Cyber Risks to Transportation Systems… and how to mitigate them

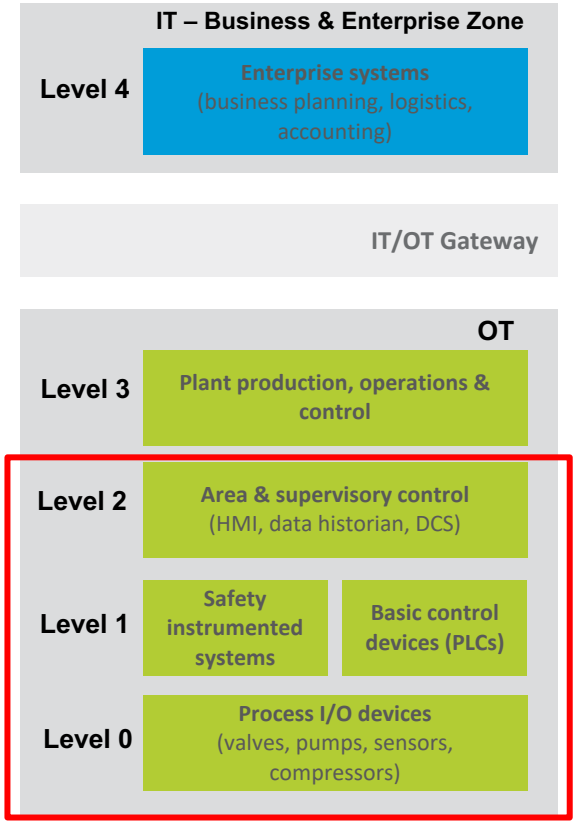
Rick Tiene
Vice President
Government & Critical Infrastructure

Mission Secure, Inc.

Component Level Cyber Protection : A New Paradigm

The Problem

Purdue Model **levels 0-2 currently lack cyber protections** leaving process control systems vulnerable when an attack penetrates into the operational technology space



Purdue ICS Cyber Model

What Current IT Protections Do (IDS/IDP/Firewalls)

- Stop entry based on known exploits and rules, not on Zero Day attacks
- Forewarn that an event might occur
- Monitor network looking for “abnormal” behavior
- Provide Data to what has happened at the network level (not specific to equipment)

The Gap - OT Protections

- Clearly understand an attack is underway and stop it from occurring - real time
- Detect attacks no matter how they are being initiated (no need for prior pattern)
- Provide detailed, specific forensic data for post event analysis
- Protect against, Zero Days, Supply Chain Attacks, Insider Attacks, ransomware, etc.

Cyber Threats to Control Systems: Physical Impact

Attacks

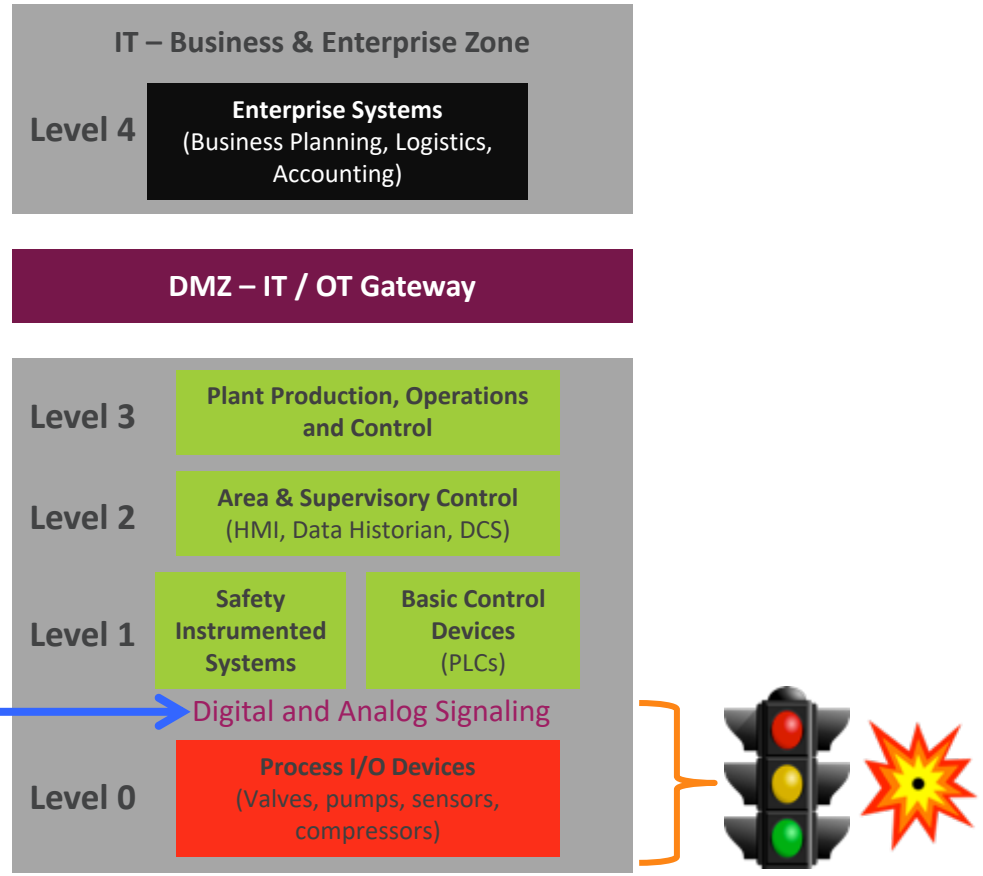
Malware
- Stuxnet
- BlackEnergy 1, 2, 3
- Havex
- Shamoon 1 &2
- Ransomware
- Sleeper Code
- Others

