Cyber Resilience as the Backbone of ITS Sustainability

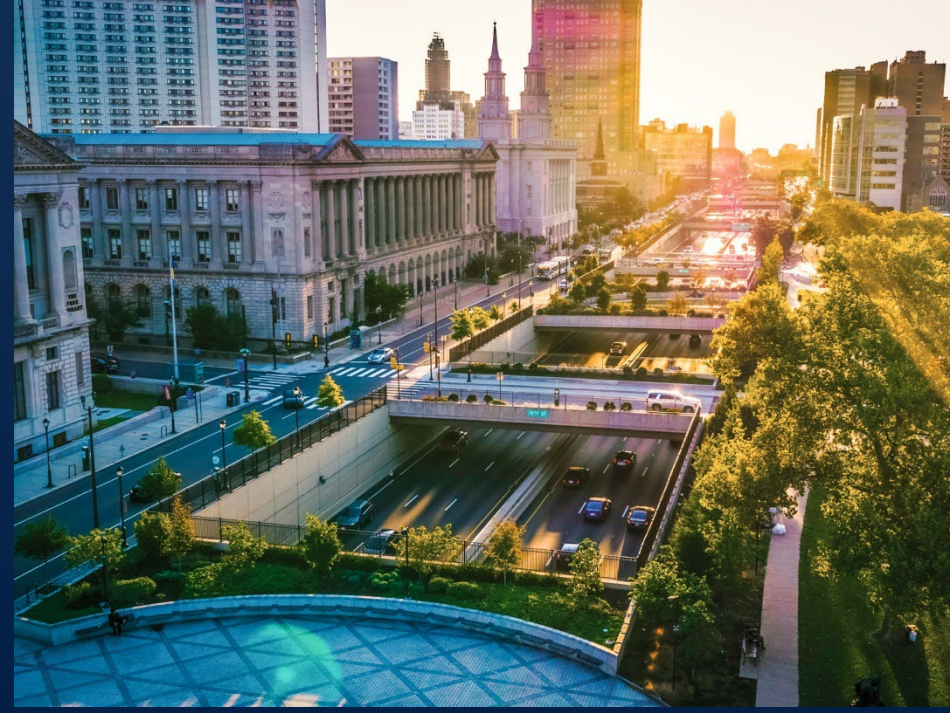
NE ITS Annual Interchange

October 9, 2025

Full-Service

Leading provider of engineering, consulting and technology services spanning three distinct verticals:

- Infrastructure
- Integrated Design and Advisory (IDA)
- GovTech



Michael Baker INTERNATIONAL | *We Make a Difference*

2025 Top 10 Most Frequent Findings in Our ITS Assessment Work

1. Insecure API programming and network design
2. Default passwords left on field devices
3. Improper network segmentation between IT and OT
4. End of Life and unpatched devices (*contain many vulnerabilities*)
5. Network device misconfigurations for ports, protocols, and services (*i.e. all traffic controllers still using insecure SNMPv2 vs v3)*
6. No comprehensive Incident Response Plans
7. No ITS/OT Cybersecurity Policies and Procedures
8. Lack of clarity between ITS/OT and IT responsibilities
9. Lack of capital and operations funding
10. Lack of Continuous Monitoring platforms such as IPS/IDS, SIEMs etc.; Traffic Management Centers operating in the blind for ITS/OT network traffic

