WHY DEPARTMENTS OF TRANSPORTATION NEED TO PRIORITIZE CYBERSECURITY

Securing **intelligent transportation systems**

siemens.com/communications-for-its

Table of contents

Imagine this: Every public transportation toll booth in your city inexplicably starts offering passengers free rides, resulting in half a million dollars in lost revenue before you can even figure out what happened.

You’ve been hacked.

The rising risk of cybercrime and lack of security infrastructure in traffic control systems pose a growing threat to our communities’ transportation management and safety. Municipalities must protect and safeguard their IT and OT systems to minimize and combat cybercrime. Intelligent Transportation Systems (ITS) aim to minimize risks and make traffic control systems more secure, reliable and efficient.

Managing risk in transportation infrastructure

As global populations grow, so will the number of vehicles on roads — leading to increased traffic congestion, longer commutes and an even greater demand for ITS.

Coordinating traffic and staying on top of its streams is a complex and demanding task for transportation system operators everywhere. Monitoring and managing increasingly complex transportation infrastructure requires reliable and secure network communications.

Effective traffic management demands knowing what is happening and where. Some examples include:

- Tracking buses on their routes
- Locating and addressing stalled vehicles
- Notifying drivers of important road and traffic conditions

In inter-urban areas, communications networks are geographically dispersed, covering hundreds of miles of roadway. Operators must ensure that there is significant bandwidth to connect thousands of devices and support hundreds of real-time video feeds, along with data gathered from roadway sensors.

To protect public safety, network subsystems must be able to detect incidents early, maximize operational uptime, and interact seamlessly.

Protecting **against hackers**

Hacking traffic control systems can be unnervingly easy. Current security measures are not as fortified as they should be, and hackers can inflict a lot of damage with just a little effort. In 2020, Dutch security researchers exploited into a vulnerability that **allowed them to manipulate traffic lights**. Their specific hack would create the appearance of a bicycle approaching a signal, causing a needless red light for cars. While that may be only a minor annoyance, it's not hard to imagine alterations which could result in unsafe conditions for all.

> "
> Now that we're talking about building these intelligent transport systems, we need to be ... sure to think more about security."
>
> – Rik van Duijn, security researcher

Hacking traffic systems can be done in various ways and for different reasons. In 2016, a 26-year-old **hacker from Texas** was arrested for reprogramming and defacing a highway sign with an inappropriate message, which could have distracted drivers and caused life-threatening accidents.

More gravely, a **Polish teenager hacked** into his local tram network, unleashing chaos and derailing four vehicles. More than 10 people were injured in the incident as the 14-year-old played with his life-sized train set. Both these instances highlight the need for protection in traffic control systems, as these infrastructures are far too vulnerable to security breaches, even from non-professionals.

A security breach could cost a Department of Transportation (DOT) millions of dollars. A **ransomware attack on the San Francisco public transport system** infected over 2,000 Municipal Transportation Agency computers, encrypting their data and operating systems, forcing the agency to open the fare gates and allow passengers free rides. It was estimated that the agency lost approximately $559,000 each day from uncollected fares.

More recently, a cable car system in Moscow was **hit by a ransomware attack** just two days after launch in 2018.
The attack forced systems to shut down to prevent damages and casualties. The incident triggered a costly security audit to clean systems from the infected software.

> "
>
> Most of these systems are automated, especially as far as security is concerned... They're automated and they're remotely controlled, either over the internet or otherwise, so they're vulnerable to cyberattacks."
>
> – Oren David, cybersecurity specialist

Embracing **cybersecurity**

While there are many advantages to operating in an increasingly connected environment, the risk of cybercrimes grows along with the rate of digitalization, posing a progressively more serious threat to the public. Apart from threatening data and operations, **cyberattacks can put peoples' lives at risk**. Comprehensive cybersecurity programs are paramount for all organizations, especially for DOTs.

Protecting the mix of technology and systems in ITS requires a wide range of technical and operational solutions. Although highly secured IT systems cannot guarantee absolute safety, low levels of IT security increase the risks of critical incidents, such as outages of traffic signal systems. The potential points of attack multiply with increased digitalization and rising complexity of transport infrastructure systems. These can include data exchanges between control centers, poorly secured facilities for remote maintenance, and the combination of IT components of different life expectancies.

