



Cyber and Physical Security for Transportation Networks

#cybersecureITS



ITS | ROCKY MOUNTAIN *chapter*



How Exposed are we today?

NEWS ANALYSIS

Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity

The hack underscored how vulnerable government and industry are to even basic assaults on computer networks.



Cybersecurity experts said Colonial Pipeline would never have had to shut down its pipeline if it had more confidence in the separation between its business network and pipeline operations. Drone Base, via Reuters



Public Safety

Hack of D.C. police cameras was part of ransomware scheme, prosecutors say



CYBERSECURITY

Huge federal hack ripples across energy industry

Christian Vasquez, E&E News reporter

Published: Thursday, December 17, 2020



Four days after a sweeping hack of government and private-sector computer networks came to light, U.S. electric utility companies are struggling to assess the fallout. Electric transmission lines are pictured. Chris Hunkeler/Flickr

THE WALL STREET JOURNAL.

SIGN IN

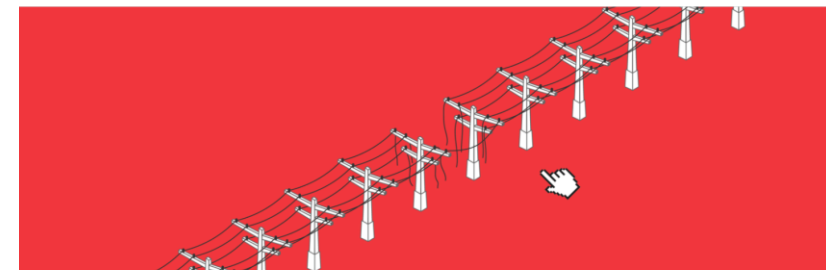


ILLUSTRATION BY JESSICA KURONEN/WSJ

America's Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It

A Wall Street Journal reconstruction of the worst known hack into the nation's power system reveals attacks on hundreds of small contractors

Critical Infrastructure- Transportation Systems Sector


What are the areas within the Transportation Sector?



Aviation	Maritime
<ul style="list-style-type: none"> ➤ Composed of airports, heliports, seaplanes bases, support services, air traffic control, and navigation facilities. ➤ Approx. 19,700 airports in the U.S., with 500 offering commercial service. ➤ Approx. 780,000 passenger flights take place across the U.S. monthly. 	<ul style="list-style-type: none"> ➤ Geographically complex and diverse system consisting of waterways, ports, and intermodal landside connections. ➤ Consists of nearly 95,000 miles of coastline, 361 ports, more than 25,000 miles of navigable waterways, and more than 29,000 miles of Marine highway.

Highway & Motor Carrier

- Composed of bridges, major tunnels, trucks carrying hazardous materials, other commercial freight vehicles, motor coaches, school buses, and key intermodal facilities.
- Includes nearly 4 million miles of roadway, more than 600,000 bridges, and 400 tunnels.



Freight Rail	Highway & Motor Carrier	Pipeline	Postal & Shipping	Mass Transit
<ul style="list-style-type: none"> ➤ Approx. 1.33 million freight cars in service. (2013) ➤ Consists of 140,000 miles of active rail track. ➤ Transports more than 70% of all U.S. coal shipments. ➤ Approx. 73 billion in operating revenue for the 7 Class 1 railroads. (2013) 	<ul style="list-style-type: none"> ➤ Composed of bridges, major tunnels, trucks carrying hazardous materials, other commercial freight vehicles, motor coaches, school buses, and key intermodal facilities. ➤ Includes nearly 4 million miles of roadway, more than 600,000 bridges, and 400 tunnels. 	<ul style="list-style-type: none"> ➤ More than 2.5 million miles of pipelines span the U.S. to transport nearly all of the natural gas and approx. 65% of hazardous liquids, including crude and refined petroleum. ➤ Above-ground assets include compressor stations and pumping stations. 	<ul style="list-style-type: none"> ➤ Includes large integrated carriers, regional and local courier service providers, mail services and mail management firms, and chartered and delivery services. ➤ Approx. 720 million letters and packages moved each day. 	<ul style="list-style-type: none"> ➤ Includes transit buses, trolleybuses, monorails, heavy rail (subway), light rail, passenger rail, commuter rail, and vanpool/rideshare. ➤ 10.3 billion passenger trips in 2012.

