Mission Secure

Virginia Emergency Management Symposium

Cyber Risks to Transportation, Water and Power Systems and How to Secure Them

Protecting OT networks and safeguarding operations with OT cybersecurity platform and 24/7 expert managed services.

Rick Tiene, VP, Mission Secure

The Titanic Disaster Scenario

Trends Driving the OT Cybersecurity Market

Industry 4.0 (IIoT)

Digital transformation is a competitive necessity and security is part of the foundation, but 64% of operations leader's report struggling to keep up with the security challenge.[1]

Risk Mitigation

Attacks targeting ICS and OT have increased by more than 2,000% since 2018. And insurance companies are dropping cyber coverage from policies and looking to not pay due to negligence.[2]

Regulations

Efforts to improve OT cybersecurity now include government, vertical-specific, international, cross industry, and critical infrastructure regulatory requirements and standards.

Ownership

Collaboration between the IT and OT domains is essential, but questions of OT cybersecurity ownership persist. But 70% of organizations plan to make the CISO responsible for OT cybersecurity.[1]

1. SANS 2019 State of OT/ICS Cybersecurity Survey, June 2019
2. IBM X-Force Threat Intelligence Index 2020, February 2020

Challenges & Threats

Awareness

60%

Across all industry verticals about 60% of organizations are still in the awareness phase .[1]

Visibility

78%

78% of organizations have partial cybersecurity visibility into operational technology.[2]

Control

2/3

Two-thirds of companies have no device/ communications level controls on internal network.[2]

Vulnerabilities

↑ 33%

It is typical for organizations to deal with 1,000's of cyber asset / vulnerability decisions each year.[4] New industrial vulnerabilities up 33% in 2 years.[5]

Threats

↑ 2,000%

Industrial cyber-attacks up 2,000% in since 2018.[6] Ransomware is the most common cyber-attack method representing 23% of incidents.[7]

Let’s Look at Some Statistics (cont.)

92%

92% of estimated costs arising from a cyber-attack are uninsured

$130 B

US Government spending over last decade in relation to cyber security US$ 130 billion

$17 B

US Government estimated spending in financial year 2020 US$ 17 billion in relation to cyber activities

The vectors and impacts of cyber threats

Attackers aim to enter the IT or OT network

IT Target → Steal Data, Ransomware, Corporate Secrets, Executive Personal Data, etc.
OT Target → Control HMI and Level 1 devices to take over the process.

