Industrial Cyber

Manufacturing Cybersecurity Handbook 2025

xage SECURITY

04 Chapter 1 Cybersecurity Imperatives for Today's Manufacturing Sector

10 Chapter 2 The Manufacturing Shift to Industry 4.0

14 Chapter 3 Building Operational Resilience Amid IT-OT Convergence

18 Chapter 4 A Structured Approach to OT Disaster Recovery

22 Chapter 5 Securing the Future of Manufacturing

28 Chapter 6 Advancing OT and IoT Maturity to defend manufacturing from the edge in

32 Chapter 7 Embedding Security into ICS by Design

36 Chapter 8 Manufacturing Resilience Begins with Proactive Strategies

40 Chapter 9 7 Steps to Strengthen OT Cybersecurity in Manufacturing

46 Chapter 10 Rethinking Risk and Embedding Cybersecurity in Engineering Culture

Supported by

xage SECURITY

Cybersecurity at the Core of Modern Manufacturing

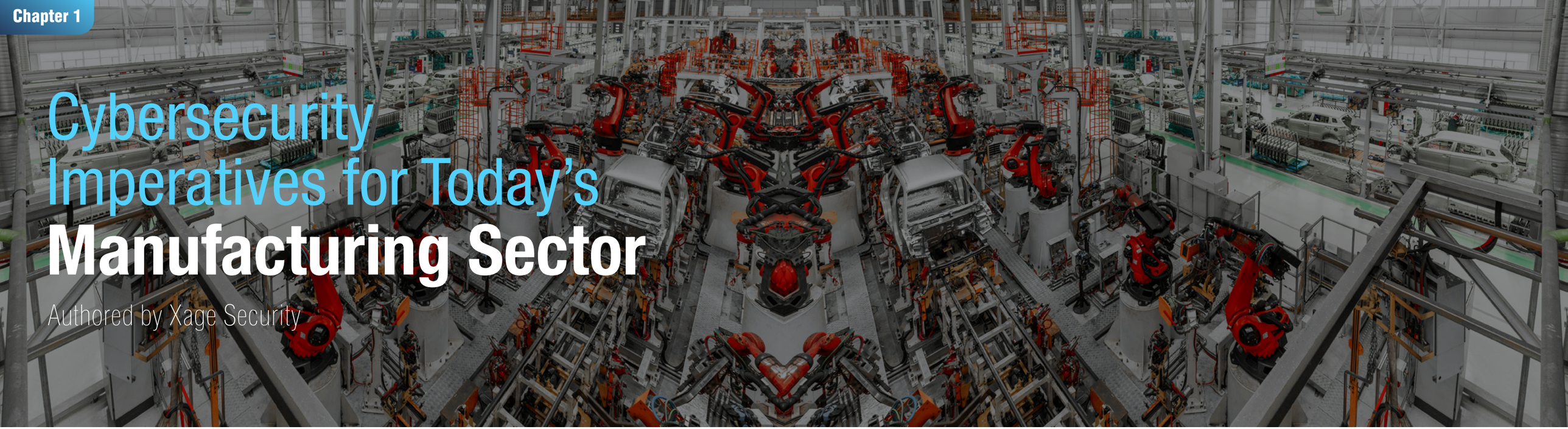
The manufacturing industry is undergoing rapid transformation. As digital initiatives accelerate and IT-OT convergence deepens, the cybersecurity risks facing production environments are growing more urgent, more complex, and more business-critical. Legacy systems, remote access, supply chain dependencies, and a rising volume of targeted attacks are all converging to test the resilience of industrial operations.

The *Manufacturing Cybersecurity Handbook 2025* offers clear, field-tested guidance for addressing these challenges. Drawing on insights from cybersecurity leaders, control engineers, and operations professionals, it presents practical strategies to secure manufacturing systems while enabling innovation and efficiency. Topics include zero trust implementation, secure remote access, network segmentation, disaster recovery, AI-enhanced detection, and embedding security into engineering and organizational culture.

This is not a theoretical guide. It reflects real-world lessons learned across sectors, from greenfield digital factories to legacy-heavy production environments. For manufacturers, cybersecurity is no longer a supporting function. It is an operational priority, a governance concern, and a foundation for long-term competitiveness.

This handbook is built to support that shift, providing knowledge and structure to help organizations move from reactive defense to strategic resilience.

Stay safe and secure,
The Industrial Cyber Team



Cybersecurity Imperatives for Today's Manufacturing Sector

Authored by Xage Security

1.1 The New Cybersecurity Landscape

As IT and OT systems become increasingly integrated, manufacturers are under growing pressure to rethink their traditional approaches to security.