Michael Baker
INTERNATIONAL

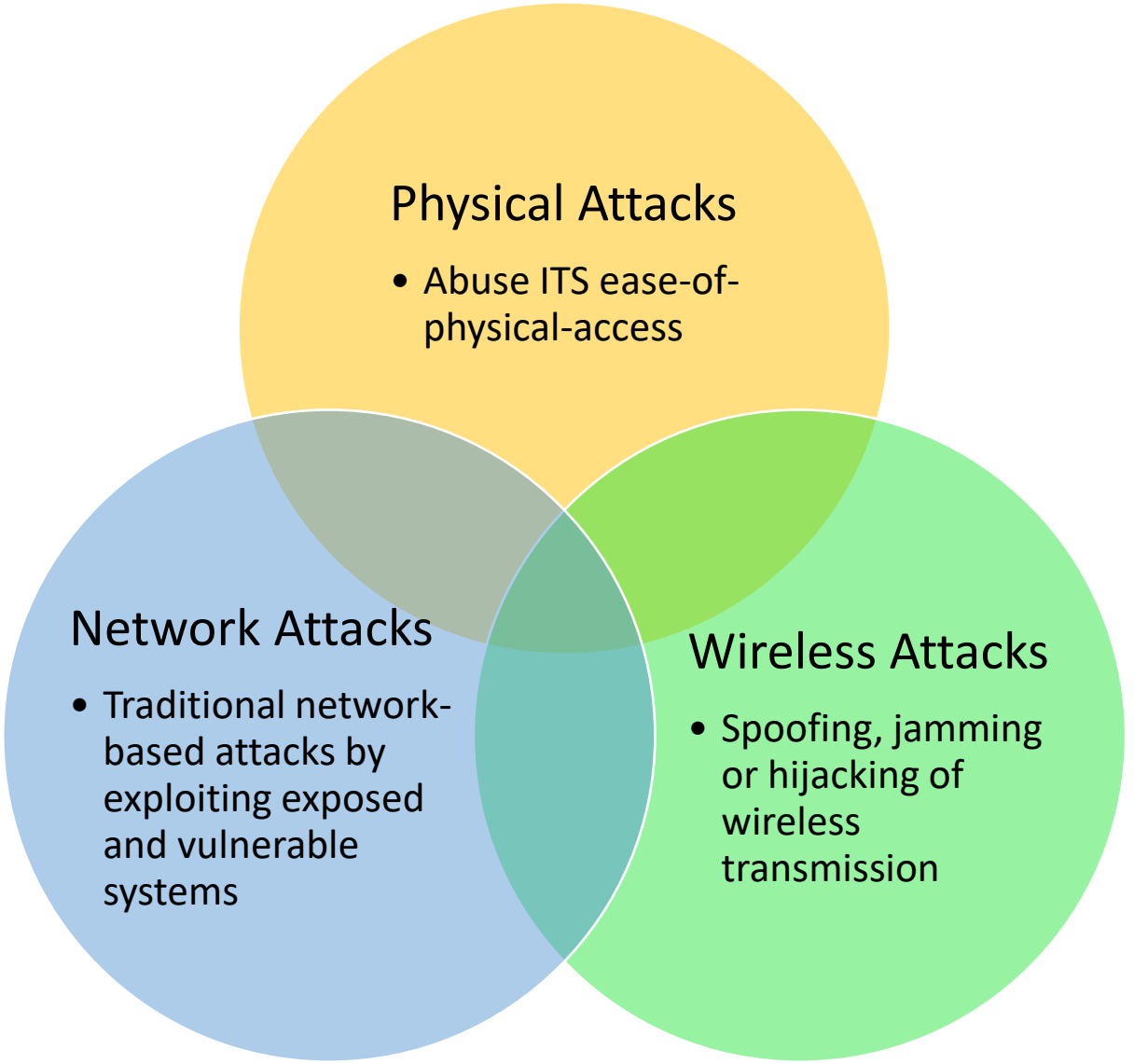
Scope of Cyber Resilience

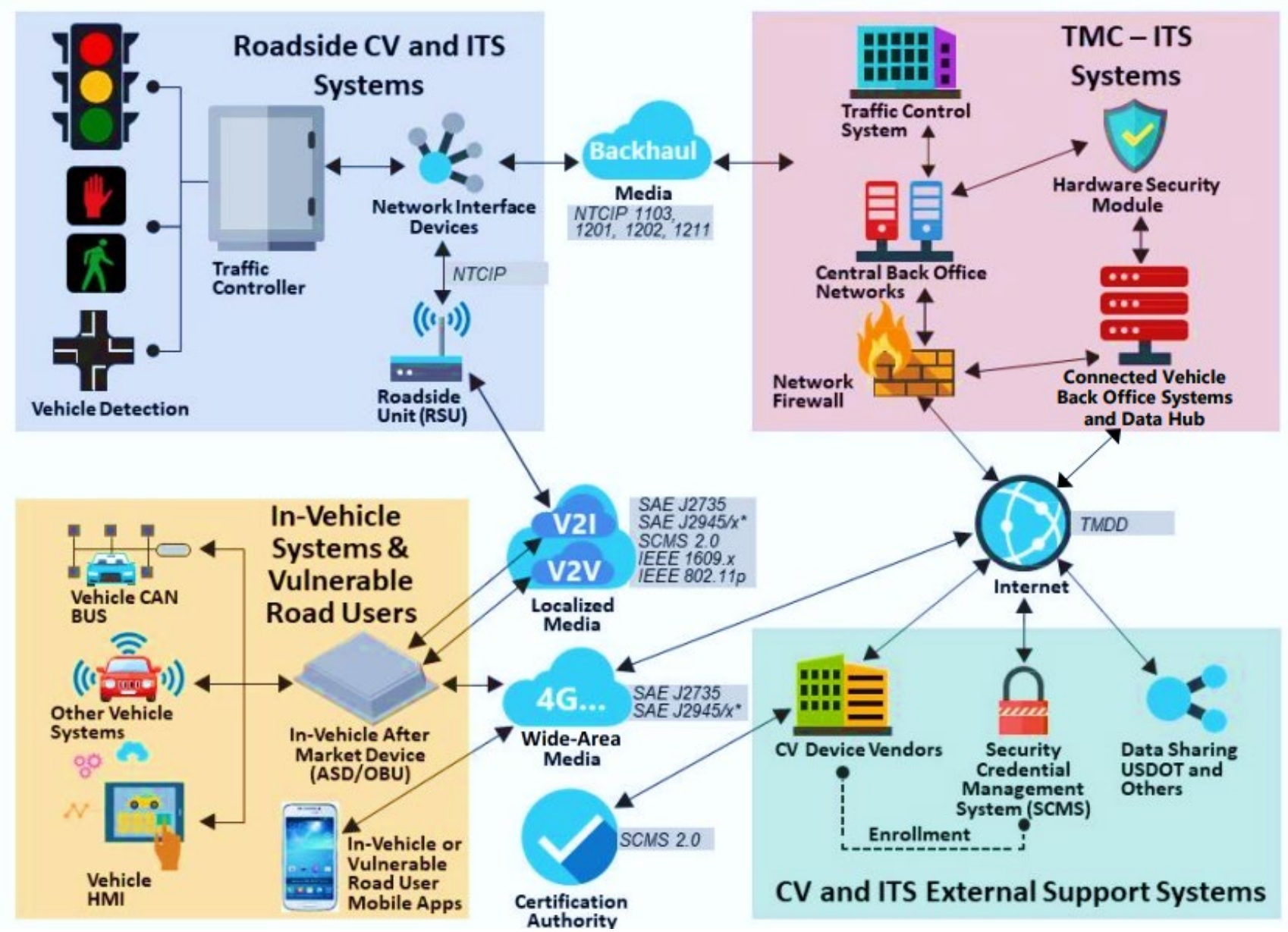
Michael Baker INTERNATIONAL

We Make a Difference

Cybersecurity Vulnerabilities

Michael Baker INTERNATIONAL





Transportation System Components and Communications

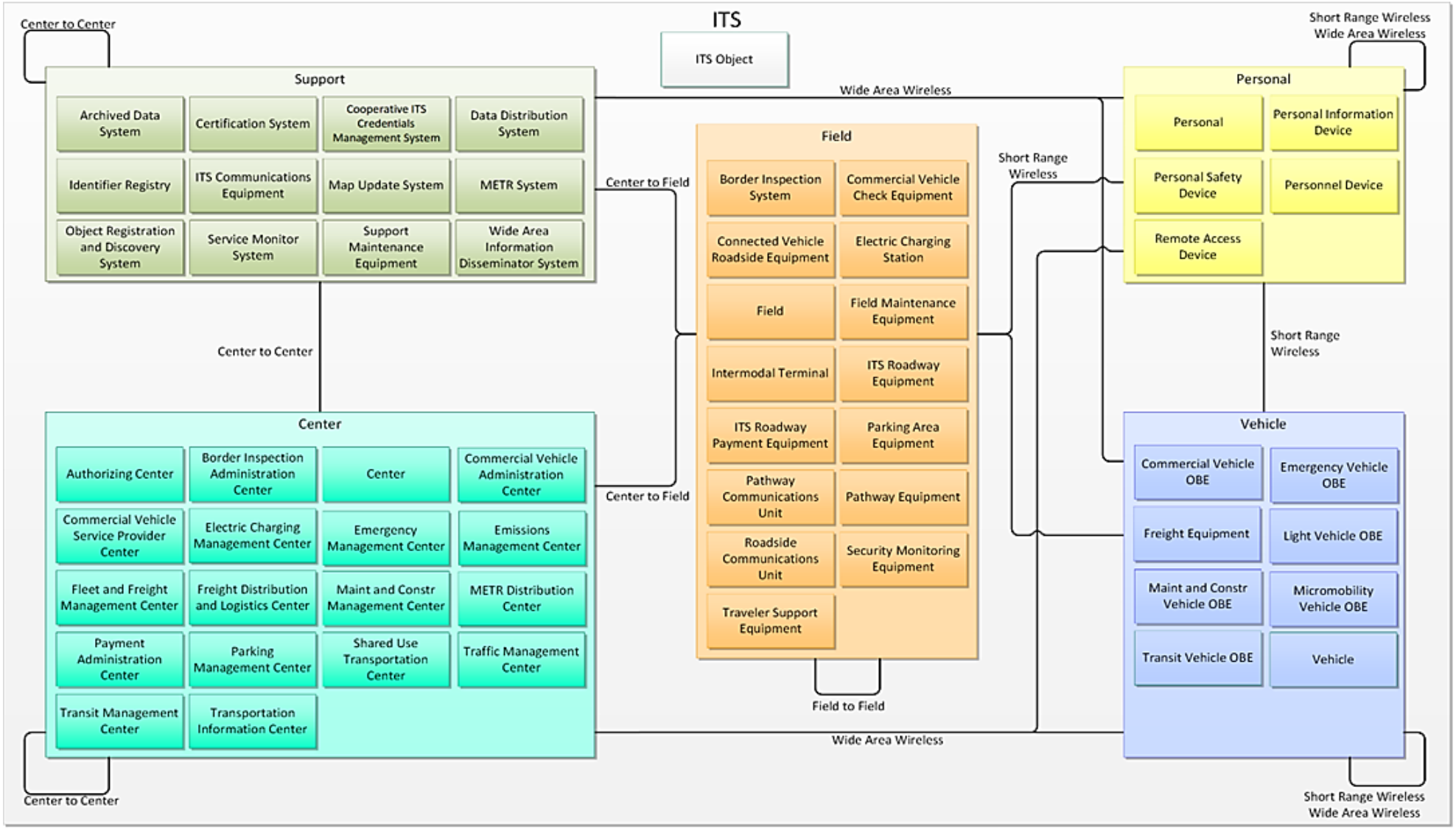
- More Systems
- More Complex
- More Vulnerabilities

Michael Baker
INTERNATIONAL

ARC-IT ITS Physical Component Overview

Michael Baker INTERNATIONAL

Source: https://www.arc-it.net/html/viewpoints/physical.html



Cybersecurity Vulnerabilities

Michael Baker INTERNATIONAL

Communications & Connectivity

- 5.9 GHz V2X
- Wi-Fi
- Fiber
- Bluetooth
- Cellular Network
- IoT Networks
- Network (Traditional IT)
  - Cloud Service Providers
  - Internet Providers

