Life Is On | Schneider Electric

How is digitalization helping railways build a more reliable, sustainable and efficient infrastructure?

by Valerie Layan
Transportation Segment President, Schneider Electric

Executive summary

By 2025, urban railways are predicted to account for nearly 900 billion passenger kilometers worldwide. To meet this growing demand, railways need to digitize their infrastructure and networks for more reliable, sustainable operations that support a greener society. This white paper examines how railways can build an infrastructure of the future that increases operational efficiency, improves sustainability, ensures reliability, and strengthens cyber security.

Introduction

Public transportation is the lifeblood of cities because it ensures people can easily and affordably get where they need to go. It's predicted that globally riders will travel nearly 50 trillion passenger kilometers per year on urban transportation networks by 2050. That's a realistic target considering how much public transportation is currently being used. In 2021 alone, an average of 5.3 million passengers per day used public transportation in Singapore and U.S. riders took nearly 10 billion trips on public transportation that year.

Beyond meeting people's travel needs, public transportation is also a pillar of most countries' sustainability programs. It builds a greener society because using mass transit instead of driving can dramatically reduce people's carbon footprint. For example, taking a train instead of a car for medium-length distances could cut a person's emissions by around 80 percent.

In this white paper, we'll focus primarily on railways – both passenger rail and metros – and buses to pinpoint 4 areas where they can improve their infrastructure:

1. Increasing reliability through digitization
2. Improving operational efficiency by gaining a complete picture of how their subsystems are working
3. Increasing railway infrastructure's electrification to reduce railways' carbon footprint
4. Boosting cybersecurity

#1 How digital technology ensures reliability

What do the world's most reliable railways all have in common? A digital backbone

1.8 billion people travel by rail every day – but reliability is a common problem

Railways – both long-distance and urban – have one mandate: provide reliable transportation that gets passengers to their destination safely and on time. That's no small feat, considering that in the EU alone railways transport over 7 billion passengers and 1.6 billion tons of freight each year. A single delay, such as a maintenance problem, can quickly escalate into lengthy secondary delays that affect other trains' operations. That has monumental consequences for busy metro systems that may be responsible for moving millions of people a day.

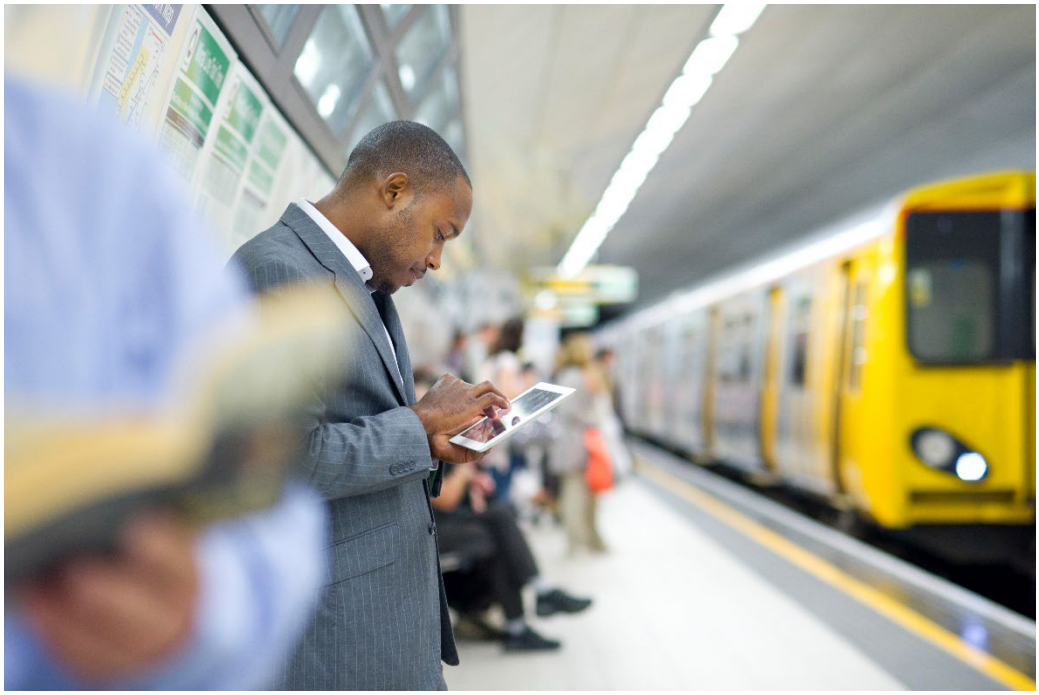
The fact is, many railways struggle to meet reliability challenges. For example, along the U.S.'s busiest passenger rail corridor, infrastructure-related issues caused 328,000 train-delay minutes in one year — the equivalent of around 700 seven-hour train trips.