The evolving threat landscape exposes long-standing vulnerabilities in many industrial environments, where legacy OT equipment was never built with cybersecurity in mind. Flat network architecture allows attackers to move laterally once inside, and the rise of remote access, while convenient, often lacks the fine-grained controls necessary to safeguard critical systems. Adding to the complexity, today's interconnected supply chains introduce third-party risks that are often opaque and difficult to monitor. A proactive and modernized security strategy is more essential than ever.
These realities expose industrial environments to a range of modern threats, from ransomware and zero-day exploits to nation-state actors.

This chapter explores critical risks, adaptive frameworks, and proactive strategies for cyber resilience in industrial environments.

1.2 Why Legacy Systems Increase Risk

Most manufacturers depend on OT systems that were never designed with cybersecurity in mind. These systems, often decades old, are built for physical reliability and safety, not for withstanding cyber threats.

Key Challenges

- **Hardcoded credentials:** Passwords are embedded directly into devices and cannot be changed easily, making them prime targets for attackers.
- **Outdated protocols:** Many systems rely on legacy communication methods that lack authentication or encryption, exposing sensitive data in transit.
- **Unencrypted communication:** Data is often transmitted in plain text, allowing attackers to intercept or manipulate critical control signals.
- **Proprietary interfaces:** Custom-built or vendor-specific technologies complicate integration with modern security tools and limit compatibility.
- **Infrequent updates:** Software and firmware updates are rare or manual, leaving systems exposed to known vulnerabilities.
- **Limited vendor support:** Older equipment may no longer be supported, making patching or securing the system difficult or impossible.
- **Remote access:** If not secured properly, it can be exploited by attackers as a gateway into the network.

To boost efficiency, manufacturers are merging IT and OT systems for real-time monitoring, predictive maintenance, and data-driven insights. However, this convergence reduces network segmentation and exposes legacy systems to IT-borne risks.

With a mix of vendor equipment and IIoT sensors, often deployed with inconsistent security controls and without central visibility, every new asset adds to an expanding attack surface.

1.3 Cyber Risks When IT and OT Meet

Modern manufacturing faces foundational security gaps. Legacy systems, flat networks, and third-party access all create serious vulnerabilities that require urgent attention.

Key Challenges:

- **Legacy OT systems:** These often run on obsolete software without basic security features. Shared credentials and weak identity management make them vulnerable to even basic intrusion techniques.
- **Flat network architecture:** With little or no segmentation, once attackers gain a foothold, they can move laterally and escalate privileges with ease.

- **IT-OT data convergence:** Integrating IT tools with OT systems introduces vulnerabilities not covered by traditional industrial protocols, leaving the convergence layer exposed.
- **Supply chain dependencies:** Manufacturers often rely on third-party software updates and remote access by vendors. Any breach in these partner systems can ripple into the manufacturer's environment.
- **Limited maintenance windows:** 24/7 operations make it hard to apply patches or upgrades, causing a backlog of unresolved vulnerabilities.

To mitigate these risks, organizations are now adopting virtual patching techniques and network segmentation strategies. Virtual patching, applied at the network level, blocks known exploits without requiring downtime. Segmentation limits lateral movement, containing threats to specific zones and enforcing least-privilege access, a key pillar of zero trust.

1.4 Balancing Digital Transformation and Cyber Resilience

Manufacturing's digital transformation brings benefits like automation, efficiency, and real-time data analysis, while also introducing new vulnerabilities. Embracing innovation securely means embedding cybersecurity into every step of the transformation, not layering it on afterwards.

Zero trust architecture is essential here. It assumes that every user, device, and connection is untrusted by default. Continuous verification, strong authentication, and fine-grained access controls ensure that only authorized activities occur, regardless of where the device or user resides.

A unified policy across IT, OT, and cloud environments reduces blind spots and supports secure tech integration. Identity-based access, segmentation, and virtual patching together build a resilient foundation that enables growth without added risk.

1.5 Proactive Cybersecurity for Operational Continuity

Reactive security is no longer sufficient. Real-time threat intelligence (TI) and proactive prevention are crucial for protecting manufacturing environments where even brief outages can cost millions.

Key Challenges:

- **Outdated Defenses:** Many manufacturers still rely on perimeter firewalls, basic intrusion detection, and manual log reviews, which can be easily bypassed by attackers.
- **Over-reliance on Detection and Response:** While important, these methods only react after a breach has occurred, leaving a critical gap in prevention.
- **Technological and Cultural Gaps:** Mid-sized manufacturers often lack advanced security tools and mature models. Without training and awareness, investments in secure architecture are less effective.
- **Alert Fatigue:** False positives overwhelm analysts, obscuring real threats and hindering effective response.

By shifting to proactive defenses and integrating automated prevention, manufacturers can reduce noise while increasing visibility into critical activities.