Events
- Aurora
- German Steel Plant
- Ukraine 2015 & 2016
- Factory controls
- Pipeline flow meter
- Cruise ships
- Dallas Siren System
- Speed cameras
- Others

Attack Sequence

1. Multiple potential points of entry
2. Enter the OT
3. Mask the actual state of the attack (physical system)
4. Take control of the CS and safety response
5. Create the impact

Purdue Control System Model



Attacker's Goal is gaining control of level 1 devices to control level 0 & process

Vulnerabilities Exist at Three Levels or Points of Attack

HMI/ATMS/operator | LEVEL 2

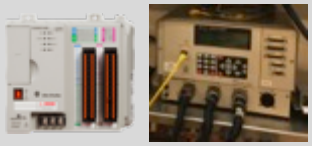
- Loss of view
- False view
- Loss of control

Operator at the Human Machine Interface (HMI) / ATMS

TCP/IP Ethernet traffic

Controller/PLC/ATC | LEVEL 1

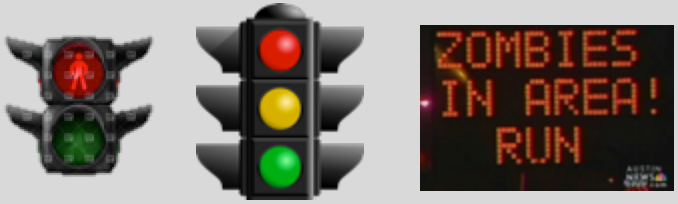
- Instruct devices, change process, cause damage
- Send “normal” signals across network to HMI
- Steal sensitive data, report false data



