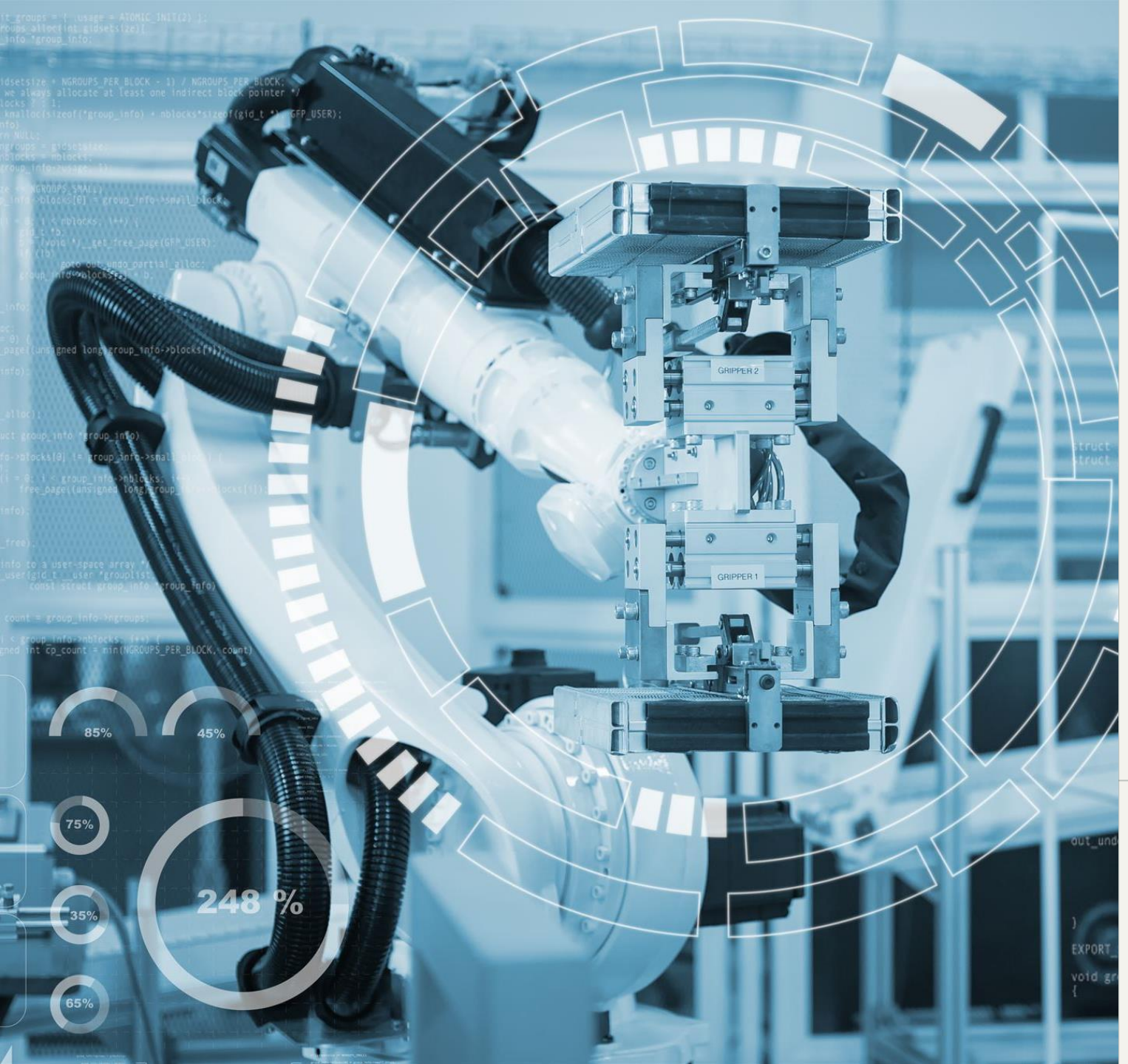


สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

OT vs. IT Security: Key Differences and Strategies for Safeguarding Industrial Automation in the Digital Age

Protecting industrial systems through tailored security methods

INTRODUCTION

Overview of Digital Transformation and Cybersecurity

Digital Transformation in Industry

Integration of IoT, AI, and cloud computing is reshaping industrial operations and enhancing connectivity.

IT Security Focus

IT security protects data and enterprise systems from cyber threats in digital environments.