1.6 Tailoring NIST, ISO Frameworks for Manufacturing Realities

Frameworks like the NIST Cybersecurity Framework (CSF) and ISO/IEC 27001 offer

valuable guidance, but they originate from IT-centric models. In OT environments, these frameworks must be adapted to avoid unintentional disruption of physical processes. To tailor these frameworks for manufacturing, organizations should:

- Focus on zero trust principles tailored to industrial operations
- Use virtual patching and protocol filtering to mitigate risks without physical intervention
- Segment networks to isolate high-risk or legacy systems
- Implement role-based and time-bound access controls

These adaptations preserve the intent of the frameworks, covering risk management and continuous improvement, while aligning with the operational realities of the shop floor.

1.7 Cybersecurity as a Governance and Performance Driver

To justify investments, cybersecurity must be positioned as a strategic enabler. Security leaders should be involved in transformation initiatives from the outset, ensuring that protection is baked into the design rather than retrofitted later.

Governance models must connect cybersecurity to measurable business outcomes.

Metrics should go beyond technical performance and include indicators like:

- Reduction in alert fatigue through automation
- Improved audit readiness and compliance scores
- Faster onboarding and secure access for third-party vendors
- Shortened deployment cycles for new technologies

Key Takeaways from Chapter 1

- Traditional cybersecurity approaches are insufficient for today's digital and interconnected manufacturing environments.
- Manufacturers need to adopt modern, proactive security strategies to keep pace with evolving threats.
- Embedding zero trust principles, network segmentation, and virtual patching into daily operations reduces risk and enhances resilience.
- These security practices enable manufacturers to innovate safely without compromising system integrity.
- Cybersecurity is a critical business imperative, essential for protecting uptime, maintaining customer trust, and sustaining competitiveness in the digital manufacturing era.

The Manufacturing Shift to Industry 4.0

Authored by M. Yousuf Faisal, Securing Things Ltd.

2.1 The Foundations

Industry 3.0 marked a major leap in manufacturing through automation, with industries mastering the hierarchical, point-to-point integration of systems across the industrial automation stack, from PLCs and HMIs to SCADA, MES, ERP, and the cloud, as outlined in the ISA 95 Part 2 model. This approach also established a crucial separation between IT and OT, enhancing security. The advent of the Industrial Internet of Things (IIoT) then opened new possibilities for digitally transforming legacy manufacturing businesses into interconnected ecosystems.

This digital transformation shifted many manual or paper-based processes toward fully integrated digital workflows. Industry 4.0 builds on these foundations, focusing on the seamless digital integration and automation of business processes by leveraging industrial data generated during Industry 3.0, data that was previously underutilized, to create actionable insights for the business.

This chapter examines the practical challenges and cybersecurity priorities faced by manufacturers still operating in Industry 3.0 environments as well as those transitioning toward fully digital Industry 4.0 operations. Drawing from real-world experience across diverse manufacturing sectors, it offers a pragmatic approach to securing modern digital factories while ensuring security investments align with operational realities.

2.2 Industry 4.0 Integration: Implementing Hub and Spoke Networks

Manufacturers operating under Industry 3.0 principles relied on a hierarchical, point-to-point approach to connect and integrate systems across the automation stack. These were functional but became brittle, complex to integrate, costly to scale, and prone to data silos. Many digital transformation initiatives fail due to the wrong strategy, architecture, technology and partners.

Those that have succeeded in the transformation to the Industry 4.0 era used a new hub and spoke architecture concept, termed as Unified Namespace (UNS) and was developed by Walker Rynolds.

Key features include:

- IIoT protocol as an open architecture, lightweight, and using a report by exception
- Broker technology uses a publish-subscribe mechanism, with ISA 95 part 2 as the master data model (Enterprise, Site, Line, Area, Cell)
- Edge-driven architecture

UNS represents the architectural foundation of the digital factory, providing a single source of truth for all organizational data, enabling real-time communication between IT and OT systems. UNS streamlines data exchange by seamless integration of data from production lines to enterprise-level systems and eliminates rigid hierarchies.

This model provides the needed security and scalability, where everything is connected to everything. However, the UNS also demands new security strategies, as all devices and applications interact through a shared name-space. As a result, any compromise can cas-cade across the organization.

2.3 Key Challenges in Securing Industry 4.0

As factories move to Industry 4.0, the expand-ed attack surface, real-time data sharing, and interconnected systems create new vectors for cyber threats.

