Unlocking Operational Resilience: IT and OT Collaboration for Manufacturing Digital Transformation

Enhancing manufacturing through integrated IT and OT strategies

Jill Klein, Head of Emerging Tech & IoT, CDW
Oscar De Leon, IoT Strategist, CDW

August 19, 2025

AGENDA

- The Evolving Landscape of IT/OT Convergence in Manufacturing
- Strengthening OT Network Security: Closing Existing Gaps
- Critical Role of Network Design and Segmentation in OT Environments
- Fostering IT/OT Collaboration: Strategies and Tactics
- Translating IT/OT Alignment Into Innovation and Cyber Defense

The Evolving Landscape of IT/OT Convergence in Manufacturing

Accelerating Smart Manufacturing: The Digital Pillars of Transformation

From IoT connectivity to AI-driven automation, manufacturers are embracing technologies to enhance operational efficiency, reduce risk, and unlock the full potential of IT and OT collaboration

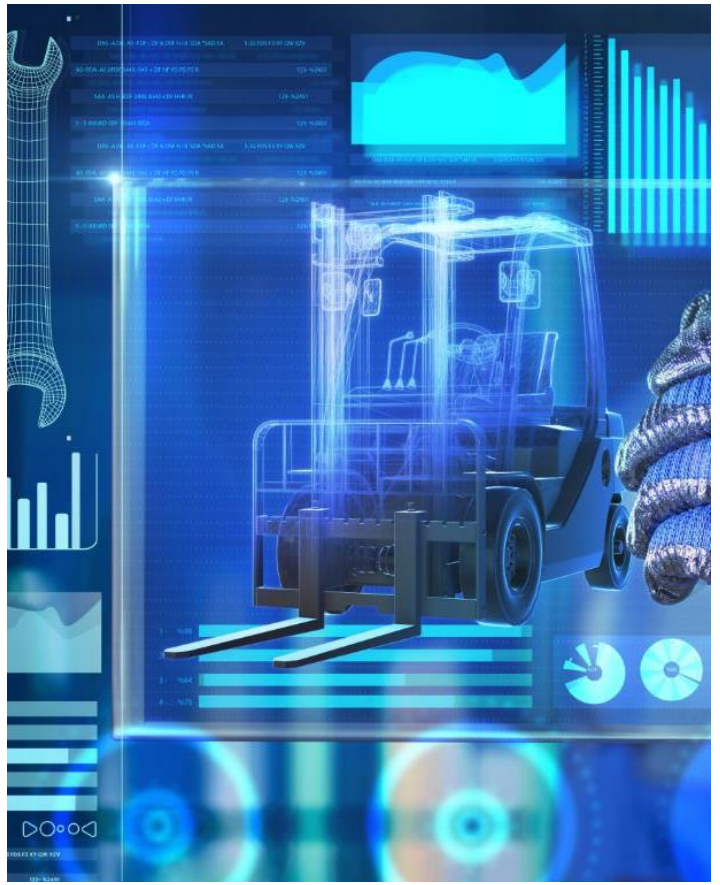
Internet of Things Adoption - IoT devices connect machines and systems, enabling real-time monitoring and improved operational efficiency.

91% of enterprises are investing in IoT and smart manufacturing.
6% consider their factories to be fully digitized **~Cisco August 2025**

AI and Automation Integration - Automation technologies streamline manufacturing processes, increasing productivity and reducing human error

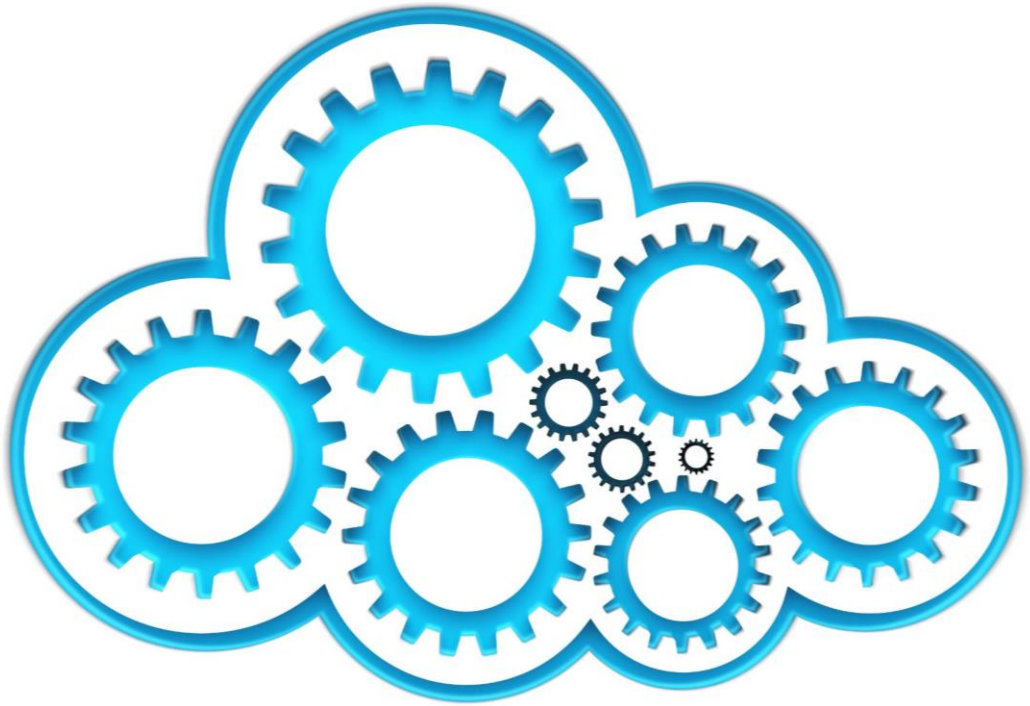
Cloud Computing Integration - Cloud platforms facilitate seamless data sharing and collaboration across IT and operational technology systems

