ALCMS and cyber security considerations

Nir Godel, PLM, Crouse Hinds Airport Lighting Products

November 06

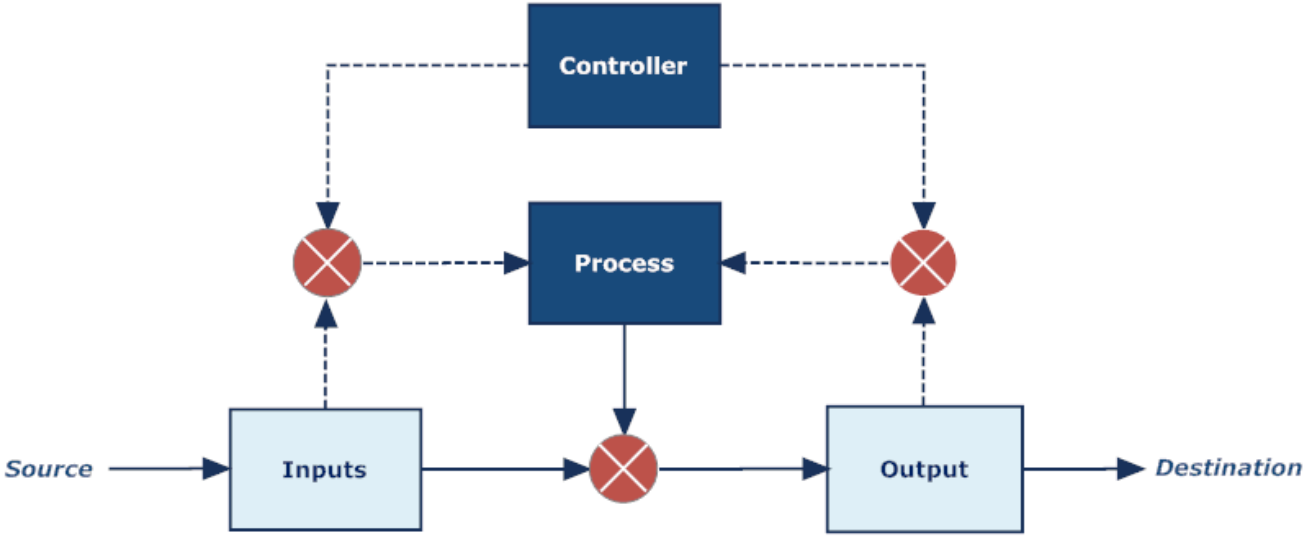
Powering Business Worldwide

“Protecting our nation’s transportation system is our highest priority and TSA will continue to work closely with industry stakeholders across all transportation modes to reduce cybersecurity risks and improve cyber resilience to support safe, secure and efficient travel,”

TSA Administrator, National Press Release, March 2023

What is Control System

- A **control system** manages, commands, directs, or regulates the behavior of other devices or systems using control loops (Wikipedia)