Incidents

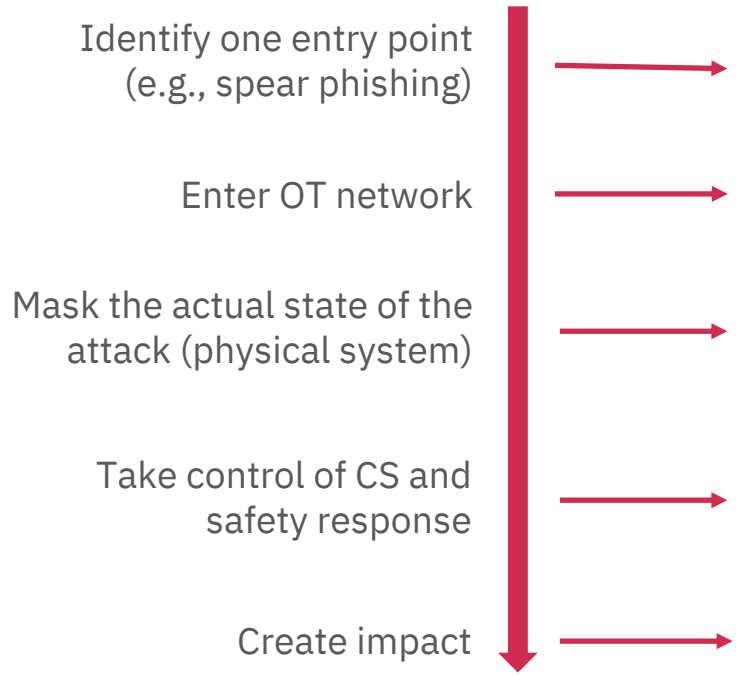
Malware

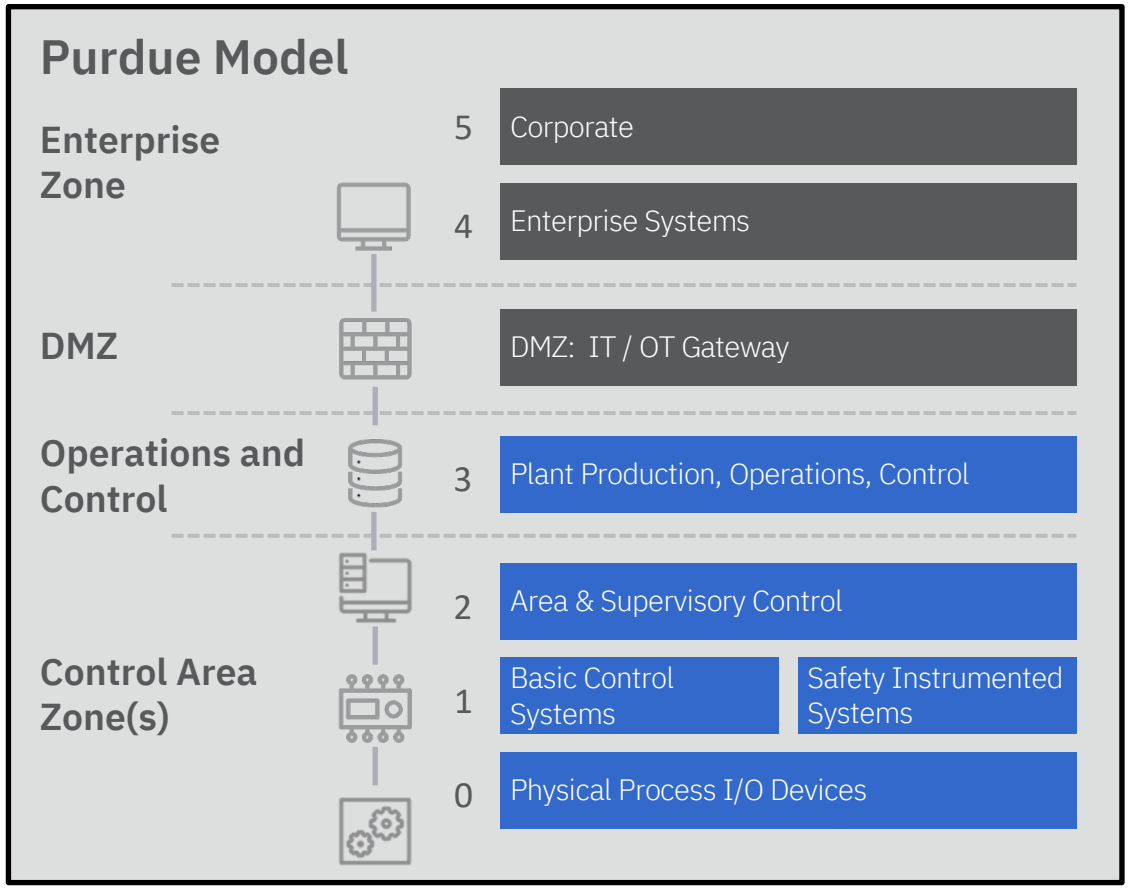
Stuxnet
BlackEnergy 1, 2, 3
Havex
Industroyer
Triton
Shamoon 1&2
WannaCry, NotPetya