OT Security Focus

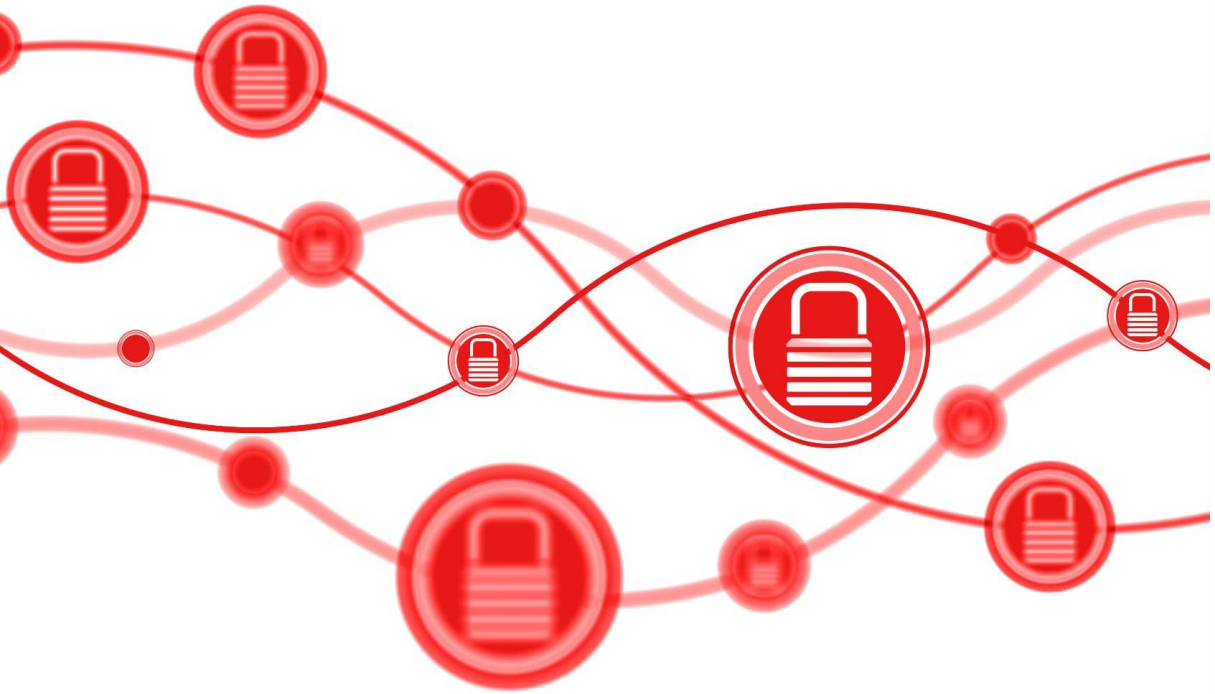
OT security safeguards physical processes and industrial control systems from operational risks.

Strategic Cybersecurity Insights

Understanding IT and OT security differences is key to protecting industrial automation effectively.

UNDERSTANDING IT SECURITY

Definition and Focus Areas of IT Security



Core Goals of IT Security

The CIA Triad ensures confidentiality, integrity, and availability of information in IT environments.

IT Assets Protected

IT security protects critical assets such as servers, databases, endpoints, and cloud services.

Security Measures

Firewalls, encryption, and access controls prevent unauthorized access and cyberattacks.

Dynamic IT Environments

Frequent updates and patches address vulnerabilities and maintain system integrity.

UNDERSTANDING OT SECURITY

Definition and Focus Areas of OT Security

Core Components of OT

OT security protects ICS including SCADA, PLCs, sensors, and actuators critical to physical process management.

Critical Industry Sectors

OT systems support manufacturing, energy, utilities, and transportation sectors requiring reliable physical operations.

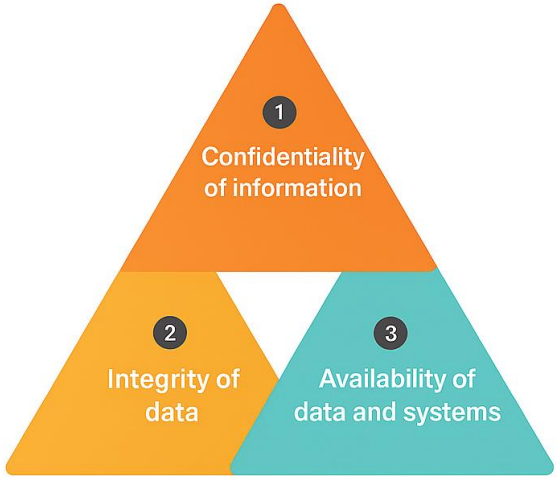
Security Objectives

OT security aims to ensure safety, reliability, and operational continuity while protecting legacy equipment.