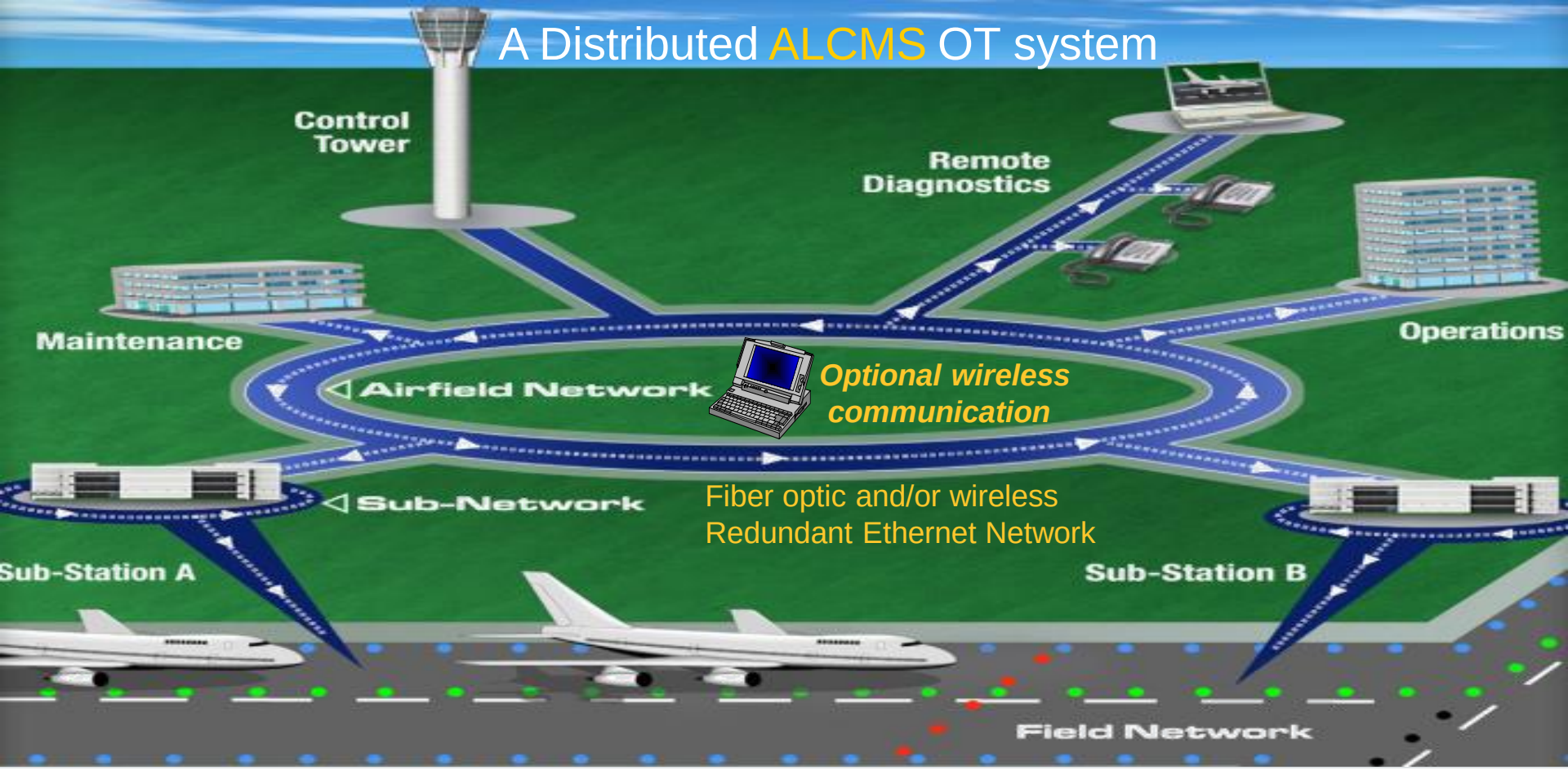


Powering Business Worldwide

What is Cyber Security

- ***Cyber Security*** is the protection of computer systems and networks from attacks by malicious actors that may result in unauthorized information disclosure, theft of, or damage to hardware, software, or data, as well as from the disruption or misdirection of the services they provide (Wikipedia)

A Distributed ALCMS OT system



Powering Business Worldwide

FAA Advisory Circular

- **AC 150/5345-56B - Specification for L-890 Airport Lighting Control and Monitoring System (ALCMS)**
- “3.2.9 ALCMS Communications Network. The communication network ties all the system computers and the electrical vault computer(s) together forming the Airport Lighting Control and Monitoring System (ALCMS). The network transmission medium may be hardwire, fiber optic cable or wireless. **This network should be used only for the ALCMS**. “

Physical/ Operational Security Protections

- Airport Physical Access
- Key Locked Enclosures
- Network Segmentation
- System Control Permission Function
- Login / Password Management
- USB Drive Limitations
- Antivirus / Malware Scans during Maintenance Visits
- Operating System Hardening

Wireless Internet Remote Access - Why?

