Assuring Mission Readiness with Resilient, Cybersecure Critical Infrastructure

Start Secure. Stay Secure. Restore Secure!

Will Hoffman, CTO, Frontline Cyber Solutions

Jeff Robertson, Senior OT Security Manager, Tetra Tech

OBJECTIVES

- “Resiliency” of Critical Infrastructure in military operations
- Key cyber engineering principles of resilient systems
- Real-world, practical application of commercial-off-the-shelf (COTS) IT/Operational Technology (OT) solutions
- Opportunities for data analytics created by convergence of OT, Facility-related Control Systems (FRCS) and IT

KNOWLEDGE PRIMER

- **“Facility-related Control Systems”**[1,2] (FRCS) monitor and control equipment and systems related to facilities (e.g. building automation, utility control, electronic security, fire & life safety, etc.).
- “**National Critical Functions**”[3] (NCF) are functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.
- **“Critical infrastructure“**[4] is/are systems and assets sustaining NCF (e.g. DoD typically refers to as Tier 1, Defense Critical Assets, or Task Critical Assets).
- **“All hazards“**[5] are threats or incidents, natural or manmade, targeting critical infrastructure (e.g. natural disasters, cyber incidents, industrial accidents, pandemics, acts of terrorism, sabotage, destructive criminal activity, or any combination thereof.)
- “**Resilience**" is the ability to prepare for and adapt to changing conditions

FRCS is...


HVAC Maintenance Services
Fire Detection & Alarm
Lighting Control & Retrofit
Security & Access Control
Smoke Control
Digital Video
Indoor Air Quality Services
Energy Supply & Load Management
Intrusion Detection
Environmental Control
Mechanical Maintenance & Retrofit
Enterprise Systems Wireless • Voice/Data Internet/Collaborative Services
Assets
On-Site
Energy Information
Water Management

WHAT IS OPERATIONAL RESILIENCY?

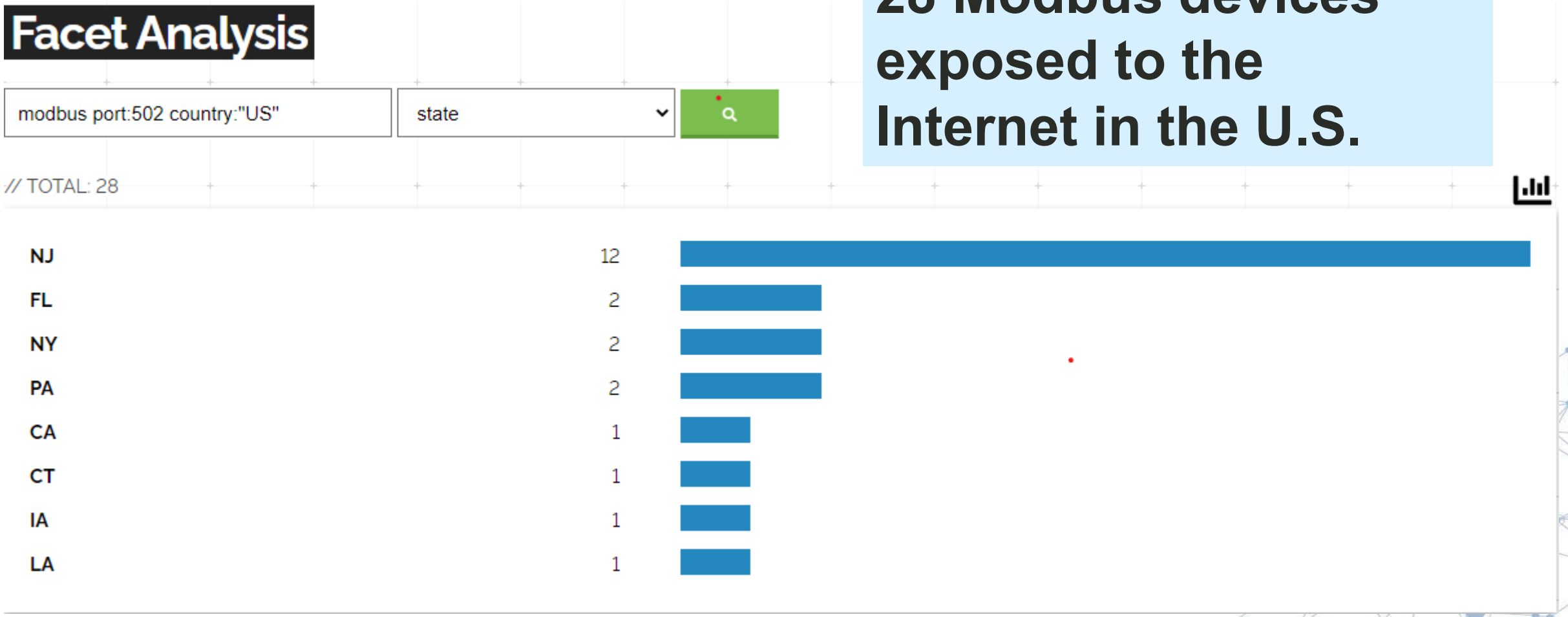
- **Resilience of Critical Infrastructure enabling military operations:**
  - "Must be secure and able to withstand and rapidly recover from all hazards"[5]
  - "Must survive and continue to operate National Essential Functions"[5]
- **"Ability of systems to resist, absorb, and recover from or adapt to an adverse occurrence during operation that may cause harm, destruction, or loss of ability to perform mission-related functions"[6]**
- **A resilient system is capable of mitigating operationally damaging effects from all hazards–which includes cyber attacks**