Vehicles

- OEM, Tier 1 and 2 Suppliers Software
- Hardware
- Connected Vehicle Communications
- Satellite Communications
- Automated Vehicles Sensors
- ADS Software Stack

Equipment

- Traffic Signal/ITS Cabinets
- Field Equipment (CCTV, DMS, Vehicle Detectors)
- Software
  - Operating Systems
  - Firmware
- Field Switches
- Coprocessors
- Edge Computing Devices
- AI Sensors
- Payment Systems

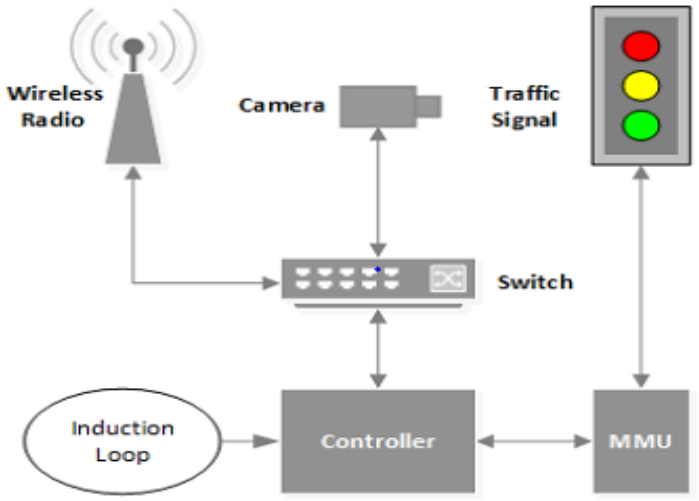
Data

- Unencrypted Data
- Authentication
- Personally Identifiable Information (PII)
- Privacy Concerns

Field Controllers – Then vs Now

Legacy Controllers

- Controller adjusts timings based on data from the induction loop
- Conflict monitor sits between the controller and signals to insure safe condition
- The radio connects to the switch and transmits controller diagnostics and other information back to the agency



Modern Control Systems

- Controllers handle complex probe data and algorithms
- Software Defined Network Switches (SDN)
- Emergency and transit perception
- Advanced Malfunction Monitoring Unit (MMU)
- Integrated V2X communication protocols to exchange data with connected vehicles
- LiDAR and Cameras for real-time detection of vehicles and vulnerable road users
- Edge Computing to analyze sensor data locally and make rapid decisions
- Predictive Algorithms for timing optimization
- Robust network connections to ensure reliable communication.

Field Controllers Most Common Vulnerabilities

- The network is accessible to attackers due to the lack of encryption especially in RF devices
  - 5.8GHz is very easy penetration
  - 900MHz with FHSS a bit harder
- Devices on the network lack secure authentication due to the use of default usernames and passwords.
- Network connected controllers still using non-secured SNMPv2.0
- The field controller or switches are vulnerable to known published exploits due to lack of patching and upkeep

