Spectrum **Security**

About *Miovision*

Miovision empowers transportation professionals, through data and infrastructure, to improve the transportation experience for everyone. With over 650 customers in 50 countries across the world, Miovision provides meaningful solutions to real challenges facing today's traffic systems.

Introduction

Securing network traffic data and infrastructure is essential to ensuring a city's safe and efficient operations. As a provider of intelligent traffic signal management solutions, Miovision knows first-hand how to manage the security risks involved.

The purpose of this document is to provide context about the security risks today and to specify the security principles that are foundational in Miovision's Spectrum solution. Spectrum is a turnkey signal connectivity and management solution built to protect and secure city traffic network data in a more open and connected world.

The Evolution of Wireless *Traffic Systems Control*

Traffic control systems have evolved. They were originally designed as standalone hardware located in traffic cabinets. They ran on fixed timing schedules created by traffic planners that used historical data.

Today, traffic control systems are more complex, networked systems that store and transmit vast amounts of new data, including continuous timing plans and integrated sensor data. Some of these systems are also software controlled and wirelessly connected, providing transportation planners with remote access to optimize traffic flow.

The introduction of wireless connectivity means that device and network security need to be addressed during the design and implementation of a networked solution. Like other Internet of Things (IoT) applications, traffic data security is a concern and must be a foundational aspect of solution design.

For traffic engineers, spending needless time and resources on securing city data is no longer required. A better solution built on wireless networks, cloud computing and remote management is now enabling the smart cities of the future.

Managing the Risks Associated with this New Model

Several risks and vulnerabilities associated with a more open and fully networked traffic management system require advanced security measures. The risks to be managed include:

Compromised device security
NTCIP (National Transportation Communications for Intelligent Transportation System Protocol) standards enable interoperability and interchangeability between electronic traffic control equipment and devices from multiple manufacturers. The consequence of this open protocol is network exposure to faulty NTCIP implementations by other, less secure vendors. Such faulty NTCIP deployments can trigger lockdown of control devices. For example, if NTCIP command orders and content are not what's expected by the device, it goes into lockdown as a security measure, and requires a traffic engineer to detect the problem and fix it.

Poor data encryption
Where vendors haven't invested in encryption, devices can receive commands with weak or no encryption. The result of this lowest-common denominator approach is data left readable and vulnerable to unauthorized users.

Unauthenticated system access

Use of default authentication settings leads to unauthorized access to command and control interfaces, a lack of audit record capabilities, and generally poor tracking of users and their activities.

Outdated security patches on servers and software

Firmware updates to devices in the field are done infrequently, if ever, because they can't be done remotely. As a result, new security patch deployments rarely make it to devices in the field once deployed.

Debugging tools could expose openings for hackers

It's common for engineers to use many test tools during product development and inadvertently leave "super user rights" enabled once debugging is complete. This creates a potential opening for hackers to access the tools on deployed devices in the field.

Other Risks – More Perceived Than Real

City officials also have concerns about extending user access to users outside of the traffic management center (TMC). Mobile and web access to signal data from outside the four walls of the TMC is a perceived risk, but in reality it's very common, controlled by VPN access and user authentication. To ease concerns, cities can make limited data available via the VPN. For example, Miovision enables read-only access to monitoring tools, and prohibits the ability to push new timing plans from outside the city's VPN. There are huge efficiencies to be gained by giving teams remote and mobile access monitoring so they can react more quickly to problems.

Concerns still linger about wireless and cloud computing architecture from city officials, who are used to fiber-based and standalone systems. These concerns are unfounded in an era when most government and enterprise computing is built this way.