Events

Aurora
German Steel Plant
Ukraine 2015 & 2016
Dragonfly 1, 2

Typical Attack Sequence





Framing The Problem

The Threats

Cyber Attacks

- Targeted attacks
- Collateral damage

Insider Threats

- Disgruntled employees
- 3rd party access – compromise devices

Human Error

- Unintentional mistakes
- Insecure equipment

IT/OT Convergence

No more air gap

3rd party remote access

Little / no visibility into OT network

Outdated, vulnerable equipment

Insiders have too much access

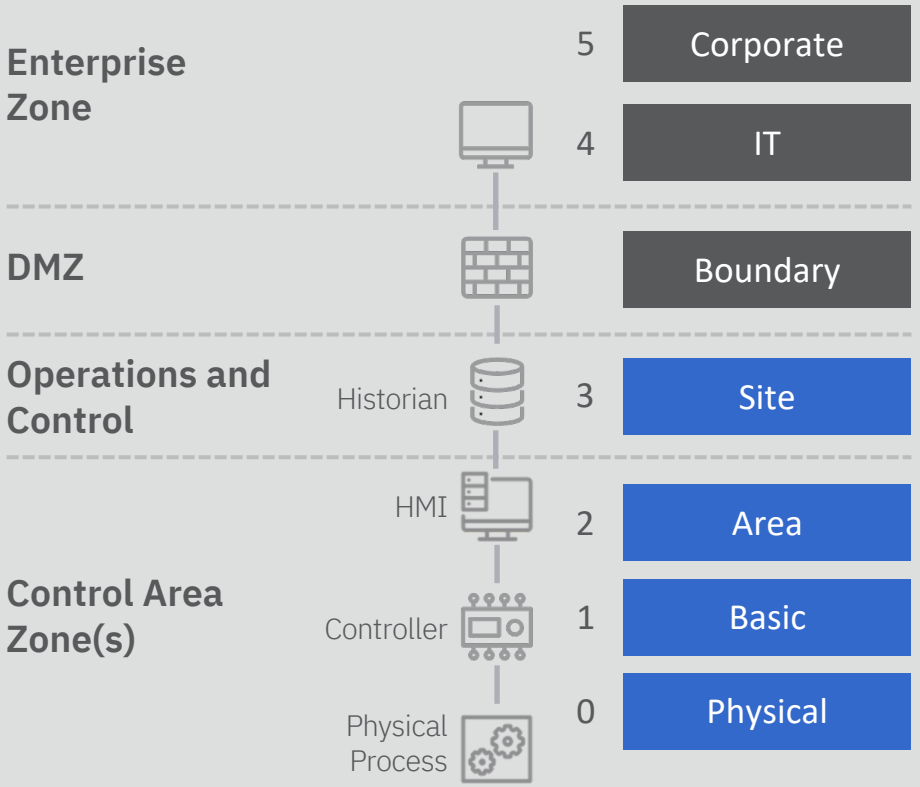
Blind to changes – maintenance

Blind to process state during attack

OT – no time to focus on security

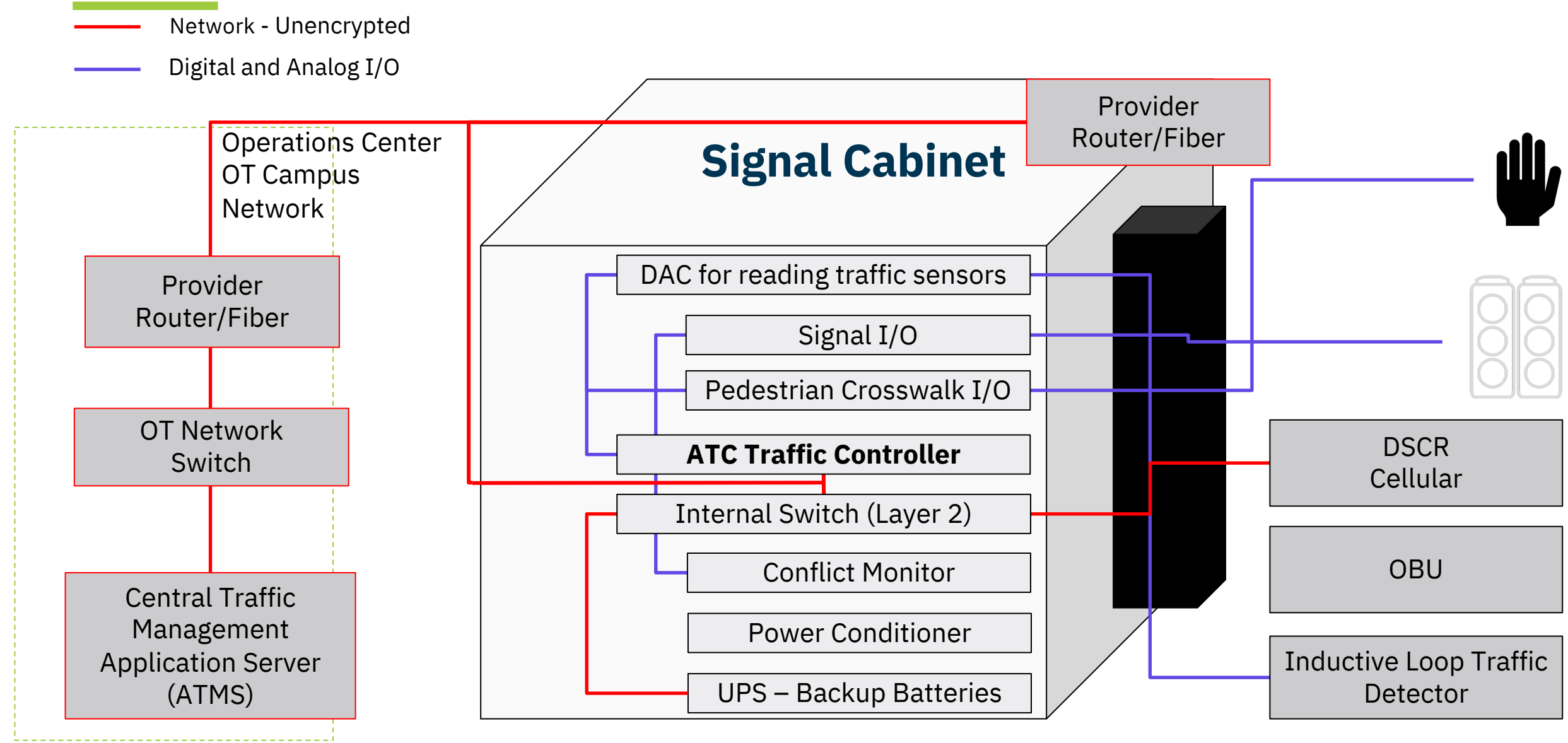
IT – little sense of OT environment