OT CYBER RISK & VULNERABILITIES

- **We consistently hear from clients…"But our OT Network is not connected to the internet". However, we routinely find at least one external connection; typically used to:**
  - Download patches/updates
  - Access systems or services hosted on the corporate network
- **OT/FRCS cyber attacks are believed to have increased in Q1 CY2022**
  - Probing from Russia and China against U.S. ICS resources
  - Globally, 45% of ransomware attacks target industrial organizations and infrastructure in North America (36% of that in the U.S.)[7]
  - 75% of ransomware attacks targeted the manufacturing sector[7]

Let's look for ICS - SHODAN scan

28 Modbus devices exposed to the Internet in the U.S.

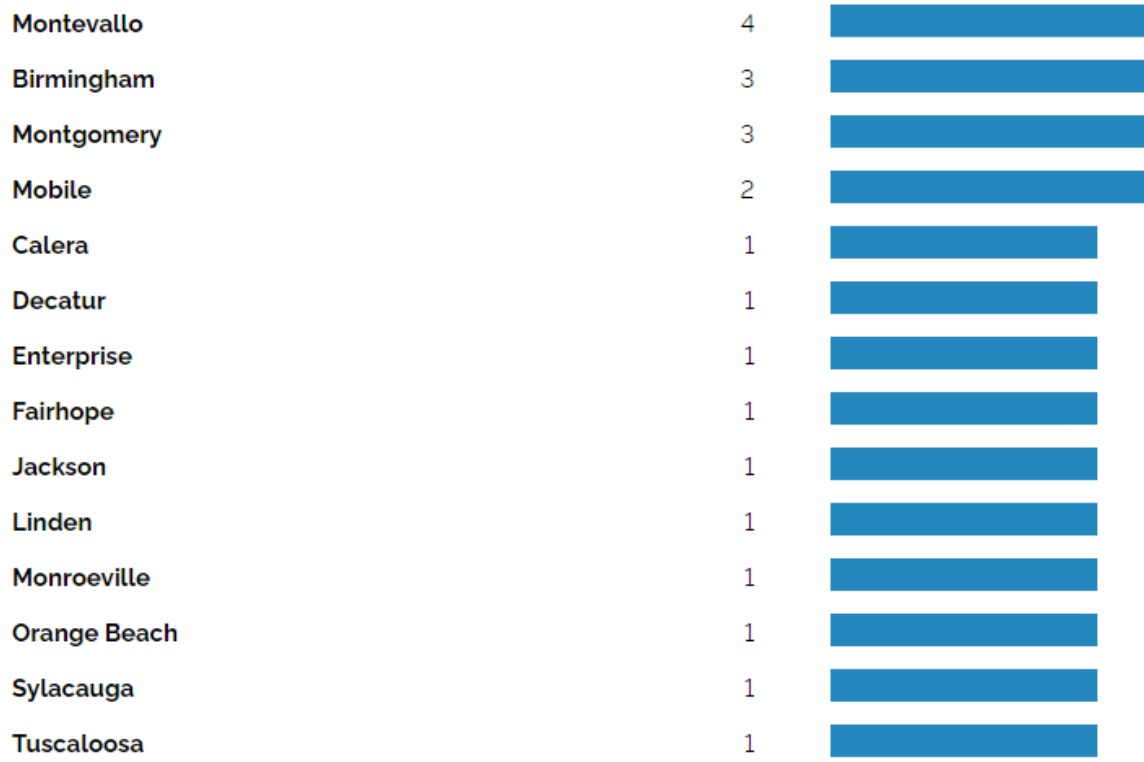


Let's look for ICS - SHODAN scan

bacnet port:47808 country:"US" state:"AL' | city

// TOTAL: 22

22 BacNET devices exposed to the Internet in Alabama




```
Instance ID: 100
Object Name: MATRIX-RTR
Vendor Name: American Auto-Matrix
Application Software: R_03_06_00
Firmware: 1.2
Model Name: AAM-Router
Description: Router
```