Data Analytics Utilization - Data analytics tools analyze manufacturing data to drive informed decision-making and process optimization



Key Findings From CDW and Manufacturers Alliance Foundation Study

Realizing the promise and navigating the pitfalls of IT/OT integration in manufacturing



Manufacturers ALLIANCE FOUNDATION

IN PARTNERSHIP WITH CDW

IT/OT Convergence Importance

Research emphasizes the increasing role of IT and OT convergence in modern manufacturing processes

Realized Benefits

Manufacturers experience operational efficiency and improved decision-making through IT/OT integration

Integration Challenges

Many manufacturers face challenges and gaps when fully integrating IT and OT domains (Resource Gaps, Skills Gaps, Technology Sprawl)

Challenges and Opportunities at the IT/OT Intersection

Balancing priorities to unlock efficiency and innovation

Integration Challenges

Differing priorities between IT and OT create challenges in achieving seamless integration and increase security risks

Operational Efficiency Opportunities

Integrating IT and OT systems enhances operational efficiency by streamlining processes and reducing downtime (OTSM)

Innovation and Resilience

IT/OT integration fosters innovation and builds resilience by enabling smarter decision-making and adaptive systems

Polling Question #1

"Which aspect of IT/OT convergence do you believe will have the most significant impact on your manufacturing operations?"

1. Enhancing OT network security
2. Improving operational efficiency through IT/OT tool integration
3. IT/OT collaboration resulting in streamlined operations
4. Accelerating innovation with emerging technology

Strengthening OT Network Security: Closing Existing Gaps

Assessment of the Current State of OT Security

A landscape of growing maturity, persistent vulnerabilities, and strategic convergence with IT systems

Progress in OT

- 52% of organizations now place OT security under the CISO, up significantly from just 16% in 2022.

Lack of Security Controls

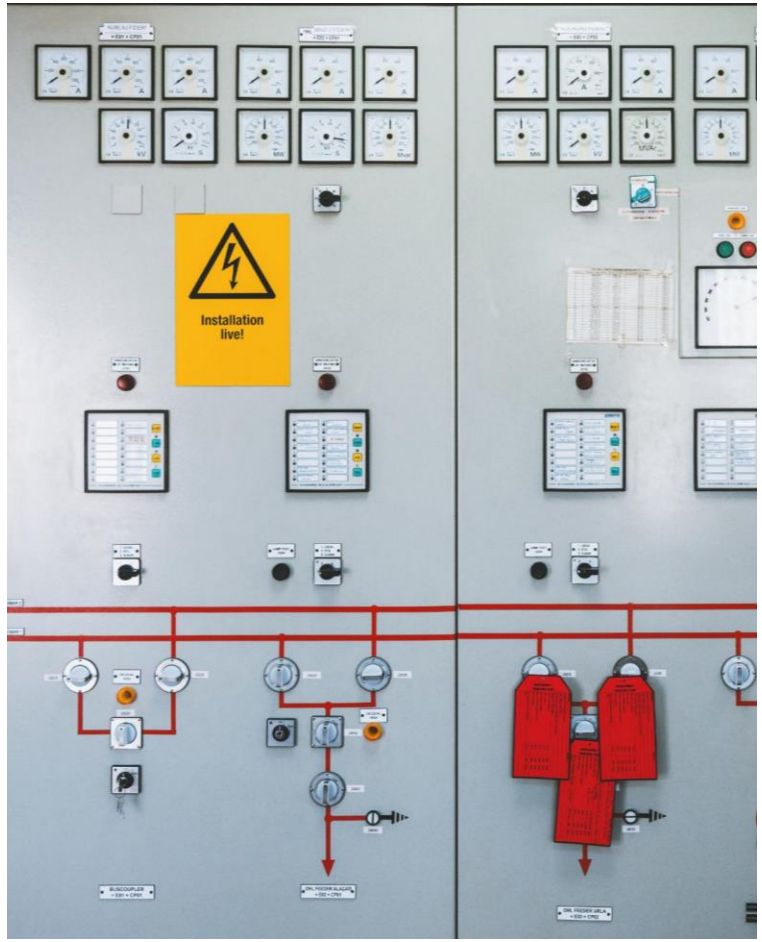
- Many OT environments do not have sufficient security measures to protect critical infrastructure assets
- Only 27% of industrial organizations report that maintain an accurate inventory of OT assets
- 69% have no inventory or inventories that are inaccurate or outdated
- 55% of OT Organizations deployed Secure Remote Access Solutions (SRA)