Traditional OT Stack per ANSI/ISA-95 and Purdue 5-Layer Model



Source: Gartner (November 2019)
Note: DMZ stands for demilitarized zone
ID: 370177

Vulnerable Traffic System



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

Traffic System 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

The Goal: Stop OT Cyber Threats Head-On

Protect OT networks and safeguarding operations.

What Makes That Possible?

Inline Policy Enforcement & Segmentation

- Inline network protection
- Failsafe security appliances

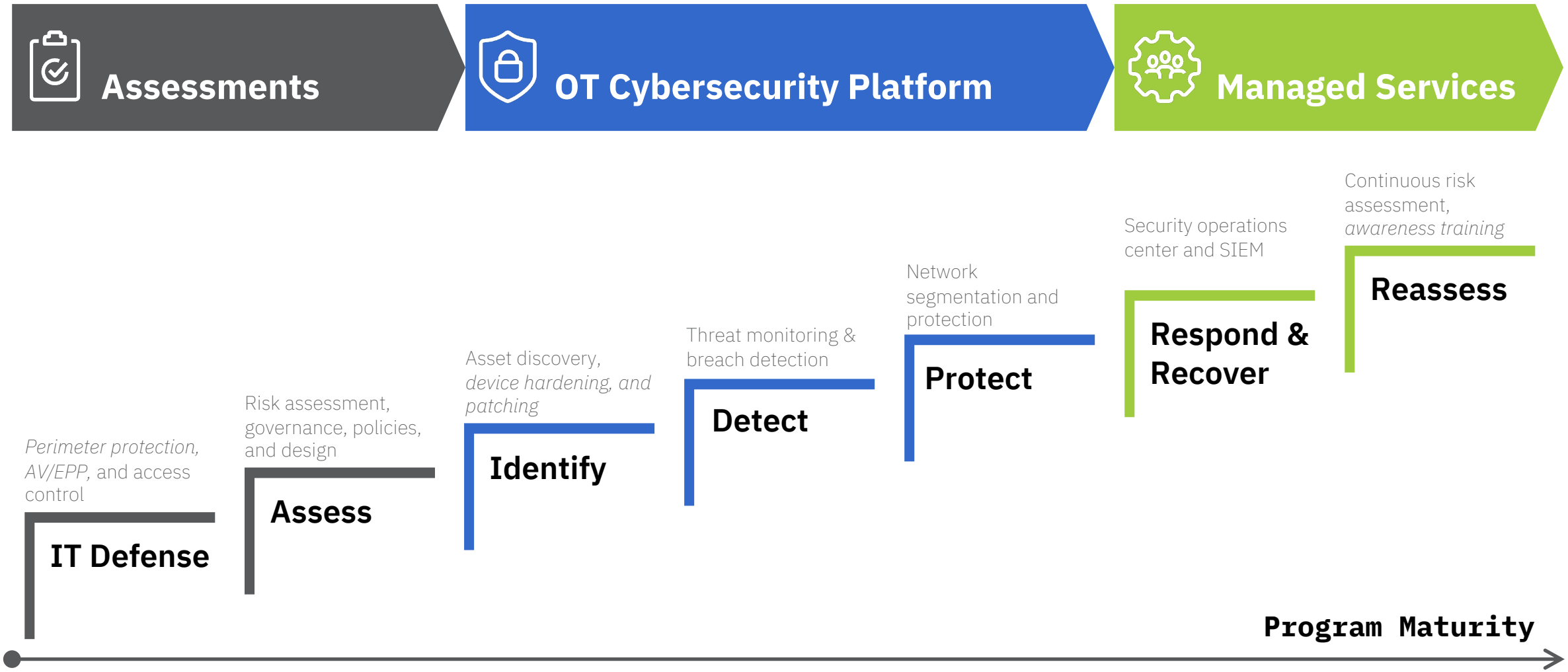
Level 0 Monitoring and Threat Detection

- Signal integrity and signal validation monitoring

24/7 Expertise and Monitoring

- OT Cyber Experts monitoring, protections, investigations, and help guide the response