Michael Baker
INTERNATIONAL

Traffic Signal Controllers Vulnerability Examples

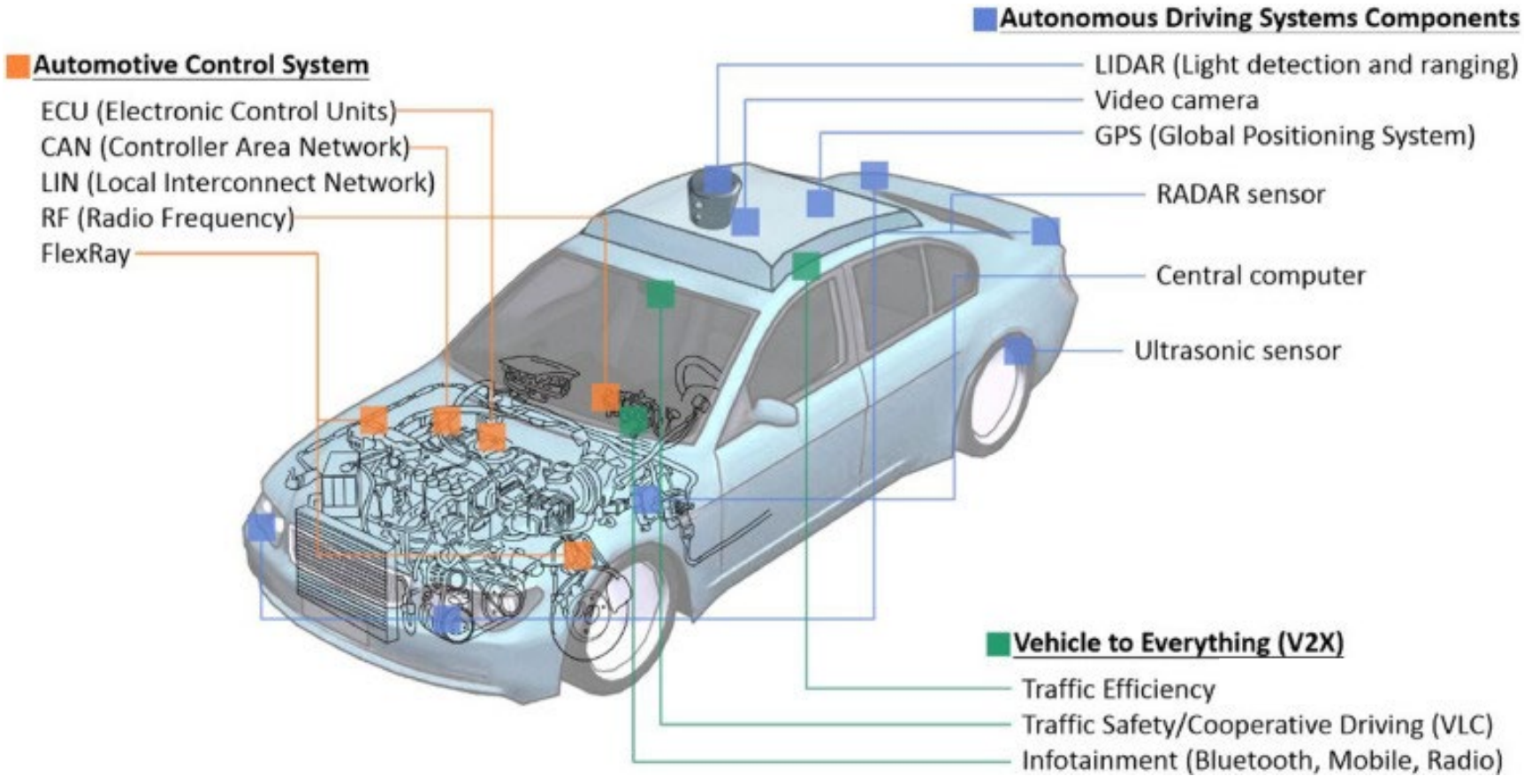
Michael Baker INTERNATIONAL

2020 - Critical vulnerability affecting traffic signal controllers made by SWARCO could have been exploited by hackers to disrupt a city's traffic lights

2023 - Econolite EOS traffic control software are vulnerable

- Configuration file accessible without authentication
- Lacked password requirement for gaining "READONLY" access to log files
- Its threat score - 9.8 out of 10

Connected Car Internal Architecture



- 150+ Electronic Control Units (ECUs) to Secure Per Vehicle
- Sensors and firmware from “Countries of Concern”

Michael Baker INTERNATIONAL

Connected Car Internal Architecture

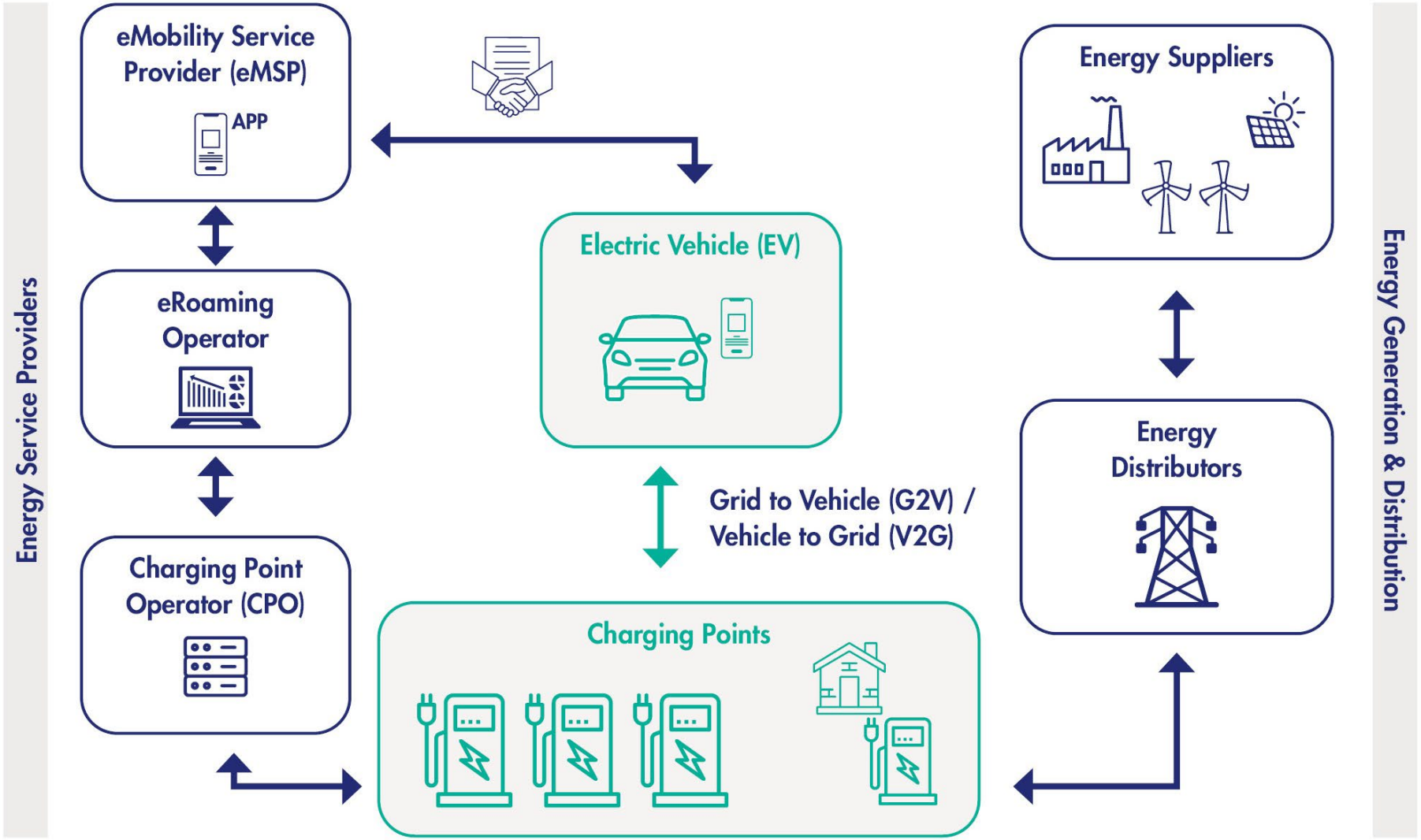
- 150+ Electronic Control Units (ECUs) to Secure Per Vehicle
- Sensors and firmware from “Countries of Concern”