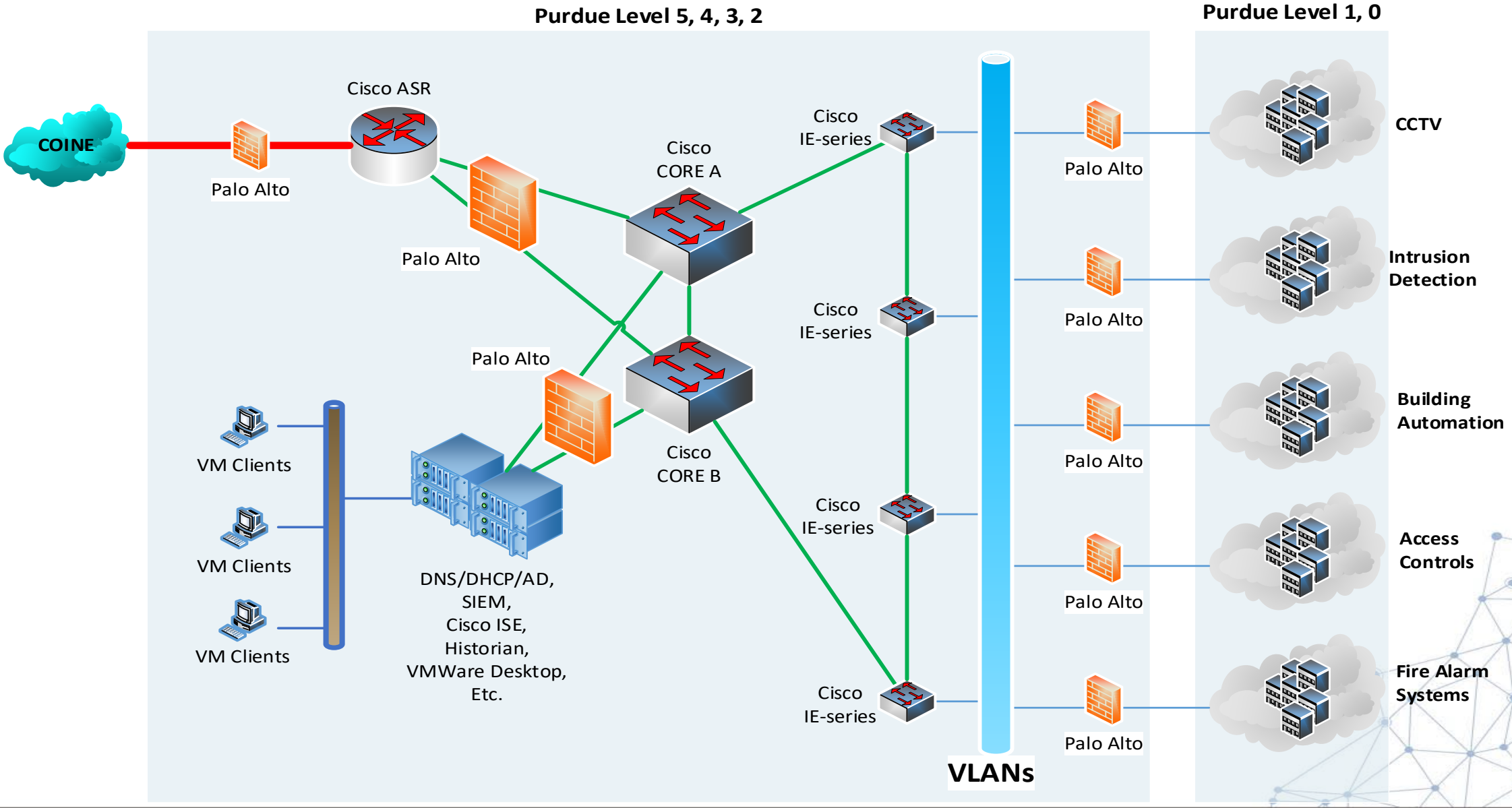
ENGINEERING DESIGN PRINCIPLES

- **Traditional IT is data-centric; FRCS is operations-centric**
- **Key characteristics of a cyber resilient, FRCS architecture**
  - Redundant & recoverable[6,8,9] (high-availability; graceful-degradation)
  - Maintains system integrity[8,9,10] (segmentation, segregation, isolation)
  - Preserves data integrity[6,10] (encryption, backup, and disaster recovery)
  - Perform behavioral monitoring[6,9,10,11] (detect deviation from baseline)
  - Performs analysis & visualization[9,10] (monitor, see anomalies, & alert)
  - Implements Zero trust[9,11] (deny all; only grant access by risk profile)
