

Securing Operational Technology (OT) and Industrial Control Systems (ICS)

Securing Operational Technology

Speakers:

- John Matlock, P.E., President of Matlock Matlock



Linktree Accounts

Moderator:

- James “Sandy” MacMurtrie
Johnson Controls

TRI - REGIONAL
JETS 2025

Society of
SAME
American Military Engineers



PRESENTER

John Matlock

Matlock and Associates, LLC
"MATLOCK"



MATLOCK

- **Sports Teams:** Philadelphia Eagles and Jacksonville Jaguars
- **Vacation Spots:** Costa Rica
- **Did You Know:** I have four kids, seven, five, two and one years old
- **Hobbies:** Skiing and Surfing
- **Cooler Project(s):** Worked on the Department of State Explosive Detection Canine Program

Learning Objectives

- Explain OT vs. IT in plain English
- Identify the big four assets that matter most
- Set three practical alerts
- Know which training/certificates fit your role

“Visibility before control.” – Robert M. Lee

Agenda

- Foundations: OT/ICS 101
- Threats: Stats, notable attacks, common patterns
- Defense: Big Four, visibility, free tools
- Action: 3 alerts, Day-1 playbook, how to act
- People: Training/certs, CIO POC/s, recap & Q&A

"Perfect is the enemy of done." - Voltaire

most impacts leverage **simple paths**, not zero-days

**TRI - REGIONAL
JETS 2025**

SAME
WINDUP STRATEGY

Story – “The Water Plant That Wasn’t”

Category: THREATS

- Bad Guy Brag” We changed setpoints, killed alarms”
- Twist: decoy revealed the same simple playbook
- Takeaway: remove exposure, watch and restore

Close the IT-> OT Paths

Foundations: OT/ICS 101



OT/ICS 101 – What Actually Runs the World

- OT moves water, power, fuel, air – physical processes
- ICS steers with HMIs, PLCs/RTUs, historians, networks
- Mission: safety & uptime, every shift



"In OT, we protect physics, not just data."

OT/ICS 101 – SILOS

An isolated grouping, department, etc., that functions apart from others especially in a way seen as hindering communication and

Departmental IT vs DPW



Operators of OT systems and the IT teams are often coming at the same problem from a different place. They often even seem to speak different languages.

Technology Passive vs Active



Active scans against the world. Protocols and how the systems communicate. Legacy life cycle as opposed to 3-year rip and replaces.

Security Locked vs Open



We all want to be more secure, but OT integrators prioritize function and operation over security, and assign admin privileges to people who might not need them.

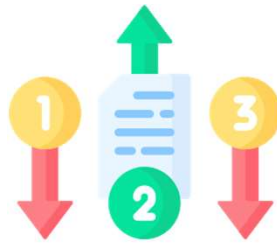
"Go talk to the engineers!"

IMPACTS OF SILOS



COMMUNICATION

How do we get to a place where the IT team and Operations are able to speak the same language and focus on solving the problem as a cross-functional team.



PRIORITY

When the CIA Triad becomes the Safety, Availability, Integrity, Confidentiality Quad Chart! (SAIC)



EFFICIENCY

Can we use the data available and the tools we already have to get more out of our teams, buildings, and equipment?



OWNERSHIP

Who owns it? Whether that is a system or problem.

Who's in charge of it and who will be the one to fix it?



"C3PO, Oh My!"

Operational Technology is Different!

IT
(Business Network, Cloud
Computing, etc.)

Data Driven

Confidentiality

Integrity

Availability

OT
(FRCS - BCS, UCS, ESS, etc.)

Safety Driven

Availability

Integrity

Confidentiality

Highest
Priority

Lowest
Priority

"Uptime and Safety must come first."

OT/ICS 101 – What Actually Runs the World

- OT moves water, power, fuel, air – physical processes
- ICS steers with HMIs, PLCs/RTUs, historians, networks
- Mission: safety & uptime, every shift



"In OT, we protect physics, not just data."