Widespread Vulnerabilities to Cyber Threats

- Insufficient OT security increases the risk of cyberattacks that can disrupt operational continuity

Operational Disruptions

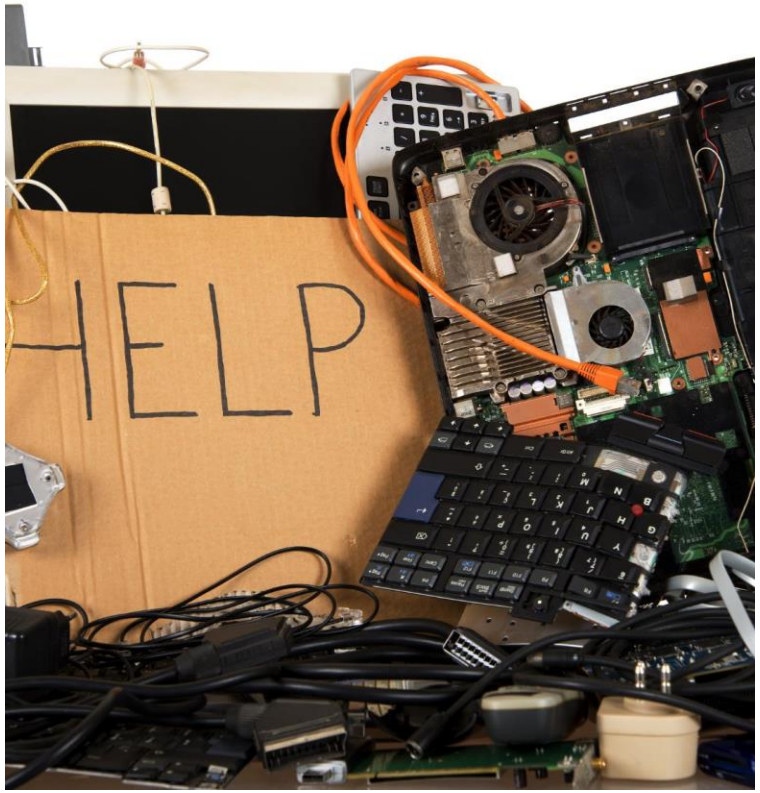
- Security weaknesses in OT can lead to operational failures impacting safety and productivity. Average cost of Downtime cost per day $1.9m



Source: The Power of Breakthroughs in IT/OT Collaboration, July 2025

Common Vulnerabilities and Risk Scenarios

Addressing legacy risks and unlocking resilience through IT/OT integration



Outdated Systems Risk

Using outdated systems increases exposure to security vulnerabilities and potential breaches. Most equipment on the manufacturing floor is over 10 years old

Weak Access Controls

Insufficient access control mechanisms can lead to unauthorized data access and security breaches

Insufficient Monitoring

Lack of proper monitoring reduces the ability to detect and respond to cyber threats timely