Digitizing railways gets people to their destination safely and on time

Modernized, future-ready railways know that improving reliability and avoiding these delays starts with adopting digital technology and advanced software, like sensors, digitized power systems, remote monitoring, and data analytics. That's because these digital technologies let railway operators make informed decisions and define new operational and maintenance strategies. Digitization programs are already well underway in many countries. For example, Germany's Deutsche Bahn is digitizing its entire network and expects these technologies will increase the network's capacity by up to 20 percent.

French rail passengers lose a cumulative 340 million minutes per year due to rail infrastructure failures or slowdowns.

UFC-Que Choisir survey



It also improves the reliability of critical equipment like signaling systems

Railway systems are complex but managing them doesn't have to be. Using digital technology simplifies operations because railways can now safely automate time-consuming activities, ensure a stable power system, and monitor assets remotely.

Digitizing signaling systems is one way that railways are ensuring safe operations and on-time trains. For example, track and signaling faults are the main cause of Norway's railway delays. However, the areas where the signaling systems have been upgraded are now the most punctual stretches in the country. Digitized signaling enhances reliability and performance.

In contrast, outdated signaling systems may not be able to gather even basic information, such as the precise location of a train, which can lead to delays and safety issues. To solve or mitigate these issues, a reliable and well-designed signaling power system plays an important role.

Reliable railways are only possible using intelligent solutions that monitor, control, and optimize electrical assets

Two of the most important areas where digitization improves reliability are:

1. **Reliable power and electrification:** Using digital systems for control and power network analysis ensures a reliable power distribution network from sub-station to overhead equipment and auxiliary systems (signaling and telecom) and to the station. Digitally-enabled MV LV electrical distribution equipment energizes the entire passenger station, with availability secured by design.

   How does it work? Consider one example of power quality. The quality of the electricity is crucial for reliable operations. But power quality is a complex issue because it is influenced by supply infrastructure and by certain electrical loads. To prevent a power quality event from threatening uptime, the challenge is often to identify the source of the power quality problem and to corroborate these sources over the entire electrical system. For example, if five locations are experiencing transient voltage disturbances at nearly the same time or with a similar signature, there is a good chance the power quality problems have a common source.

   A comprehensive power management system will supply the information needed to identify these sources so the power quality issue can be addressed.

Condition-based maintenance brings a huge boost in efficiency: around a 10 percent improvement in efficiency and a 60 percent reduction in time-consuming manual diagnostics.

McKinsey

2. **Reliability through better maintenance:** Keeping equipment in working order while optimizing operational expenditure is one of railways' biggest reliability challenges. Railways maximize uptime using digital technology with advanced data analytics and remote monitoring capabilities. The technology uses real-time information into equipment's condition so railways can quickly react to problems and perform the right maintenance at the right time to prevent potential asset failures and extend their lifespan.

   Let's look at one clear example of how reliability is improved through better maintenance. Diagnostic tools can verify the health of electrical components and compare current performance to how the equipment performed when new. The condition-based maintenance

approach conducts diagnostics by collecting health and performance data from digital sensors, then sending those data to analytics software for processing to identify and understand any performance anomalies. Remote experts can review the results and make highly-informed maintenance recommendation that make sure the system keeps running.

Learn how technology has transformed Shanghai Metro's reliability and maintenance

In Shanghai in 2021, 3.6 billion passengers were transported by subway or metro.

Statista

Shanghai Metro is the second busiest rail system in the world. It carries 10 million passengers – 52% of the city's residents – every day and is also the world's biggest metro by route length, with 482 miles of subway lines. To manage this complexity and provide safe, reliable, and efficient transportation, Shanghai Metro needed to ensure an uninterrupted and stable power supply and increase operational efficiency. It met this goal by upgrading its LV/MV power system to guarantee the electrical facilities' safety and security and support normal systems' operations.