> "A cyberattack or threat could affect everything from municipal transportation, to high-speed transit rail that operates between cities… It could create crashes or chaos on the highways or even on city streets."
>
> – Srini Subramanian, cybersecurity principal, Deloitte & Touche

Why **penetration testing?**

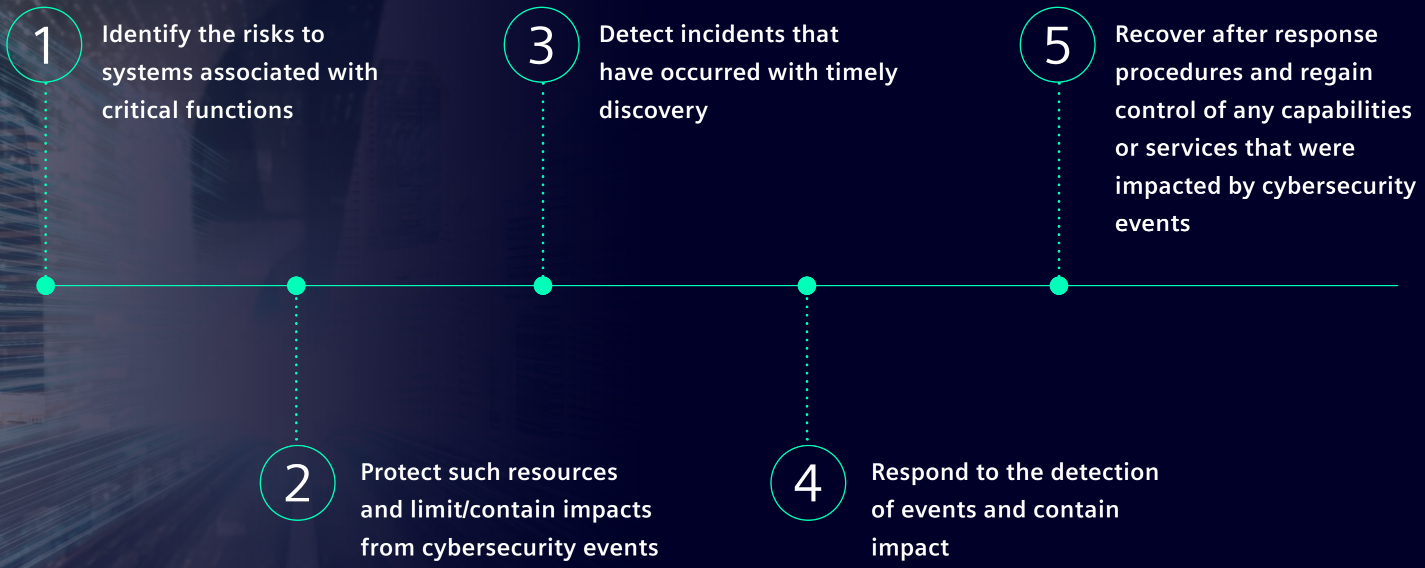
Penetration testing is one of the Center for Internet Security's (CIS) **Top 18 critical security controls for effective cyber defense**. It is also included in the program security activities from the **National Institute of Standards and Technology** (NIST) "Technical Guide to Information Security Testing and Assessment". **The Cybersecurity Framework** (CSF), created through collaborations involving governments, academia and the private sector, aims to provide guidelines to establish new cybersecurity programs and fortify existing frameworks. The CSF mechanisms urge organizations such as a DOT to do the following:

- **Describe their current cybersecurity posture**
- **Describe their target state for cybersecurity**
- **Identify and prioritize opportunities for improvement**
- **Assess progress toward the target state**
- **Communicate cybersecurity risk among internal and external stakeholders**

Managing risk in transportation infrastructure
Protecting against hackers
Embracing cybersecurity
Fortifying cybersecurity for ITS
Identifying risks within the environment
Implementing an end-to-end approach
Threat detection
Future-proofing your network
Case studies
RUGGEDCOM for ITS
Bridge and digital tunnel communications systems
Your end-to-end solution

Core functions of cybersecurity

The **Framework** focuses on five core functions needed to enhance an ample cybersecurity program:



1 **Identify the risks to systems associated with critical functions**

2 **Protect such resources and limit/contain impacts from cybersecurity events**

3 **Detect incidents that have occurred with timely discovery**

4 **Respond to the detection of events and contain impact**

5 **Recover after response procedures and regain control of any capabilities or services that were impacted by cybersecurity events**

Penetration testing helps provide indicators for cybersecurity event probabilities, highlighting vulnerabilities and the efficacy of current defenses. Furthermore, penetration testing helps identify potential impacts on systems and services, allowing organizations such as DOTs to prepare contingency plans in case of an attack.