Agencies With Knowledge and Assistance



**Homeland
Security**



**CYBERSECURITY
& INFRASTRUCTURE
SECURITY AGENCY**



NIST

**National Institute of
Standards and Technology**

U.S. Department of Commerce



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

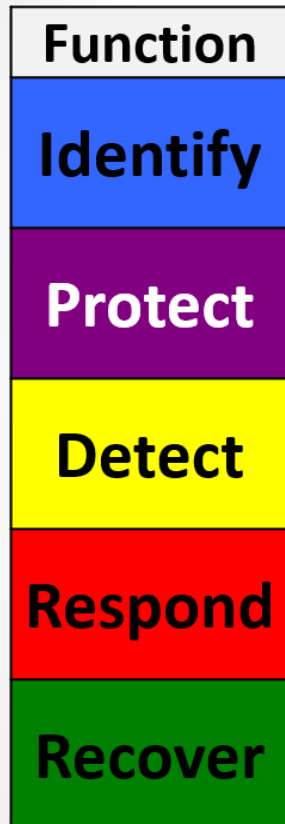


**Center for
Internet Security®**

Confidence in the Connected World®

NEMA
Setting Standards for Excellence

NIST Framework Core



- **Identify** – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- **Protect** – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- **Detect** – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond** – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
- **Recover** – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Traffic could be worse....

“DOTs are traditionally built around building and maintaining asphalt and concrete. That’s our bread and butter,” said Alan Davis, an assistant state traffic engineer for the Georgia transportation agency who serves on a national panel researching the best ways to prepare transportation systems for cyberthreats. “But there’s also this other world that operates that infrastructure. This world is a new thing for a lot of DOTs.”

STATELINE ARTICLE April 24, 2018

By: Jenni Bergal

Topics: Business of Government & Transportation

TRAFFIC

Hackers could bring traffic to a halt, Ga. Tech research finds, and Atlanta isn't likely to fare well in an attack

The research found it would take hacking a surprisingly small percentage of cars to shut a city down.



The traffic landscape is changing

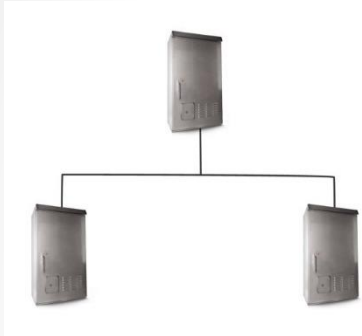


Drivers & vehicles are more connected than ever before

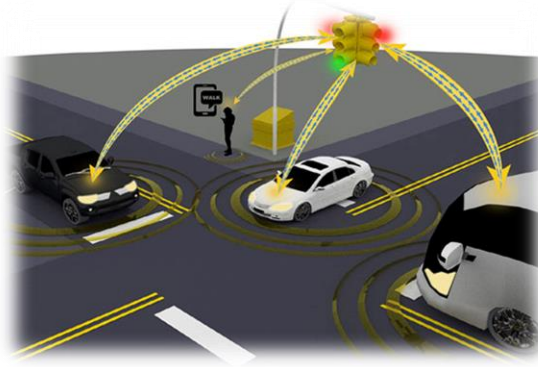
More traffic flow and more intelligence available on the roadways

Agencies are becoming more connected and prolific use of the internet and wireless

Challenges



- Interconnected cabinets
- Traffic cabinets contain direct access to critical infrastructure network
- Network is state wide



- V2I networks
- Vehicle to Infrastructure is growing at an exponential rate



- Assets in Cabinet
- Average of \$30K+ in standard cabinets



- Cyber Secure ITS
- Protection of systems and secure data from attack and exploitation

