

PROTECTING FIELD DATA & SYSTEMS: CYBERSECURITY in OT

Bradley Nash, ExxonMobil

As OT environments become increasingly interconnected, traditional perimeter-based security models are no longer sufficient. The attack surface has expanded beyond defined network boundaries to include:

- Third-party vendors
- External remote access pathways
- Unmanaged and unknown connections
- Physical access vectors such as unauthorized devices

To address these challenges, an External Network Connectivity Maturity Model was developed, which outlines a structured path from basic visibility to fully controlled and automated connectivity governance.

The model progresses through five key stages:

1. Third-Party Awareness – Understanding who has access to your environment
2. Connection Visibility – Identifying all external network connections into ICS
3. Design Governance – Enforcing architecture and security reviews for connectivity
4. Centralized Access Control – Consolidating and controlling interactive access pathways
5. Data Brokerage & Segmentation – Reducing direct system-to-system interaction through controlled data flows

A major risk highlighted in the field is the continued reliance on “sneaker net” practices, where unauthorized USB devices or unmanaged laptops are introduced into OT environments without visibility or control. These pose a significant threat vector that bypasses traditional network controls.

The presentation will further address:

- Vendor trust and contractual enforcement mechanisms
- Inventory and classification of connected assets within ICS environments
- Centralized monitoring of all external interactions
- Opportunities to automate enforcement, monitoring, and response

Effective OT perimeter security is no longer about blocking access—it’s about controlling, validating, and continuously managing all interactions with the environment.

External Connectivity Maturity