Shanghai Metro is also leveraging IoT technology with features like remote monitoring, which improves daily maintenance and operations, and a data analysis system that allows for emergency maintenance. The result: improved operational efficiency, sustainability and asset performance. Learn more about how digital technology ensures safe, reliable, and efficient railway operations by reducing power outages and preventing disruptions.

#2 Why having a big-picture view of subsystems helps railways optimize operations

The High Price of Inefficiency and How Railroads Fight Back

Railways are missing opportunities to boost operational efficiency

Passenger and freight railway activity is predicted to double by 2050. But even today, many railways lack full visibility into their subsystems and awareness of how they interact because the subsystems are working in silos. This lack of integration negatively affects railways' overall efficiency and performance.

These 3 subsystems are the prime targets for optimization

Let's take a closer look at the three railway subsystems where improvement is often needed:

- **Rail electrical distribution** – Electrical distribution subsystems are the backbone of railways because they ensure railways have a reliable power supply that is always available for critical and auxiliary consumers, such as traction substations and overhead lines. For example, electrical distribution subsystems prevent downtime using automated power restoration features that isolate faults and automatically restore power to unaffected areas of the system.
- **Tunnel management** – Railway tunnel management subsystems control and manage tunnels' ventilation and auxiliary systems, as well as other functions like telecom, draining, and signaling using an integrated solution.
- **Passenger station management** –Railways' passenger station subsystem, which includes power systems, building facilities, and third-party subsystems, is managed using integrated control systems. For example, railways could use a building management system to help manage ventilation in an underground metro station.

Step 1: Optimize and centralize each of these subsystems

The first step toward subsystem optimization involves remote centralization. Railways that adopt remote centralized subsystem management now have new ways to improve operational efficiency because they can remotely manage, supervise, and control subsystems from their control center. For example, passenger stations can use remote centralized management to control the station's HVAC, lighting, elevator and escalators to maximize operational efficiency while ensuring passenger comfort and safety.

They can also use these remote capabilities to monitor subsystems' performance because railways are able to access real-time information about asset health. This lets operators quickly identify and address maintenance issues without even leaving the building. The result is less time spent on maintenance and eliminating unplanned downtime.

Step 2: Integrate subsystem data to see the full picture

Railways have better visibility when looking at subsystems as a whole – rather than by individual systems. Why is it important to have end-to-end operational visibility? Railways can't improve efficiency if they don't know how systems and data are being used.

A united operations center (UOC) aggregates and visualizes data from individual subsystems to give railways a big-picture view, like a single pane of glass. A UOC that uses a "system of systems" approach can converge both process and non-process information sources like HMI/SCADA, analytics, engineering diagrams, and GIS sources under one platform. Centralized operations also bring other efficiencies. For example, they improve integration and collaboration across functional departments by letting them share information and coordinate daily activities and processes.

ADIF boosted operational efficiency by 20% by focusing on sub-systems that feed this bigger picture

The Spanish railway ADIF is focused on developing its high-speed rail network – the longest in Europe — and upgrading its rail infrastructure. The result of this growth is that ADIF must now centrally manage almost 3,300 kilometers of high-speed rail network with more than 170 electrical substations.

Spanish railway ADIF increased operational efficiency by 20% using a centralized power management application for traction substations and auxiliary services.

Schneider Electric

To do this, ADIF uses Schneider Electric's centralized power management application for traction substations and auxiliary systems. This technology brings a real-time, single view of the high-speed national rail network through integrated main and back-up control centers. It optimizes energy through integrated monitoring and energy management systems. The result is a reliable power supply for traction and signaling systems using 1,000 cabinets covering the whole network. It has already led to a 20 percent improvement in operational efficiency.

eBus for Zero-emission Public Transportation

#3 How going electric cuts public transportation's carbon footprint

Diesel bus emissions pose environmental and health risks

The transportation industry is one of the largest contributors to greenhouse gas emissions. That's predicted to get even worse over the 30 years. Diesel buses, the most widely used form of public transportation, are a major offender. These heavy polluters are responsible for 25 percent of the black carbon emitted by the transportation sector, which is harmful to both people and the environment.