Where some ITS Systems are Lacking

- 1) Network port security solutions, and the use of certificates to authenticate devices is not widely adopted
- 2) There does not appear to be widespread adoption of software/application whitelisting among TMC operators
- 3) The majority of TMC organizations have not performed a skills gap analysis to understanding the skills and behaviors of their workforce
- 4) The importance of patch management is not widely acknowledged
- 5) **Multi-factor authentication is still lacking across many TMC systems**
- 6) TMCs need to implement routine incident response exercises
- 7) There is an identified shortage of dedicated versus consolidated IT staff for TMCs

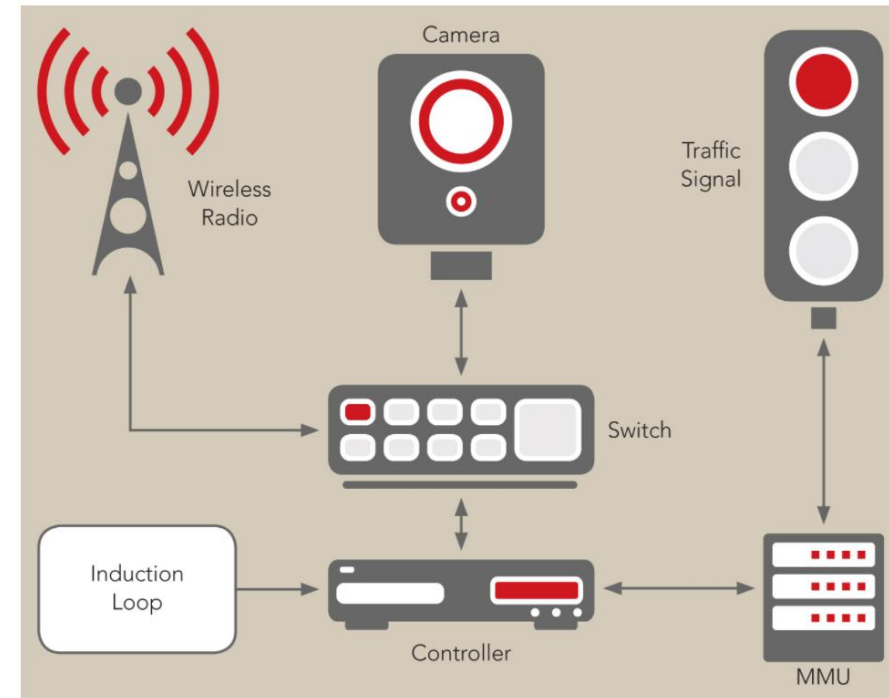
Note: Information provided FHWA and USDOT

Am I Really Secure?

“There is a cyber-war under way,” says Doug Couto, independent IT security consultant and a former chief information officer for the Michigan State Government.

“Cyber attacks numbering in the region of 750,000 happen every day against the Michigan Government alone. There are vulnerabilities in traffic signals connected to the internet and risks associated with ITS software and hardware.

“When I was working for Michigan I could see all of this ITS technology being created and thought someone ought to pay more attention to built-in security. Systems are only as strong as their weakest link and people can find weaknesses and exploit them.”



A schematic reveals how many potentially vulnerable areas there are in a typical light installation.

Targets in an ITS cabinet might look like this...

