Cybersecurity Challenges in Transportation Systems

Anwesh Tuladhar

Ph.D. Student advised by Dr. Xinming (Simon) Ou

Department of Computer Science and Engineering

University of South Florida

Acknowledgement

This research is supported by the National Science Foundation NSF CRISP Award No. 1638301:

CRISP Type 2: Integrative Decision Making Framework to Enhance the Resiliency of Interdependent Critical Infrastructures.

In collaboration with the City of Tampa Transportation Management Center

Motivation: Transportation and Technology

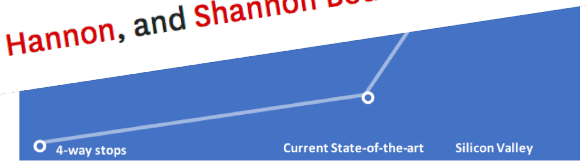
- Current status
  - Adapt techn… …nprove usa…
- Emergi…
  - Conn…
  - Auton… …nology

GOVERNMENT

Technology Is Changing Transportation, and Cities Should Adapt

Harvard Business Review

by Stefan M. Knupfer, Eric Hannon, and Shannon Bouton



Tech and the future of transportation: From here to there

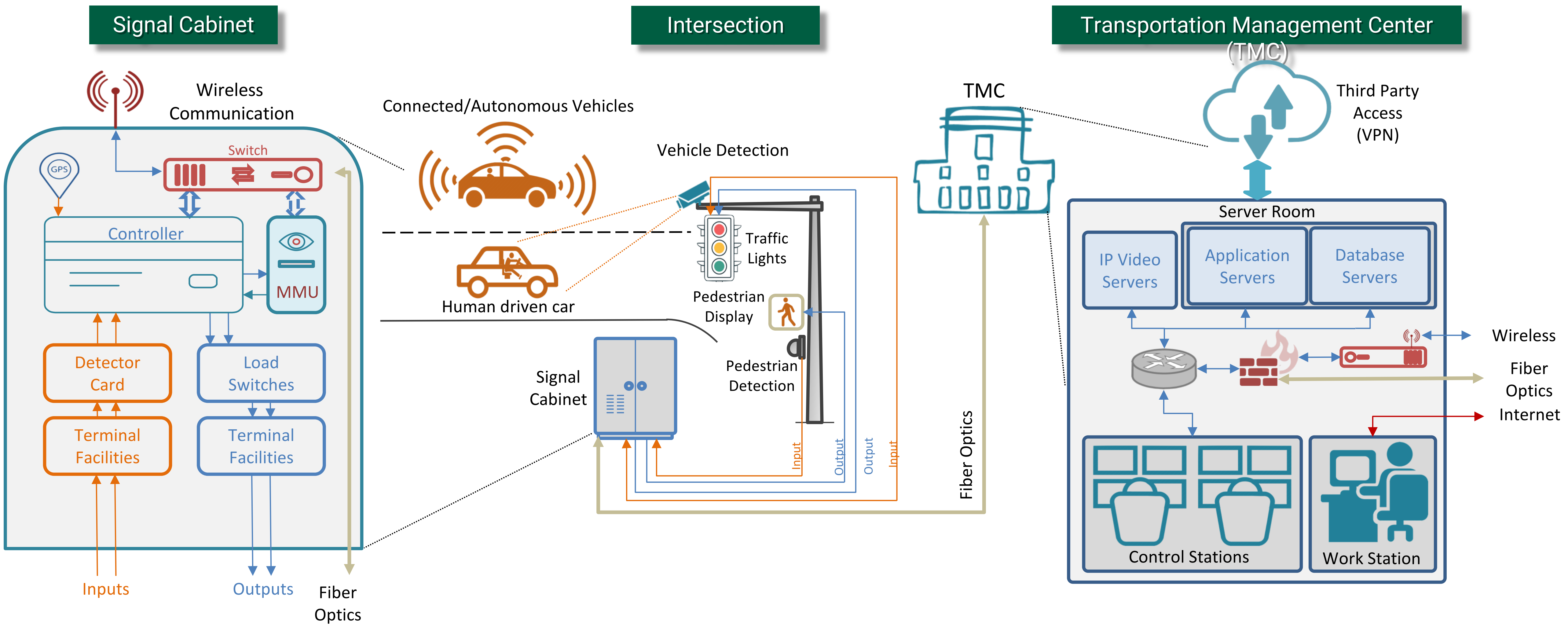
Transportation is about to get a technology-driven reboot. The details are still taking shape, but future transport systems will certainly be connected, data-driven and highly automated.