Converting municipal diesel bus fleets to 100% electric buses, or eBuses, as they're better known, can turn the climate-change tide by reducing vehicle emissions and eliminating air pollution. While the transition to passenger electric vehicles (EV) has been underway for several years, now eBuses are stepping into the spotlight as a way for cities, local governments, and transit authorities to meet their urban transportation sustainability goals for a greener future.

In contrast, a single eBus can save 60 tons of CO2 per year

What makes eBuses such a green solution? A single eBus running 200km per day saves 60 tons of CO2.

A single eBus can save 60 tons of CO2 in a year.

FORESIGHT Climate & Energy

There are already nearly 600,000 e-buses on the road globally in one year compared to a diesel bus. For example, the European Commission's ZeEUS (Zero Emission Urban Bus System) project is testing eBuses in over 90 urban bus system networks across Europe, which has added up to more than 20 million kilometers driven in pure electric mode.

eBuses also help cities meet environmental regulations

Urban transportation decisions tend to be made a city level. By moving from diesel to eBuses, cities enjoy benefits that include:

- Improving sustainability: Transitioning to eBuses make cities greener and healthier. They reduce diesel exhaust emissions and air and noise pollution, which improves people's health and helps cities meet their sustainability targets, especially when eBuses are fueled by electricity that comes from renewable sources.

- **Meeting passengers' demands:** The public wants greener transportation, if the rise in EV is any indication. Cities can meet this need with eBuses, which provide the environmental benefits passengers want while also improving passengers' experience because eBuses they are reliable and quieter.
- **Complying with regulations**: Cities that use eBuses are future-ready because they meet existing stringent city- and country-level requirements and are prepared for new ones. For example, the European Union requires a quarter of new buses purchased by public authorities to be zero-emission by 2025. In addition, the EU's "Fit for 55" legislation brings the transportation industry, which is responsible for roughly 20 percent of total EU greenhouse gas emissions, fully into the EU decarbonization process. It proposes to rapidly increase the use of electric vehicles by banning new fossil-fuel passenger vehicles by 2035.

eBus fleets are only as reliable as their electrical infrastructure

Transitioning from diesel-fueled buses to electric is just the first step toward greener transportation. Cities must also focus on end-to-end electrical distribution solutions that ensure reliable and resilient power for bus depots' charging stations. This could be crucial in some geographies facing grid reliability issues that lead to outages.

To understand the best approach, and whether a microgrid is part of the ideal solution for eBus electrical infrastructure, consulting services play an important role. These services help set a strategy for success by right sizing electrical distribution and EV based on fleet usage, such as kilometers per day and time to charge, as well as right sizing a microgrid for on-site renewable consumption and resiliency. Consulting services can define an energy-sourcing strategy based on grid capacity, tariffs, sustainability requirements, and resiliency challenges, including PPA and carbon offset.

There are 3 main types of solutions for eBus electrification infrastructure for different cases:

- **Bus depot electrification tied to the grid** using MV-LV power distribution and power monitoring and control solutions with the option to procure green energy for end-to-end sustainability goals.
- **Bus depot electrification and microgrid** using the grid and an on-site microgrid for when grid capacity is not sufficient, grid tariff needs optimization, or to self-consume and increase sustainability.
- **Depot electrification and microgrid tied to the grid** that can be islanded for 100% of the critical charging needs in case of unstable

While the first approach above is the most common and is regularly met with success, let's look at an interesting example of the third approach in the list.

Montgomery County aims to save 155,000 tons of GHG with its fleet electrification infrastructure project

Maryland's Montgomery County is creating a green, electric future with its first-of-a-kind public bus fleet electrification infrastructure project. The project advances the county's sustainability goals with a resilient system that improves its transit operations' reliability while decarbonizing public mobility using fleet electrification and microgrid technology that integrates solar PV, on-site power generation, battery energy storage.

The Brookville bus depot has been electrified and powered by a microgrid able to run in islanded mode. Its microgrid is sized to meet peak demand and ensures power resilience for continuous operations — even during service disruptions to the main grid, such as extreme weather and power outages. Montgomery County is planning for the future with its new cloud-based infrastructure because it can accommodate additional DER assets or EV charging infrastructure as the fleet grows.