« Emergency start-up » systems disguised as JBL speakers for 2.0 car thefts

2015 to 2023, researchers and pentesters are still actively hunting!

Michael Baker INTERNATIONAL

Electric Vehicle Charging Ecosystem



Securing Everything, Everywhere, All At Once

- **It Takes A Village**, Cybersecurity is a team sport and collaboration across stakeholder groups is key not just “nice to have”

- **Cyber-Informed Engineering** is a key methodology for securing engineering designs and “baked in cyber” vs. “bolted on”

Michael Baker
INTERNATIONAL

Vast Stakeholder Landscape Increases Need for Collaboration

U.S. Department of Transportation
Federal Highway Administration

Michael Baker
INTERNATIONAL

Traffic Management Center

We watch the physical roads, BUT who's watching ITS data packets? Is it IT, ITS/OT, both or no one?

- Must include Continuous Monitoring of all Field Device Data Packet Traffic
- Must have network software platforms such as SIEMs, IPS, IDS – Splunk, Dragos, Tenable OT, and many others
- Shortage of dedicated ITS/OT focused cybersecurity staff - Must resolve hiring and/or training needs to overcome this gap

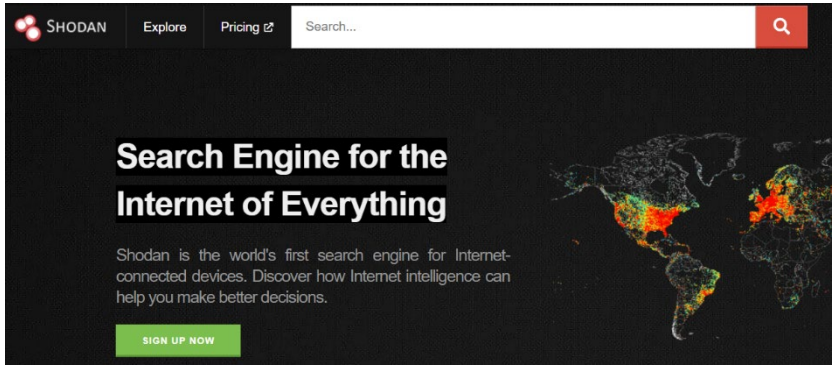
Search Engines for all Non-Secured IoT

SHODAN and CENSYS

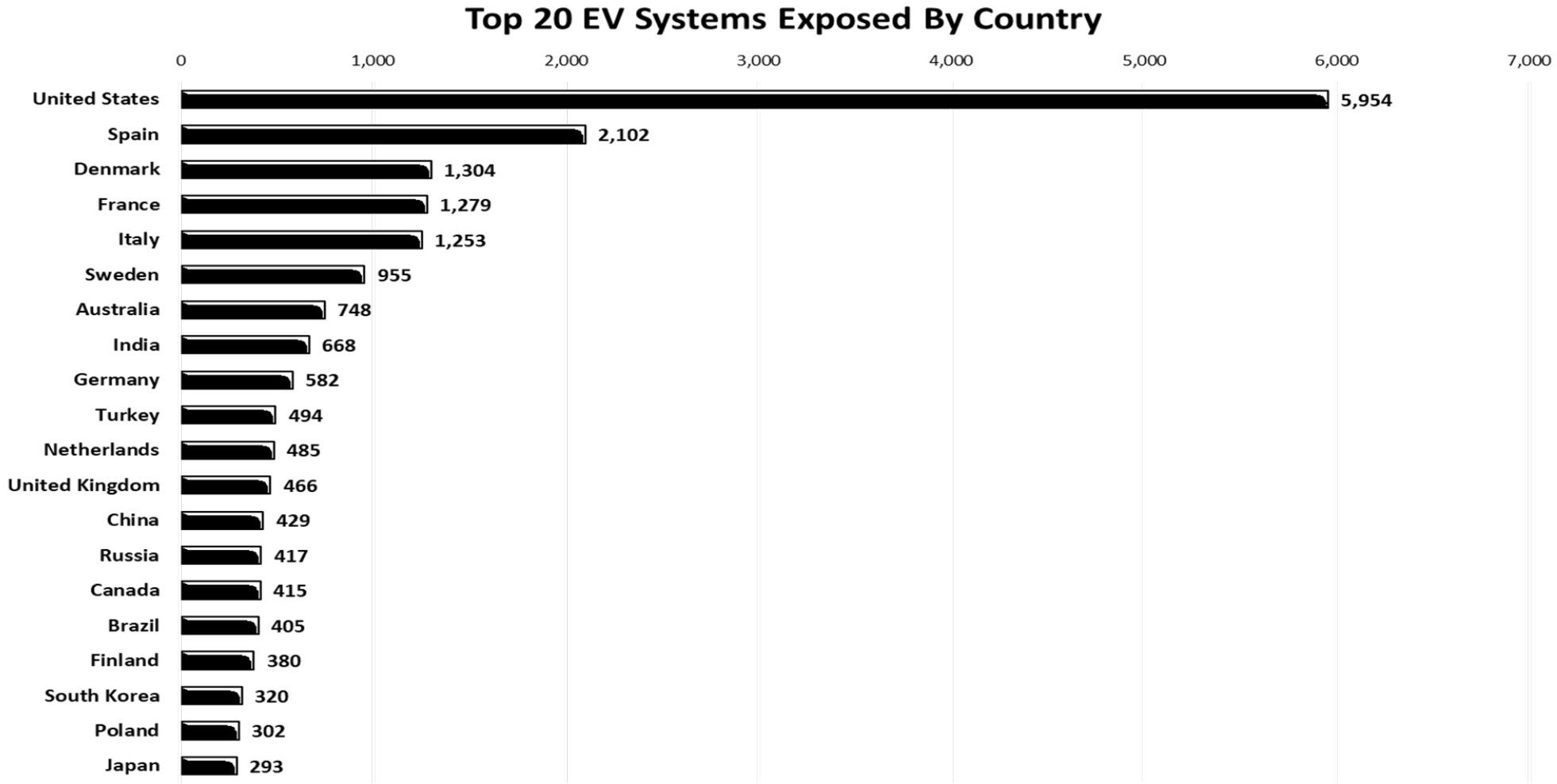
- Legal search engines to find non-secured devices connected to the Internet