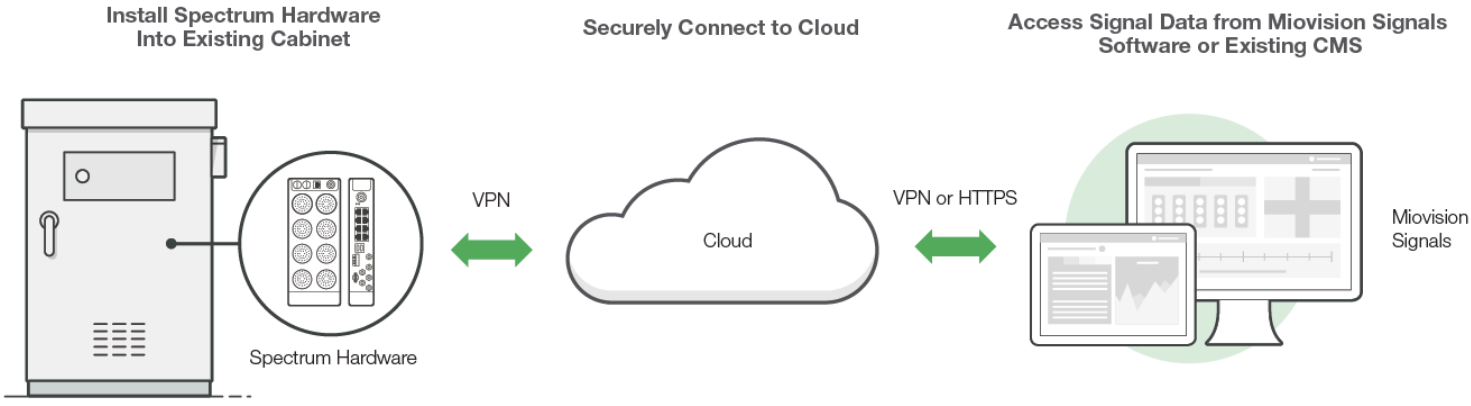
In fact, wireless is no more risky than fiber, yet provides much faster response to attacks or outages. In addition, systems can be brought back online remotely and more quickly with wireless. "Cell on Truck" solutions allow for rapid deployment of cell sites to deal with such outages. With hardwired solutions, resolution can take weeks.

Regarding cloud computing, some cities are concerned with the fact that the solution and data live outside their walls, and that it's not city-owned IT infrastructure. To ease those concerns, cloud-based providers like Miovision and Amazon Web Services (AWS) have security teams focused on monitoring and regularly patching systems. It's safe to say security monitoring from cloud specialists is superior to a few security personnel on a city's IT team. These security measures for cloud-based computing have earned the trust of the CIA and the US Department of Homeland Security.

Designing a Secure Solution: *Traffic Signal Connectivity and Management*

Miovision's Spectrum creates a secure, virtual network that connects and improves existing traffic infrastructure, allowing it to communicate safely with a city's traffic team, wherever they are. It is an easily installed solution that provides traffic engineers with access to signal data and tools they need to more effectively solve the city's traffic problems. Spectrum integrates with existing hardware and provides encrypted LTE wireless connectivity to a secure, cloud-based, software platform. Spectrum allows remote management in compliance with the city's security policies.

Miovision's Spectrum has been engineered with network, data, and device security as a top priority. The product development team of experts uses a comprehensive Security Software Development Lifecycle (s-SDLC) in the development and engineering of all software.



- Installed in under 20 minutes
- Integrates with NEMA and TEES (170/2070) traffic cabinets

- Encrypted 4G LTE connectivity
- Embedded security and VPN
- Serial-over-LTE support built-in

- Provides a suite of monitoring tools & performance measures using Miovision Signals (via HTTPS connection)
- Access and administer your traffic equipment using existing software (via VPN connection)

Spectrum is hosted on AWS within a Virtual Private Cloud, which maintains best-in-class compliance for data security and integrity. It supports the following certifications: .9999999 AWS Uptime Guarantee, ISO 27001 Certification, DDoS Mitigation, PCI DSS Certification, FedRAMP Certification, NIST 800-171 Compliance.

Core components of Spectrum include:

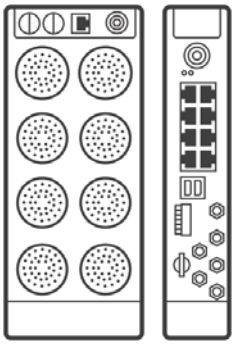
Miovision Signals Software

The cloud-based software package that accompanies Spectrum hardware offers all of the necessary tools to remotely manage traffic signals, including monitoring and alerting functionality. Users can remotely access signal telemetry, fault alerts, video streaming, traffic data, and network information via cloud architecture.

Miovision Connect

Using serial-over-LTE technology and secure VPN, Connect provides a secure connection between control cabinet hardware and the cloud. This includes third-party software such as Central Management Systems (CMSs), Advanced Traffic Management Solutions (ATMSs) or Malfunction Management Unit (MMU) vendor software.

Spectrum SmartLink and Interface Hardware



Reads and transmits traffic data information over LTE via a private Internet Protocol Security Virtual Private Network (IPsec VPN), which encrypts all data between the cabinet, traffic signals, Spectrum Camera360 and the cloud. This embedded VPN ensures all communication from the cabinet to the operations center are protected and secure. The hardware enforces security protocols that protect the broader infrastructure network if a physical cabinet is compromised.