Once the fleet transitions to electricity, it will save an estimated 155,000 tons of greenhouse gas emissions over the microgrids' lifetime.

Want to learn more? Read our white paper with Guidehouse: Linking Clean Energy and Clean Mobility via Resilient Microgrids: How Energy as a Service Business Models Foster Sustainability Solutions.

#4
How railways can protect themselves from cybersecurity risks

Will your railway stand up to the next cyberattack?

Cybersecurity attacks are a major threat to railways' safety and operations

Cybersecurity attacks can be devastating for railways and metro systems – financially and operationally – and they're increasing in number of attempts and severity. A study on cybercrime across industries found that attacks are up 67 percent in the last five years with the average cost of cybercrime around $13 million. In some cases, the goal is to disrupt critical infrastructure, while other attacks are financially motivated, such as ransomware, or to gain access to company or consumer data.

Cybercrime has risen around 67 percent in the past five years across 16 industries, including travel.

Accenture survey

There have already been cybersecurity breaches on railway and metros around the world, including in Denmark, Germany, New York City, and Spain. Even relatively minor attacks can be damaging and affect both railways and passengers. For example, it has taken Philadelphia's transit authority months to recover from a 2020 malware attack. The consequences included blocking employees' access to their email and preventing the metro system from sharing real-time information with passengers. A cyberattack on critical infrastructure can be particularly dangerous because it can cause safety issues, such as if digital signaling systems are affected in a breach.

That's because the modern technologies that make railways safe and reliable also make them a target

All areas of the railways' business are being digitized, including operations, infrastructure, systems, and technology. Digitization makes rail transportation safer, and more reliable, efficient, and sustainable, and improves passengers' experience. The downside is that digitization also introduces cybersecurity risks.

There has been a proliferation of cyberattacks on critical infrastructure and railways are vulnerable due a number of factors, including:

- It increases the number of connected devices being used, which also increases the amount of data being generated.
- There is a new level of interconnectedness, including connecting processes to the cloud, IT infrastructures, and third-party systems.
- Digital connectivity on rail transportation, such as Wi-Fi on board, enhances passengers' travel experience. However, connecting passengers to on-board technology can also lead to security breaches.
- Employees are responsible for an estimated 88 percent of cybersecurity breaches. These are usually caused inadvertently, such as using poor password protection or downloading a malware-infected attachment. The rise of bring your own device (BYOD) in the workplace also introduces new risks from employees.

However, railways can protect themselves by focusing on the three pillars of cybersecurity

With the right foresight, planning, and protection in place, railways' cybersecurity concerns are alleviated. That's because railways know they have the systems in place to prevent and stop an attack. This is possible by basing cybersecurity efforts around the IEC 62443 standard.

IEC 62443 provides a comprehensive framework for cybersecurity that addresses security from initial product development using a secure development lifecycle in which security in considered and evaluated throughout products' lifecycle. The standard offers a consistent, simplified way to define the level of cybersecurity management and is designed for the secure development of products used in industrial automation and control to provide a systematic set of cybersecurity recommendations.

Railways that base their cybersecurity plan on IEC 62443 take a "secure by design" approach. The efforts focus on these three pillars:

1. **People:** Railway employees know and follow good cybersecurity practices to protect assets and prevent breaches.
2. **Processes:** Railways benefit from a comprehensive set of best practices, processes, and procedures.
3. **Technology:** Railways' operations, assets, personnel, and passengers are protected by using cybersecure products and software and a cybersecure architecture.

Here's an example of how the three pillars improve cybersecurity

A railway control center is one example of how railways that focus on all three of these pillars can become more secure. Control centers are the foundation of railways' operations. They are the base for monitoring all train activity, directing and dispatching emergency responses, and coordinating services. Having all of these critical services in one place also makes them a prime target for a cybersecurity attack because an attack could have very serious consequences for safety and railway operations.

Railways can protect their control centers by ensuring employees follow recommended cybersecurity practices, controlling access privileges for workers who can physically or digitally access the center, and spreading awareness of the importance of cybersecurity. Railways manage processes by conducting risk analyses, testing and verifying security, and putting plans into place for preventing and recovering from a breach. And finally, railways use cybersecure technology to detect intrusions and protect from attacks and uphold system integrity.