  - Detects malware & intrusions[6,9,10,11]

ENGINEERING CYBER RISK MANAGEMENT

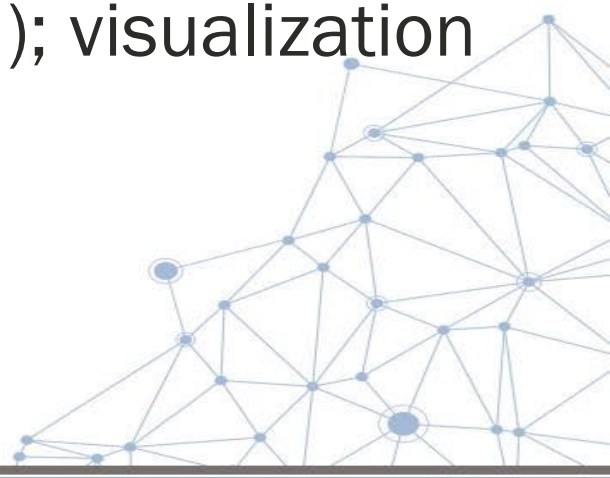
- **Perform functional system decomposition for "…identification of mission critical functions and critical components …"[12]**
  - Discover NCFs & critical Data/Assets/Applications/Services (DAAS)[13]
  - Idaho National Labs -- "consequence-driven" engineering[14]
- **UFC 4-010-06 Cybersecurity design process; Risk Management Framework (RMF)**
- **Facility and System Testing and Commissioning**
  - Inspection/Assessment against common set of cyber standards
  - Assure Cybersecure, Reliable and Safe operation of critical systems