Managing risk in transportation infrastructure

Protecting against hackers

Embracing cybersecurity

Fortifying cybersecurity for ITS

Identifying risks within the environment

Implementing an end-to-end approach

Threat detection

Future-proofing your network

Case studies

RUGGEDCOM for ITS

Bridge and digital tunnel communications systems

Your end-to-end solution

Fortifying **cybersecurity for ITS**

As cities and municipalities continue to transition toward digitalization and automation, **transportation systems become increasingly susceptible to cyberattacks.**

ITS aims to help coordinate road traffic, making transport safer and more efficient. Yet transportation management systems, like all systems, are subject to risks that might harm software, hardware, or data security from such devices and networks. Digital networks, with their inherent system complexity, demand comprehensive IT and OT cybersecurity measures to safeguard their infrastructures and the society they impact.

A fundamental element of an effective cybersecurity program is the focus on security by design. As a result, ITS systems are built with security features at the forefront that help save time and resources, minimizing risks and reducing costs during an effective cyberattack.

With a cybersecurity-centered program, organizations avoid the chaotic and expensive replacement of a component, or a network outage.

> "Digitalization can indisputably contribute to making rail transport safer, more efficient and more convenient for both passengers and freight, but it also exposes systems to cybersecurity risks. ... Indeed, we must be aware that cyber threats are as versatile and dynamic as the digital world and its applications."
>
> – Tommaso Spanevello, UNIFE (The European Rail Industry