It starts with employees because railway's cybersecurity is only as strong as its weakest link

Let's break this down for a closer look at each of the pillars. Cybersecurity is everyone's responsibility, and it begins with employees. Railways reduce the risk of an attack or data breach by actively involving staff in cybersecurity improvements and giving them ownership over keeping assets cybersecure. This includes mandatory, ongoing training in cybersecurity best practices as part of a company-wide security culture. Railways must create and enforce formalized standards and guidelines, including basic protocol like password regulations, multifactor identification, incident management actions, and user access controls.

Railways can solve the “people problem” by partnering with cybersecurity experts who provide individualized guidance and advice for boosting security. For examples, railways can gain access to end-user training and collaborative resources, as well as instruction on how to put these policies into place, including what to do in an event of a cyber incident.

Railways must also use established processes and clear procedures to help ensure cybersecurity

Railways must establish robust cybersecurity processes, policies, and clear procedures for addressing emerging vulnerabilities and ensuring railways’ security. This includes actions like making regular threat-risk assessments, implementing a strong patch management system, and conducting information security gap analyses.

Threat and risk analyses identify threats that apply to an operator, their impact, and the probability of these threats. Then railways can identify what level of cybersecurity must be met and define the way forward to reach it, taking into account the initial risk analysis.

By working with cybersecurity vendors to follow IEC 62443 best practices, railways know their information is secure and can have confidence that their processes and equipment are up to date and protected from unauthorized access, such as hackers accessing assets or control systems remotely.

Further peace-of-mind comes with the support of especially advanced vendors like Schneider Electric, who complete rigorous independent IEC 62443-3-3 Security Level 1 certification with TÜV.

Then there is an arsenal of technological tools to bolster railways’ cybersecurity

Using products, services, and solutions with built-in cybersecurity features brings end-to-end protection from cyberattacks. Assets are digitized safely using secure products and software that follow a certified process and a secure network architecture guided by IEC 62443 so products are protected through their entire lifecycle.

For example, a defense in-depth network infrastructure involves a multi-layer, multi-technology, and multi-party strategy taken from a system perspective. Thus, the critical parts of the network will be safe even if an attacker manages to access a part of the operation.

Learn how a railway in Southeast Asia boosted its cybersecurity while updating its power system

A leading rail and transport authority in Southeast Asia recently undertook a project to upgrade its power system and replace its power supply. The goal was to help ensure the traction power supply’s reliability and safety and reduce shutdown time while upgrading the existing system.

Cybersecurity was an important facet of the project because all solutions had to fully comply with the railway’s cybersecurity controls and requirements, as well as meet all government regulatory requirements. This customized solution required a resilient, standards-based strategy and approach.

For example, the railway strengthened its operational technology (OT) network with defense-in-depth strategies, such as ensuring that connected systems are patched close to any known vulnerabilities whenever possible. The strategy also included adding layered protection and practices across the digital system with a "zero trust" cybersecurity architecture in which users have only the necessary access to equipment and applications so that the railway can prevent unauthorized users and detect abnormal access.

Conclusion

It's clear that public transportation use will continue to grow in the coming years. To meet this need, operators must focus on using digital technology to provide efficient, reliable, sustainable, and cybersecure transportation. The technology ensures infrastructure is efficient and sustainable while also contributing to a better passenger experience and a greener society.

About the author

Valerie Layan was appointed as Transportation Segment President in September 2018. She is responsible for developing the transportation market for Schneider Electric globally. The transportation segment focuses on the infrastructure of airports, railways and public urban transportation, as well as ports and roads. Addressing key challenges from urbanization, sustainability and building smarter cities, Valerie is responsible for Schneider Electric's global strategic customers, delivering unique customer value and solutions to address their needs – supporting both End Users as well as value chain players. Prior to taking this position in the company, Valerie held several roles in the Digital Energy Division, as Line of Business Vice President. Previously Valerie worked 20+ years in the Colo and Telco Industry at Nortel, Nokia and Colt. She has brought this in-depth and long-standing experience and knowledge of End-to-End Digitized & Cloud based Solutions to Schneider Electric. She graduated from the Institut Polytechnique de Lorraine and London Business School.