RAIL AND TRANSIT

ENTERPRISE SECURITY STRATEGIES

Securing rail and mass transit in an era of converging threats

accentureconsulting

Digitization is transforming rail and transit from its historic dependence on manual mechanics and human operators to a modern industry that's now partially automated and increasingly interconnected.

While successive waves of technology create immense benefits and new opportunities for owners and operators to transform their services, the speed of change and sheer complexity of rail and transit makes it one of the most challenging critical infrastructures to secure.

Specifically, the rapid convergence of operational technology (OT), information technology (IT) and the "Internet of Things" (IoT) across its highly-dispersed infrastructure is creating potential new vulnerabilities which expose rail and transit networks to new risks, ranging from cyber-attacks to circumstantial accident risk.

FOR THESE REASONS, SECURITY STRATEGIES MUST EVOLVE. FAST.

TECHNOLOGY CONVERGENCE AT SPEED AND SCALE

Changing business models, cost pressures, aging assets and ever-increasing regulation are driving an irreversible convergence of core technologies within the modern rail infrastructure, enabling greater efficiencies, repeatability, scalability of operations at the front end, as well as smarter backoffice functions, cloud adoption and enhanced customer services.

Convergence also allows operators to harness drones and other autonomous or unmanned vehicles, biometric and other sensors, artificial intelligence (AI), robotic process automation (RPA), advanced video analytics and other innovations to optimize operations across their physical networks, assets and infrastructure.

When we talk about convergence in critical rail infrastructure, we're primarily focused here on three increasingly interconnected domains:

Information Technology (IT)	**Operational Technology (OT)**	**Internet of Things (IoT)/Industrial Internet of Things (IIoT)**
Encompassing core business IT systems used to run rail and transit functions, management and processes.	Being rapidly deployed to control physical rail network operations and (typically aging) assets such as refueling systems, signals and switches.	A growing network of "smart" physical objects, products, sensors and devices for data capture, monitoring and remote control.

Globally, rail and transit is witnessing increasing automation of services and operations across these IT, OT and IoT/IIoT domains, as well as in supervisory control and data acquisition (SCADA) systems and related industrial control systems (ICS). Each technology system has distinct security requirements, protocols and characteristics. But any ecosystem is only as secure as its weakest link, so when they converge, a weakness in one domain or at the point of intersection can impact the security posture of the entire connected infrastructure, even when highly dispersed and oftentimes siloed.

NEW RISKS TO RAIL INFRASTRUCTURE

In the increasingly crowded, complex rail and transit technology environment, security risks are evolving at pace. Security in the digital realm (IT/OT/IoT) is converging rapidly with security in the physical realm, creating greater vulnerabilities, dependencies and threats which can allow circumstantial accident risk to go undetected and malicious activity to be more easily hidden or disguised, with indicators of compromise harder to identify.

Across industries globally, attacks on critical infrastructure—increasingly led or supported by cyber-attacks—are increasing year on year, while also becoming more sophisticated. Transportation makes an attractive target because of the possible large-scale consequences. The late-2018 disruptions at London Gatwick Airport caused by drones are a stark demonstration of how new technologies can cause such disruptions at low cost and with increased challenges in identifying perpetrators. As a result, rail and transit operators must be fully prepared to secure themselves holistically and reduce the security risk to their assets, people and passengers from both physical and cyber-threats. Potential vulnerabilities must be identified and understood—especially where they straddle these two domains—with the right controls in place to mitigate risk, whatever the source.

A clear example of this is the evolution of the technologies and processes that support rail and transit operations. Where rail networks once relied on people to read and respond to human-controlled signals, trains and network operations are increasingly reliant on interconnected devices "talking" to each other to run these operations. To assure these operations today, it's therefore essential to secure every digital asset and its potential connections both to other digital devices and to the infrastructure and assets it helps to run.

Take, for example, positive train control (PTC) systems. These are designed to automatically stop a train before certain accidents occur, to prevent train-to-train collisions and to avoid derailments due to excessive speed and train movements through misaligned track switches. Because they depend on connected devices transmitting data to/from the vehicle for monitoring and operating conditions, there could be dramatic consequences if any aspect of the system was compromised—whether accidentally or via a hack attack.