Transportation systems inherits the Cyber-security problem.

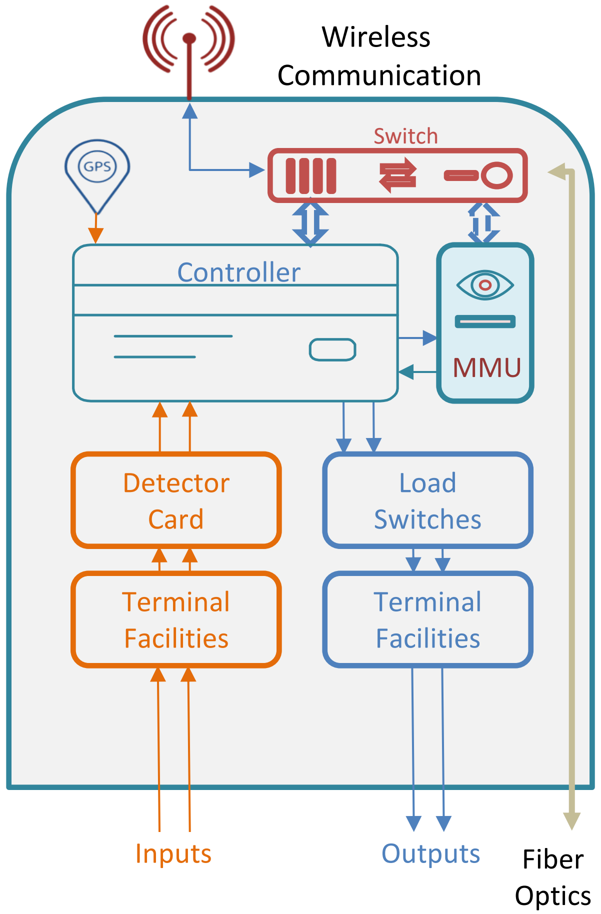
Outline

- Case study: City of Tampa Transportation Management Center
  - Overview of the current transportation system
  - Cyber risk analysis
- Demo
- Conclusion and Take away