Analog & digital signals

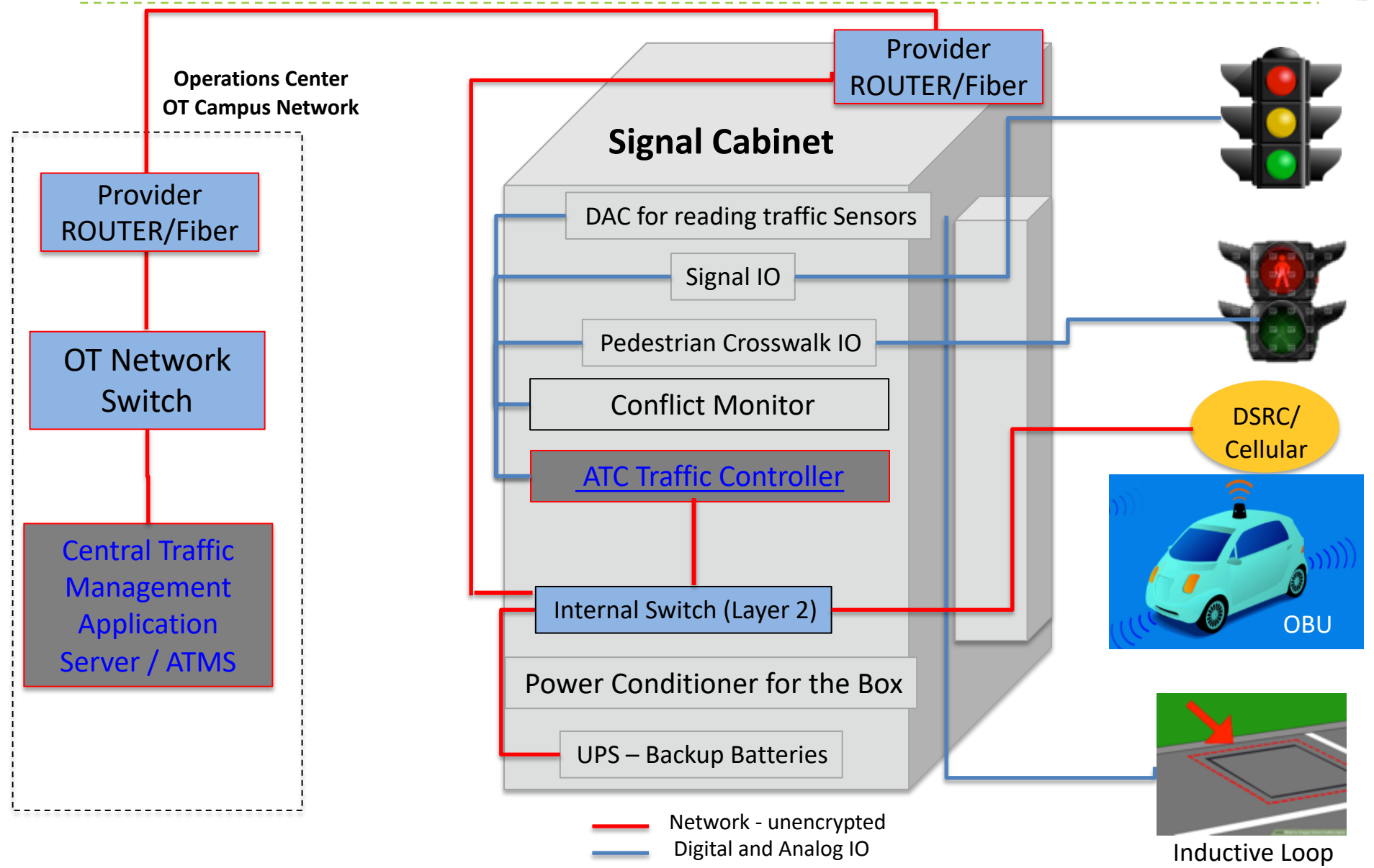
Field device/process | LEVEL 0

- Remotely configurable sensor
- Get between sensor/ATC
- Sending false data to trick ATC



Successful attacks impact public safety in traffic systems

Typical Traffic Signal Cabinet - unprotected



Sample Traffic System Vulnerabilities

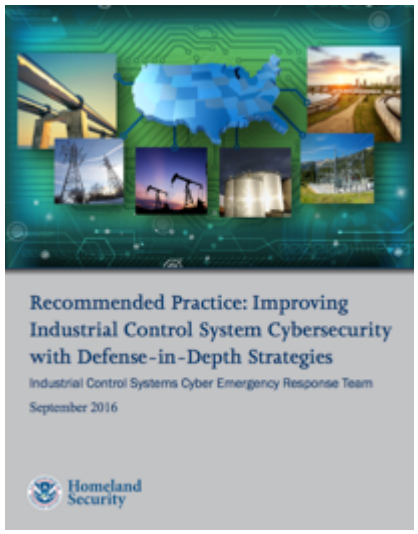
Issue	Problem	Impact
No true "closed" system	• RF / Wireless • Vendor/contractor access • Third party carriers • Other regions/partners • Drill or universal keys $ online • Ops center network risks • Connected vehicles	• Easy to gain access to field cabinet and take control • **Backhaul to ops. Center and all other cabinets** • **Take control of entire system**
No authentication / UDP / unsecured communications	• Anyone can access controller / issue commands / connect / change/wipe • Control the power management systems • Man in the middle attacks	• Take over intersections • Flash mode / must physically go to cabinets to reset / would not know • Yellow / green / no red • **Change/wipe configs/OS. Own controller and UPS** • Multiple power system manipulations
Extra unsecured services on ATC	• Telnet, FTP, basic security	• Easy access for adversaries to critical functions/configs.
RSU vulnerabilities	• Unencrypted wireless • Basic security on devices	• Change the SPAT information, tell car/bus improper signal info

Selection of Traffic Security Vulnerabilities Continued

Issue	Problem	Impact
No OT network monitoring	• Lack OT traffic visibility	• Don't know if being attacked or recon underway
No prevention	• No way to stop an attack • Can't block access • Can't block rogue commands • Can't block ransomware/malware	• Change signals, go dark • Lock up controllers • Wipe controllers • Power issues • Overcharge/blow up batteries
No restoration capability	• Must go to all cabinets, manually restore	• Huge time and resource issues, may not solve issue just reset and then attack replay
No forensics	• No idea where attack came from, how, where else it may be	• Guessing about the cause, where it could happen next, how to recover
Physical access risks	• Access by contractors, police, fire, rescue • Remote locations • Physical security challenge	• Hundreds/thousands of opportunities to install rouge devices and go up/down network

