the setup of transportation IoT networks by easing device onboarding, providing more efficient operations and greatly increasing security. ALE helps transit and transportation organizations unlock the full potential benefits of IoT by providing enhanced levels of network intelligence, automation and security.
Want to learn more?

For more information about ALE’s IoT solutions, go to ALE IoT Security.

Connected Transportation

At Alcatel-Lucent Enterprise we help you connect transportation systems with technology that works. With global reach and local focus, we deliver networking and communications built for transportation systems, to deliver mobility, security and safety.