Overview of the Transportation System

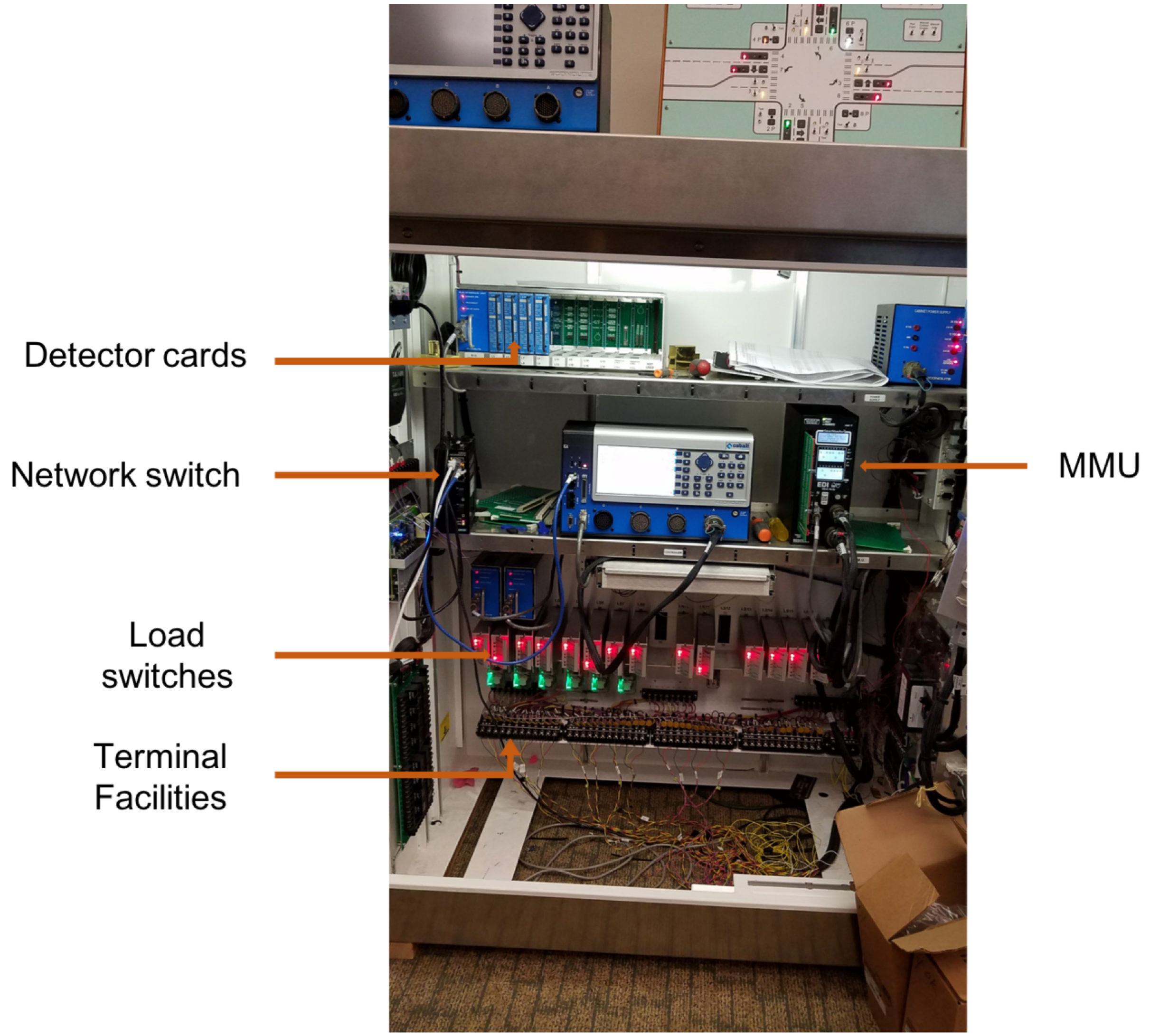


Signal Cabinet



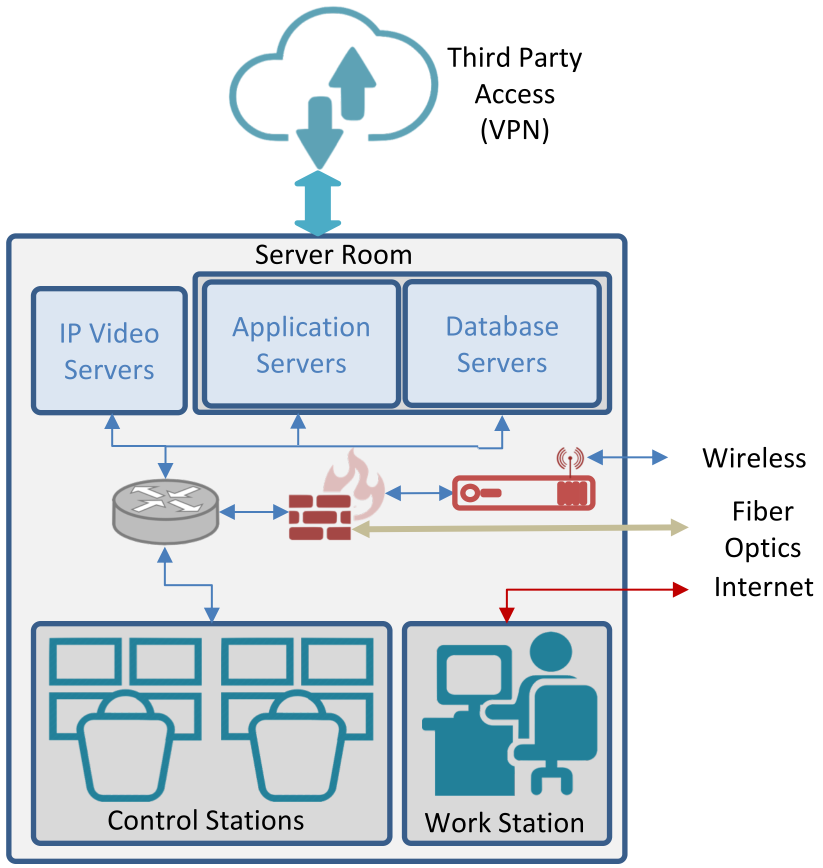
- Role: Control the intersection
- Brain: Controller
  - OS: Linux(2.6.3x or greater) based
  - Driven by:
    - Programmed signal timing
    - Detector inputs
    - External requests: Transit Signal Priority (TSP), pre-emption (trains)
  - Ways to program:
    - Direct: Front panel, LAN connection with laptop, data-key, USB
    - Wireless: Wi-Fi Connection with tablet
    - TMC: Centracs, client applications
- Watch dog: Malfunction Management Unit (MMU)
  - Role: Enforce the safety/conflict policies
  - Driven by: soldered circuit board
- GPS: Account for time drift to maintain coordination
- Communication: Fiber optics, wireless, twisted copper