Trains are also increasingly dependent at one end on bulletins from the dispatch system to indicate speed limits and construction zones for example, and at the other on the signal and switch status from wayside data communication. This involves increasingly connected signals at wayside points across the network to implement automatic train protection systems. Extreme vigilance is required to ensure at all times the integrity of the software both on the dispatch side and in the locomotive; in the communication layers (e.g. radio, cells, WiFi) between the train and the dispatch; between the train and the wayside; and between the train and the server, without fail.

In research by the Ponemon Institute, **66 percent** of respondents said digitization has made their critical infrastructure more vulnerable to security compromises, and about **68 percent had lost confidential information** or experienced disruption of their operations in the previous year.[1]

WHAT OBSTACLES MUST BE OVERCOME?

DIFFERENCES BETWEEN DOMAINS

Currently, the key principles for safeguarding all IT/OT/IoT domains are based on established IT security thinking. Yet entire networks of interconnected machines exist in the OT domain, often using proprietary or non-IP protocols to communicate with each other. The fact is, OT and IoT devices present different types of risk, and simply extending established security models to include the OT and IoT domains exposes the rail infrastructure to new cross-domain risks. Although conventional IT security thinking is relatively mature, it only extends from cloud through to connected IT devices (mobile or fixed). Unfortunately, this model breaks down for OT and IoT devices, which can't be regarded as "just another end point" to be managed: they require a different approach.

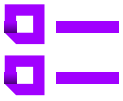
The differing operational requirements of OT and IT systems impact their ability to respond and adapt to these threats.

OPERATIONAL TECHNOLOGY DOMAIN (OT)		BUSINESS PROCESS DOMAIN (IT)
Limited data capacity and computing power	⟷	High data capacity and computing power
Safety operations are critical	⟷	Few safety critical operations
High availability and integrity are vital with less stringent confidentiality requirements	⟷	Confidentiality and integrity are vital while availability is important
Critical operations and systems at edge of network with human operators at the center	⟷	Critical operations and systems at center of network, human users at edge
Long lifecycle resulting in unsupported legacy infrastructure	⟷	Continuous equipment upgrade with short lifecycles
Essential equipment and operations remotely deployed at edge of network	⟷	Essential equipment and operations concentrated at center of network
Slow response to threats—rapid patching might be impossible due to outages	⟷	Rapid response to threats, patching and reboots acceptable

INSECURE SYSTEMS AND DEVICES

Convergence is greatly multiplying the number of potentially vulnerable connections across the critical rail infrastructure. The presence of IoT and IIoT devices continues to grow across all rail and transit operations—sometimes as a bolt-on to OT—with sensors proliferating across vehicles, platforms, physical infrastructure, signaling, switching and staff. Many of the OT and IoT tools being implemented require specialized knowledge and expertise; this then impacts on the ability of those charged with security and risk reduction to effectively understand what is happening in those tools and consequently identify anomalies or nefarious activities. Added to this, because OT and IoT devices typically lack built-in security, they both have inherent vulnerabilities. If given an IP address, each IoT device could create a new unsecured access point into the organization's IT networks, introducing new threats and challenges.

Also, as more OT and IoT devices become IP-enabled, more machine data will be generated and transmitted for central monitoring and analysis across the network. And with IT increasingly connected with OT, hack attacks are being seen which move across this connection in both directions, sometimes to access data, sometimes to access control systems. Security measures must also extend to IoT-enabled devices used by the public, including their mobile devices and the internet connections these make to networks housed in rail and transit infrastructure and provided as a public service.



In an Accenture survey of **1,400+ C-suite executives**, including chief information security officers, IoT topped the list of technologies expected to raise cyber-risk as it is more widely adopted, with **77 percent saying it will increase cyber-risk** moderately or significantly.[2]

LIMITED RISK VISIBILITY ACROSS A COMPLEX, DISPERSED NETWORK

Traditional IT security approaches have limited touchpoints with physical systems, OT environments, and the IoT realm. At the same time, rail and transit infrastructure is highly-dispersed both geographically and administratively. In many other industries—including in other modes of transportation such as aviation—the infrastructure is concentrated locally. In rail and transit, several thousand kilometres of track, stations, and supporting infrastructure plus thousands of rolling-stock assets need to stay secure.