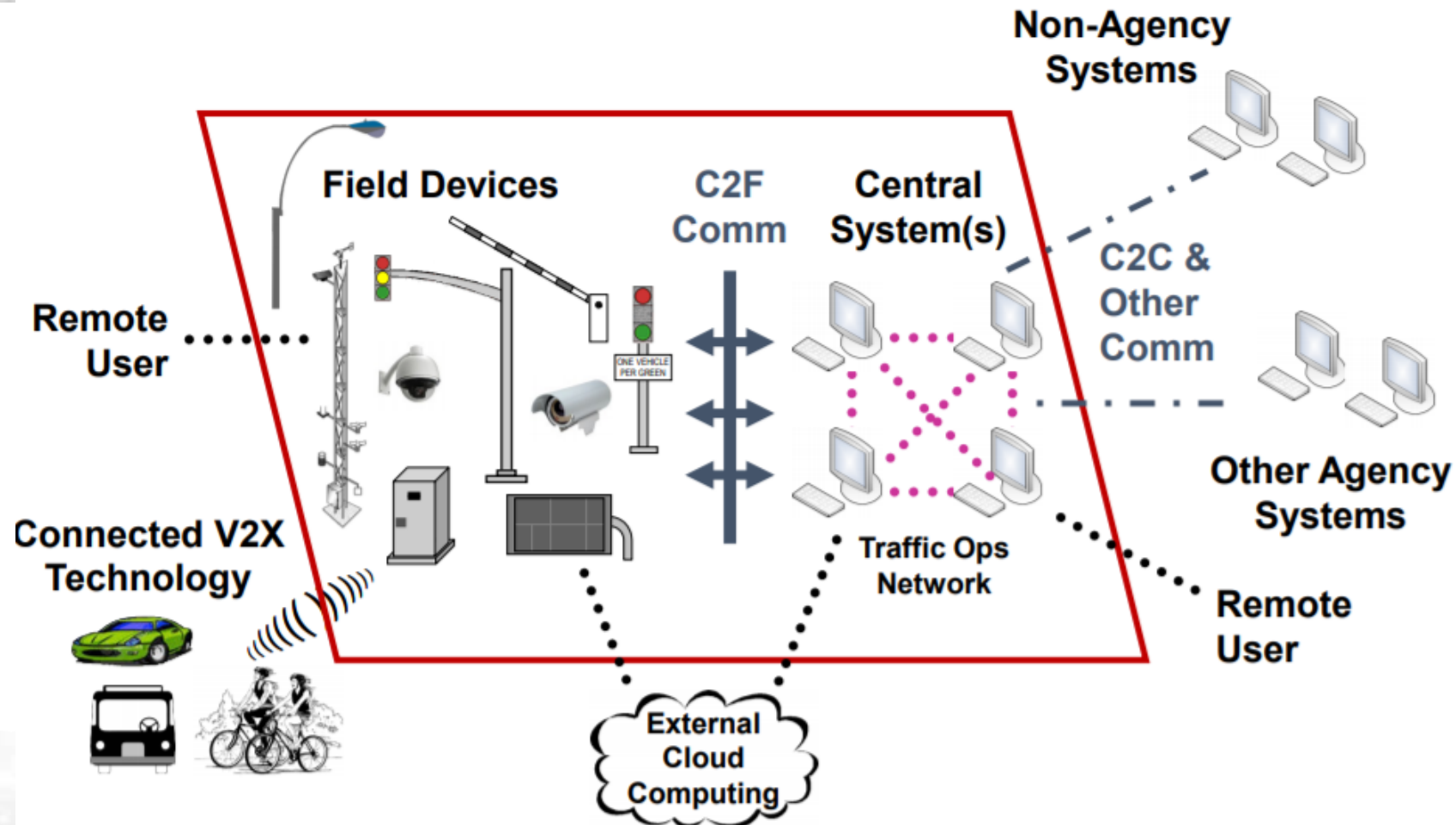
Compliment of ITS International

Securing ITS around the Big Game in ATL

GA Dome- Super Bowl

- 1.5-mile Secured Perimeter around Mercedes Benz Stadium suggested by DHS
- Secure all infrastructure and cabinet hardware
- Control Access in/out of Traffic Cabinets
- Enable System-wide security for Traffic Infrastructure and cabinets
- Advanced Monitoring Capabilities