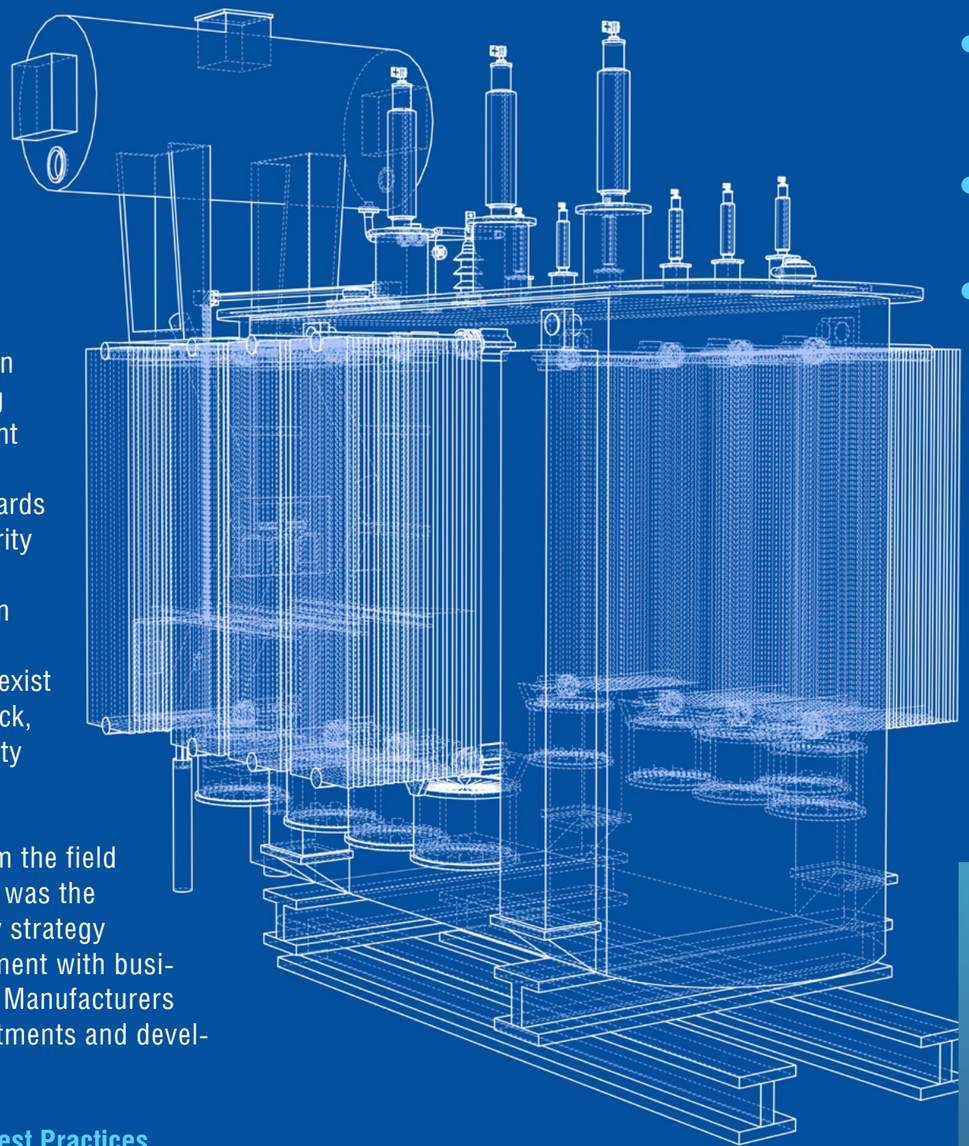
Key challenges:

- **New Attack vectors:** IIoT and edge devices, UNS, Industrial DataOps, cloud interfaces. Introduced new types of protocols, systems, applications, and hence new vulnerabilities, an addition from the industry 3.0 environment.
- **Network Architecture:** based on the new 4.0 event-driven architectures, adapting and ensuring secure network designs and segmentation of traffic.
- **Data Security & Governance:** security of industry 4.0 data throughout the data lifecycle and across all layers of the automation stack (both at rest and in motion). With more data accessible to more people across the organization, ensuring the integrity, confidentiality, and availability of production data is more complex.
- **Real-time operations:** The need for real-time decision-making means traditional security controls that introduce latency are no longer viable.
- **Legacy device integration:** Many factories are hybrid environments, with modern digital interfaces operating alongside legacy equipment that requires gateways to convert data to new standards and lacks embedded security capabilities.
- **Identity complexity:** Human and non-human identities (e.g., machines, sensors) exist across all layers of the stack, demanding rigorous identity and access management.

A recurring observation from the field in the manufacturing sector was the lack of a clear cybersecurity strategy and security program alignment with busi-ness and operational goals. Manufacturers struggled to prioritize investments and devel-op a cybersecurity strategy.