- Don’t let your ITS devices show up on this search, used by black and white hats

https://www.shodan.io/ and https://censys.com/

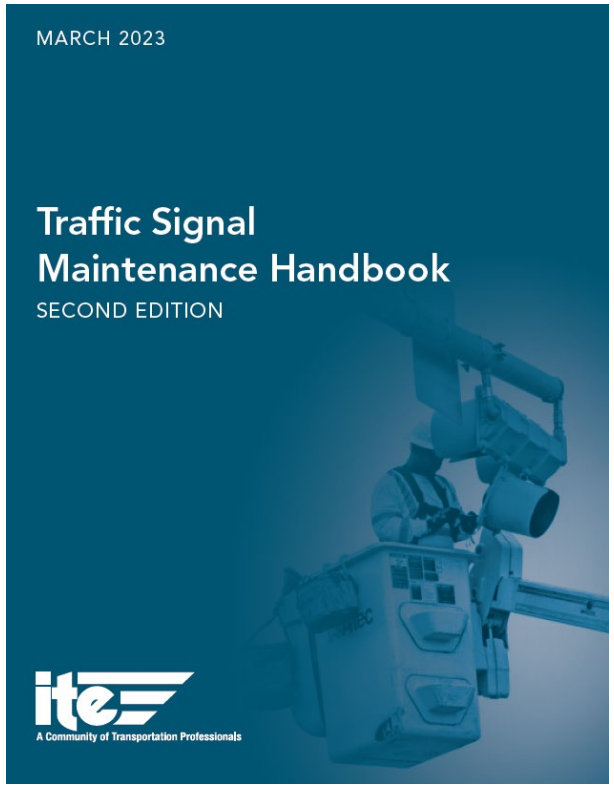


Example for Exposed EV Charging Systems

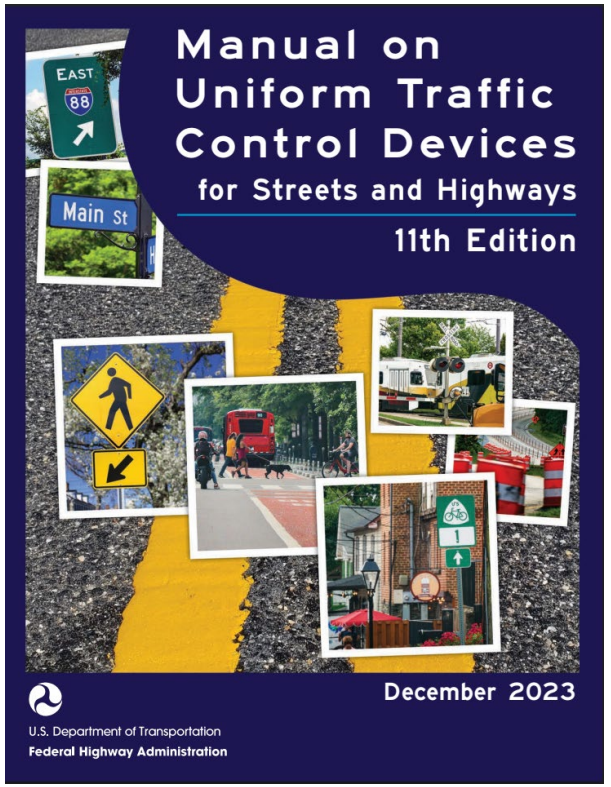


Source: 2024, Fred Gordy, Michael Baker International

Cybersecurity in National Guidance



Cybersecurity integrated into ITE Traffic Signal Maintenance Handbook 2023



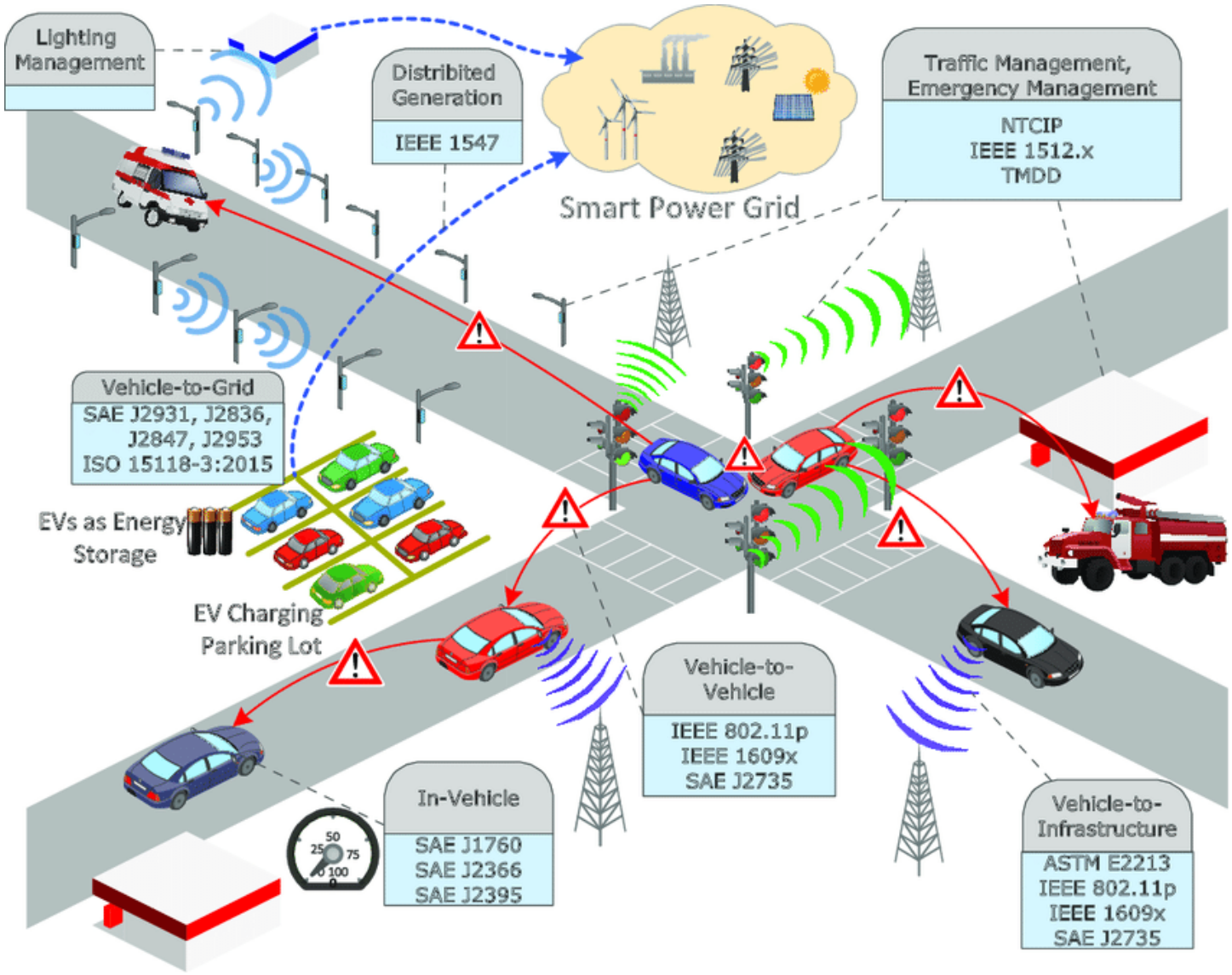
No cybersecurity mentioned in the MUTCD 11th Edition

Cybersecurity Standards

- Guidelines
  - NHTSA recommendation to follow National Institute of Standards and Technology's (NIST's) documented Cybersecurity Framework
  - ISO/SAE 21434, "Road Vehicles – Cybersecurity engineering"
  - Auto-ISAC, Best Practices
  - SAE J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems
  - UNECE WP.29 Cybersecurity Regulation
  - NEMA TS 8-2018 "Cyber and Physical Security for Intelligent Transportation Systems (ITS)"
  - USDOT RSU Specification

ITS Standards

Michael Baker INTERNATIONAL



We Make a Difference

More Best Cybersecurity Practices

- Implement and strengthen physical security measures around ITS devices and/or facilities.
- Apply network segmentation, monitoring, detection, and blocking systems.
- Conduct regular security audits to make sure there are no gaps in the network, hardware, software and firmware.

THANK YOU

Jim Katsafanas, PE, PTOE
National Connected and Automated Vehicle technology Director
jkatsafanas@mbakerintl.com
412-269-4635

Michael Baker INTERNATIONAL | *We Make a Difference*