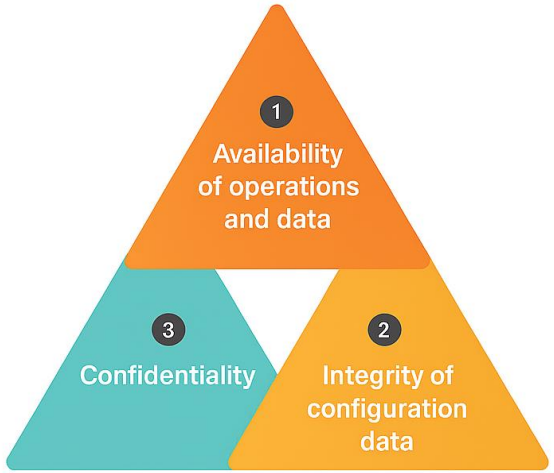
Challenges in OT Security

Legacy systems with limited security features require strategies to avoid downtime and operational disruption.

KEY DIFFERENCES BETWEEN IT AND OT SECURITY



CIA Triad



AIC Triad

Comparing Security Priorities in IT and OT

TRIAD	IT SECURITY (CIA)	OT SECURITY (AIC)
First Priority	Confidentiality	Availability
Second Priority	Integrity	Integrity
Third Priority	Availability	Confidentiality
Focus	Data protection	Operational continuity

Comparative Analysis of IT and OT Security

ASPECT	IT SECURITY	OT SECURITY
Primary Focus	Data protection	Physical process protection
Risk Tolerance	Moderate	Very low
Update Frequency	Regular patches	Infrequent, due to uptime needs
Asset Lifespan	Short (3-5 years)	Long (10-30 years)
Protocols	TCP/IP, HTTPS	Modbus, DNP3, OPC-UA

THREAT LANDSCAPE

Common Threats in IT and OT Environments

IT Security Threats

IT systems face ransomware, phishing, and data breaches risking sensitive data and operations disruption.

OT Security Threats

OT environments face sabotage, equipment damage, and safety risks impacting physical infrastructure.

Shared IT-OT Vulnerabilities

Interconnection of IT and OT creates shared vulnerabilities needing integrated security measures.

CHALLENGES IN OT SECURITY

Unique Obstacles in Securing OT Systems

Legacy System Limitations

Many OT devices lack built-in security features and are hard to monitor or update due to their legacy design.

Patching Risks

Applying patches can disrupt critical OT operations, making vulnerability management complex and risky.

