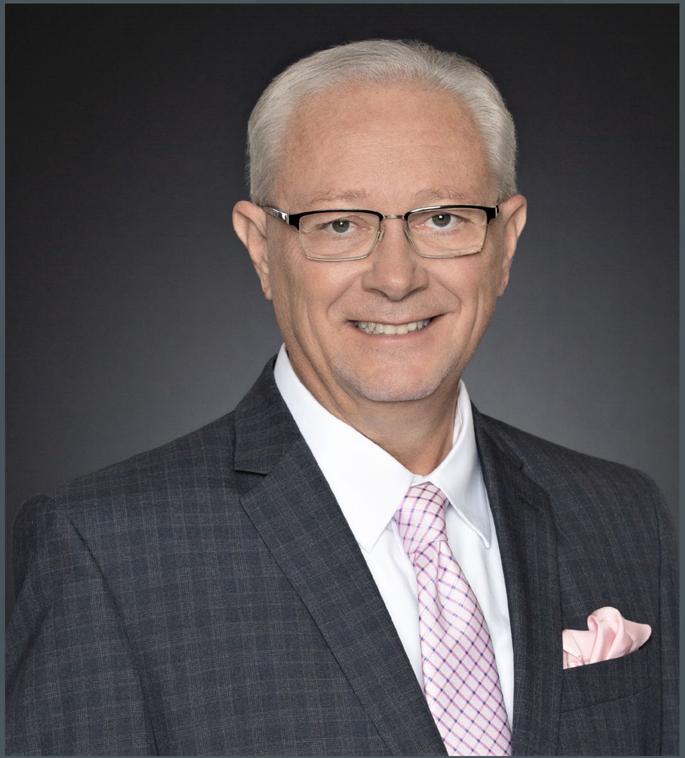
Automated, Connected, Electric and Shared (ACES) Vehicles
….. And the Expanded Cybersecurity Threat Surface



STEVE JOHNSON, MSC, CISSP, CVP

HDR, SR. CONTROL SYSTEMS CYBERSECURITY SPECIALIST

Florida Automated Vehicle Summit, 2023

AGENDA

- Introduction and Overview of Cyber Threat Surface / Attack Vectors
- Typical ITS Threat Surface
- Expansion of the Threat Surface with CAV
- Expansion of the Threat Surface with EV
- Expansion of the Threat Surface with Shared Use,
- Best Practices

Introduction and Overview of Cyber Threat Surface / Attack Vectors

Attack Surface Meaning

The attack surface is the number of all possible points, or attack vectors, where an unauthorized user can access a system and extract data. The smaller the attack surface, the easier it is to protect.

> Organizations must constantly monitor their attack surface to identify and block potential threats as quickly as possible. They also must try to minimize the attack surface area to reduce the risk of cyberattacks succeeding. <u>However, doing so becomes difficult as they expand their digital footprint and embrace new technologies</u>.

The attack surface is split into two categories: the digital and physical.