Key Terms in Operational Technology OT?

- Industrial Control Systems (ICS) – a collective term used to describe different types of control systems and associated instrumentation, which include the devices, systems, networks, and controls used to operate and/or automate industrial processes
- Supervisory Control and Data Acquisition (SCADA) – is a computer-based system for gathering and analyzing real-time tie data to monitor and control equipment that deals with critical events
- Facility-Related Control Systems (FRCS) – are ICS that are comprised of Building Control Systems (BCS), Utilities Control Systems (UCS), Electronic Security Systems (ESS), Fire Alarm Systems (FAS) and even Business Systems
- Control Systems (CS) – manage, command, direct, or regulate the behavior of other devices or systems. They can range from a single home heating controller using a thermostat to large industrial control systems which are used for controlling processes or machines.

ICS is “transportation” where SCADA is “air traffic control.”

Threats: Stats, notable attacks, common patterns



Statistics – OT Facts and Signals

Category: THREATS

- Industrial ransomware: trending up year-over-year
- Initial access reality: 58% of ICS/OT incidents start in IT (pivot into OT).
- Most impacts leverage simple paths, not zero-days

Monitor the IT conduits into the OT network.

most impacts leverage **simple paths**, not zero-days

**TRI - REGIONAL
JETS 2025**

SAME
ENTRY POINTS

Notable OT Attacks — Recent Highlights

Category: THREATS

- Water: Unitronics PLC/HMI internet exposure
- Energy: Ukraine grid (protocol misuse, Industroyer2)
- Cross-sector: PIPEDREAM/INCONTROLLER tooling

Different sectors, similar entry paths

most impacts leverage **simple paths**, not zero-days

**TRI - REGIONAL
JETS 2025**

SAME
PROCESSES, SAME

The Modern Threat — They Speak Your Protocols

- Adversaries use your protocols & vendor tools
- Goal: change the process, not just steal data
- Open paths + weak creds = “no-exploit” wins

If paths are open, exploits are optional.

Defense: Big four, visibility, free tools



most impacts leverage **simple paths**, not zero-days

**TRI - REGIONAL
JETS 2025**

SAME
PRODUCTION WAY

The Big Four — Protect These First

- PLC — the brain (logic → physics)
- HMI — the steering wheel (who's driving?)
- EWS — the keys (pushes logic/firmware)
- Historian — the black box (truth for ops/IR)

Guard the Big Four and risk drops fast.

most impacts leverage simple paths, not zero-days

**TRI - REGIONAL
JETS 2025**

SAME
WINDUP DAY

Visibility First — If You Can't See It, You Can't Stop It

- Watch one control segment, passively
- Baseline one full shift
- Learn who talks to PLCs, and when

One mirror port + one shift = clarity.

most impacts leverage **simple paths**, not zero-days

**TRI - REGIONAL
JETS 2025**

SAME
ANALYSIS WAY

Free Software — Start Here

- Wireshark — targeted packet captures
- Zeek — “who-talked-to-whom” logs
- Suricata — rules-based alerts
- draw.io — quick maps for allow-lists

Zero-cost tools, high-value insight.

most impacts leverage **simple paths**, not zero-days

**TRI - REGIONAL
JETS 2025**

SAME
SINGLE ATTACK METHOD EVERY TIME

Three Simple Alarms

- New talker → PLC (not on allow-list)
- Writes after hours (outside maintenance windows)
- ICS on wrong VLAN (e.g., Modbus on office Wi-Fi)

Rules, always passive, no scanning, no inline boxes.

most impacts leverage **simple paths**, not zero-days

**TRI - REGIONAL
JETS 2025**

SAME
SINGLE ATTACK VECTOR

Day-1 Playbook — Do This Before Lunch

- Mirror one control switch (observe only)
- Write the allowed-talkers list (who/when/ports)
- Gate remote access via jump host + MFA
- Save a clean backup of controller logic

Momentum beats perfection.

most impacts leverage **simple paths**, not zero-days

**TRI - REGIONAL
JETS 2025**

SAME
SINGLE-AGENT, MULTI-ENVIRONMENT

Simple How to Act — See, Decide, Contain, Recover

- See: compare traffic to your allow-list
- Decide: investigate new/off-hours events
- Contain: block the source, not the process
- Recover: restore last known good; document

Calm, simple, repeatable actions.