IT/OT Integration Vulnerabilities

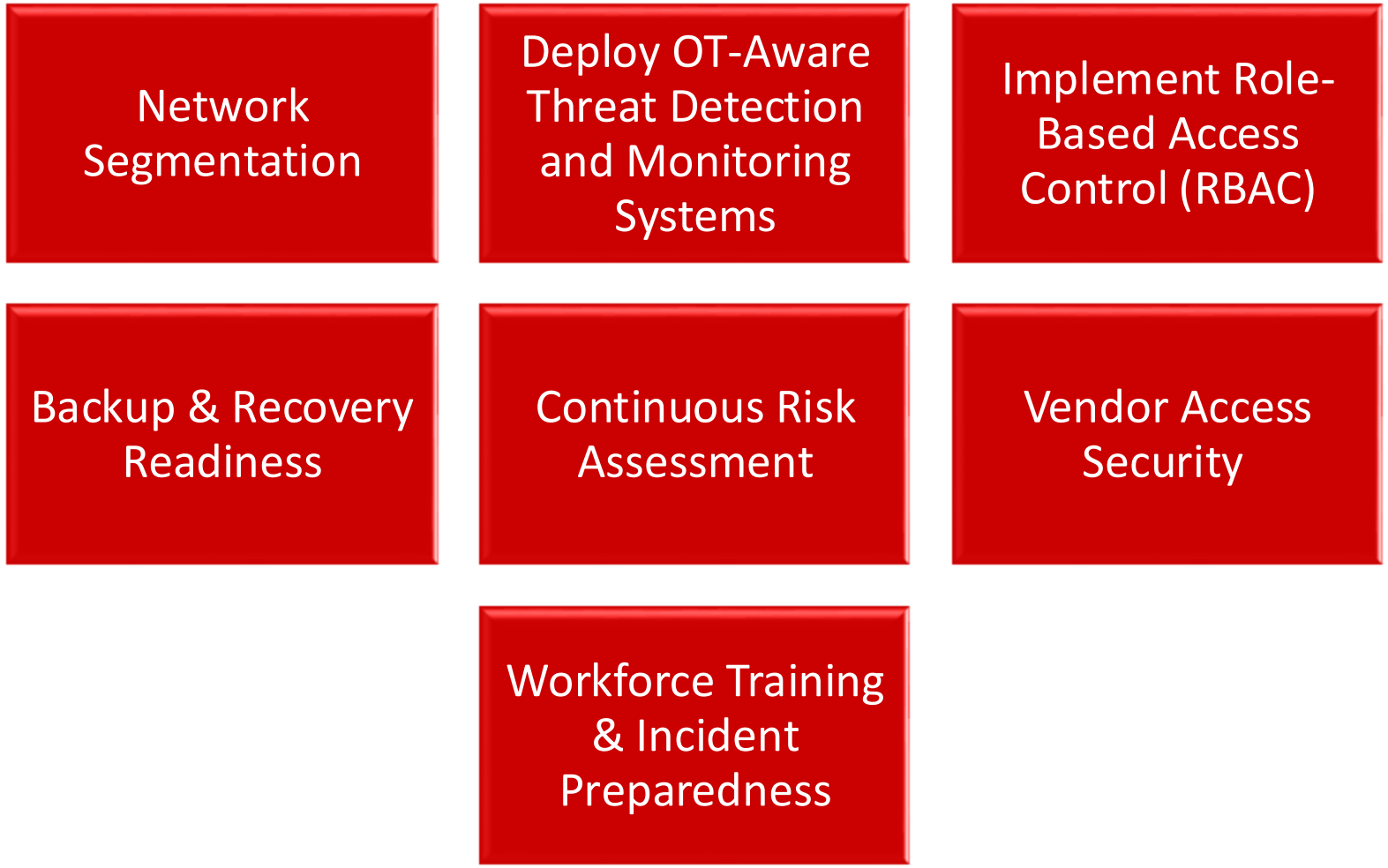
Integrating IT and OT systems can introduce new vulnerabilities if not properly secured

Increased frequency of cyber attacks

OT (Operational Technology) environments have become a prime target for cyber attacks because they sit at the intersection of national infrastructure, economic stability, and physical safety.

Actionable Steps to Enhance OT Network Protection

Emphasis is placed on asset inventory, identity and access management (IAM), and threat detection



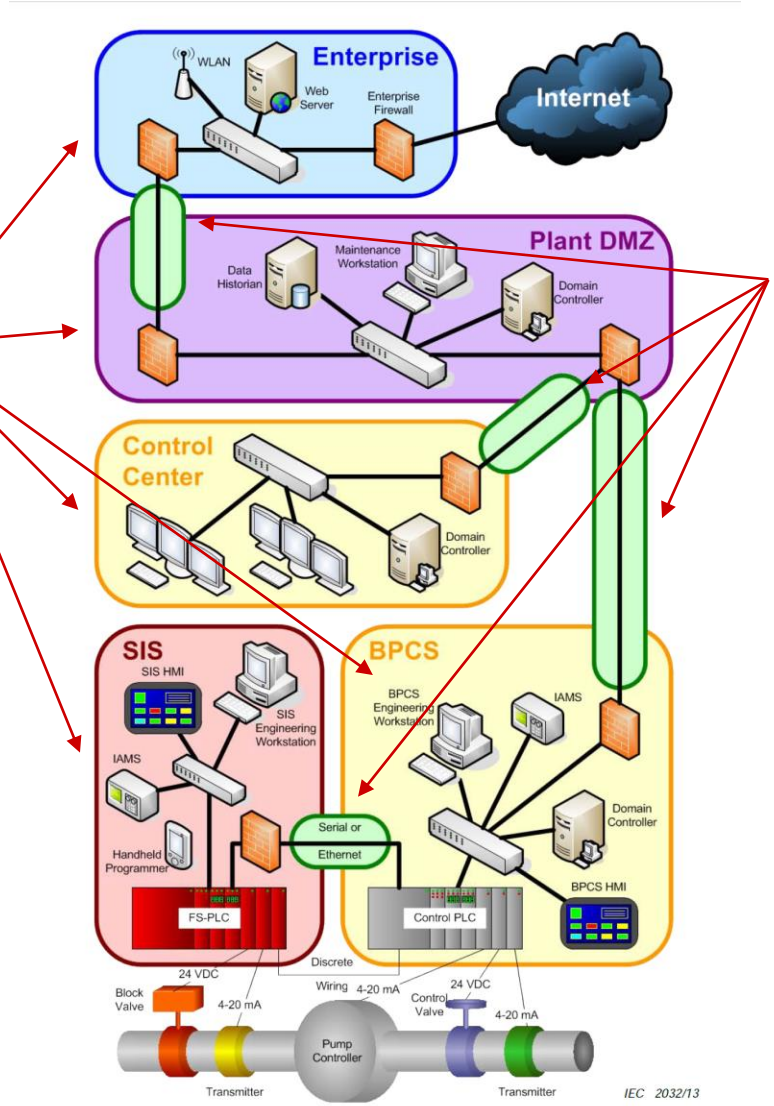
Critical Role of Network Design and Segmentation in OT Environments