The Six Pillars of a Secure and Open Network for Traffic Management

To control the risks above, Miovision has adopted the following six pillars in the design of the Spectrum solution using a “defense in depth” approach to security. These pillars work together to fail-safe other systems and redundantly protect the city’s infrastructure.

Miovision Security Pillar	Security Risks Controlled
Encryption	Readable data exposed to unauthorized users like hackers
Key Management	Unauthorized system access
User Authentication	Insecure logins, poor activity auditing
Robust and Private Networking	Device security
Secure Data Storage	Device security
Security Response Process	Unresolved security breaches

Encryption

Spectrum connects to traffic cabinets using an encrypted and authenticated OpenVPN connection. Using Serial-over-LTE, the VPN can also be extended to connect existing CMS and ATMS software directly to the cabinet. Data storage and processing are done on secured servers isolated from direct access to the Internet.

Miovision Signals is accessed via HTTPS and is configured to prefer use of a forward secret, elliptic curve based negotiation of an AES-128 key and SHA-256 based MAC (ECDHE-ECDSA-AES128-GCM-SHA256). Spectrum SmartLink connects via VPN to the cloud. This OpenVPN connection uses AES-128, configured with CBC mode. Endpoint authentication is via OpenVPN’s pre-shared key authentication mode. These are the same algorithms used by banks and governments.

Key Management

Every Spectrum SmartLink unit is provisioned with unique cryptographic keys, which are used to authenticate to the cloud. These keys are used as pre-shared secrets for authenticating the OpenVPN connection. A provisioning server is used to ensure a sufficient amount of cryptographic entropy is included in each key.

The use of unique keys ensures that each unit is identifiable, and that a physical attack on one single unit does not compromise other units. This keying material can be updated remotely to allow for easy in-field management.

User Authentication

Secure login is required to access Miovision Signals. Each user is required to access the system by entering their personal username and password. Two-factor authentication can be enabled via Google Authenticator or Duo Security. Additional checks can be done on characteristics of the access request, such as IP filtering, geofencing, time of day/week, or a change in location or device used to login.

User management is based on granular permissions and privileges based on roles. Settings can be configured to control access rights in the platform. User permissions restrict who can perform what functions, and activity is logged.

Robust and Private Networking

Spectrum does not require customized infrastructure, servers or IT support. Serial-over-LTE requires a single UDP port to be opened on any existing firewall.

The VPN is designed to ensure that Spectrum initiates all communication. This ensures that a physically compromised cabinet restricts access to the cloud and other signal infrastructure. The IP addresses of devices are not externally accessible and are on a private network.

The use of Amazon Web Services allows Spectrum to mitigate DDoS attacks, coming with a 99.99999% uptime guarantee. Spectrum leverages the reliable networks and secure practices of our wireless and cloud partners. This includes dedicated and fully staffed security teams at Miovision and AWS who focus on monitoring the systems, deploying patches, and evolving the system to respond to future and unknown threats.

Secure Data Storage

Data acquired with Spectrum and stored in the cloud is encrypted using Amazon Web Service's (AWS) Key Management System (KMS). KMS ensures data is encrypted at rest using AES-256 in Galois Counter Mode (GCM).

This data resides on the Signals Platform, which is housed in the AWS Cloud. Various governments rely on AWS to secure their information, including the C.I.A. and the Department of Defense.

AWS security measures meet the requirements of these organizations, adhering to standards such as ISO 270001, PCI DSS, NIST 800-171, and FedRAMP.

All customer data is confidential and protected via inbound and outbound network traffic filtering to prevent data leaks. Data is backed up several times daily. Backups are transferred over an encrypted link and periodically deleted. Multiple secure data centers, each with redundant internet connections, ensure connectivity is available at all times.

Security Response Process

Miovision understands that security is a continually evolving aspect of product engineering. We work with external security experts to improve our products by:

a) Alerting our customers of security vulnerabilities at www.miovision.com/security.
b) Accepting external reports of vulnerabilities in our products at secure@miovision.com.
c) Engaging external experts to proactively test and review the security of our products.
d) Providing the city the ability to remotely patch deployed hardware.

Smart cities are looking to take advantage of the evolution in traffic control systems from standalone hardware to better solutions built on wireless networks, cloud computing and remote management.

As a provider of intelligent traffic signal management solutions, Miovision is committed to ensuring a city's safe and efficient operations by providing products that secure network traffic data and infrastructure.

Spectrum is the best and most secure way to connect your traffic signals.

Please contact us to find out how Spectrum can connect your signal data while making your city's traffic signal network safer and more efficient.

Learn more about the world's most trusted traffic data platform at Miovision.com