It can thus be difficult to view, monitor and analyze data moving across and between the different technology domains, as well as to identify where risks arise and are pinpointed across this vast infrastructure. And the old data collection parameters of some OT means it can't be relied on to provide an adequate monitoring feed, thus creating blind spots across the critical rail infrastructure.

This will become ever more complex. The introduction of autonomous vehicles and the increasing automation of operational functions will further remove human interactions with IT/OT/IoT, increasing reliance on non-human monitoring of all systems and their interconnectivity to detect anomalies or suspicious activities. In this sense, another emerging risk is drone or UAV hacking, which will also need to be considered within the overall security mix.

The increasing **convergence of IT and OT service providers**, which Gartner predicts **will reach 50 percent by 2020**, has exposed the OT environment to greater security threats that current cybersecurity practices do not seem fully prepared to meet.[3]

THE AIR GAP ILLUSION

There is a common misconception, the "air gap myth", that if there is no physical or wireless connection between OT equipment and any external IT network, that it is then protected from remote attack.

However, as vividly evidenced in the Stuxnet attacks, this isn't true. In these attacks, over 1,000 uranium enrichment centrifuges were destroyed by a sophisticated self-replicating virus thought to have been carried into the site on an infected USB pen drive and infected laptops. Insecure rail infrastructure could be vulnerable in the same way.

Both connected and air gapped systems need robust security systems that seamlessly cover all layers of the **Purdue** stack[4], with strong cyber and intrusion defenses to ensure the air gap can't be bridged by employee and contractor devices or infected equipment/malware moving from one domain to another.

The **Purdue Enterprise Reference Architecture** (commonly known as the Purdue Model or Stack) is a commonly used **architectural reference model for control systems**. It contains five levels:

LEVEL 4 addresses **business logistics systems**

LEVEL 3 addresses the **manufacturing operations systems**

LEVEL 2 addresses the **control systems**

LEVEL 1 addresses **intelligent devices**

LEVEL 0 addresses the **physical processes**

SECURITY SILOS

The failure to take a joined-up security approach will create even greater vulnerabilities at the edges and intersections between the different security domains. Many areas of security, safety and risk still operate in fragmented silos, both across the IT/OT/IoT domains and also across business groups who "own" different dimensions of each (e.g. rail operations versus IT operations versus cybersecurity versus safety and security). Added to this, data sourced from disparate technologies isn't typically being viewed holistically through "a single pane of glass", which would provide a complete view of what is happening across an entire infrastructure.

As such, there's a growing risk that threats emerging in one silo, such as IT operations, won't be recognized and correlated with those in another silo, say, OT operations—all made more complex by the highly-dispersed infrastructure already noted. Another concern is that data will be assessed based on its origin, whether a computer network or web traffic, without correlating it with all available security-related data, including public video, CCTV and access control sources.

Then there's the risk of duplicating security tasks rather than adopting a coherent approach that drives new efficiencies by introducing innovations in AI and RPA to screen all security-related data across the entire enterprise, using human operators only for the most crucial decisions.

In a survey of IT, ICS, and SCADA security practitioners by the SANS Institute, **69 percent considered threats** to ICS systems to be high or severe, and **44 percent considered unsecured** IIoT devices added to the network to be the top threat vector.[5]