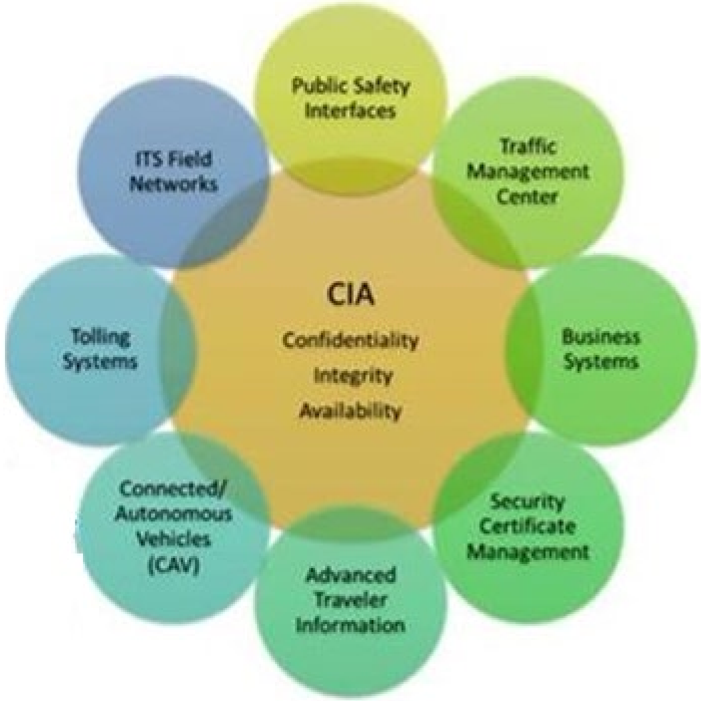
Digital Attack Surface

The digital attack surface area encompasses all the hardware and software that connect to an organization's network. These include applications, code, ports, servers, and websites, as well as shadow IT, which sees users bypass IT to use unauthorized applications or devices.

Physical Attack Surface

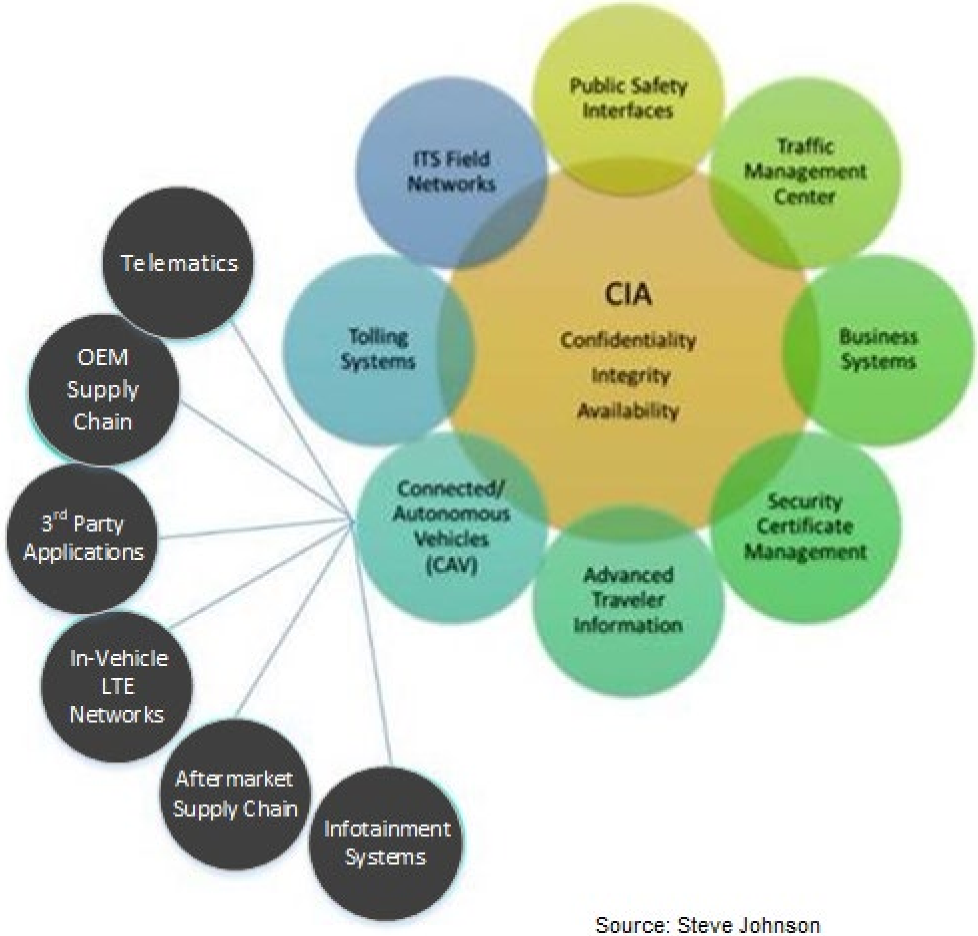
The physical attack surface comprises all endpoint devices that an attacker can gain physical access to, such as desktop computers, hard drives, laptops, mobile phones, and Universal Serial Bus (USB) drives. The physical attack threat surface includes carelessly discarded hardware that contains user data and login credentials, users writing passwords on paper, and physical break-ins.