Principles of Effective Network Architecture

Foundational principles that power secure, scalable, and intelligent network infrastructure

Zones

Grouping of logical or physical assets based upon risk or other criteria, such as criticality of assets, operational function, physical or logical location, required access (for example, least privilege principles) or responsible organization.



Conduits

Logical grouping of communication channels that share common security requirements connecting two or more zones

Segmentation into Zones and Conduits

Goal – Align zones with specific countermeasures required to meet the assigned security level target (SL-T) and establish conduits for secure zone-to-zone communication.

Benefit – Enables access management based on the least privilege principle and enhances control over lateral movement within the system.

IEC/ISA 62443-3-2 Requirement

Safety-related IACS (Industrial Automation and Control Systems) assets should be organized into zones that are either logically or physically separated from non-safety-related IACS assets. If separation is not possible, the entire zone must be classified as a safety-related zone. Additionally, sub-zones within these zones are allowed and can be used to further isolate assets that may pose a risk.

Risk Matrix Example

Likelihood		Consequence Severity		
		A	B	C
	5	High	High	Med-high
	4	High	Med-high	Medium
	3	Med-high	Medium	Med-low
	2	Medium	Med-low	Low
	1	Med-low	Low	Low

IEC 62443 RISK

Applying the risk formula to cybersecurity

Risk (R)= Likelihood (L) x Consequence (C)

L= Likelihood of successful cyber attack (L_{sa})

$R = L_{sa} \times C$

L_{SA} is a function of (V) vulnerability and (T) threat

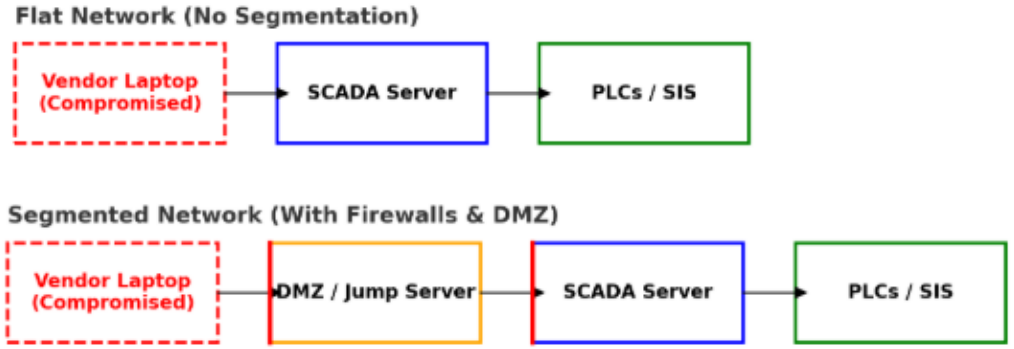
T is a function of thread agent skills motivations and target attractiveness

$R = V \times C \times T$

Risk Management Tool:
Rank unmitigated risks
Estimate mitigated risks versus risk tolerability