Identifying risks within the environment

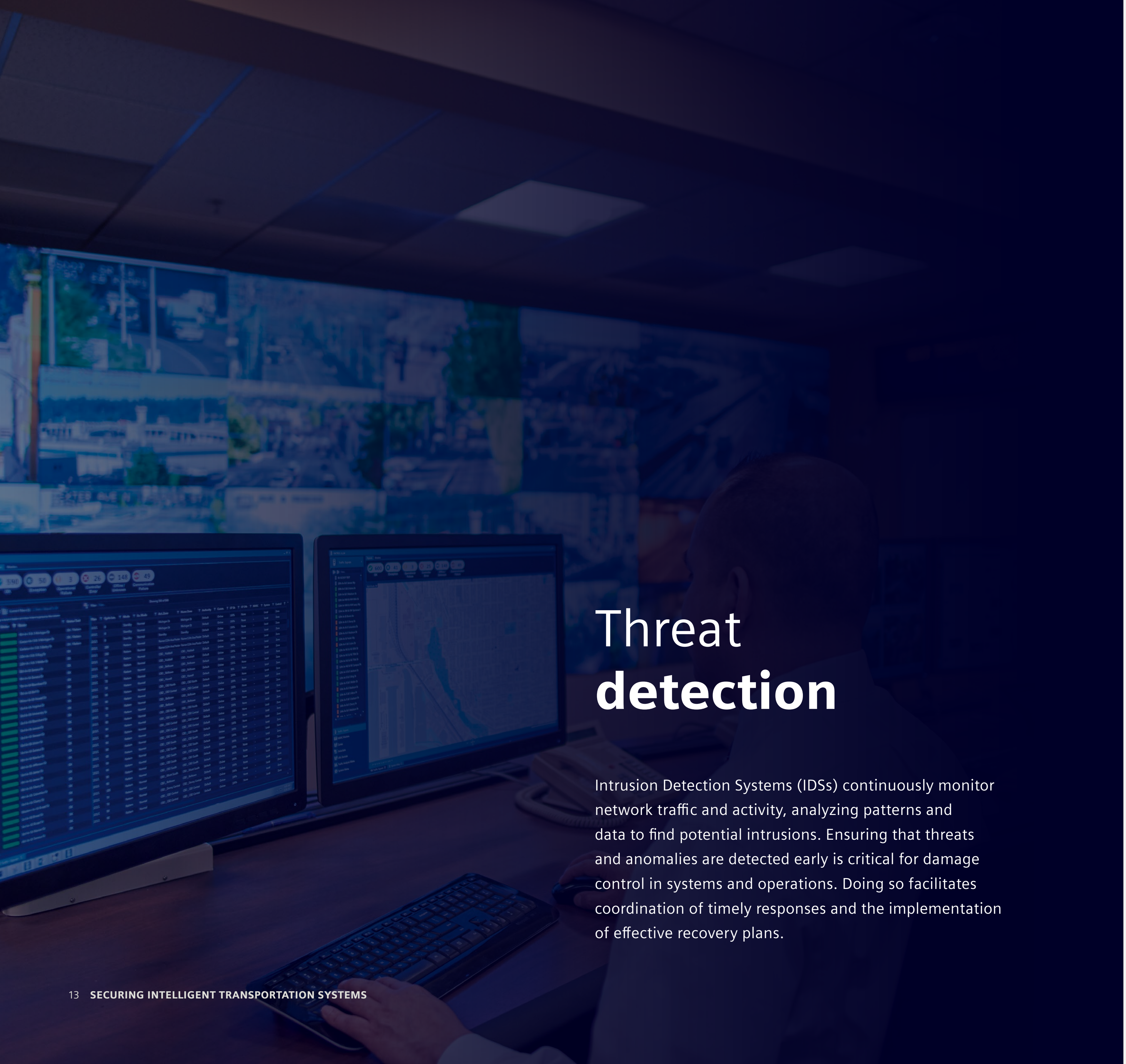
Continuous security testing is a prerequisite for cybersecurity. According to **SonicWall**, over 268,000 new malware variants were detected in 2020, a 74% increase from 2019. Furthermore, in 2020, ransomware incidents rose by 62%, and Internet of Things (IoT) malware incidents increased by 66%, **for a total of 56.9 million attacks against IoT devices**. Penetration testing is paramount for system security as new threat vectors emerge by the day.

It is not a matter of if you will be hacked; it is a matter of when and if you will be ready.

Implementing an **end-to-end approach environment**

Intelligent solutions for traffic networks require holistic security measures that begin in the planning phase and continue well after ITS implementation. A "defense in depth" strategy demands a multilayered security approach, covering all system infrastructure aspects for strengthened and fool-proofed cybersecurity solutions.

Communicating securely without compromising access or allowing unauthorized intrusion is a key challenge. Doing so demands continuous monitoring of all interfaces, such as those between offices and OT networks, or remote maintenance access points.



Threat **detection**

Intrusion Detection Systems (IDSs) continuously monitor network traffic and activity, analyzing patterns and data to find potential intrusions. Ensuring that threats and anomalies are detected early is critical for damage control in systems and operations. Doing so facilitates coordination of timely responses and the implementation of effective recovery plans.

Future-proofing your network

Cities can realize the full benefits of digitalization only when they face the reality that greater connectivity leads to unprecedented vulnerabilities. Future-proofing your network is critical for both ensuring public safety and driving economic growth. A future-proof network is designed from end to end with cybersecurity in mind. This approach includes the automation of cybersecurity monitoring and control so that cybersecurity is intrinsic to every part of OT operations.

Zero-day vulnerabilities

Traditional cybersecurity measures look for known vulnerabilities and provide updates or signature files to detect them. They do not address zero-day vulnerabilities – those vulnerabilities that have compromised a system but haven't yet been detected or identified. A future-proof network is capable of handling these threats proactively by envisioning and enacting Cybersecurity by Design and fostering a culture that actively enables evolving end-to-end solutions. True cybersecurity is a journey, not a destination.

> "There are two types of companies in the world: Those that know they've been hacked, and those that don't."
>
> – Misha Glenny, cybersecurity expert

Case **studies**

Stamford ITS **shortens commutes**

With an intelligent transportation system, **Stamford, Connecticut**, has put itself in position to master and overcome both current and future challenges in the transportation sector. Stamford, which is less than 40 miles from Manhattan, has a population of 130,000 and is the fastest-growing municipality in the state.