2.4 Recommendations and Best Practices

In Industry 4.0 environments, ultimately, the smart factory must be treated as an integrated system of systems, not a collection of isolated components. Cybersecurity can no longer be an afterthought and bolted on; it must be designed into every layer of the automation stack and therefore, securing the entire data lifecycle (from collection and normalization to analysis, visual-ization, and cloud integration).
Security architects and practitioners must:



- **Start with business context:** Understand manufacturing workflows, identify dependencies, and map business-critical assets and data flows.
- **Adopt a layered security approach:** Apply defense-in-depth principles at each layer of the automation stack, from edge sensors to cloud analytics platforms.
- **Design for resilience, not perfection:** Accept that complete prevention is unattainable, and progressively build focus on detection, containment, and recovery.
- **Embed security in project lifecycles:** Integrate security activities into OT project phases from planning to decommissioning.
- Secure the UNS ecosystem:
  - Ensure secure onboarding of devices into the UNS ecosystem
  - Enforce role-based access control and encryption for publish-subscribe inter-actions
  - Monitor node behavior for anomalies and enforce policies at the data level
- **Address IT dependencies:** Many OT systems rely on IT infrastructure, and neglecting these dependencies can result in production outages.
- **Build a collaborative culture:** Establish cross-functional teams spanning IT, OT, engineering, and cybersecurity. Align incentives and share ownership of outcomes.

Key Takeaways from Chapter 2

- Cybersecurity must evolve from static, perimeter-based defense to dynamic, system-wide resilience in response to the interconnected nature of Industry 4.0 environments.
- Universal principles like visibility, risk-informed prioritization, and in-tegrated architecture apply across both legacy sites and greenfield smart facilities.
- Aligning cybersecurity with operational realities and business objectives builds trust, enables innovation, and supports sustainable digital transformation.

Building Operational Resilience Amid IT-OT Convergence

Authored by Tim Chase, Manufacturing ISAC and Larry Grate, EOSYS Group

3.1 Introduction: Bridging IT and OT

In the rapidly evolving landscape of industrial digital transformation, the line between Information Technology (IT) and Operational Technology (OT) is increasingly blurred. Manufacturers are integrating enterprise platforms with control systems to streamline operations, enhance visibility, and boost responsiveness. But as IT-OT convergence deepens, so does the risk profile. Interdependencies that once seemed trivial are now critical points of vulnerability.

The most successful manufacturers today are not just those who adopt the latest technologies, but those who can operate through IT disruptions without bringing production to a halt. This chapter explores how organizations can build operational resilience by understanding IT-to-OT dependencies, planning for system degradation, and designing architectures that enable continuity even amid outages.

3.2 Understanding the Hidden Risks

The convergence of IT and OT systems introduces not only technical complexity but hidden operational risks that are often underestimated. These risks stem from a mix of overlooked dependencies, fragmented system knowledge, and an overreliance on upstream data sources.

Key Challenges:

- **Underestimated IT–OT dependencies:** Systems such as ERP (Enterprise Resource Planning), MES (Manufacturing Execution Systems), and inventory tracking platforms serve as lifelines for production operations. Yet many manufacturers treat these as IT domain concerns, unaware that a disruption in these systems can paralyze production lines.
- **Expanded attack surface through cloud adoption:** Migrating core enterprise tools to the cloud, especially ERP and supply chain platforms, brings efficiency, but also exposes critical workflows to network-based threats. These platforms often become high-value targets for ransomware and denial-of-service attacks.
- **Unseen interconnectivity and undocumented data flows:** Legacy systems with hard-coded integrations, third-party middleware, and one-off automation scripts create a web of dependencies that are not always captured in architecture diagrams or risk assessments. When a component fails or is compromised, these hidden links reveal themselves in the form of cascading failures.
- **Limited visibility and underinvestment in OT risk assessments:** Many organizations view comprehensive OT assessments as too costly or resource-intensive, especially in sectors with tight margins. This results in reactive, post-incident remediation rather than proactive resilience planning.