Signal Cabinet: Safety features



- Controller:
  - Powered through MMU so that it cannot be taken out of the loop
  - Username and password (Not used).
  - 3 access levels: administrator, data change level, data display level (Default is admin).
  - Has a backup database.
- MMU:
  - Hardwired/soldered input.

Transportation Management Center (TMC)

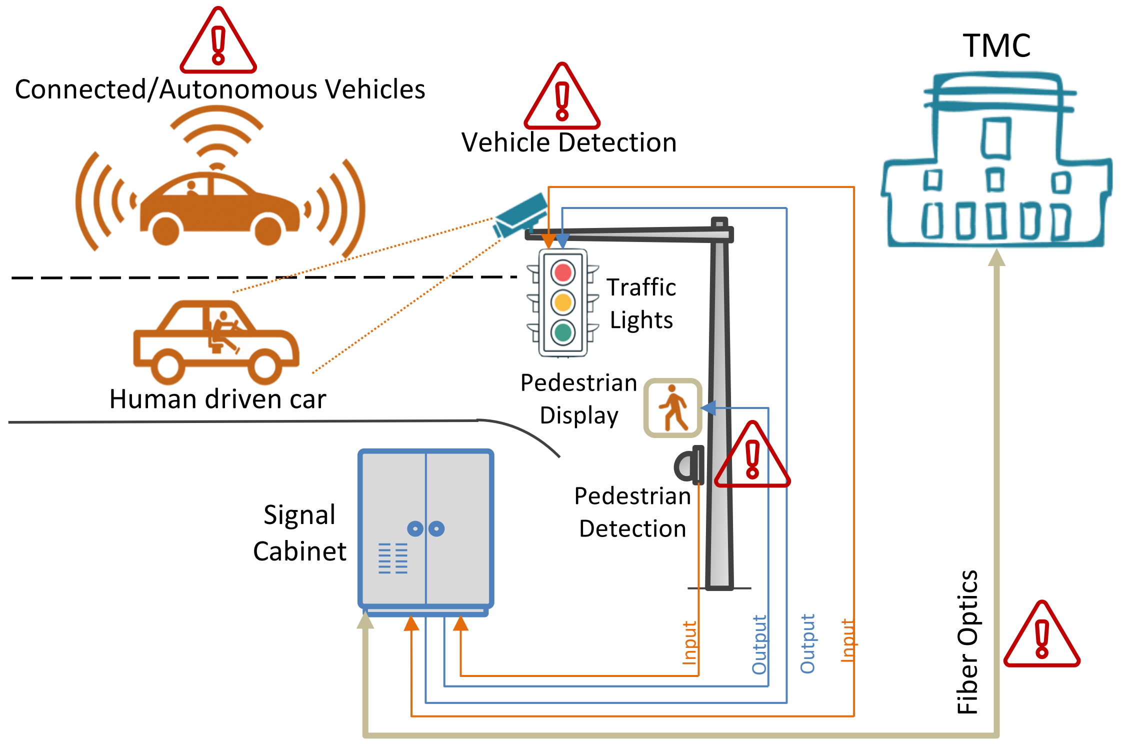


- Role: Monitor and control ALL intersections
- Communication:
  - Protocol: NTCIP level 2 compliant
  - Wireless: Mesh network, single hub in TMC can manage 20 spokes
  - Third party access through VPN
- Applications:
  - MTCS:
    - MS-DOS based (legacy twisted copper support)
    - Command and Control type system.
    - If command and feedback vary: Controller runs it’s stored timings.
  - Centracs 2.0:
    - Advice and Consent type system (Controller is stand alone)
    - Can view status of each controller, view reports for single controller or for a zone, check logs
  - Connected Signals:
    - Mobile app that shows signal timings (red light notifier).
    - Have a network sniffer in the main switch.