FRCS TOPOLOGY

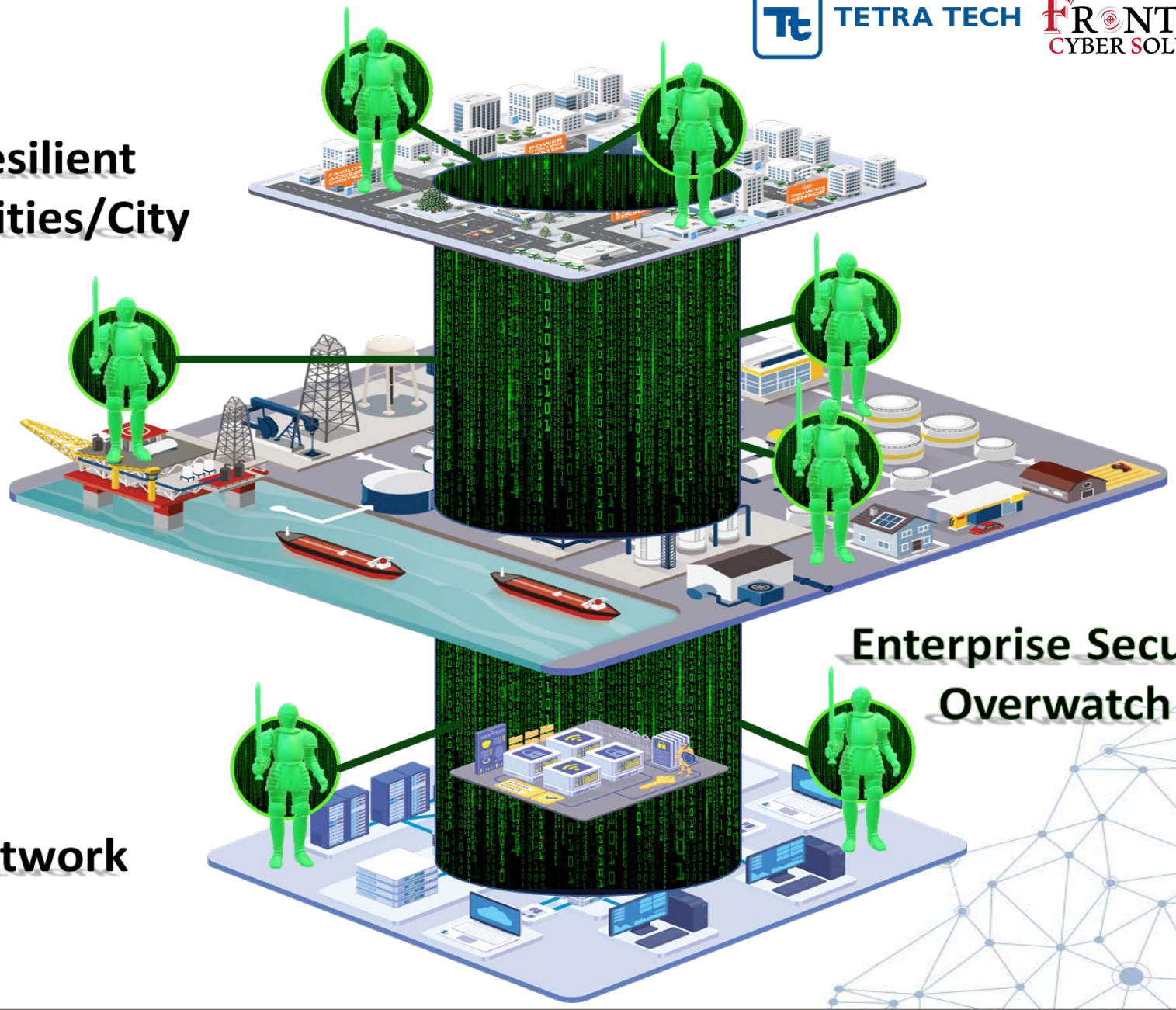


PRACTICAL INTEGRATION OF COTS

- **Implemented at Purdue-model Levels 5, 4, 3, & 2 (IT-centric)**
  - Network devices rated for industrial conditions
  - Virtualization and Zero Client workstations
  - Identity/Access Management; context-based (e.g. user, time, location, and access type)
  - Security Information and Event Management (SIEM); visualization
    - Intrusion & Malware detection
    - Asset identification
    - Event correlation