How ITS is growing



Physical Access Control

Old School



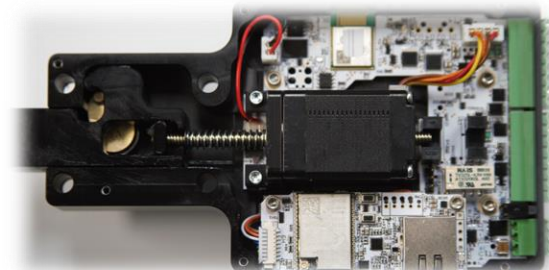
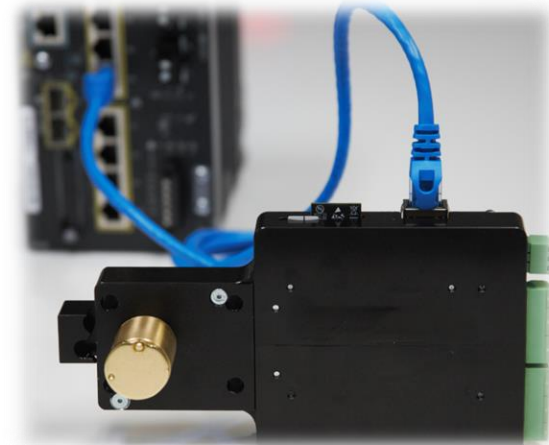
#2 Key

Intelligent Lock



Smart Key

NEW SmartLock 8000



Smart lock Gen 3

Intelligent Cabinet Lock – Access Control



So what does this have to do with my ITS network

At the end of the day, no defense is impregnable against determined adversaries, cyberattacks and data breaches are **inevitable**. With this in mind, we have to have an effective alert, containment, and mitigation processes.

The principle of defense is to assume compromise and take countermeasures:

- ✓ Deploy sound physical security measures to prevent access to devices
- ✓ Quickly identify and respond to ongoing security breaches.
- ✓ Contain the security breach and stop the loss of sensitive data.
- ✓ Preemptively prevent attacks by **securing** all exploitable avenues.
- ✓ Apply lessons learned to further strengthen defenses and prevent repeat incidents.

What's next for 2021





#CyberSecureITS

Steve Bowles
Director IoT Operations

steve@360ns.net

770.718.7437

www.360ns.net

www.cybersecureits.org

Notes

Executive order, May 12, 2021, President's Executive Order on Improving the Nation's Cybersecurity (EO 14028) enhancing security of the software supply chain. Following standards and other.

NIST as it relates to ITS and Transportation

Identify- where are potential threat vectors

Protect- access control, physical security, data security, server based centralized password management, securing access to infrastructure. Network security such as AAA, Authentication Authorization, Accounting. Maintaining systems and updated software with SOP. Protect through software and physical access. Cabinet security to secure the edge with intelligent locks and keys.

Detect- utilizing detection software that monitor the profiles of network activity. We worked with GDOT using ICE to monitor format of traffic per port per device. This is similar to using antivirus software such as Malware for operators computers.

Respond- Plan for the worst and hope for the best. Ensure that configurations are standardized so that there is commonality across the network and ease of recovery. Have procedures in place to recover configurations and software platforms. Use server based backup. Use a network change configuration and compliance management solution. Maintain firmware management and vulnerability to eliminate potential threats.

Recover- Maintain high level of business continuity with config backups and system backups in order to minimize downtime and interruptions. City of Augusta, we implemented business continuity plan that automates backup that saves all configurations daily so that immediate recovery is possible.

Notes: NIST Framework and statement

Cyberattacks are a serious threat to our economy and national security. Government agencies at all levels need to be able to detect, defend and respond to threats.

To address the growing cyber risk, the National Institute of Standards and Technology (NIST), in partnership with private sector industry, developed the Cybersecurity Framework (CSF), which provides a high-level taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes.

How to improve security posture today.

National Standards- NIST, DHS-CISA, CIS center for internet security, NEMA, and many other federal and state agencies are at the ready to assist, guide and direct agencies as to the best practices for securing critical infrastructure.