TARGET THE NEW HIGH-RISK HOT-SPOTS

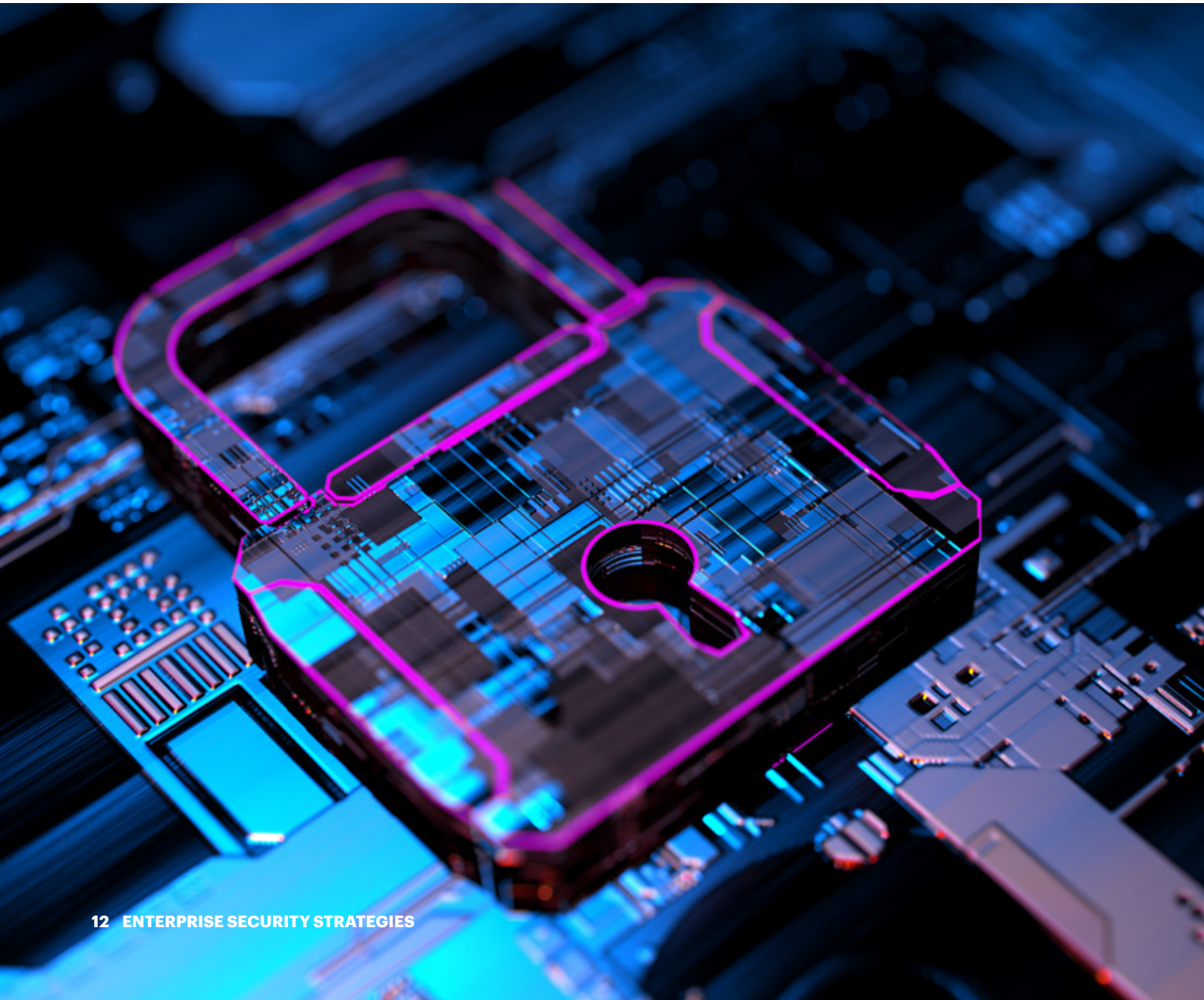
The impact of convergence will increasingly give rise to specific scenarios that could expose rail and transit owners and operators to greater security risk. A spectrum of examples include:

- When each of the IT, OT and IoT domains is **owned and managed by the operator**—and managing the security risk is mostly within their own control.
- When the OT and IoT is **owned and managed by a third party and the operator has to rely on them to manage security**—often with insufficient control, insight and understanding of how it is done and the potential risk implications.
- In parallel with this, there's a growing risk from IT and OT **owned and operated by third-party vendors**, such as food and beverage retailers, **operating in the same physical environment and connecting to the same IP networks as the rail operator**.
- When smartphones and other IoT devices are **brought into the operator's environment and connected to it**, via public WiFi.
- When **high volumes of connected IoT micro-devices are deployed in geographically disparate parts of the physical infrastructure**—such as across a national or trans-border rail network—to monitor variables like traffic patterns, load-bearing, weather and topography conditions.
- When having to handle the **massive rise in IP traffic due to the extra volumes and varied complexities of IT/OT/IoT data** that will be generated by connecting all devices across the entire network—then holistically monitoring that same data via a "single pane of glass" to identify potential anomalies.

ADOPT A HOLISTIC APPROACH FOR DEFENSE IN DEPTH

For all of these reasons, rail and transit present a different set of security risk challenges to other large complex infrastructures. While many lessons can be drawn from other industries (e.g. the live monitoring for security risks of the complex equipment required for massive automated mining operations) to support rail and transit, ultimately solutions must be tailored to the specific characteristics of the industry.