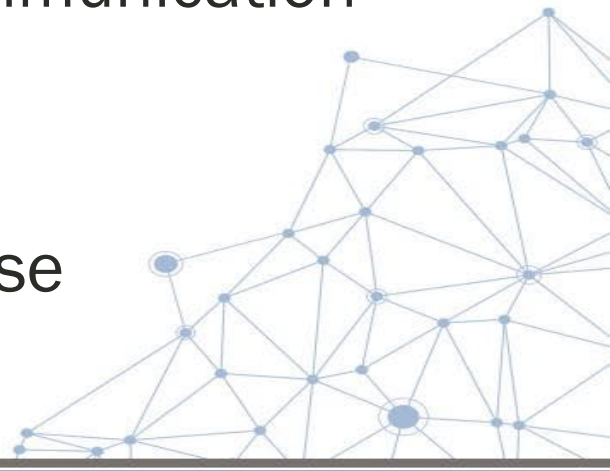


Operational View (OV-1)



PRACTICAL INTEGRATION OF COTS

- **Enterprise security "overwatch" (Monitors Levels 5 through 1)**
  - Monitors both IP and non-IP traffic at source
  - Collects full Packet-Capture (PCAP); FIPS 140-2 encryption
  - Builds full-domain, network model (IT, OT, and IoT)
    - Hybrid active system scanning (includes geolocation and metadata)
    - Visualization engine; models network nodes & communication pathways
  - Detect, characterize & alert on anomalies
    - Machine/Learning; event assessment and response
    - Records event forensics



BEST PRACTICES

- **Embodies NIST, UFC, UFGS and DoD standards/requirements**
- **Scalable architecture; build as much or as little as needed**
- **Assure safe and reliable operation of critical functions during attack**
- **Layered defense; zero-trust**
  - Assumes exploitation (i.e. enemy has compromised network)
  - Both IP + non-IP traffic; real-time monitoring, anomaly detection, and logging
- **Real-time enterprise visibility on cyber-health of system**
- **Correlate and analyze infrastructure and systems' performance data**
  - Enterprise/building condition-based modeling
  - Predictive maintenance analytics

BENEFITS OF DATA ANALYTICS

- Machine-Learning (M/L); baselines “normal” & watches for anomalies
- Predict equipment failures; initiate logistics request for replacement
- Identify sub-optimal equipment performance; auto-generate workorder
- Identify hazardous system configurations – alert operators
- Use-Case:

  Situation: During the routine electrical work, a contractor accidentally trips a maintenance isolation switch which takes a redundant UPS buss offline – putting missile launch operations at risk.

  Outcome: M/L algorithms detect dangerous system configuration and alert operators real-time; restoring redundancy before mission system outage.

CONCLUSION

- **We discussed…**
  - What is a resilient system
  - Threats to a resilient system
  - Things to consider during cyber engineering process
  - Integrating COTS products in system implementation
  - Benefits organizations can gain from data analytics

Assuring Mission Readiness with Resilient, Cybersecure Critical Infrastructure

Jeff Robertson, Jeff.Robertson1@tetratech.com

Will Hoffman, whoffman@frontlinecyber.us

REFERENCES

1. UFC 4-010-06, 19 September 2016, Change 1, 18 January 2017
2. UFGS-25 05 11, May 2021
3. Securing Industrial Control Systems, A Unified Initiative FY 2019-2023, Cybersecurity and Infrastructure Security Agency, July 2020
4. Section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. 5195c(e))
5. Presidential Policy Directive 21, Critical Infrastructure Security and Resilience, February 2013
6. DoDI 8500.01, Cybersecurity, March 2014
7. https://www.dragos.com/blog/industry-news/dragos-industrial-ransomware-analysis-q1-2022/
8. DoD Control Systems Security Requirements Guide, Version 1, Release 1, January 2021
9. NIST SP 800-82r2, Guide to Industrial Control Systems (ICS) Security, May 2015
10. NIST SP 1800-32, Securing Distributed Energy Resources: An Example of Industrial Internet of Things Cybersecurity, April 2021
11. Department of Defense (DOD) Zero Trust Reference Architecture Version 1.0, February 2021
12. DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)
13. Department of Defense (DOD) Zero Trust Reference Architecture Version 1.0 February 2021
14. Department of Energy, National Cyber-informed Engineering Strategy, June 2022