Segmentation Examples

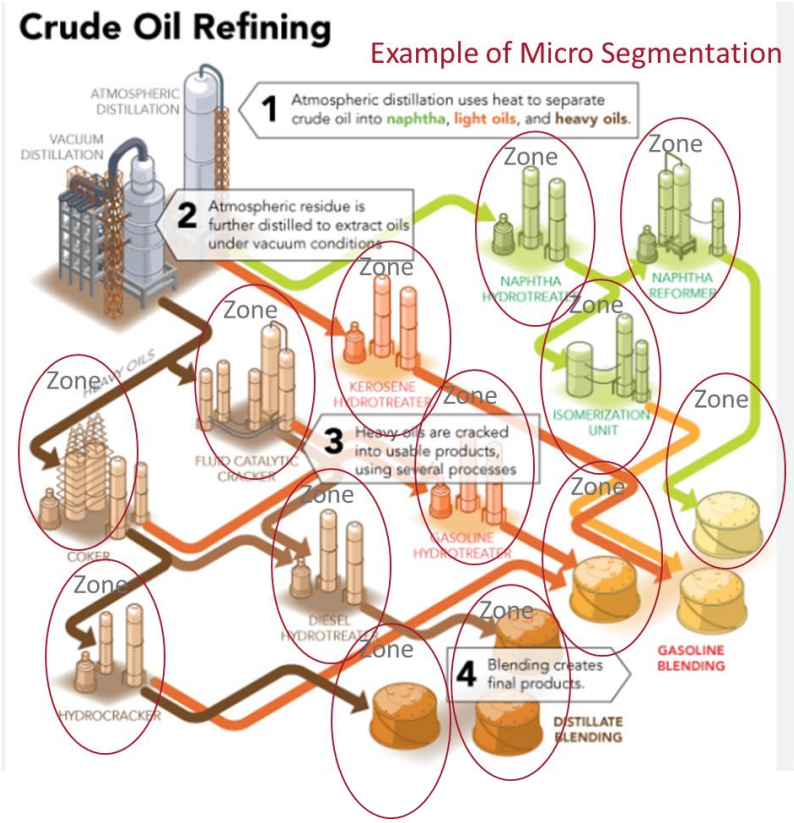
Step in Attack	Flat Network	Segmented Network
Initial compromise	Attacker gains foothold on vendor laptop	Same
Lateral movement	Unrestricted — attacker reaches PLCs in minutes	Blocked by firewall between DMZ and control zone
Privilege escalation	Attacker controls SCADA & SIS	Attacker stuck in DMZ, needs new exploit for firewall
Operational impact	Plant-wide shutdown	Only affected cell isolated, rest continue running

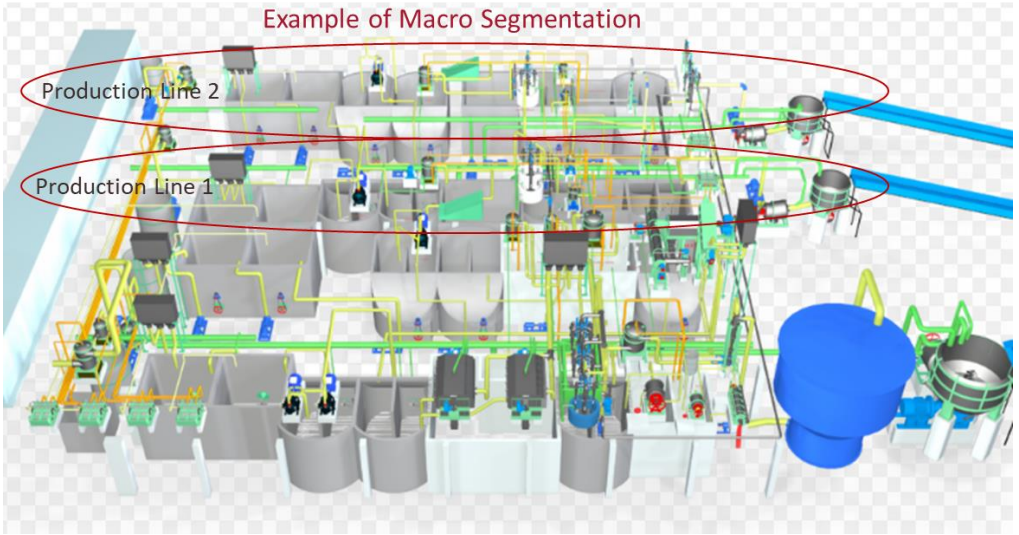


SEGMENTATION

Macro-segmentation – Segment at a production/process incorporating multiple control systems and manufacturing stations

Micro-segmentation – Segment by individual subsystems that make up a given production process





Polling Question #2

What is the biggest challenge your organization faces in achieving IT/OT convergence?"

1. Lack of skilled personnel
2. Integration of legacy systems
3. Ensuring cybersecurity
4. Aligning IT and OT priorities

Benefits of Segmentation for Security and Resilience

- Containment of Malicious Activity
- Protection of Critical Assets
- Slowing Down the Attack (Buy Time)
- Limiting Operational Impact
- Easier Incident Response & Recovery
- Compliance and Audit Benefits

Fostering IT/OT Collaboration: Strategies and Tactics

Building Cross-Functional Teams and Culture

Uniting expertise to power innovation and agility

Joint Ownership

Promoting joint ownership fosters responsibility and accountability among IT and OT team members

Building Trust

Trust between IT and OT professionals is essential for effective teamwork and project success

