CSAAP

Course One

Introduction to Cybersecurity and Airport Administration

Module Six

Managing Advanced Airport Cybersecurity Operations, Threat Intelligence, and Future Preparedness

Technical deep dive into securing critical airport systems, operationalizing threat intelligence, executing advanced incident response, and preparing for emerging threats.

Cuyahoga Community College

Sponsored by the US National Science Foundation

Agenda

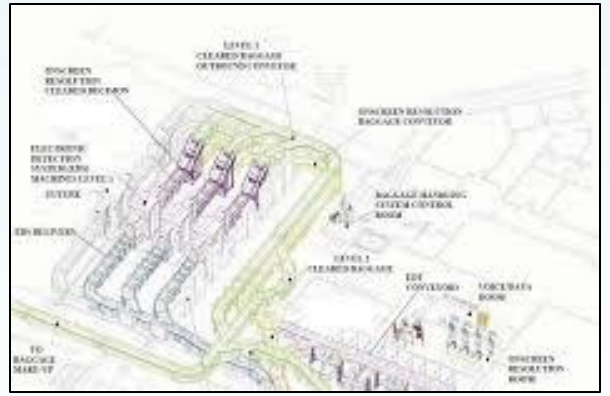
- Securing Airport Operational Technology (OT): System-Specific Deep Dives
- Fostering a Technically-Adept Cybersecurity Culture
- Operationalizing Cyber Threat Intelligence (CTI) for Active Defense
- Executing a Technical Cyber Incident Response for OT Systems
- Analyzing & Mitigating Emerging Technical Threats
- Course Synthesis and Final Reminders

Objectives

- Analyze specific vulnerabilities, threats, and mitigation measures for airport OT systems like BHS, Airfield Lighting, and BMS (addresses Outcome 2.1, 5.4, 5.5).
- Explain the role of encryption and intrusion detection systems in protecting OT communications and data that supports flight operations (addresses Outcome 2.2, 2.3).
- Develop a cyber incident response protocol for a specific attack scenario on a flight operation system (addresses Outcome 2.5).
- Assess the cybersecurity of systems used in capital development projects, especially those involving OT/ICS integration (addresses Outcome 6.3).
- Evaluate emerging cyber threats from NextGen, UAVs, and AI, and propose technical mitigation strategies (addresses Outcome 2.4, 3.5).

Deep Dive: Baggage Handling System (BHS) Security

- **Vulnerabilities:**
  - *Often runs on legacy, unpatched operating systems (e.g., Windows 7).*
  - *Commonly has a "flat" network architecture allowing for easy lateral movement; utilizes unauthenticated industrial protocols*
  - *Has insecure vendor remote access points.*
- **Threats:**
  - *Ransomware encrypting sortation controllers and servers, causing a complete system halt (Availability attack).*
  - *Malicious data manipulation leading to incorrect baggage routing and potential security screening bypasses (Integrity attack).*

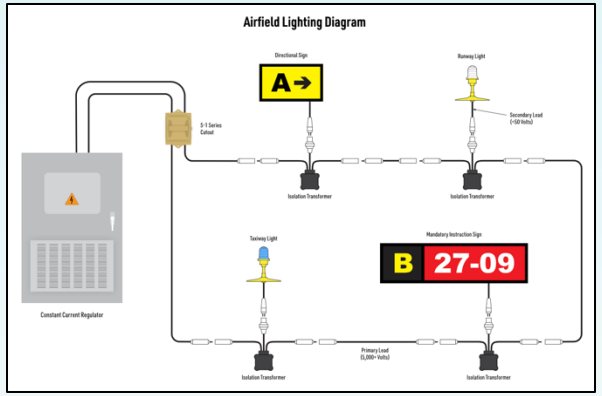


Deep Dive: Baggage Handling System (BHS) Security (Cont'd)

- **Mitigation Measures:**
  - *Implement network segmentation using firewalls to create a secure BHS "zone" that strictly limits traffic to and from the IT network (aligns with IEC 62443 principles).*
  - *Deploy application whitelisting on BHS control servers to prevent unauthorized software or malware from executing.*
  - *Enforce multi-factor authentication (MFA) and granular access controls for all remote vendor maintenance sessions.*

Deep Dive: Airfield Lighting & NAVAID Security

- **Vulnerabilities:**
  - *Legacy serial-to-ethernet converters lacking security controls*
  - *Unauthenticated and unencrypted command-and-control protocols*
  - *Insufficient physical security of control cabinets and junction boxes on the airfield.*
- **Threats:**
  - *Unauthorized commands to disable runway or taxiway lights during low visibility operations*
  - *Manipulation of Precision Approach Path Indicator (PAPI) light signals to mislead pilots*
  - *Denial-of-service against airport-owned NAVAID interfaces, impacting flight integrity.*

