OT/IoT Segmentation Playbook

Securing Industrial and Connected Device Networks

BlackHawk Data

blackhawk11.com

EXECUTIVE SUMMARY

Operational Technology (OT) and Internet of Things (IoT) devices present unique security challenges due to their specialized nature, long lifecycles, and critical role in business operations. This playbook provides a practical methodology for implementing network segmentation to protect these assets while maintaining operational continuity.

Effective OT/IoT segmentation reduces the attack surface, limits lateral movement, and ensures that compromised IT systems cannot directly impact critical industrial processes. This guide aligns with industry frameworks including the Purdue Model, IEC 62443, and NIST Cybersecurity Framework.

OT/IOT SECURITY CHALLENGES

Unique Risk Factors

OT and IoT environments differ fundamentally from traditional IT in several critical ways:

Factor	IT Environment	OT/IoT Environment
Availability	High availability expected	Continuous operation mandatory
Change Management	Regular updates accepted	Changes require validation
Security Patches	Automated patching common	Patches may require recertification
Device Lifespan	3-5 year replacement cycle	15-20 year operational life
Network Protocols	Standard TCP/IP	Industrial protocols (Modbus, DNP3, etc.)

Table 1: IT vs OT/IoT Environment Differences

Compliance Requirements

OT/IoT segmentation is driven by regulatory and industry requirements:

- NERC CIP: Critical infrastructure protection for electric utilities
- IEC 62443: International standards for industrial automation security
- NIST SP 800-82: Guide to OT security
- FDA Guidance: Cybersecurity for medical devices
- TSA Directives: Pipeline cybersecurity requirements

SEGMENTATION STRATEGY

Purdue Model Alignment

The Purdue Model for Control Hierarchy provides the foundation for OT network segmentation:

Level	Name	Description	Security Zone
Level 0	Physical Process	Sensors, actuators,	Critical Zone

		physical equipment	
Level 1	Basic Control	PLCs, RTUs, basic controllers	Critical Zone
Level 2	Supervisory Control	HMI, SCADA, engineering stations	Operational Zone
Level 3	Site Operations	Manufacturing execution systems, historians	Operational Zone
Level 4	Business Planning	ERP, scheduling, reporting	Enterprise Zone
Level 5	Enterprise	Corporate IT, internet, cloud	Enterprise Zone

Table 2: Purdue Model Levels

Zone Design Principles

Effective zone design follows these principles:

1. Group assets by function and criticality: Similar systems in same zone
2. Minimize cross-zone traffic: Only necessary communication allowed
3. Implement defense in depth: Multiple security controls at each boundary
4. Enable monitoring: Full visibility into zone-to-zone traffic
5. Plan for growth: Design zones to accommodate future expansion

Conduit Architecture

Conduits are secure communication channels between zones. Each conduit should:

- Be explicitly defined with documented business justification
- Implement protocol-aware inspection and filtering
- Support both north-south (hierarchical) and east-west (peer) communication
- Include redundancy for critical operational paths
- Enable logging and monitoring for security analysis

IMPLEMENTATION PLAYBOOK

Phase 1: Discovery

Comprehensive asset discovery is the foundation of effective segmentation:

6. Passive discovery: Monitor network traffic to identify all connected devices
7. Active scanning: Use specialized OT-safe scanning tools where appropriate
8. Physical inspection: Validate network diagrams against actual connectivity
9. Asset inventory: Document device details including manufacturer, model, firmware version
10. Communication mapping: Identify all required protocols and peer relationships

Phase 2: Design

Design segmentation architecture based on discovery findings:

11. Define security zones based on criticality and function
12. Map required conduits between zones
13. Select appropriate security controls for each boundary
14. Design monitoring and logging infrastructure
15. Create implementation timeline with maintenance windows

Phase 3: Deployment

Execute segmentation deployment with minimal operational impact:

16. Deploy monitoring infrastructure first for baseline visibility
17. Implement firewall rules in monitor-only mode
18. Validate rule effectiveness and tune policies
19. Enable enforcement during planned maintenance windows
20. Document all changes and update network diagrams

Phase 4: Validation

Verify segmentation effectiveness and compliance:

21. Test security controls against defined requirements
22. Validate operational functionality is maintained
23. Conduct penetration testing to verify segmentation
24. Review compliance against applicable frameworks
25. Establish ongoing monitoring and maintenance procedures

TECHNOLOGY SOLUTIONS

OT/IoT segmentation requires specialized security technologies:

Technology	Function	Key Features
Industrial Firewall	Zone boundary protection	Protocol-aware inspection, low latency
Unidirectional Gateway	Data diode implementation	Physical one-way data transfer
Network TAPs/SPAN	Traffic monitoring	Passive, non-intrusive visibility
Asset Discovery	Device inventory	Passive discovery, vulnerability identification
SIEM	Security monitoring	OT-specific parsers, correlation rules

Table 3: Segmentation Technologies

BEST PRACTICES

BlackHawk Data recommends the following best practices for OT/IoT segmentation:

26. Engage operations teams early: Security must support operational requirements
27. Test in non-production first: Validate all changes in a representative environment
28. Document everything: Maintain accurate network diagrams and policy documentation

29. Plan for incident response: Ensure security teams can access OT networks when needed
30. Monitor continuously: OT networks require 24/7 security monitoring
31. Review regularly: Audit segmentation effectiveness quarterly

Additional considerations for specific industries:

- Manufacturing: Protect production lines while enabling MES integration
- Energy: Implement NERC CIP compliance with operational reliability
- Healthcare: Secure medical devices while ensuring patient care continuity
- Transportation: Protect critical infrastructure with high availability requirements

CONCLUSION

OT/IoT segmentation is essential for protecting critical infrastructure and connected devices from cyber threats. By following this playbook, organizations can implement effective segmentation that enhances security while maintaining operational continuity.

The key to success is understanding that OT/IoT security requires a different approach than traditional IT security. Close collaboration between security and operations teams, combined with specialized tools and methodologies, ensures successful outcomes.

For OT/IoT segmentation assessment, design, and implementation services, contact BlackHawk Data industrial security specialists at blackhawk11.com.