Cybersecurity Awareness Gap

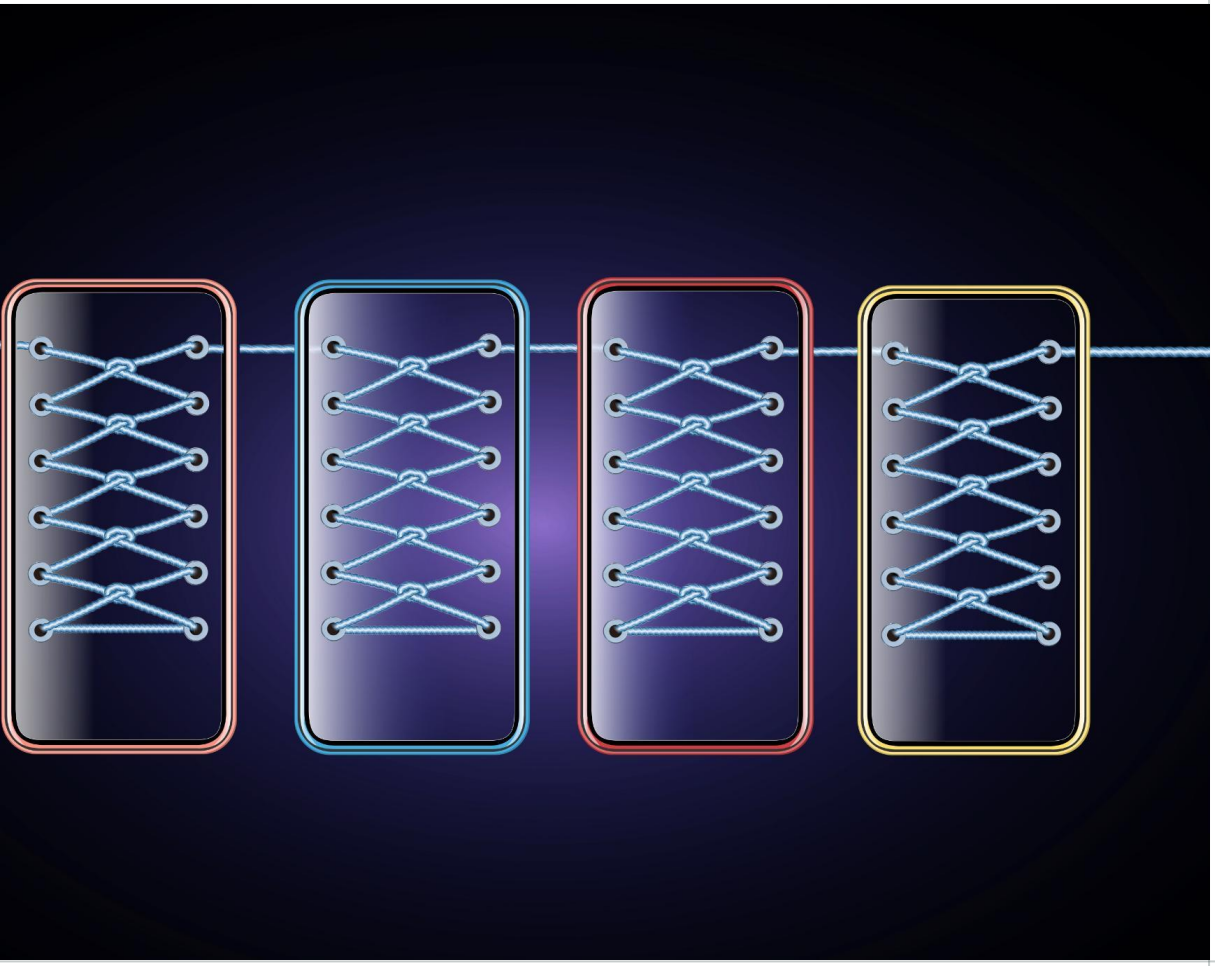
OT personnel often prioritize operational efficiency over security, leading to limited cybersecurity awareness.

Need for Specialized Solutions

Effective OT security requires specialized solutions and a cultural shift to prioritize cybersecurity in operations.

BEST PRACTICES FOR OT SECURITY

Effective Strategies for Protecting OT Systems



Network Segmentation

Segmenting OT networks with air gaps and DMZs isolates critical systems from external cyber threats effectively.

Asset Inventory and Vulnerability Assessment

Maintaining accurate asset inventories and conducting regular vulnerability assessments are vital for risk identification and mitigation.

Secure Access and Authentication

Implementing secure remote access protocols and strong authentication prevents unauthorized entry into OT systems.

Utilize Secure OT Protocols: Adopt industrial communication protocols with built-in security features (e.g., OPC UA, Secure Modbus) to ensure authentication, encryption, and integrity of data exchanged between devices and systems.

Continuous Monitoring and Collaboration

Continuous threat monitoring, incident response, and IT-OT collaboration ensure rapid detection and unified security efforts.

CONVERGENCE STRATEGY

Managing IT/OT Integration Risks and Benefits

Benefits of IT/OT Convergence

Integration of IT and OT improves efficiency, provides real-time data insights, and enhances decision-making.

Risks of Integration

Convergence increases attack surfaces and system complexity, raising cybersecurity and operational risks.

Mitigation Strategies

Unified governance, shared security tools, and cross-training help manage risks and promote collaboration.

Strategic Planning and Evaluation

Continuous evaluation and strategic planning ensure a secure and resilient IT/OT infrastructure.

IT/OT Convergence with Gateway Strategy

Secure Data Exchange

Gateways enable controlled data exchange between IT and OT networks while minimizing cybersecurity risks.

Protocol Translation and Filtering

Gateways enforce protocol translation, traffic filtering, and access control to prevent unauthorized access.

Operational Integrity and Compliance

Gateways isolate critical OT systems from IT threats, maintaining operational integrity and security compliance.

CONCLUSION & RECOMMENDATIONS

Final Thoughts and Actionable Insights

Unique OT Cybersecurity Needs

OT environments have distinct security requirements different from traditional IT systems and need specialized approaches.

Collaboration Between Teams

Effective cybersecurity requires close collaboration between IT and OT teams to build resilient infrastructure.

Shared Security Responsibility

Security should be a shared responsibility across all departments to foster a culture of cybersecurity awareness.

Tailored Security Strategies

Implementing customized cybersecurity strategies protects industrial automation systems in the digital era.