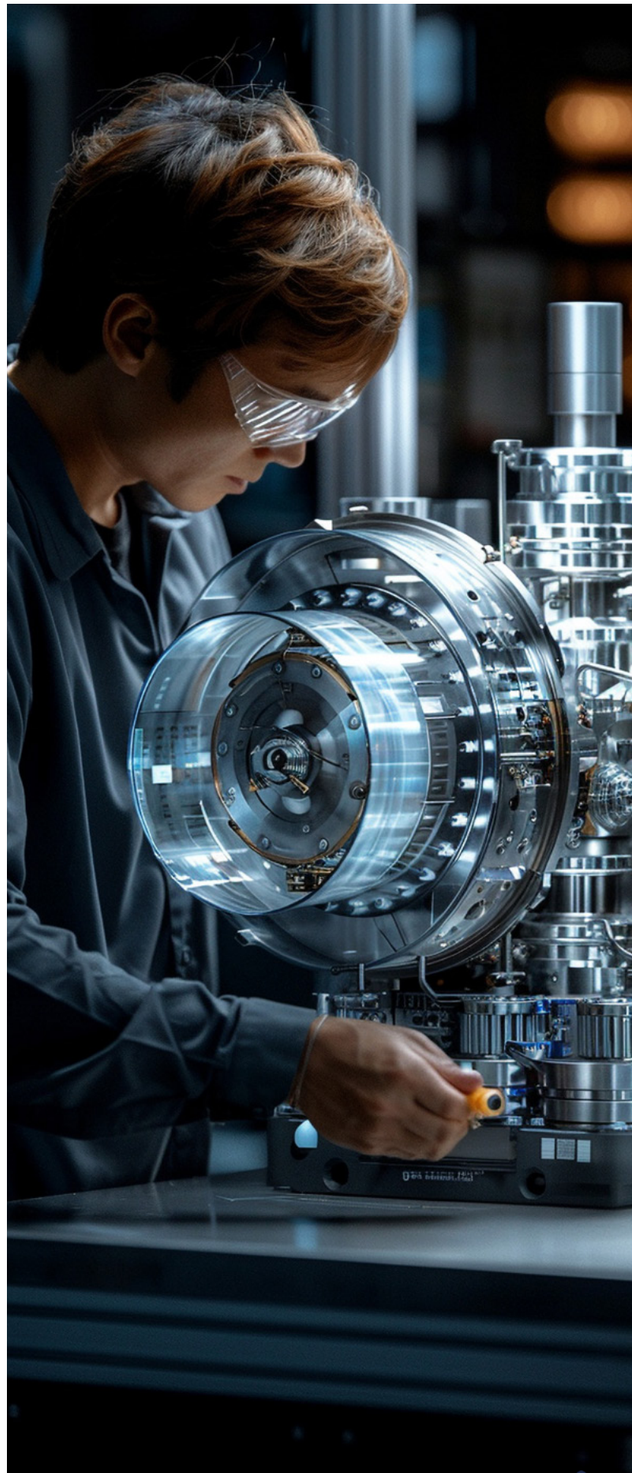
Overcoming these challenges demands a shift in mindset, from viewing cybersecurity as an IT issue to embedding resilience in every layer of the operational fabric.

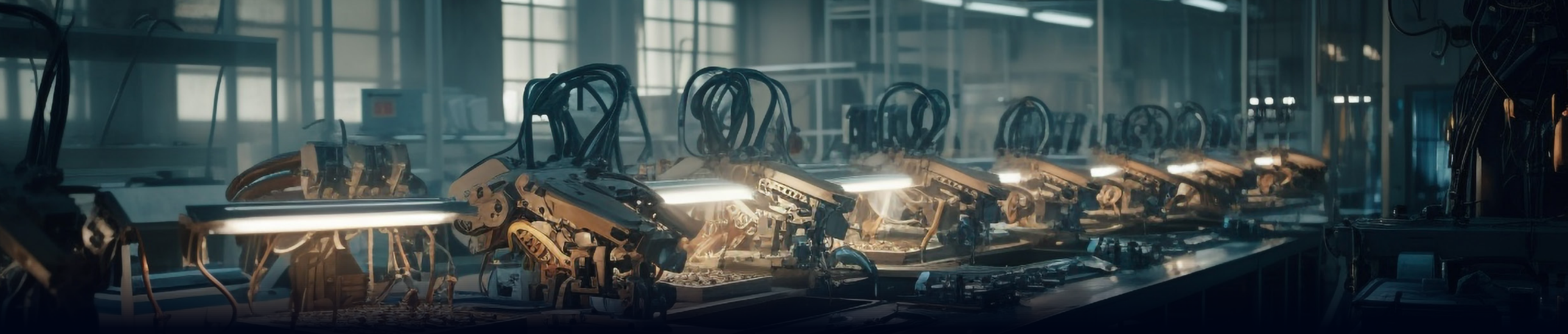
3.3 Real-World Lessons from the Field

Field data and incident disclosures consistently reveal a troubling pattern: production halts are increasingly tied to IT disruptions. These are not always the result of targeted attacks on OT networks. More often, the trigger is a compromised ERP instance, a failed authentication service, or a collapsed cloud-based workflow platform.

- For example, a global manufacturer suffered a two-day shutdown across three continents when a ransomware attack encrypted their SAP ERP system. Although the OT networks remained technically unaffected, production ground to a halt because operators could no longer receive job instructions, access inventory systems, or track outputs.

- **Why It Matters:** ERP systems serve as the nerve center of modern manufacturing. When they go down, OT teams lose critical context, what to produce, in what sequence, and using which materials. Without fallback mechanisms or manual workarounds, organizations are forced into precautionary shutdowns, sacrificing uptime for safety.





- **Insight:** Cloud-hosted platforms like MES are increasingly popular, especially in greenfield operations. But when internet connectivity fails or when cloud platforms experience outages, plant personnel may be left without access to production schedules, quality parameters, or historical performance data. Unless systems are architected with local caching or buffered data paths, even a short outage can spiral into hours of lost production.

In interviews with operations leaders, a common theme emerges: many organizations only discover the extent of their IT-OT dependencies during incidents.

A manager at a leading pharmaceutical manufacturer shared:

"We thought our OT network was isolated. Turns out three production steps relied on data from an ERP that went offline, and we didn't have a fallback."