ASSESS DESIGN

First Steps to STRONG cybersecurity

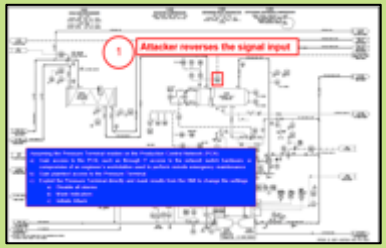


Assess OT network and specific asset/systems

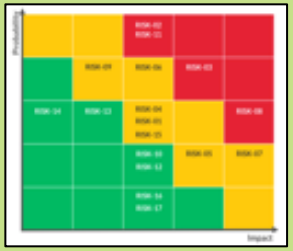
- ✓ Understand As-Is, identify security gaps
- ✓ Detailed look (P&IDs, network drawings, security settings)
- ✓ Optional hands-on red teaming
- ✓ NIST/DHS/IEC 62443 standards basis for methodology
- ✓ Live, Passive OT traffic analysis to see what is happening

Design enhanced cyber defense architecture, identify mitigations

- ✓ Strengthen existing protections, identify new mitigations
- ✓ Scorecard and clear, actionable, prioritized roadmap



Current system security posture



Risk and Business Prioritization

Architecture and Solution Recommendations

Security Implementation Roadmap

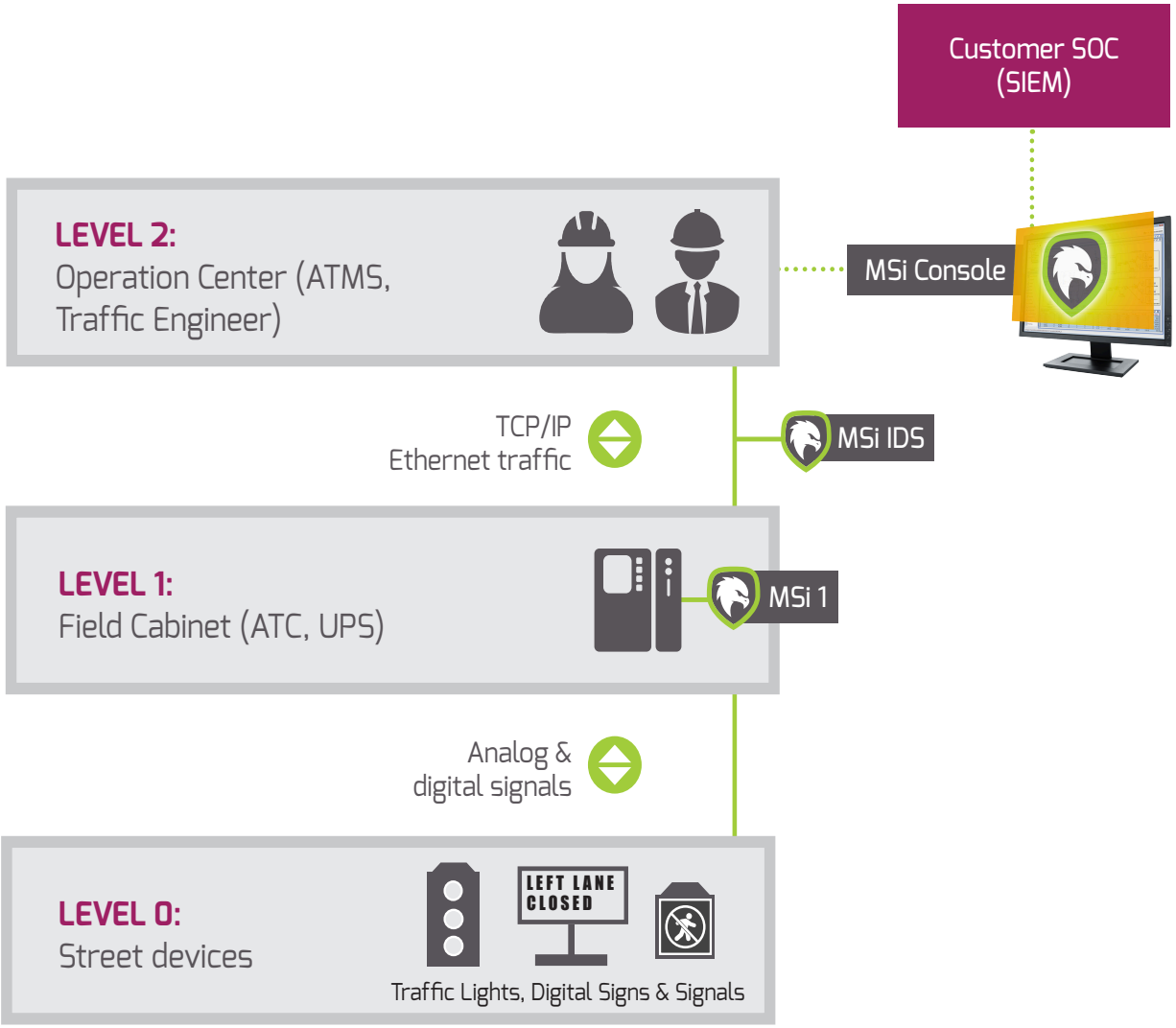
Identify low hanging fruit and cost effective path to close gaps