Three Steps in the Process:



OT Cyber Defense Platform Components

Security Management Console

Central Management

Primary user interface for visibility, and used to manage segmentations, protections, and signal-integrity monitoring.

Security Appliance

Visibility, Segmentation and Protection

Passively monitors OT traffic on the IP network, and provides inline network segmentation and protection of OT assets.

Signal-Integrity Sensor

Continuous Signal-Integrity Monitoring

Passively monitors electric signals at the physical level (Level 0) to detect changes that may indicate possible compromise or failure.

Note:
The Mission Secure Platform is a patented product of Mission Secure, Inc. covered by US Patents No. 9697355, 9942262, 10205733, 10250619, and 10530749.

OT Cybersecurity Platform with 24/7 Managed Services

24/7 Managed Services

Managed Protection & Incident Response – Add-on service to augment internal teams monitoring visibility and protections; and providing investigations and remediations.

Security Management Console

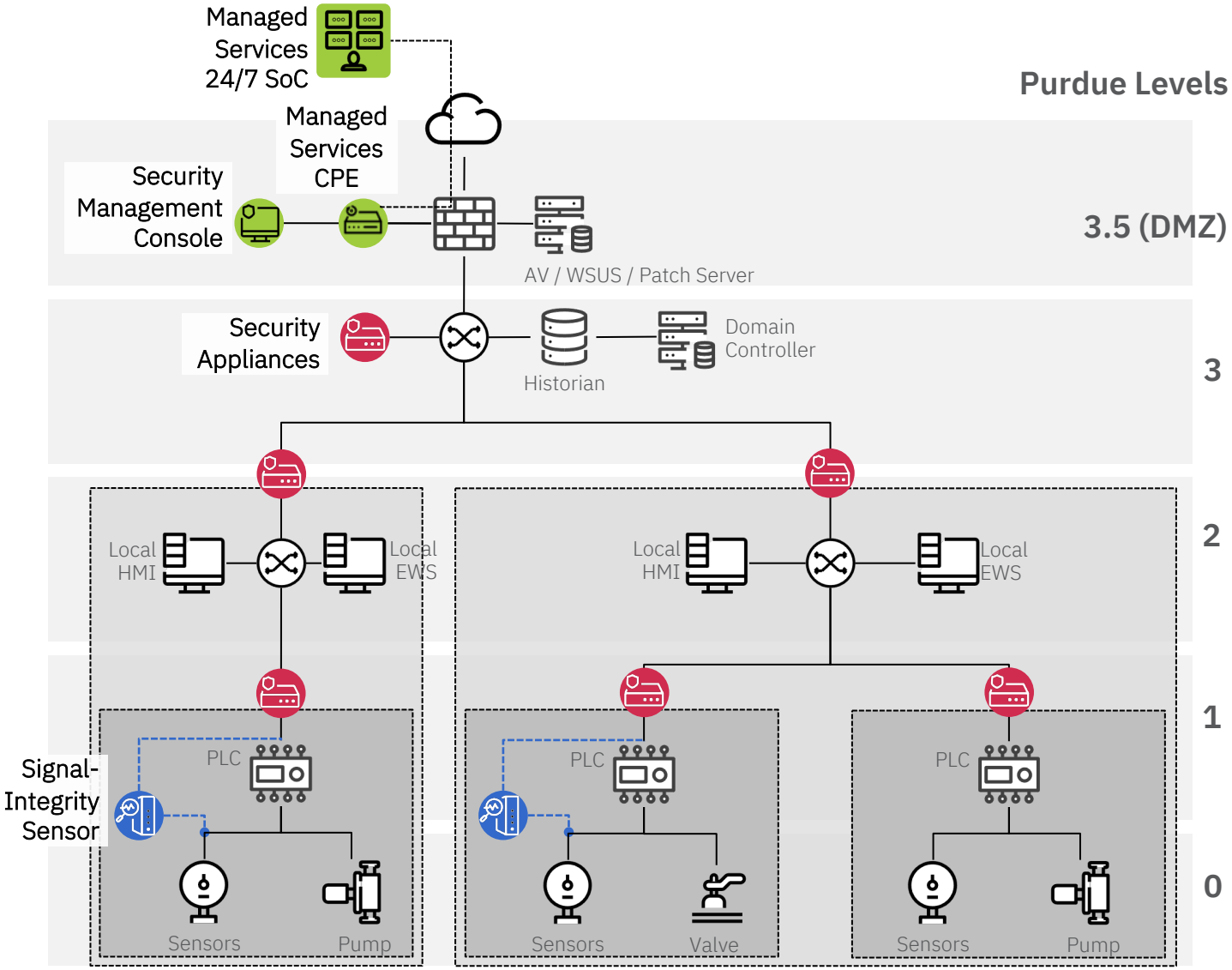
Central Management – Primary user interface for visibility, and used to manage segmentations, protections, and signal-integrity monitoring.