Stamford recently invested in its own ITS, relying on an advanced communications network to optimize traffic signals at the city's 200-plus intersections. Like many American cities, Stamford had previously relied on an outdated traffic system. The old system lacked remote access for monitoring and controlling, and low data speeds and bandwidth limited its functionality.

The project has **significantly shortened travel times** during morning commutes on what previously were highly congested roadways during rush hours. **Transportation Bureau Chief Jim Travers** explains that the new ITS system helps all users on the roads, including cyclists and pedestrians. Accidents have declined, along with the rates of severe injuries and pedestrian deaths. Stamford's roads are both less congested and safer for everyone.

> "Transportation plays a big role in the local economy and quality of life because of our own needs in Stamford, our inter-city and inter-state needs, and our proximity to New York City. So we had to design and build a new IP-based network to achieve any meaningful transfer of data for a reliable, forward-looking ITS."
>
> – Veera Karukonda,
> signal systems engineer for Stamford.

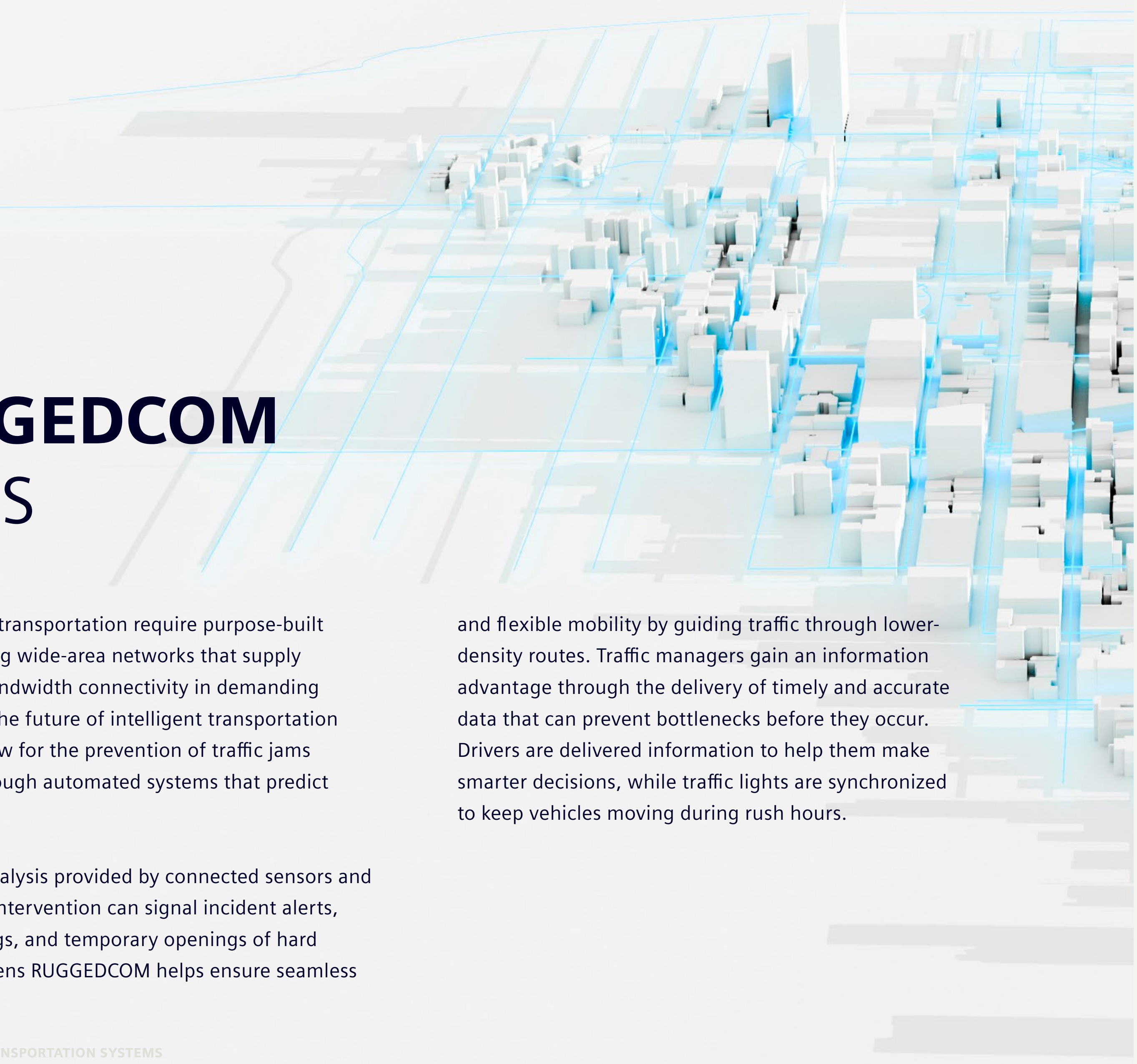
Stamford transitioned from an unreliable, low visibility, manually operated traffic signal network, to a secure, efficient, state-of-the-art network with remote monitoring and control. This restructuring enables secure remote access for monitoring and control by Stamford's traffic signal engineers at the city's operations center, which created a significant improvement in operational efficiencies.