Implement a Platform to protect

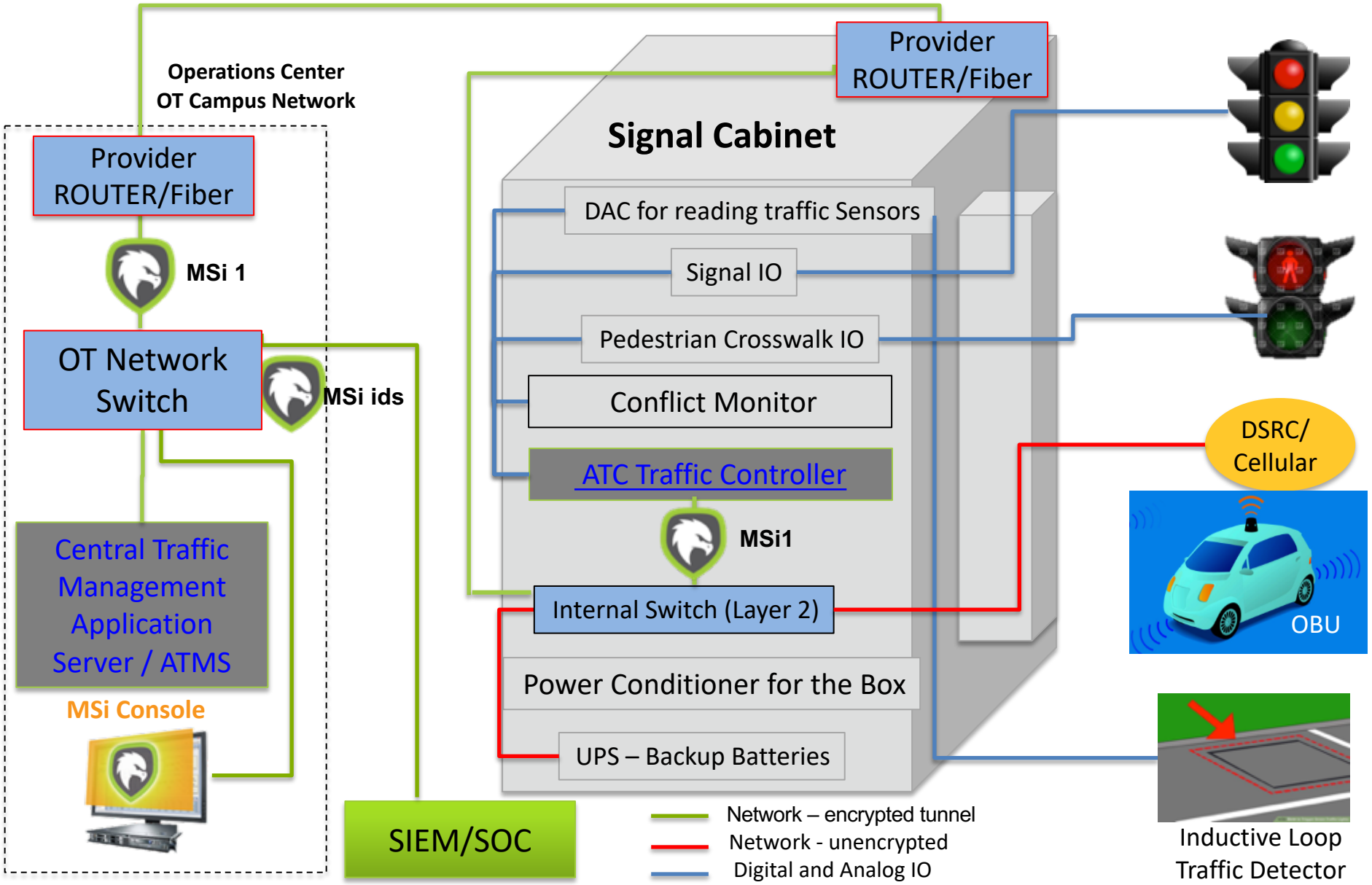
Selected Features

LEVELS 0-2

- Monitor network traffic
- Controller configurations
- Block Scans/Ddos
- Block ransomware
- Restrict access to/from
- Inspect/block bad commands
- Encrypt traffic
- Corrective actions
- Forensic data gathering