TYPICAL ITS THREAT SURFACE


Public Safety Interfaces
Traffic Management Center
Business Systems
Security Certificate Management
Advanced Traveler Information
Connected/ Autonomous Vehicles (CAV)
Tolling Systems
ITS Field Networks
CIA
Confidentiality
Integrity
Availability

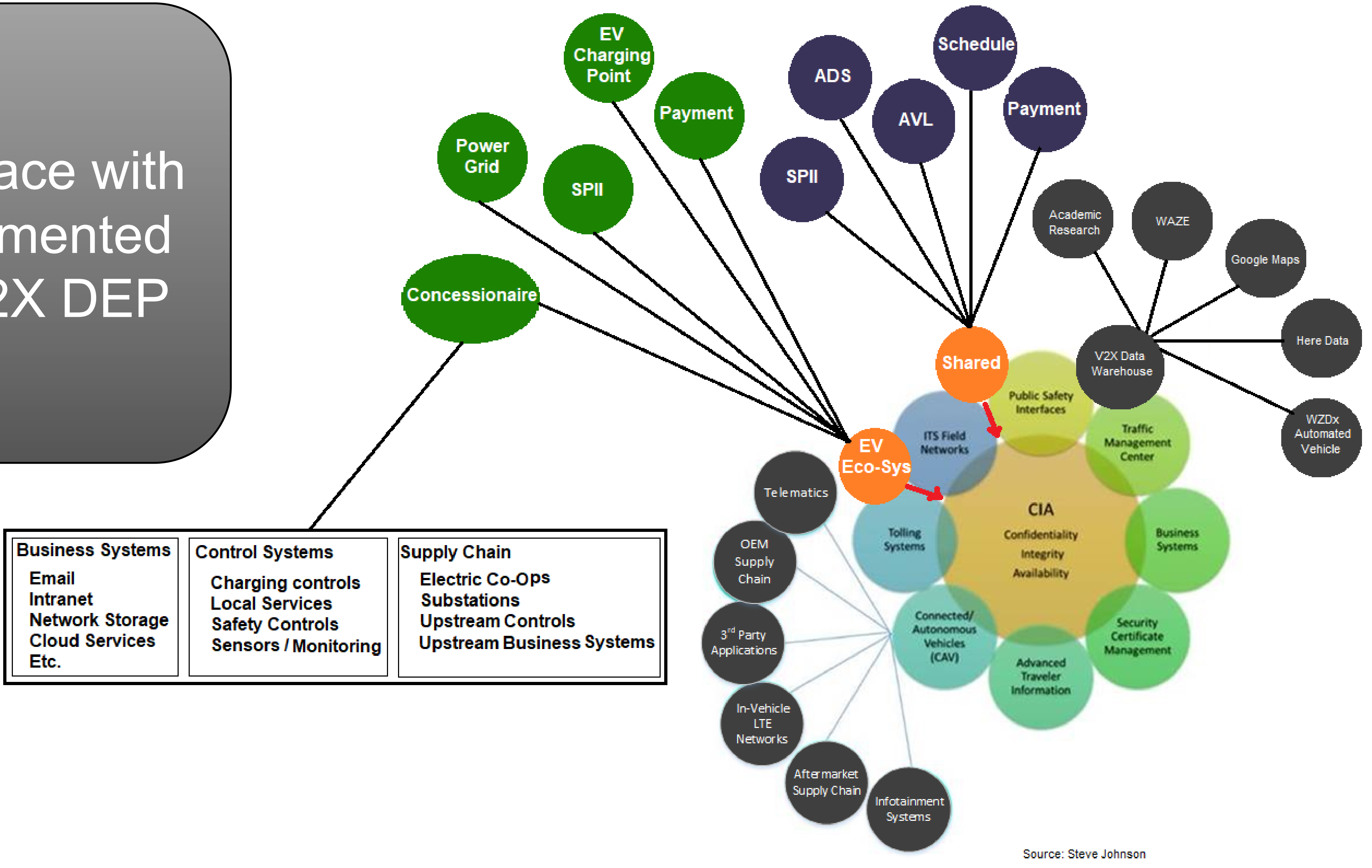
Source: Steve Johnson

EXPANDED THREAT SURFACE - CAV



Source: Steve Johnson

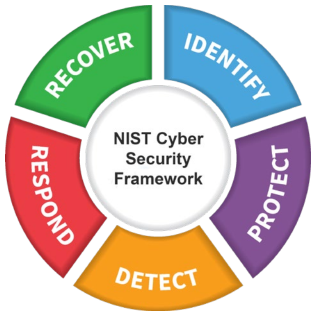
Threat Surface with Fully Implemented ACES + V2X DEP

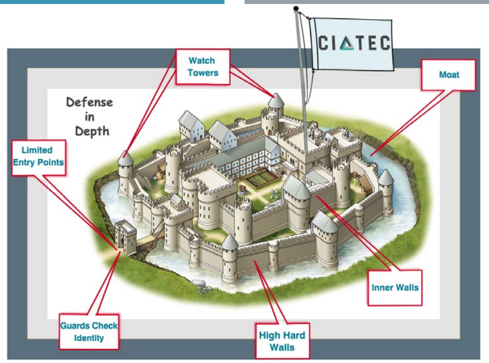


Business Systems	Control Systems	Supply Chain
Email	Charging controls	Electric Co-Ops
Intranet	Local Services	Substations
Network Storage	Safety Controls	Upstream Controls