Shared Goals

Aligning shared goals unites cross-functional teams towards common objectives and success

Cross-Training Benefits

Cross-training enhances skills and understanding, bridging gaps between IT and OT disciplines

Communication Frameworks for Successful Collaboration

Connecting teams with purpose, clarity and trust

Regular Meetings

Scheduling consistent meetings fosters open communication and keeps teams aligned on goals and progress

Transparent Reporting

Clear and open reporting practices enhance trust and enable informed decision-making among collaborators

Conflict Resolution Mechanisms

Implementing conflict resolution methods ensures constructive handling of disagreements and maintains team harmony

Alignment Between IT and OT for Improved Outcomes

Driving performance through partnership

Strategic Alignment

Aligning IT and OT strategies ensures unified objectives and coordinated efforts across the organization

Enhanced Security

Collaboration between IT and OT improves cybersecurity defenses and protects critical infrastructure

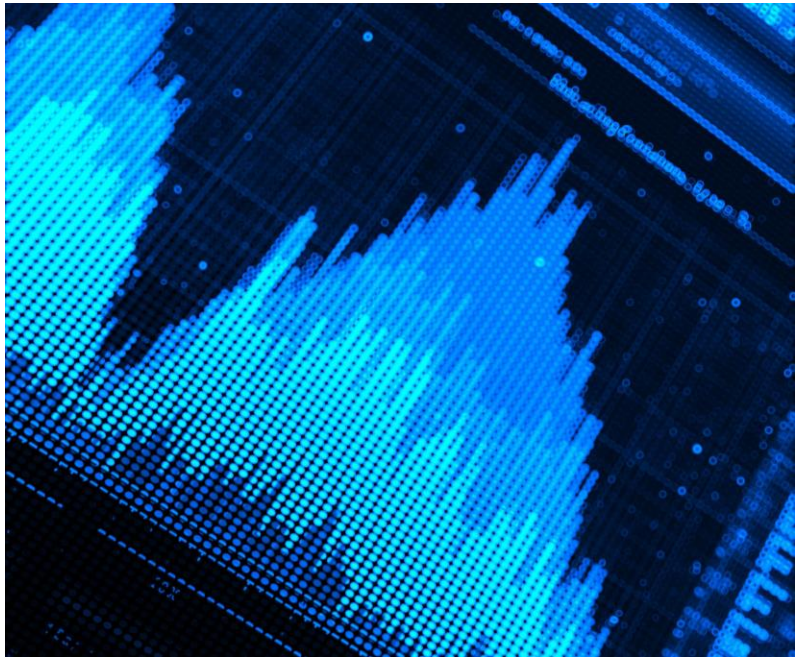
Increased Agility and Innovation

Integrated IT and OT enable faster decision-making and foster innovation in operations

Translating IT/OT Alignment Into Innovation and Cyber Defense

Impact on Decision-Making and Operational Speed

Making faster, data-driven decisions by improving visibility into operations



Impact on Decision Making

Real-Time Insights:
OT data (machine performance, production rates, quality metrics) flows directly into IT systems like ERP, MES, and BI tools.

Managers get a single, unified view of operations, supply chain, and business KPIs.

Predictive Capabilities:
Machine learning models in IT can use historical and real-time OT data for predictive maintenance, demand forecasting, and process optimization.

Better Risk Assessment:
Combining OT operational data with IT financial and supply chain data improves ROI calculations for production changes.

Cross-Department Collaboration:
Decisions are based on shared, consistent datasets between engineering, operations, and business units.

Impact on Operational Speed

Faster Incident Response:
With unified monitoring, alerts from OT (e.g., abnormal PLC commands) can trigger immediate IT-side investigations.