Security Appliance

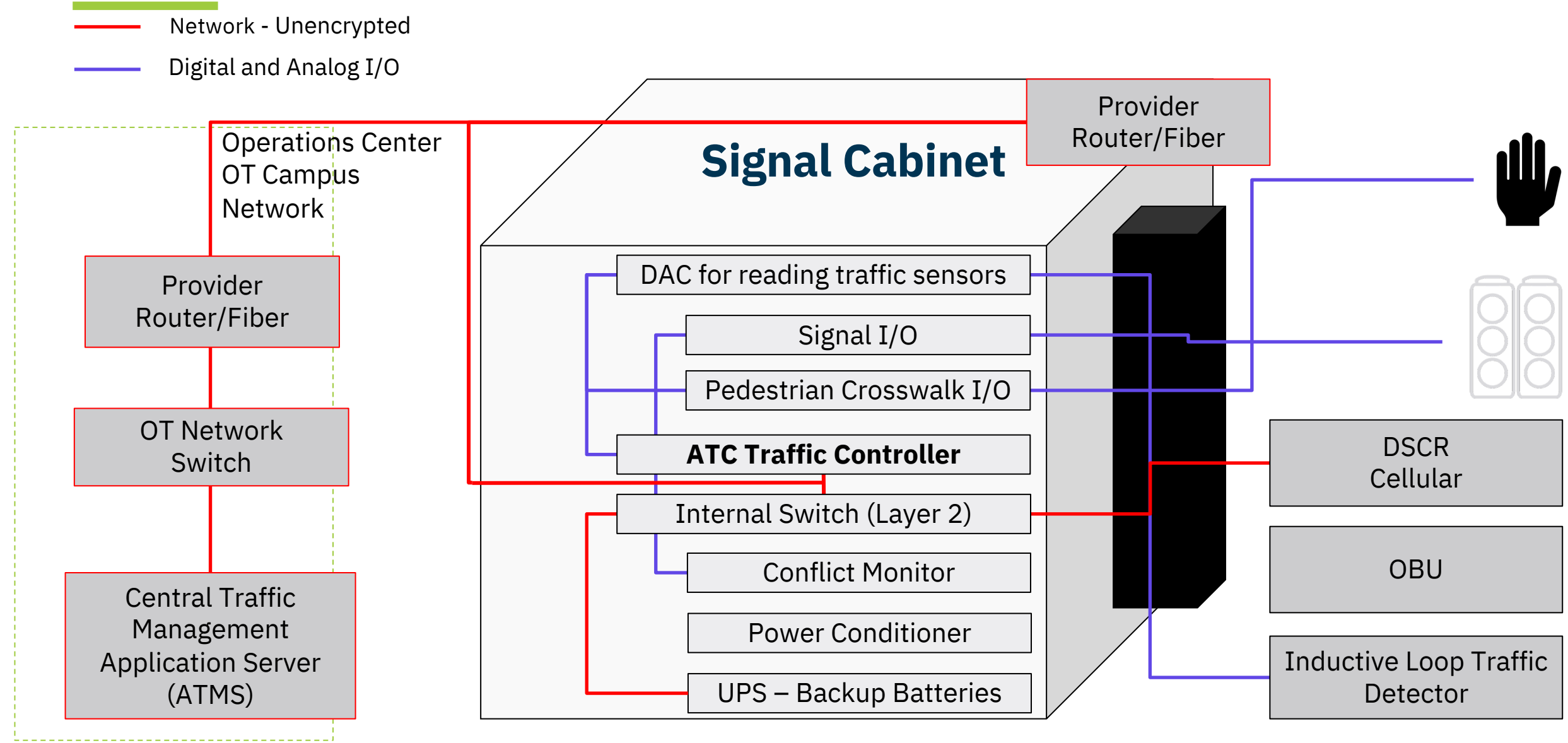
Visibility, Segmentation & Protection –
-Passively monitors OT traffic on the IP network,
-Provides active inline network segmentation and protection of OT assets.