Modernizing **rugged Clark County's infrastructure**

Clark County, Washington connects 425,000 residents across urban, suburban and rural terrain, stretching from coastal floodplains to foothill elevations higher than 4,000 feet. With harsh weather conditions and double-digit population growth booms, their ancient network desperately needed modernizing. But the sprawling nature of the coverage area coupled with budget constraints meant upgrading traffic corridors one-by-one. The county realized it needed not just a product, but a partner to help implement a management software solution and provide ongoing product and service support for its entire system.

> "We needed a rock-solid communications network to be able to generate, retrieve and use traffic management data — even if we didn't yet know what that data was going to be."
>
> – Rob Klug, traffic signals manager, Clark County Public Works

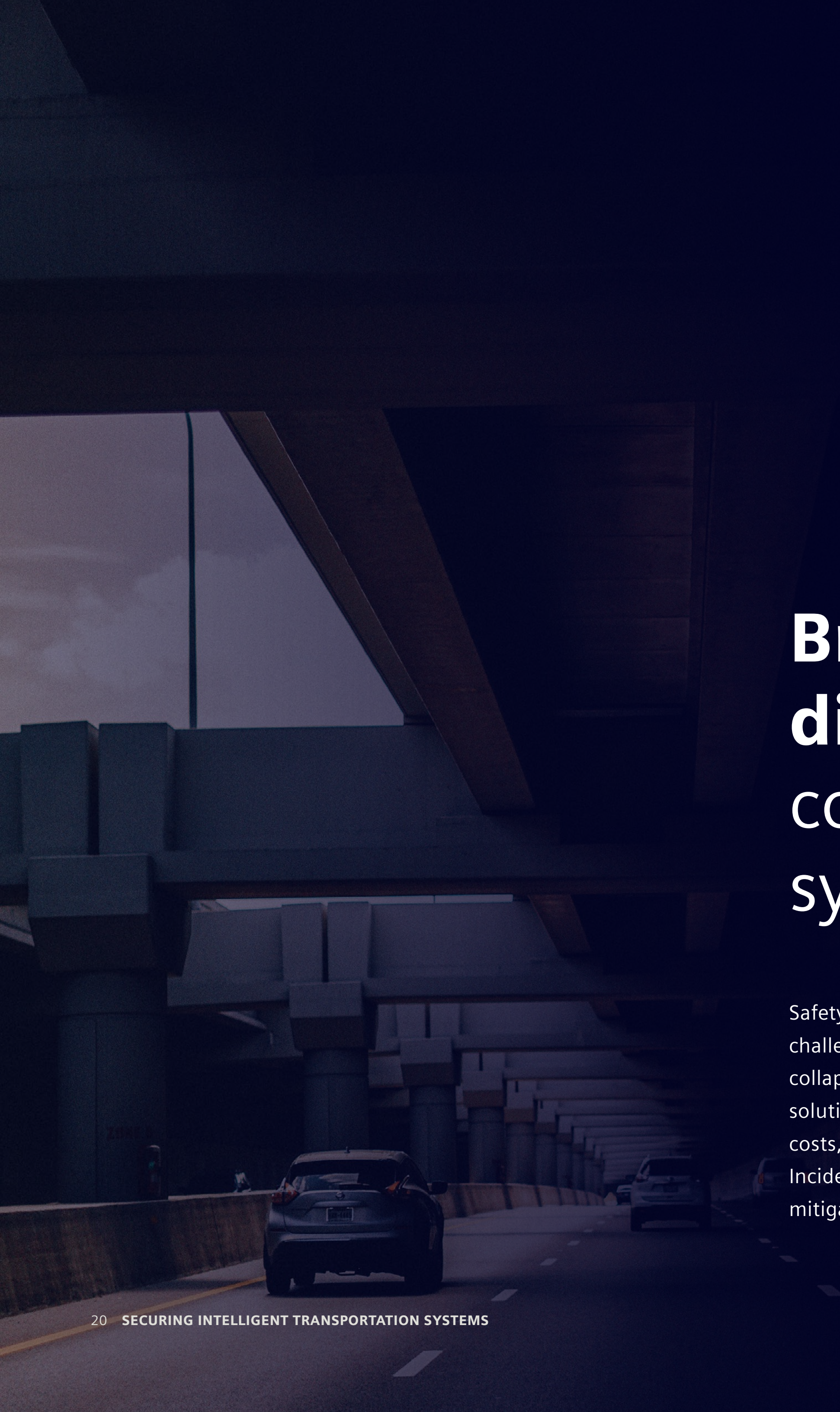
While Clark County began modernization in 2008, it has continued to take advantage of different RUGGEDCOM offerings since then. These include everything from fiber implementation to legacy device connection, network segmentation, and network management. With an operating temperature range of -45 to 180 degrees Fahrenheit and Class 1 Division 2 hazardous location compliance, RUGGEDCOM provides the rock-solid, dependable communications network Clark County needed.