- ALCMS Manufacturer Troubleshooting Support
- Low-Cost Solution for Roaming Laptop
- Airport IT connection for Cyber Security Diagnostic
- ALCMS Connection from Remote Site

There is no FAA Engineering Brief or Guidance on such Remote Access

Wireless Internet Remote Access – Secured VPN Appliance

Enables secured connection using a firewall between the Internet line and the ALCMS computer.

Secured Measures:

- Requires wired connection between the ALCMS computer and Internet. When not used should be disconnected.
- Requires preinstalled security file from the remote computer
- To connect need to know the remote IP
- Requires Login and password

Airport IT is usually not responsible on the ALCMS and as such won’t approve.

Military Specific Requirements

Air Bases require meeting SCAP (Security Content Automation Protocol) following STIG (Security Technical Implementation Guides) Benchmark for each computer.

Specific requirements for operating system limitations and enhanced security

Eaton Crouse Hinds Airport lighting created a software package and maintain scripts to implement those requirements

Each computer runs a test and get a score indicating how robust those requirements are implemented (Green, Yellow, Red)

Note: Some requirements can’t be implemented as they compromise the system required operation.

I.E. – Tower automatic logout contradicts FAA requirement of Tower Login default.

Why is OT Cybersecurity Important?

Codes and Standards

TSA issues new cybersecurity requirements for airport and aircraft operators

Requirements enhance cybersecurity resilience by focusing on performance-based measures.

National Press Release
Tuesday, March 7, 2023

WASHINGTON – Today, the Transportation Security Administration (TSA) issued a new cybersecurity amendment on an emergency basis to the security programs of certain TSA-regulated airport and aircraft operators, following similar measures announced in October 2022 for passenger and freight railroad carriers. This is part of the Department of Homeland Security's efforts to increase the cybersecurity resilience of U.S. critical infrastructure and follows extensive collaboration with aviation partners.

Powering Business Worldwide

Why is OT Cybersecurity Important?

Codes and Standards

What does the TSA cybersecurity order mean to you?

- **Airports and Aircraft Operators**

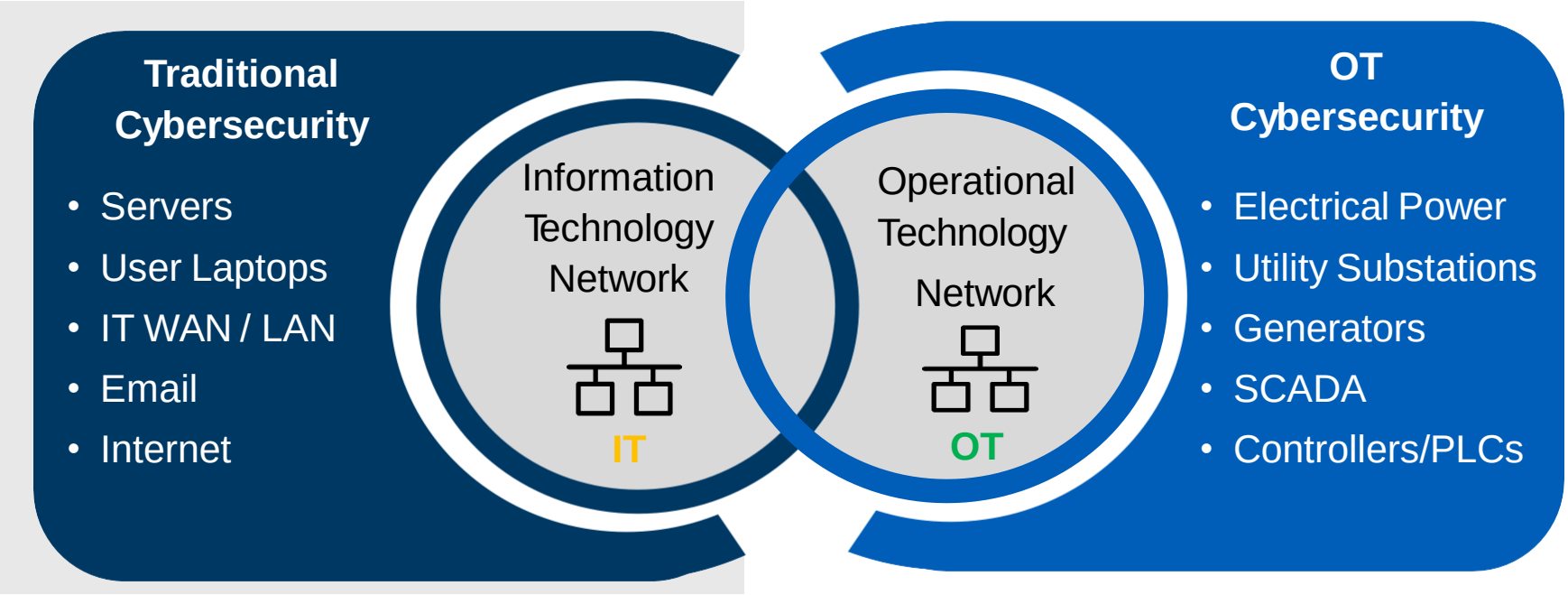
Key areas of the TSA order and how to implement