People: Training/certs, CIO POC/s, recap & Q&A



most impacts leverage simple paths, not zero-days

TRI - REGIONAL
JETS 2025

SAME

IT & OT Training and Certifications – Roadmap

- **Foundations:** (ISC)² CC, Security+
- **ICS-Focused:** GICSP, ISA/IEC 62443, GRID, GCIP
- **Leadership:** CISSP, CISM, CISA
- See DoD 8149 Qualification Guide

JUST GRADUATED WITH A CYBERSECURITY
DEGREE AND A DOZEN CERTIFICATIONS....



THERE WOULD BE JOBS

Pick by charted job role and your next 12-month career goal.

most impacts leverage **simple paths**, not zero-days

**TRI - REGIONAL
JETS 2025**

SAME
ANALYSIS WAY

CIO Cybersecurity POCs — Who Owns What

- **CIO/CISO:** policy, risk, funding
- **OT/Facilities:** windows, safety, operations
- **Network:** paths, segmentation, jump host
- **IR Lead:** contain, restore, comms cadence
- **Vendors/MSPs + CISA Region:** support & escalation

Clear roles prevent confusion during incidents.



CIO Cybersecurity POCs



CYBERSECURITY PROGRAM OVERSIGHT

CIO2 CYBERSECURITY MANAGEMENT



CIO2: William Smiley
Cybersecurity Division Director
904-542-9056 | william.l.smiley4.civ@us.navy.mil



CIO: Andrea Freeman
Command Information Officer
904-542-4191 | andrea.l.freeman.civ@us.navy.mil

CIO4 CYBERSECURITY INFRASTRUCTURE AND ENGINEERING



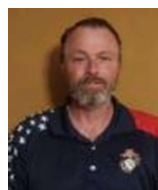
CIO4: Antonio Jefferson
Operation Technology Division Director
904-542-5839 | antonio.s.jefferson2.civ@us.navy.mil



CIO2.1: Lydell Sapp
Construction and Design Contracts Review /
Cybersecurity Commissioning (CyCx)
904-542-8484 | Lydell.d.sapp.civ@us.navy.mil



CIOD: Joseph Ellis
Defensive Cybersecurity Operations
Analyze Cyber Threats and Vulnerabilities
(904) 403-8323 | joseph.p.ellis.civ@us.navy.mil



CIO41: Bobby Kelley
Control Systems Platform Enclave Brch Manager
ACAS, HBSS and VMWARE Support
904-542-2490 | bobby.j.kelley.civ@us.navy.mil



CIO42: Kevin Gaddist
Facilities Related Control Systems Brch Manager
AMI, SCADA, DDC, and HVAC Support
904-542-8495 | kevin.k.gaddist.civ@us.navy.mil



CIO43: Paddy Jackson
Information Systems Security Engineer Lead
DRAGOS / Cybersecurity Threat Analysis
904-542-5488 | paddy.o.jackson.civ@us.navy.mil

most impacts leverage **simple paths**, not zero-days

**TRI - REGIONAL
JETS 2025**

SAME
ANALYSIS WAY

What We Discussed — Five Moves This Week

1. Defend **physics & uptime** (OT $\neq$ IT)
2. Map conduits
3. Guard the **Big Four** first
4. Baseline + **3 alerts**
5. Start **Day-1**



Act small, win big, repeat.



Contact Us



John Matlock, Matlock

Phone: 571.858.3710

- E-mail: john.matlock@matlockllc.com



Linktree Accounts

“Make the network tell the truth—before an adversary makes it tell a story.” — John Matlock

Q&A / Discussion