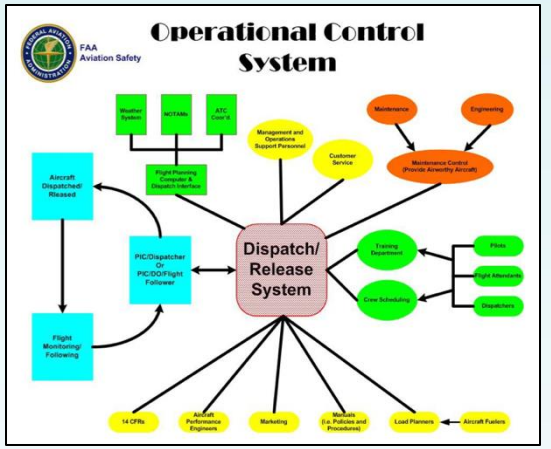


Deep Dive: Airfield Lighting & NAVAID Security (Cont'd)

- **Mitigation Measures:**
  - *Place airfield lighting controls on a highly isolated and monitored network segment with a dedicated OT-aware Intrusion Detection System (IDS).*
  - *Implement physical security measures such as locked cabinets and tamper-evident seals for control hardware.*
  - *Use encrypted protocols (e.g., SSH, TLS) for any management or maintenance access to the control system servers.*

Deep Dive: Airport Operations Control Center (AOCC)

- **Vulnerabilities:**
  - *High degree of system integration with numerous third-party data feeds (e.g., weather, flight schedules, airline data)*
  - *Reliance on complex Resource Management Systems (RMS) for gates/stands*
  - *Human operators susceptible to social engineering under high-stress conditions.*
- **Threats:**
  - *Manipulation of the Flight Information Display System (FIDS) to display false gate, time, or cancellation information*
  - *Ransomware attack on the RMS, preventing allocation of gates and hardstands*
  - *Compromise of digital radio dispatch systems, disrupting ground crew communications.*

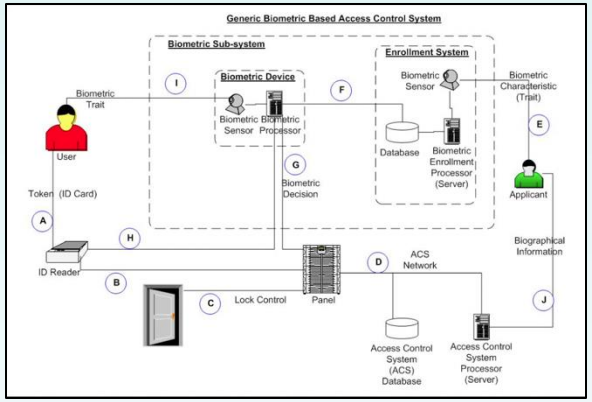


Deep Dive: Airport Operations Control Center (AOCC) (Cont'd)

- **Mitigation Measures:**
  - *Implement a "Zero Trust" architecture within the AOCC network, where systems must continuously authenticate to each other and access is granted on a per-session basis.*
  - *Deploy data diodes or rigorous input validation and sanitation gateways for all incoming third-party data feeds to prevent malicious data injection.*
  - *Conduct high-fidelity, pressure-tested incident response simulations specifically for AOCC staff and scenarios.*
  - *Ensure critical AOCC systems like RMS have redundant, resilient architectures with tested failover capabilities.*

Deep Dive: Physical Access Control System (PACS)

- **Vulnerabilities:**
  - *Legacy unencrypted communication protocols between card readers and controllers (e.g., Wiegand)*
  - *Potential for SQL injection or cross-site scripting on web-based management interfaces*
  - *Insufficient network segmentation from the corporate IT network*
  - *Weak credentialing processes allowing for social engineering.*
- **Threats:**
  - *Creation of unauthorized "ghost" badges in the database to access secure areas*
  - *Cloning of legacy access cards to bypass physical controls; denial-of-service attack against the PACS server*
  - *Disabling all badge readers and causing operational chaos*
  - *Using a compromised PACS workstation as a pivot point to attack other airport networks.*



Deep Dive: Physical Access Control System (PACS) (Cont'd)

- **Mitigation Measures:**
  - *Transition to modern, secure credential technologies like Open Supervised Device Protocol (OSDP) which supports encrypted communication channels.*
  - *Conduct regular web application security testing on PACS management interfaces and harden the underlying database servers.*
  - *Enforce strict network isolation for the entire PACS infrastructure (servers, controllers, readers) from other IT and OT systems.*
  - *Integrate PACS event logs into the airport's Security Information and Event Management (SIEM) system to monitor for anomalous access patterns (e.g., a badge used in two distant locations simultaneously).*

Building a Technically-Adept Security Culture

- Move beyond general awareness to provide role-specific technical cybersecurity training that aligns with ICAO guidance
- **Example for Maintenance Techs:** Train on secure procedures for connecting to OT equipment, such as using dedicated, hardened laptops that are scanned for malware before and after use.
- **Example for Procurement Staff:** Train on how to interpret vendor security documentation (e.g., SOC 2 reports) and write technically specific cybersecurity requirements into RFPs for new capital projects.
- **Example for IT/Cyber Staff:** Provide cross-training on the unique characteristics of OT protocols (e.g., Modbus, BACnet) and the operational impact of OT system failures.