TMC: Safety features

- Transportation network is isolated from the outside world.
- Network:
  - Firewall
  - Virtual Private Network (VPN)
- MTCS:
  - Easy detection of command and feedback inconsistence.
- Centracs:
  - Username and password
  - Logs every change made to signal timing (version control like)
  - Provides alerts, logs and reports.

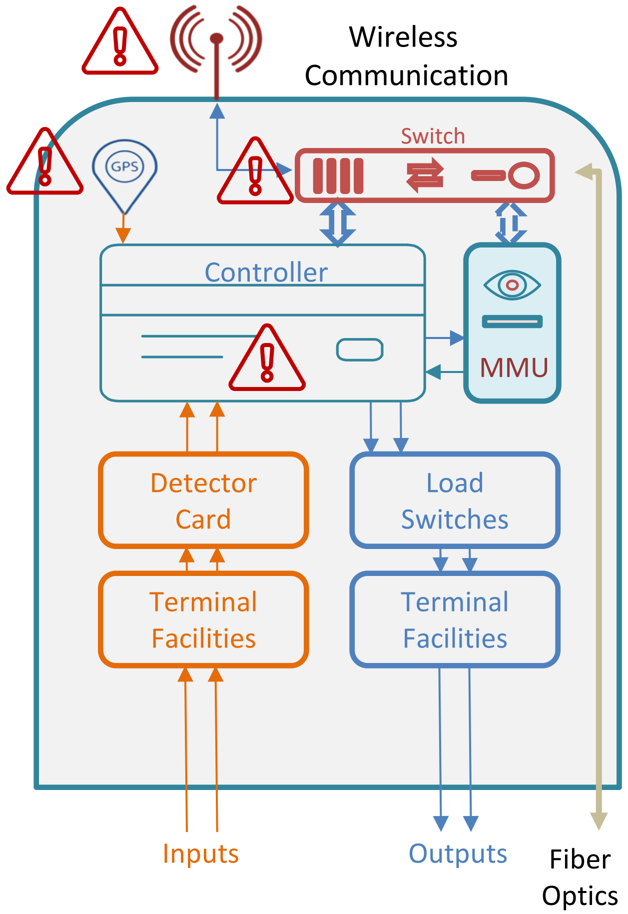
Risk Analysis: Intersection



- Vehicle detection:
  - Cerrudo (2015) and Ghena et al (2014) have shown that wireless vehicle detectors can be hacked.
  - Impact: Congestion
    - Always runs a full cycle. Equivalent to a stuck pedestrian button.
    - Side street never gets serviced.
  - Resolution: Can be detected using monitoring tools (Waze, Bluetoad, CCTV)
- Fiber optics:
  - Impact: Loss of communication.
  - Resolution: Easily detected.
- Connected Vehicles:
  - Miller et al (2015) showed that cars can been hacked.
  - Challenges:
    - Vehicles get a bigger say.
    - More devices to hack.
- Other issues:
  - Privacy issues.
  - Transmitting massive amount of data.