Typical Traffic Signal Cabinet – Protected



One New Solution: 4 Main Components

MSi Console

- Virtual Appliance, VM ware or MSi Cloud
- Operator & SOC interface to cyber OT world
- Managed/visualize data from MS ids
- Manage fleet of Sentinels & MSi 1's
- Understand system state
- Investigate detected incidents / troubleshoot
- Manage corrective actions
- Forensic information down to level 0
- Perform virtual MSi Sentinel functions
- Analyze OT data and perform AI
- Integrate with SOC, SIEM and third party IT systems

MSi ids

Levels 1 and 2 network monitoring

Visibility

- Passively detect abnormal OT traffic
- Remotely trouble shoot OT issues

MSi 1

Level 1 cyber defense

Protection

- Protect PLCs, safety systems, RTUs, Digital relays, flow controllers, Intelligent Electronic Devices and more

MSi Sentinel

Levels 0- 1 cyber defense

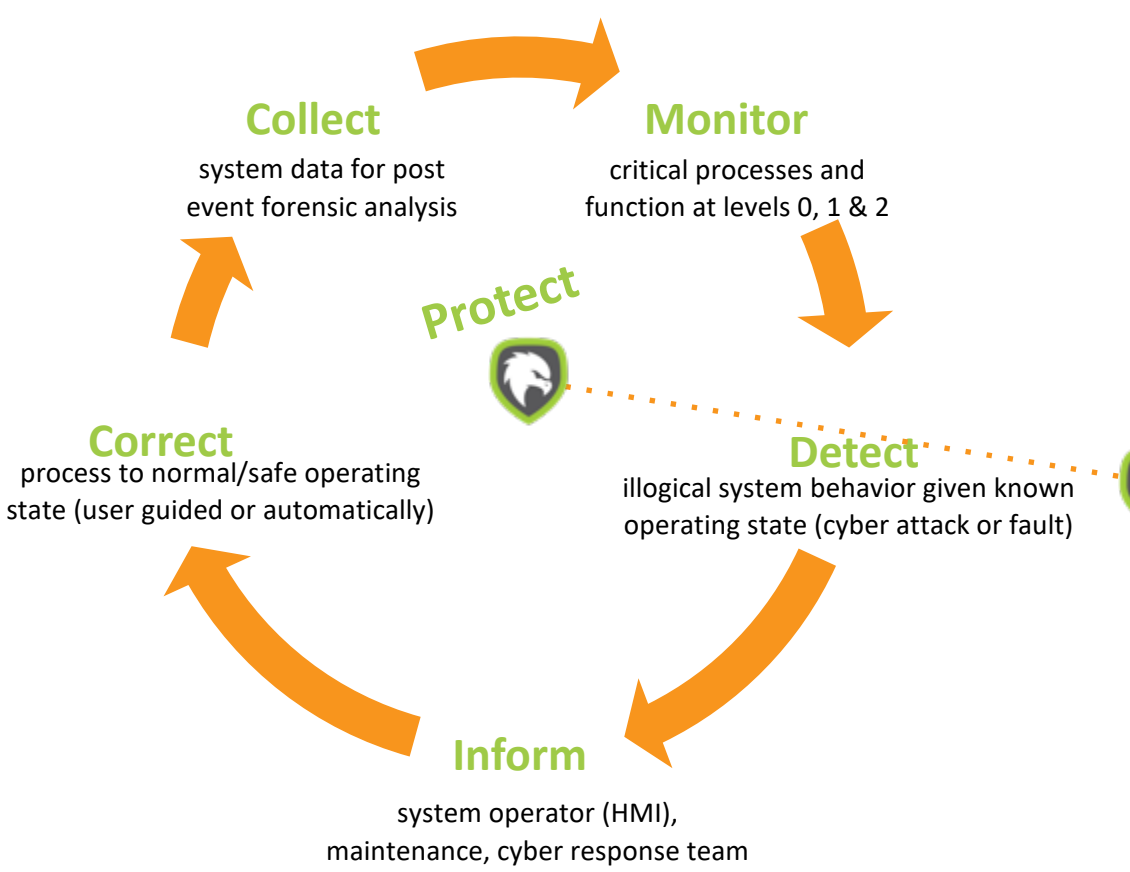
Visibility and Correction

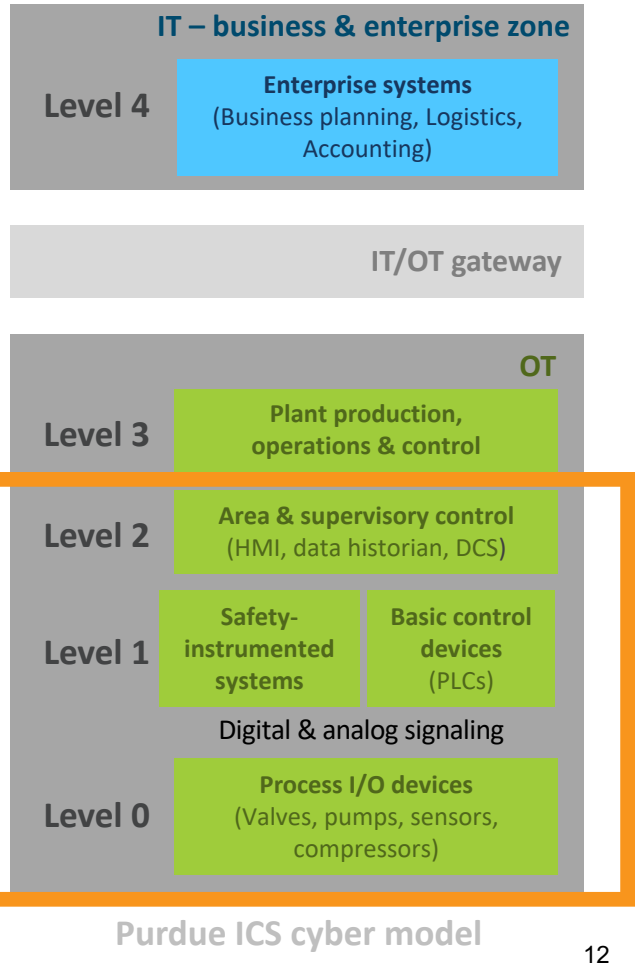
- Validate operational processes at digital and analog signals, controller, HMI
- System Aware
- Horizontal and vertical analysis

Level 0-2 Protection, Industrial Grade, Military Strength, Cost Effective

What's Needed? - Full Circle of Protection

Protection from Cyber Attacks





Purdue ICS cyber model

Sample: Pre-scoping Initial Thoughts & ICS Cyber Security Framework

Example Areas on the Right Path

+ Some IT best practices (VPN, antivirus, disaster recovery plan, data backup)
+ Firewalls implemented, possible network segmentation
+ OT system network diagram exists (but more detail is needed)

Example Areas Needing Improvement

⊗ IT/OT interaction described as limited, need more info
⊗ 3rd Party Remote Access
⊗ Wireless used at Secured Plant
⊗ Commercial versus industrial network equipment
⊗ No continuous OT network monitoring
⊗ No patch/update testing environment
⊗ No periodic review of user access rules
⊗ No cyber security at flow meters/control cabinets/critical controllers