These stories underscore a vital truth: you cannot protect what you do not understand, and you cannot maintain uptime if you are unaware of your dependencies.

3.4 Recommendations and Best Practices

Building resilience is not just about better firewalls or more sensors; it is about changing the way manufacturing systems are architected, managed, and tested. Manufacturers should:

1. Secure Executive Buy-In Early

Operational resilience must be framed as a business continuity priority, not just a technical one. This alignment helps justify investment in assessments, fallback mechanisms, and incident simulations. Executives are more likely to support proactive efforts when they understand the potential financial impact of unplanned downtime.

2. Conduct Cross-Functional Tabletop Exercises

Run simulation scenarios where ERP or MES platforms become unavailable. Include OT, IT, operations, and maintenance teams. These exercises often reveal undocumented dependencies and highlight gaps in emergency playbooks. One manufacturer discovered through tabletop planning that barcode scanners on the line relied on a cloud inventory service, a single point of failure.

3. Leverage Network Traffic Analysis and Monitoring Tools

Modern traffic analysis can uncover real-time data flows between IT and OT networks. Passive monitoring solutions help build an inventory of communications, revealing shadow integrations and undocumented linkages. Tools like industrial IDS (Intrusion Detection Systems) can also alert on abnormal IT-originating requests into OT zones.

4. Design for Disconnected Operation

Architect systems with isolation in mind. This includes:

- Local buffering of MES data to PLCs and HMIs
- Segmenting critical OT functions from internet or enterprise dependencies
- Enabling secure remote access through ZTNA or jump hosts
- Ensuring core production can continue using cached job orders and material lists

A large automotive supplier implemented a "degraded mode" for their stamping lines, allowing basic operations to continue for up to eight hours without ERP input.

Key Takeaways from Chapter 3

- IT and OT integration brings efficiency but also increases fragility. Failure in one domain can lead to disruption in the other.
- Organizations need full visibility into their digital ecosystem, including IT tools that indirectly support OT operations.
- Maintaining production, even in a degraded mode, requires proactive engineering and architectural planning.
- Tools are important, but cross-functional collaboration and shared awareness are essential to handle disruption effectively.
- Resilience must be embedded from the start when migrating to the cloud or implementing smart factory solutions.
- In a converged environment, resilience means adapting to disruption, managing interdependence, and maintaining control during uncertainty.

A Structured Approach to OT Disaster Recovery

Authored by Saltanat Mashirova, Honeywell

4.1 Introduction: Critical Approaches to Disaster Recovery in OT Cybersecurity

Disaster recovery in OT environments is an increasingly critical aspect of modern industrial cybersecurity. While much of the focus in cyber resilience planning has historically cantered on backup procedures and IT continuity, OT systems demand a more nuanced and robust approach. These systems underpin physical processes, and their disruption can result in data loss or downtime, as well as serious safety, operational, and economic consequences. This chapter outlines a practical, field-tested framework for OT disaster recovery in manufacturing environments. It consolidates lessons from complex OT deployments, real-world risk assessments, and multiple successful implementations across sectors such as oil and gas, LNG, and discrete manufacturing.

4.2 Key objectives of OT disaster recovery

The core objective of OT disaster recovery is not merely system restoration, but the swift reestablishment of safe and functional plant operations after a cyber incident.

Key goals include:

- Preparing personnel to respond effectively in a crisis
- Managing incidents to limit their spread and impact
- Reducing recovery time while maintaining safety and integrity
- Restoring mission-critical plant operations within an optimal recovery window.

Disaster recovery must be distinguished from related planning efforts. It exists within the broader structure of business continuity management (BCM), which also encompasses business continuity plans, emergency procedures, crisis communications, and IT contingency planning. Each element plays a distinct role, but only together do they provide comprehensive protection.

Key Metrics	Purpose
Maximum Tolerable Downtime (MTD)	The longest acceptable downtime before serious consequences occur
Recovery Time Objective (RTO)	Target time to restore operations
Recovery Point Objective (RPO)	Acceptable amount of data loss, based on backup timing

Phase	Description
Activation and Notification	Identify disaster, notify stakeholders, assess outages, activate response plan
Recovery Execution	Restore operations via backup access, system restoration, and failover processes
Reconstitution	Validate data integrity, system configuration, and ensure operational functionality

4.3 Phases of OT disaster recovery

OT disaster recovery is structured around three essential phases, each critical for ensuring operational continuity and safety. Alongside these phases, specific metrics guide recovery planning and validation to meet industrial requirements. *See tables below.*

These phases and metrics, grounded in rigorous risk assessments and practical testing, form the foundation for effective OT disaster recovery. Precise recovery planning is vital in high-stakes industrial settings, where even minutes of downtime can have major consequences.