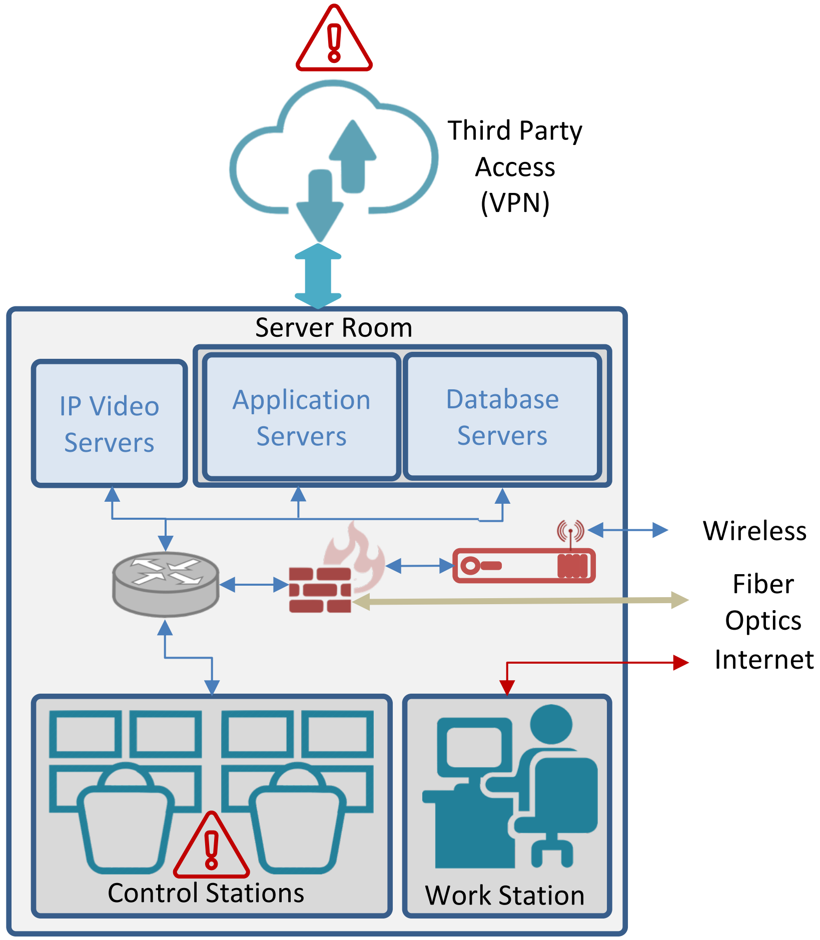
References:
1. Cerrudo, Cesar. "An emerging us (and world) threat: Cities wide open to cyber attacks." *Securing Smart Cities* (2015).
2. Ghena, Branden, William Beyer, Allen Hillaker, Jonathan Pevarnek, and J. Alex Halderman. "Green Lights Forever: Analyzing the Security of Traffic Infrastructure." *WOOT* 14 (2014): 7-7.
3. Miller, Charlie, and Chris Valasek. "Remote exploitation of an unaltered passenger vehicle." *Black Hat USA* 2015 (2015).