⊗ No OT Disaster Recovery plan and backup
⊗ No security assessments/audits

Quick Look: Current *AS-IS* Score: 10% (weak)

CSF / Status	Target Architecture
5. Recover	Recovery Plan Improvements Communications
4. Respond	Response Planning Communications Analysis Mitigation Improvements
3. Detect	Security Continuous Monitoring Detection Processes Media Protection
2. Protect	Access Control Awareness and Training Data Security Information Protection Maintenance Protective Technology – Level 0 and 2
1. Identify	Asset Management Business Environment Governance Risk Assessment/ Risk Management

Not Addressed Some Effort Better Progress

How to address?
Deep Dive Vulnerability and PEN testing (Sandbox)

Cyber Risk / Attack / Protect / Test Matrix

How to address?
People, Process, Technology

- ✓ Awareness
- ✓ Cybersecurity training
- ✓ Tailored security controls
- ✓ Policies & Governance
- ✓ Incident recovery plan
- ✓ Equipment PEN testing

- ✓ Harden OT network
- ✓ Harden field cabinets
- ✓ Ongoing equip. testing
- ✓ Continuous OT and field cabinet monitoring
- ✓ Blocking to/from cabinet
- ✓ ATC real time monitoring
- ✓ Encryption ATMS/ATC
- ✓ Dual form authentication
- ✓ Complex passwords
- ✓ ATC key pad features
- ✓ No IP addresses written in cabinet
- ✓ Data collection

How it works

- Provide **visibility** of OT network traffic and **protection** for key controllers/network
- Install low cost, **security appliances** ($200 - $500 each) on site:
  - ☑ Sit in front of each system control unit and access to/from Cloud
  - ☑ Block unwanted activity (ingress and egress)
  - ☑ Stop Malware or Ddos from attacking controllers
  - ☑ Look for changes to controller settings
  - ☑ Map normal traffic and monitor for abnormal behavior
  - ☑ Understand true system state (i.e. temperature)
  - ☑ Encrypt traffic between controllers and to/from Cloud
  - ☑ Collect data for forensics around event
  - ☑ Multiple protocols (Modbus, CIP, OPC, BacNet, Serial & Ethernet)