Cloud Services	Sensors / Monitoring	Upstream Business Systems
Etc.		

Source: Steve Johnson

BEST PRACTICES





Fla. Admin. Code R. 60GG-2.001

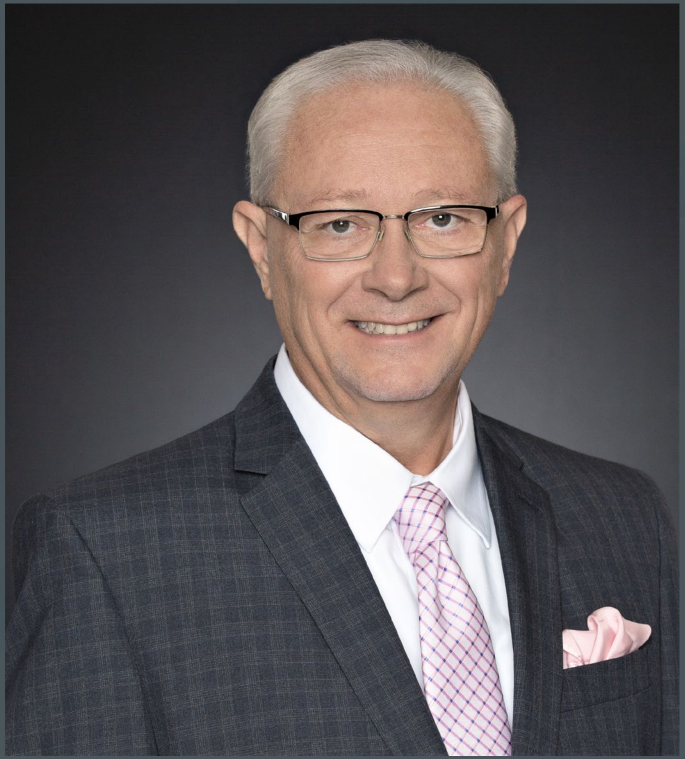
Challenges

- Regulated vs. Non-regulated Industries
- Evolving Standards and Laws
- Rapidly Advancing Technology
- Workforce Development
- Specialized Skills
- Continuous Monitoring

Baseline Best Practices

- Follow an Established Risk Management Framework (NIST CSF / FAC 60GG)
- Implement Defense in Depth
- Implement Security by Design
- Use Consultants as extension of staff
- Include incident response in recurring exercises.

Thank You
Questions?



STEVE JOHNSON, MSC, CISSP, CVP

HDR, SR. CONTROL SYSTEMS CYBERSECURITY SPECIALIST