To be effective in an increasingly interconnected and automated world, rail and transit security must be managed as an end-to-end holistic process and offer multi-layered defence, spanning conventional IT plus the growing OT and IoT/IIoT security risk domains, while recognizing the distinct characteristics of each.

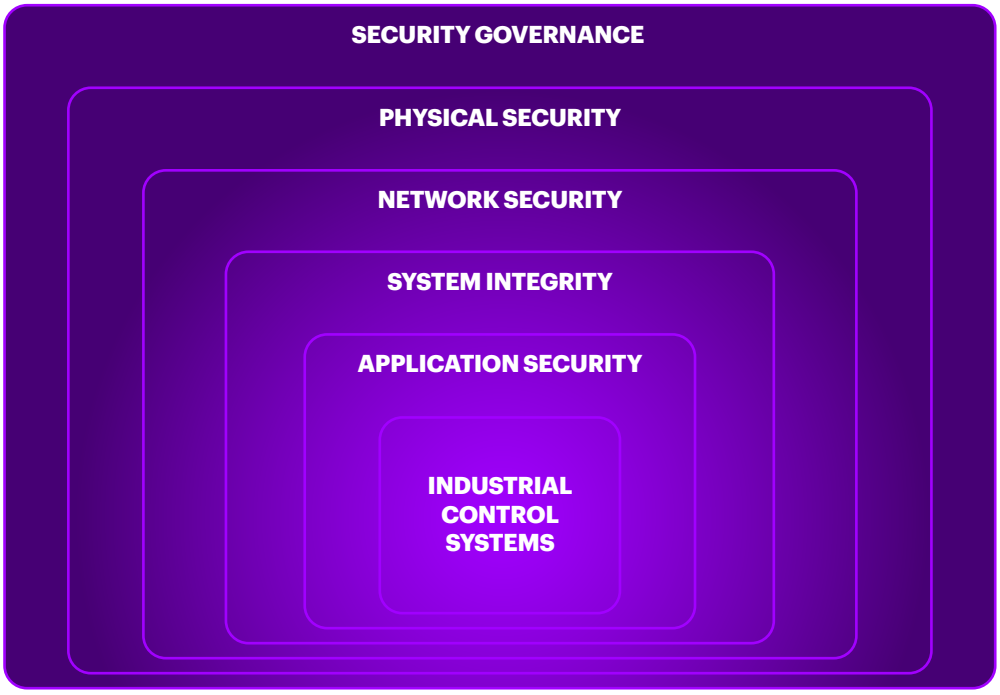


SEVEN STEPS TO STRENGTHEN SECURITY

1. CREATE DEFENSE IN DEPTH
2. ADDRESS RISK HOLISTICALLY
3. INCIDENT RESPONSE PREPAREDNESS
4. SECURE CROSS-DOMAIN CONNECTIVITY AND DISPERSED INFRASTRUCTURE
5. COORDINATE ACCESS CONTROL
6. EMBRACE AI AND RPA
7. FUTUREPROOF NEW CAPABILITIES

1 CREATE DEFENSE IN DEPTH

Adopt a multi-layered strategy laterally and vertically across the entire new technology stack/network. Multiple levels of digital defense and monitoring will detect risks before they become critical and hinder malicious attacks, increasing the probability of preventing an incident.



2 ADDRESS RISK HOLISTICALLY

Ensure that your enterprise security architecture addresses security risks holistically across the entire stack/network—including IT, OT, IoT/IIoT monitoring and the physical dimensions of technology solutions, from device-level authentication to system-wide resiliency models.

INCIDENT RESPONSE PREPAREDNESS

Introduce security incident and event management (SIEM) capabilities across the entire rail and transit enterprise with real-time visibility of all security-relevant data–IT/OT/IoT, audio and video, open-source and web-based—to provide the clearly actionable intelligence that command and control teams need to respond fast.

Test and practice incident response plans on a regular basis to ensure you continue to be prepared and keep evolving your capabilities.

SECURE CROSS-DOMAIN CONNECTIVITY AND DISPERSED INFRASTRUCTURE

Review all connections between IT and OT to ensure any data connections between the two are risk assessed, secured and plugged into the monitoring capabilities. Similarly, review all connections between IoT devices and OT to ensure the same, including the overall security of each IoT device. And across widely-dispersed infrastructure and assets—especially given that many rail networks cross national borders. Build security into these directly through connected sensors and similar monitoring means to provide the full situation awareness needed.