Risk Analysis: Signal Cabinet



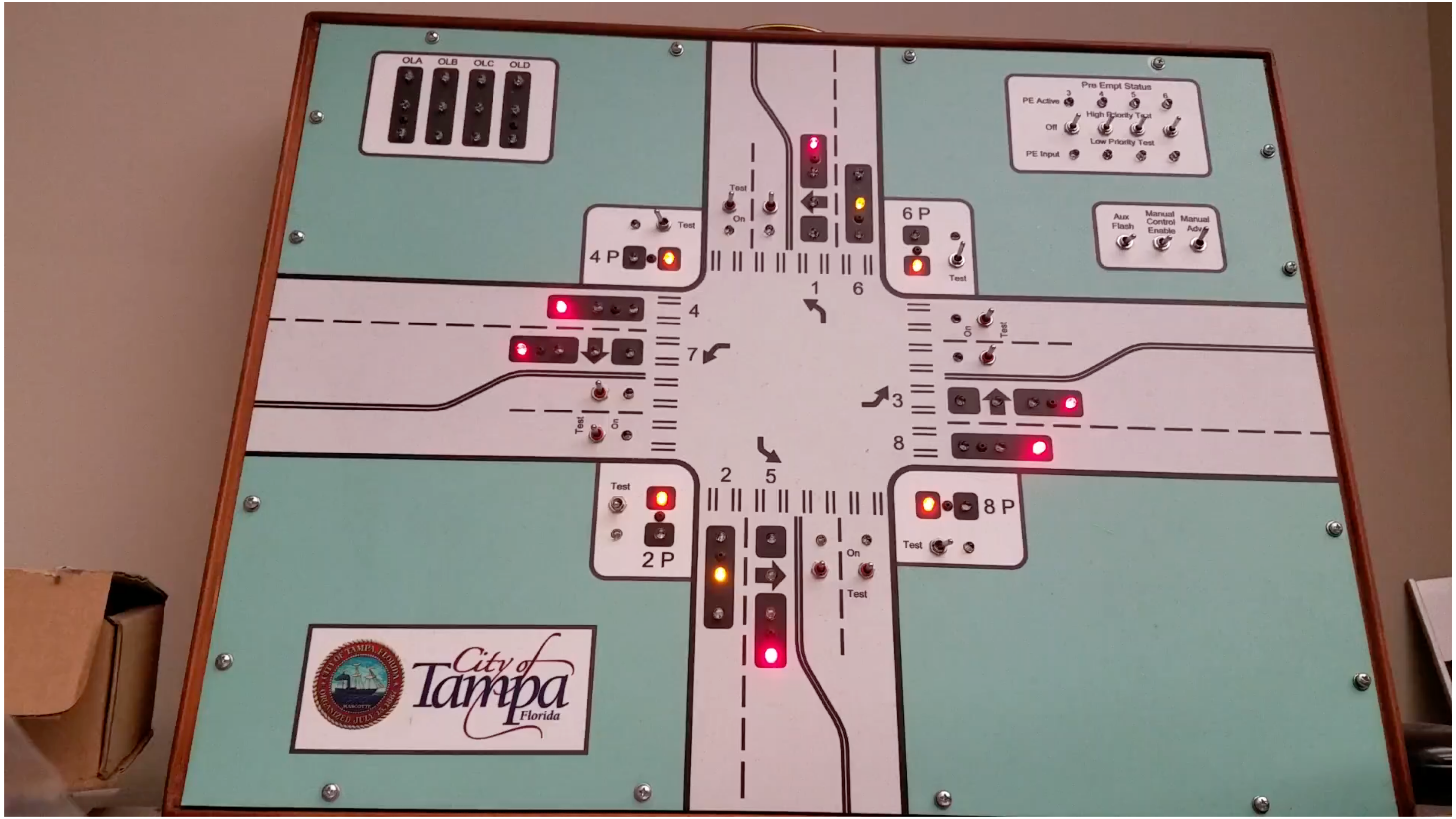
- Wireless Communication:
  - <u>Outcome</u>: Gain access to controller.
  - <u>Resolution</u>: Disable SSID broadcast, enable encryption, do not use default configuration/credential
- Controller:
  - Ghena et al (2014) have shown it can be compromised.
  - <u>Outcome</u>: Change signal timing, update firmware.
  - <u>Impacts</u>: Congestion, diminished safety
    - But MMU maintains safety.
  - <u>Resolution</u>: Disable debug port, enable password protection, enable access control
- Network:
  - <u>Outcome</u>: Gain access to all communication
  - <u>Impacts</u>: Denial of Service (DoS) attack
  - <u>Resolution</u>: Firewalls

Risk Analysis: TMC



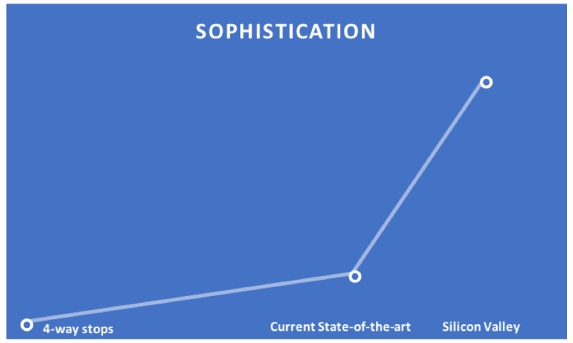
- Control stations:
  - Social engineering.
- Third party access:
  - Are they following security practices?
  - Outcome: Access to entire infrastructure.

Demo


OLA
OLB
OLC
OLD
Pre Empt Status
PE Active
Off
High Priority Test
Low Priority Test
PE Input
Aux Flash
Manual Control Enable
Manual Adv
4 P
6 P
2 P
8 P
Test
On
1
6
4
7
3
8
2
5
City of Tampa
Florida

Conclusion

- Cybersecurity is **currently** not a major concern for transportation systems.
  - reliance on the isolated network and physical protection of devices.
  - i.e. all the systems are within the trust boundary.
- However existing architecture poses serious cybersecurity threats for the **emerging** transportation technologies.
  - With connected and autonomous technologies, the isolation assumption is no longer valid.
  - Plus the gap between current and emerging technologies is vast.
  - The stakes are much higher in transportation than in traditional IT systems.




Harvard Business Review

GOVERNMENT

Technology Is Changing Transportation, and Cities Should Adapt

by Stefan M. Knupfer, Eric Hannon, and Shannon Bouton

Questions ?