RUGGEDCOM for ITS

Departments of transportation require purpose-built solutions creating wide-area networks that supply reliable, high-bandwidth connectivity in demanding environments. The future of intelligent transportation systems will allow for the prevention of traffic jams on freeways through automated systems that predict traffic flow.

Through data analysis provided by connected sensors and systems, traffic intervention can signal incident alerts, weather warnings, and temporary openings of hard shoulders. Siemens RUGGEDCOM helps ensure seamless and flexible mobility by guiding traffic through lower-density routes. Traffic managers gain an information advantage through the delivery of timely and accurate data that can prevent bottlenecks before they occur. Drivers are delivered information to help them make smarter decisions, while traffic lights are synchronized to keep vehicles moving during rush hours.



Bridge and digital tunnel communications systems

Safety incidents in bridges and tunnels present unique challenges. The risk of fast-moving fires, structural collapses and longer escape routes demands innovative solutions. To ensure public safety and lower operational costs, network subsystems must interact seamlessly. Incident detection times must be short, with fast mitigation responses.

Managing risk in transportation infrastructure

Protecting against hackers

Embracing cybersecurity

Fortifying cybersecurity for ITS

Identifying risks within the environment

Implementing an end-to-end approach

Threat detection

Future-proofing your network

Case studies

RUGGEDCOM for ITS

Bridge and digital tunnel communications systems

Your end-to-end solution

Your **end-to-end solution**

Combatting cybercrime against transportation control systems requires a partner, not just a product.

A partner does not simply protect your inventory and documentation, they provide ongoing risk assessment and evaluation of potential vulnerabilities in your infrastructure. Nobody else gives you the kind of dedicated resources for each market that Siemens does. We bring the best, top-of-the-line solution from leading IT security partners.

Network reliability

The best way to save time and energy is to invest in a system that will last a long time and hold up under even the toughest conditions.

Additionally, nobody else offers an internal power supply, which removes a possible point of failure from your systems. Choosing a reliable, independent solution now will keep you from having to answer tough questions later.

Automatic updates

Investing in RUGGEDCOM means you don't have to overwhelm anyone with additional tasks, potentially compromising your cybersecurity. Not only will you receive automatic updates, our fully managed service will also proactively take charge to keep you current in your cybersecurity solutions.
That's the Siemens difference.