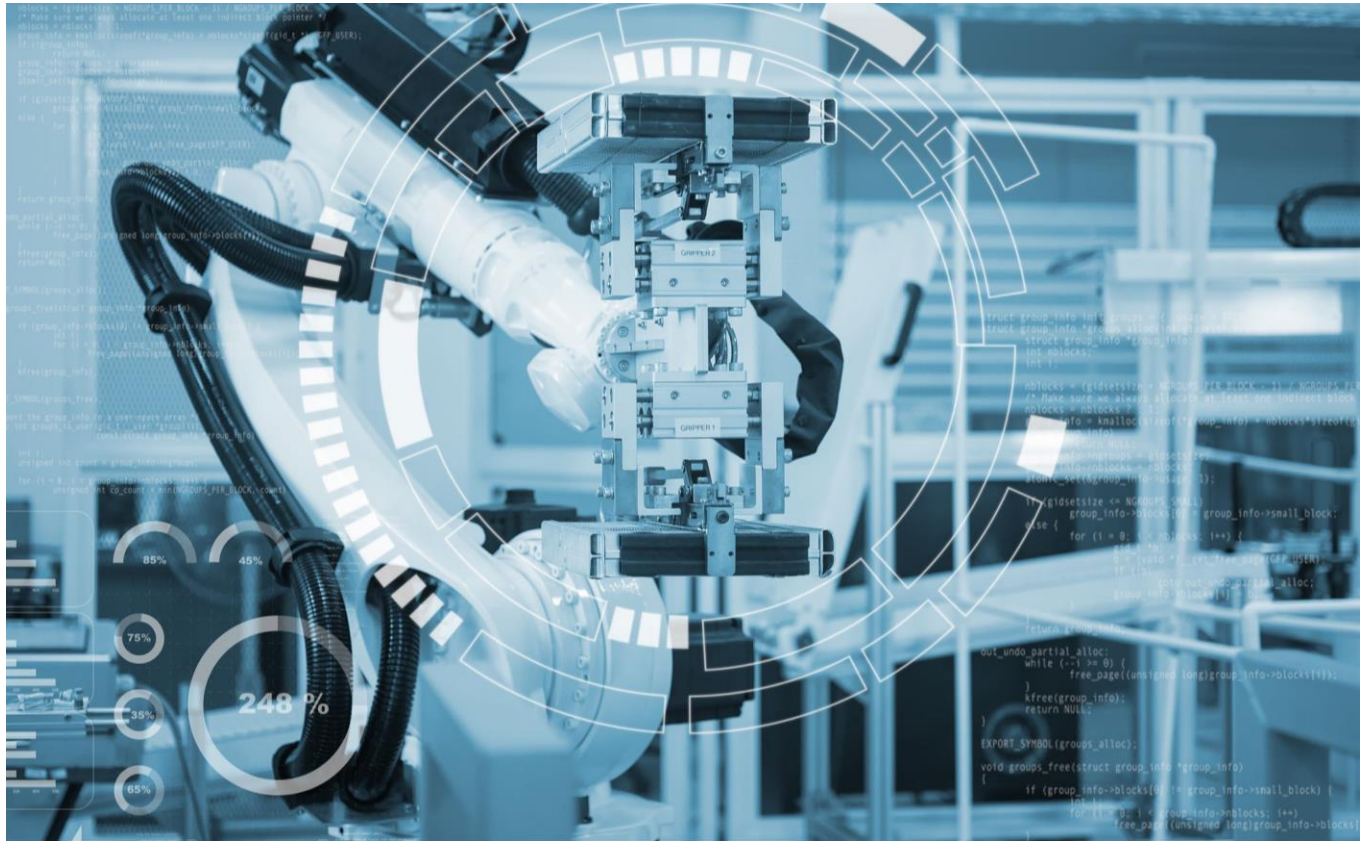
Shorter Downtime:
IT-driven automation can quickly push updated recipes, configurations, or schedules to OT systems.

Adaptive Operations:
Production can be dynamically adjusted based on real-time market demand, inventory levels, or logistics constraints.

Streamlined Maintenance:
Maintenance scheduling can be optimized based on OT sensor data rather than fixed intervals and reducing unnecessary stops.

Accelerating Innovation Through Unified Strategies

Powering smart manufacturing through teamwork and technology



Enabler	Effect on Innovation
Unified data access	Aligns strategy across departments
Digital twins & simulations	Safe, fast testing of new ideas
Predictive & prescriptive analytics	Enables proactive change
Cross-domain collaboration	Breaks down silos, sparks co-creation
Rapid compliance & market adaptation	Shortens time-to-market
Continuous improvement integration	Sustains innovation momentum

Enhancing Cybersecurity Posture with Integrated Approaches

Effective network design and segmentation are foundational to resilient manufacturing operations

Category	Advantage
Visibility	Unified monitoring & correlation
Response	Faster cross-domain incident handling
Risk	Enterprise-wide risk prioritization
Access	Coordinated IAM with least privilege
Containment	Segmentation to stop spread
Vendor Security	Consistent third-party controls
Intelligence	Combined IT & OT threat feeds
Compliance	Streamlined audits & reporting
Resilience	Continued operations during incidents
Culture	Collaboration between IT & OT teams

Polling Question #3

Which digital pillar do you think will drive the most significant transformation in your manufacturing processes?

1. IoT connectivity
2. AI and automation integration
3. Cloud computing integration
4. Data analytics utilization

Conclusion

IT and OT Collaboration

Strong collaboration between IT and OT teams is essential for resilient manufacturing operations and seamless integration.

Robust Security Measures

Implementing strong security protocols protects manufacturing systems from cyber threats and operational disruptions.

Effective Network Design

Well-designed networks ensure reliable connectivity and support resilient manufacturing processes.

Culture of Innovation and Defense

Promoting a unified culture of innovation and defense drives continuous improvement and operational resilience.

Resources

1. CDW.com/manufacturing

2. https://www.manufacturersalliance.org/itot-collaboration