Signal-Integrity Sensor

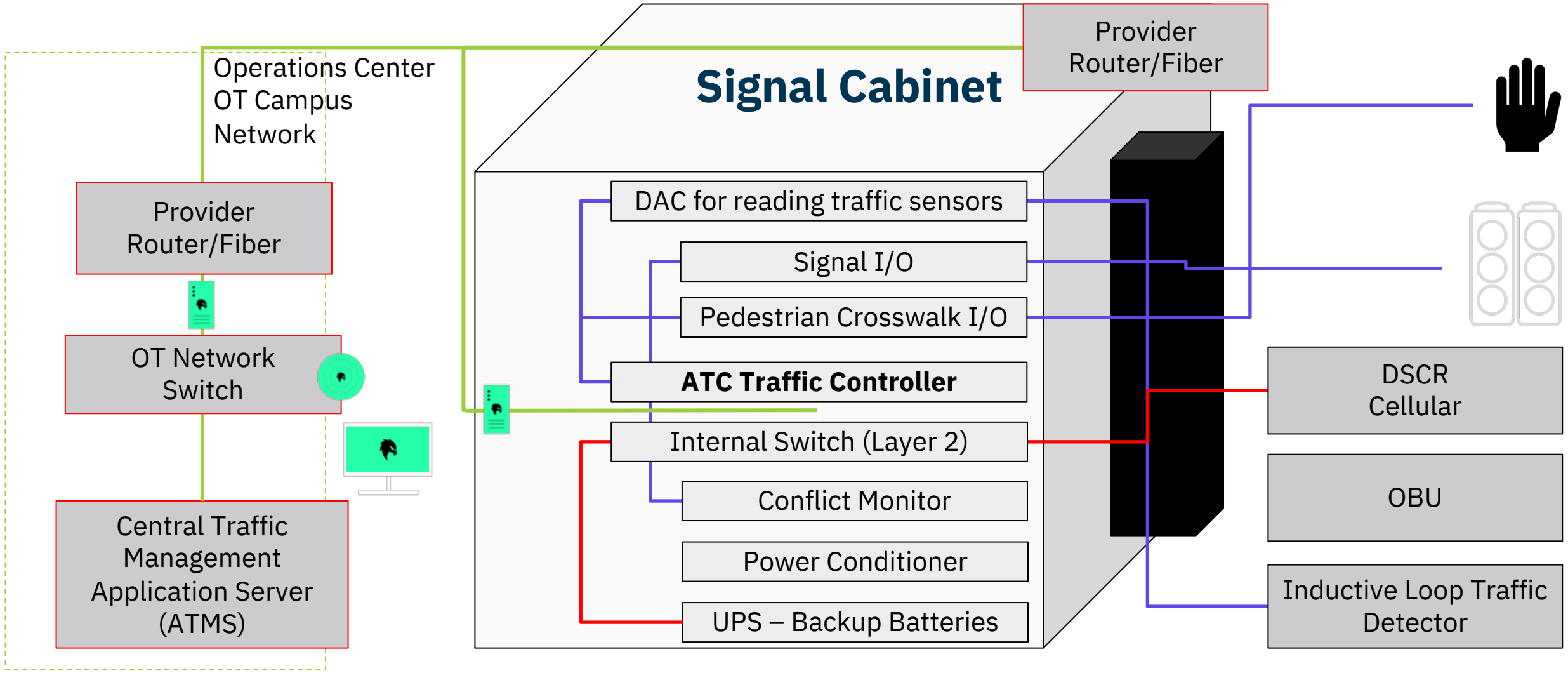
Signal-Integrity Monitoring – Passively monitors electric signals at the physical level (Level 0) to detect changes that may indicate possible compromise or failure.