- **MSi Console** on premise or hosted in the cloud to centrally monitor, manage, alert
  - ☑ Centrally manage multiple appliances/assets, configuration, rules
  - ☑ Notify MSi / building manager / engineer of attack
  - ☑ Corrective action – restore controllers to last known good state
  - ☑ Show all is “ok” at building or when/where issue exists (like NEST)
- Optional 24/7/365 monitoring and incident response

MSi 1 – Level 1 Defense for Traffic Control Devices

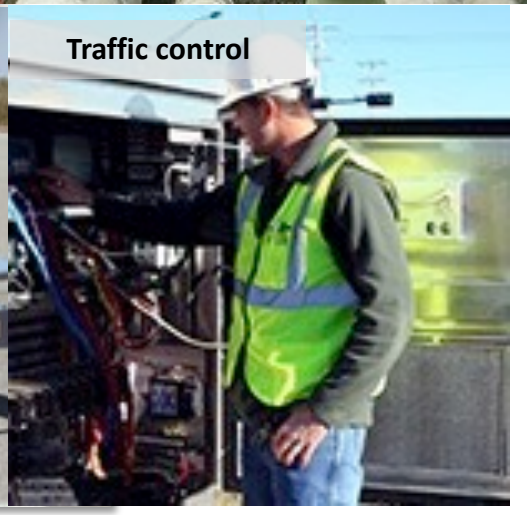
Key Advantages

- ✓ Protect traffic controllers, power management and other traffic control devices from cyber attack
- ✓ Prevent unauthorized access **AT** field cabinet **TO** traffic controllers & UPS
- ✓ Prevent unauthorized access **FROM** field cabinet **TO** central traffic management and other field cabinets on the same network
- ✓ Block unwanted/bad/illogical commands from going to field cabinet controllers
- ✓ Prevent ransomware from taking control of traffic systems
- ✓ Ensure continued operations in the event of an attack
- ✓ Low cost / high impact cyber solution to high impact problem
- ✓ Brings end point protection and layered cyber security to the field

Select Features – far more than another firewall

- ✓ Two factor authentication for protected device access
- ✓ Gateway for IP traffic to/from protected controllers/devices
- ✓ Encrypts all traffic to/from central TMS & protected controllers/devices
- ✓ Inspect and block bad commands, denial of service
- ✓ Stop ransomware from being loaded on controllers
- ✓ Prevent UPS from being “smoked”
- ✓ Validate control logic/settings and firmware
- ✓ Collect traffic and machine data for forensics
- ✓ Inform operator and key personnel
- ✓ Automated or user in the loop corrective action to restore protected device to known-good configuration
- ✓ Easy to install, low price point per cabinet (<$500)

MSi Platform Being Applied to Many Control Systems



Early adopters in defense, oil & gas, power & transportation

Is it Secure and Hardened for Industrial Environments?

Military Strength

Arizona Cyber Warfare Range

- ✓ Red team industry cyber experts performed month long evaluation
- ✓ MSi passed and AZ CWR endorses MSi Platform as cyber solution for control systems

US. Department of Defense Information Systems Agency (DISA)

- ✓ DISA Security Technical Implementation Guide (STIG) rigorously applied
- ✓ Numerous security features inherent down to the kernel level

Global Fortune 10 Company: lab test, red teaming and internal audits

NERC and Johns Hopkins Applied Physics Lab technical reviews

- ✓ NERC creating a new category of protections, MSi first and being endorsed

Industrial Grade

- ⊙ Industrial compute boards, minus 40 degrees to plus 80 degrees Celsius
- ⊙ Mean time to failure rated at 13+ years
- ⊙ Multiple OT protocols, digital and analog, Ethernet & serial supported

Secure, Hardened, Cost-Effective Level 0-2 Protection for *ANY* Industrial Device

Our Story

- Cyber defense software/hardware company
- Protect control systems of key physical assets
- R&D ongoing since 2010 @ Univ. of Virginia on behalf of U.S. Dept. of Defense
- MSi founded in 2014, licensed original UVa IP and began commercializing a product platform and services
- Decades of commercial, military, energy, hardware/software, cyber security (offense & defense), and complex industrial control systems expertise
- Based in Charlottesville, VA
- **Successful projects: industrial control systems, autonomous air and ground vehicles, law enforcement vehicles, Navy ship control systems, refineries, drilling rigs, tank farms/pipelines, traffic controls and more**

Contact Info

Rick Tiene

Vice President

Government & Critical Infrastructure

tiene@missionsecure.com

434.284.8071 x732

703-618-9100 cell

Office

300 Preston Avenue, Suite 500

Charlottesville, VA 22902

434.284.8071 main office