COORDINATE ACCESS CONTROL

Deploy new capabilities to seamlessly integrate stringent physical and digital identity and access controls across the infrastructure—and the systems that monitor both—to prevent unauthorized access and ensure that anomalies can be identified and acted upon immediately.

EMBRACE AI AND RPA

Take advantage of rapid advances in AI, machine learning and RPA to create smarter ways to improve risk monitoring and management across the whole enterprise, helping to identify, verify and validate actors, activities and incidents more effectively and efficiently.

FUTUREPROOF NEW CAPABILITIES

Put security and risk mitigation at the forefront when introducing new technology capabilities to the rail and transit network, from monitoring vehicles, passengers and infrastructure to adding new interactivity to noticeboards, public WiFi networks, passenger apps and ticket vending machines.

ENSURE CONTINUITY WITHOUT COMPROMISE

In a fast-changing environment, "staying secure" is a relative concept and constant awareness of new risks will always be required. As we've seen, IT/OT/IoT technology convergence is taking the complexity of rail and transit security to a new level that simply cannot be ignored.

It's vital to maintain a clear focus on the business context and understand that more than ever, security isn't simply a technology problem, it's a commercial imperative. But with the right approach, you can stay constantly prepared to keep your rail and transit networks moving and your business running smoothly.

TRAVEL WITH A TRUSTED RAIL SECURITY PARTNER

Accenture delivers advanced security solutions and managed security services to safeguard every aspect of large, complex rail and transit critical infrastructures.

Building on our in-depth technical expertise and broad industry experience in IT, OT and IoT/IIoT and their convergence, we take a holistic, comprehensive approach to security, addressing requirements, technologies, processes and human factors.

Over the last decade, we have built world-leading practices in OT/ICS security and in IoT/IIoT security—supporting clients worldwide in reducing security risks on everything from the smallest IoT sensor to the largest, complex industrial operations. We also provide managed security services, security monitoring, and risk reduction solutions to thousands of critical infrastructure clients in every industry—including rail and transit operators in North America, Europe, the Middle East and Asia.

To support these and our security offerings, we have global alliances with world-leading vendors specializing in AI, RPA, incident management, identity and access management, endpoint protection, analytics, IoT and advanced threat-hunting. And we are constantly innovating via our Cyber Labs to outpace emerging threats, not just on devices but the network connectivity and applications they support. Putting these into play, we can help you identify and address potential security concerns as soon as they arise, regardless of their type and origin, helping you to minimize exposure to risk and vulnerability, across your entire network.

ARE YOU READY TO **STEP UP SECURITY** FOR AN INTER-CONNECTED WORLD?

EVERY JOURNEY STARTS WITH A SINGLE STEP

Find out more about taking it with Accenture.

www.linkedin.com/showcase/accenture-industrial/

@AccentureInd

CONTACTS

ALDEN CUDDIHEY
Rail and Transit Global
alden.cuddihey@accenture.com

MICHAEL ENGLISH
Rail and Transit NA
michael.english@accenture.com

PIERRE-OLIVIER DESMURS
Rail and Transit EALA
p-olivier.desmurs@accenture.com

KEVIN O'BRIEN
Security NA
kevin.obrien@accenture.com

CLAUDIO BACALHAU
Rail and Transit AAPAC
claudio.bacalhau@accenture.com

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 469,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

REFERENCES

1 https://www.accenture.com/t20180803T064557Z__w__/us-en/_acnmedia/PDF-83/Accenture-Cyber-Threatscape-Report-2018.pdf, page 34 and footnote 35.

2 https://www.accenture.com/us-en/insights/security/securing-future-enterprise-today

3 https://www.accenture.com/t20180803T064557Z__w__/us-en/_acnmedia/PDF-83/Accenture-Cyber-Threatscape-Report-2018.pdf, page 34

4 http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.194.6112&rep=rep1&type=pdf

5 Gregory-Brown, Bengt. "Securing Industrial Control Systems-2017." June 2017. SANS. https://www.sans.org/reading-room/whitepapers/analyst/securing-industrial-control-systems-2017-37860