Operationalizing CTI for Proactive Airport Defense

- Implement a process to automatically ingest structured Cyber Threat Intelligence (CTI), such as indicators shared via STIX/TAXII protocols from the Aviation ISAC (A-ISAC).
- Feed CTI directly into technical security controls for automated action:
- **Firewall/IPS:** Ingest malicious IP addresses and domains to automatically create block rules.
- **SIEM:** Use new indicators to create correlation rules that search for and alert on suspicious activity in logs.
- **EDR:** Push file hashes of known malware to endpoint security tools to detect and quarantine threats on workstations and servers.
- Use strategic and operational CTI to inform vulnerability management priorities and guide incident response tabletop scenarios.

Incident Response Scenario: PACS Compromise

- **Scenario:** An alert from an IDS indicates a Physical Access Control System (PACS) controller is attempting unauthorized communication with an external IP address.
- **Technical Response Steps:**
  - ***Detection & Analysis:*** *Confirm the alert using network packet capture tools (e.g., Wireshark) to analyze traffic. Correlate the destination IP with CTI feeds to confirm it is malicious.*
  - ***Containment:*** *Immediately implement a firewall rule to block the malicious IP. Based on the CIRP, logically isolate the PACS network segment from the broader airport network to prevent lateral movement.*

Incident Response Scenario: PACS Compromise (Cont'd)

- **Technical Response Step (Cont'd):**
  - ***Coordination with AEP:*** *The CIRP action triggers a notification to the Airport Operations Center. The AEP is partially activated to dispatch physical security personnel to manually monitor key access points affected by the contained PACS segment.*
  - ***Eradication & Recovery:*** *Identify the compromised controller, wipe it, and restore its configuration from a known-good backup. Monitor the system intensely as it is carefully brought back online.*

Incident Response: FIDS Data Integrity Attack

- **Scenario:** The Airport Operations Control Center (AOCC) receives multiple calls from airline staff and passengers reporting that Flight Information Display Systems (FIDS) throughout the terminals are showing incorrect gate assignments and false flight cancellation notices, causing passenger confusion and crowding.
- **Technical Response Steps:**
  - ***Detection & Analysis:*** *The security team correlates AOCC reports with network monitoring data. They analyze traffic to the FIDS content server and identify unauthorized commands originating from a compromised marketing department workstation that has improper network access to the FIDS management interface. Log analysis reveals a successful spear-phishing attack on the workstation as the initial entry point.*
  - ***Containment:*** *Immediately isolate the compromised workstation from the network to sever the attacker's access. Implement an emergency firewall rule to block the FIDS content server from accepting commands from any source other than a dedicated, secure management terminal located within the AOCC.*

Incident Response: FIDS Data Integrity Attack (Cont'd)

- **Technical Response Step (Cont'd):**
  - ***Coordinate with AEP & Crisis Comms:*** *Activate the CIRP, which triggers a notification to the AOCC and Public Information Officer (PIO). The AEP's communication annex is initiated: use the Public Address (PA) system and official airport social media channels to advise passengers of the FIDS issue and direct them to airline staff or airport websites for accurate flight information. Deploy operations staff with manual signage to critical areas.*
  - ***Eradication & Recovery:*** *Re-image the compromised workstation from a known-good build. Conduct a full vulnerability scan and integrity check of the FIDS server and its data. Manually verify and correct all flight data on the FIDS content server before gradually restoring its normal update feeds under heightened monitoring.*

Analyzing and Mitigating Future Technical Threats

- **NextGen ADS-B:** Assess the risk of signal spoofing attacks using Software Defined Radios (SDRs). Mitigate by integrating ADS-B data with other surveillance sources like ground radar or Multilateration (MLAT) for verification before use in airport systems.
- **UAVs & C-UAS:** Analyze cyber threats to the Counter-UAS system itself, such as RF jamming of its detectors or data spoofing to create false negatives. Mitigate by selecting C-UAS technology with anti-jamming capabilities and strong data integrity features.
- **Artificial Intelligence (AI):** Evaluate the risk of sophisticated data poisoning attacks, where adversaries subtly corrupt AI training data to create blind spots in security screening or threat detection models. Mitigate with rigorous data validation, integrity checks, and model monitoring.

Conclusion

- **Recap:** Advanced airport cybersecurity requires dedicated strategies for securing complex Operational Technology (OT), fostering a technically-adept security culture, operationalizing threat intelligence, executing incident response, and adapting to emerging threats.
- **Key Principles:**
  - *Implement defense-in-depth for OT systems, recognizing their unique vulnerabilities and safety impacts.*
    Empower all airport personnel through targeted, role-based training to create a resilient "human firewall."
  - *Leverage collaboration and information sharing (e.g., A-ISAC) for proactive, intelligence-driven defense.*
  - *Ensure resilience through well-tested incident response and business continuity plans that integrate cyber and physical operations.*
  - *Adopt a "security-by-design" mindset to address the risks of future technologies like NextGen, UAVs, and AI.*

Airport Project Preview

- In the next course, you will join tabletop exercises to put the cybersecurity concepts from this course into practice
- These projects will mimic the airport environment, IT and cyber teams, and EOC/AOC using the Incident Command System
- Thanks for being part of this class!