What do the orders say	Implementation strategies
Develop network segmentation polices and controls	Assess new and existing systems regularly to ensure alignment with industry standards
Create access control measures	Perform secure commissioning and hardening Regularly assess to add, change, or delete accounts
Build continuous monitoring and detection policies and procedures	Deploy Network Intrusion (Threat) Detection technologies developed for OT environments
Apply security patches and updates in a timely manner	Leverage asset inventory and vulnerability management tools/services and create a regular maintenance activity

Powering Business Worldwide

Start the Cybersecurity Journey with Collaboration

A cybersecurity strategy is only as strong as its weakest link.



Leverage the knowledge from all resources and allow them to focus on what they know best!

EATON
Powering Business Worldwide

Develop Trusted Airport – OT Manufacturer Partnership

- **Industry knowledge & experience:** Ensure that there is technical expertise in your industry, as well as, the OT components in your environment.
- **Cybersecurity expertise:** Pair the technical expertise with cybersecurity experience from certified companies and resources.
- **Agnostic:** Ability to service broad portfolio of devices and systems.
- **Strong service teams:** Look for partners with strong service teams.
- **Scale:** Review a partner's ability to scale to meet your organizational needs.
- **Staying Power:** Consider partners that have been in the industry for an extended period of time with a high certainty of being able to provide extended support.
- **Certified:** Products, services, and resources are backed up with industry recognized standards and certifications.

Powering Business Worldwide

Understand Complete Lifecycle Cybersecurity

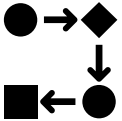
Effective cybersecurity is applied throughout the lifecycle…

Powering Business Worldwide

Consider All Elements of a Cybersecurity Program

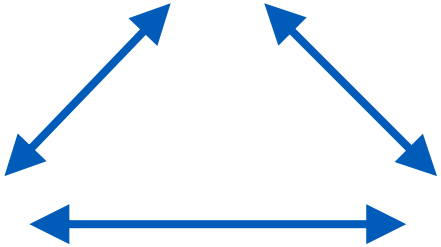
People

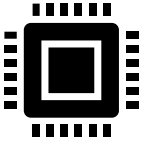
Ensure your employees, contractors, partners, and stakeholders are well trained on the Dos & Don’ts



Processes

Put a polices and procedures in place and implement continuous improvement - know what to measure & how to respond





Technology

Analyze your connected device architecture – address vulnerabilities based on risk, investment, and cost avoidance

Powering Business Worldwide

Eaton Cyber Security Center Of Excellence

- Every new Eaton product line development require cyber security assessment.
- Periodic cyber security assessments to identify and resolve risks
  - Internal Software Enhancements
  - Threat Mitigation
  - Messages within the ALCMS software encrypted
  - Additional Login/Password for ALCMS internal tools including development, configuration and troubleshoot

Summary

Cyber Security in Airports is getting more and more attention.

Airports will have to follow TSA guidelines and will need a proven partner to support future cybersecurity needs.


Powering Business Worldwide