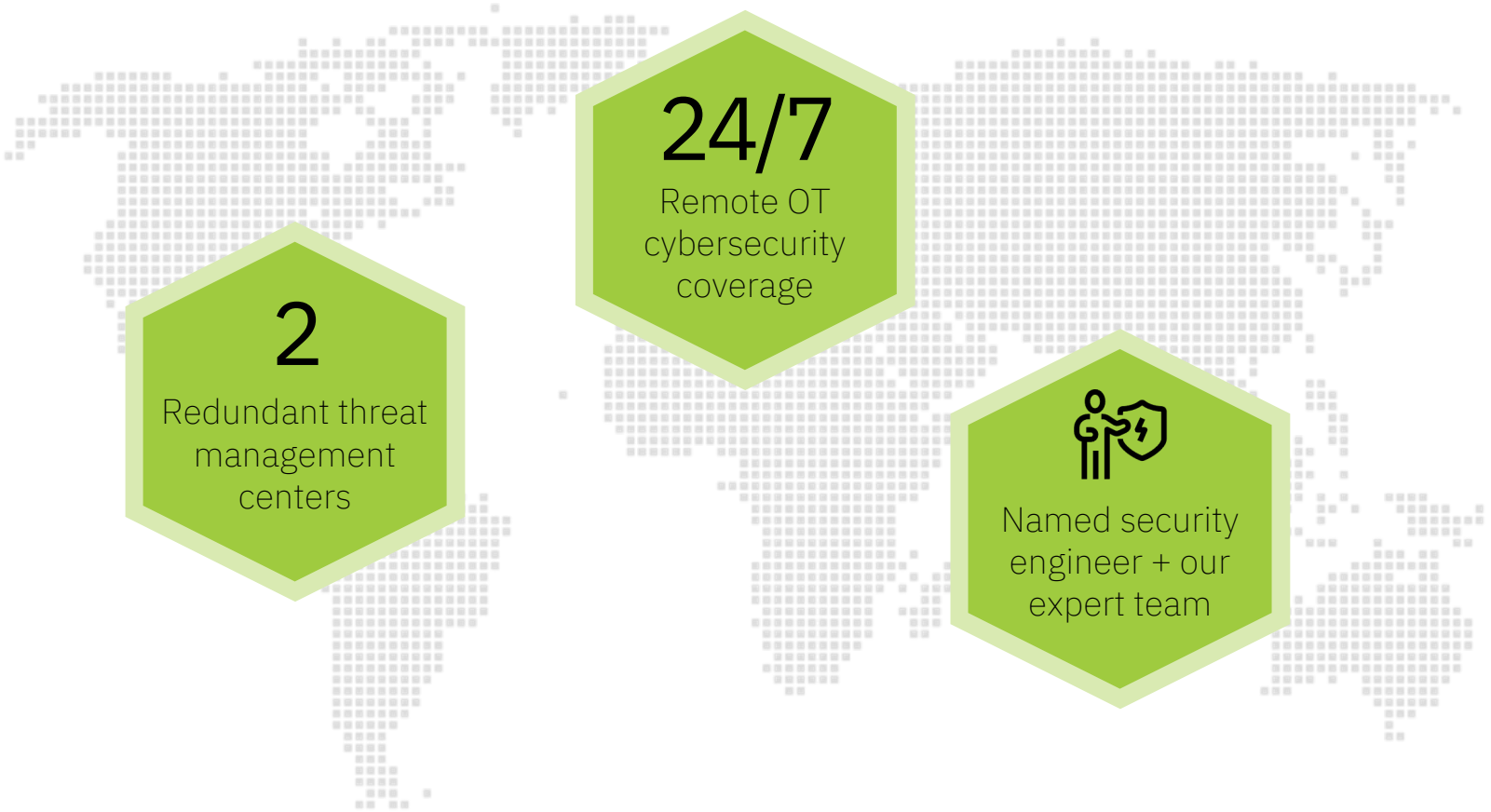
Vulnerable Traffic System



Protected Traffic System



Managed Services



Managed Visibility – continuous OT asset, and communications monitoring

Managed Protection – baselining, analysis, configurations and tuning

Analysis and Hunting – on-going OT network analysis, threat hunting, and reporting

Response and Support – security incident response, investigation and support

Contact information

Mission Secure

1770 St. James Place
Suite 420
Houston, TX 77056
www.missionsecure.com

300 Preston Avenue
Suite 500
Charlottesville, VA 22902

Rick Tiene
VP, Smart Cities, Government,
and Critical Infrastructure
tiene@MissionSecure.com
m. 703.618.9100
www.missionsecure.com