4.4 Recognizing Disaster Scenarios and Triggers

Not every event constitutes a disaster. Disaster thresholds should be aligned with process safety escalation levels.
These range from:

- SD3 (normal operations)
- SD2 (localized incidents)
- SD1 (widespread but manageable disruptions)
- SD0 (true disaster scenarios)

SD0 involves situations where manual recovery is infeasible and downtime exceeds MTD. Examples include complete ransomware encryption, total network loss, or corrupted firmware on control systems.

4.5 Planning and Execution

A robust recovery plan must define roles and responsibilities, scenario-based strategies, and clear reconstitution procedures. Rather than focusing solely on systems, recovery should

prioritize function. Essential control functions such as DCS, SIS, and BPCS take precedence, followed by systems that coordinate production (like MES) and supportive infrastructure such as voice networks and historians.

Mapping dependencies is critical. Some systems must be restored in a specific sequence; for example, a domain controller may be required before a batch server can operate. Others have co-dependencies or rely on shared network resources. These interrelationships must be clearly understood and incorporated into recovery planning.

OT recovery can follow the "Black Start" approach from process safety, where systems are methodically brought back online in a validated sequence:

Power and Core Networking: Restore foundational infrastructure first to enable connectivity.
Control System Servers, HMIs, Historians, and Controllers: Bring back critical control components next.
Prioritization Based on Functional Map and Dependency Analysis: Follow a carefully planned order reflecting system interdependencies and operational priorities.

This structured sequencing helps ensure safe, reliable recovery without risking cascading failures.

4.6 Reconstitution and Post-recovery Validation

Reconstitution goes beyond restoration. It involves validating that all control systems, safety instrumented systems, and support tools are configured correctly and functioning as intended. This includes alarm settings, automation status, logging functionality, and credential management. Close collaboration between cybersecurity and operations teams is essential to confirm a safe and reliable restart.

4.7 Looking ahead: Focused on automation and AI

AI can support OT disaster recovery by streamlining workflows and improving readiness without replacing human oversight. It can automate routine tasks like documentation and configuration checks, map system dependencies more effectively, and provide real-time insights to guide recovery efforts. AI tools may also simulate scenarios to improve planning and help prioritize recovery actions. However, in safety-critical environments, human judgment remains essential. AI should enhance, not replace, the expertise of recovery teams.

Key Takeaways from Chapter 4

- OT disaster recovery requires a tailored approach focused on restoring safe, functional plant operations, beyond just IT backup plans.
- It is part of broader business continuity management, including emergency procedures and crisis communications.
- Recovery occurs in three phases: activation and notification, recovery execution, and reconstitution with validation.
- Planning relies on key metrics: maximum tolerable downtime (MTD), recovery time objective (RTO), and recovery point objective (RPO).
- Disaster thresholds align with process safety levels, distinguishing between normal operations, incidents, and true disasters.
- Recovery plans prioritize function over systems and clearly map system dependencies and interrelationships.
- The "Black Start" approach restores power and networking first, followed by critical control components in sequence.
- Post-recovery validation ensures all control and safety systems are correctly configured and operational.
- Automation and AI may assist recovery workflows but human oversight remains essential for safety.

Securing the Future of Manufacturing

Authored by Xage Security

5.1 Emerging Trends

As manufacturing embraces digital transformation, the cybersecurity landscape is shifting. New technologies such as artificial intelligence (AI), machine learning (ML), automation, adaptive architectures, and advanced detection tools are driving a proactive, intelligence-led approach to defending industrial environments.

This chapter will explore these emerging trends and their role in helping manufacturers shift from reacting to anticipating threats, especially quantum-enabled cyberattacks.

5.2 Smarter Security with AI and ML

AI and ML are enabling manufacturers to shift from reactive to predictive cybersecurity.

Key Advantages:

- **Real-Time Analysis:** Analyze massive volumes of operational and network data in real-time.
- **Anomaly Detection:** Detect subtle behavioral anomalies that human analysts might miss.
- **Threat Prediction:** Predict likely threat vectors based on emerging patterns.
- **Automated Response:** Automate threat containment decisions to minimize human response time.

Predictive cybersecurity is especially critical for environments with minimal tolerance for downtime.

Ransomware, for example, can escalate faster than human-led processes can respond. AI-driven systems bring adaptability to cybersecurity by enforcing dynamic access control.

Rather than relying on static rules, they continuously monitor behavior, risk, and context to adjust access permissions. Suspicious activity may trigger multi-factor reauthentication or immediate access revocation, all while minimizing disruption to operations.

AI's strength lies in its ability to support zero trust principles, evaluating users not only by identity or role, but by behavior and emerging risk indicators. This reduces the potential for insider threats, credential misuse, and lateral movement, while still maintaining operational efficiency.

Remember: Manufacturers should maintain a human-in-the-loop model in safety-critical situations to preserve oversight where automation may fall short.

5.3 Evolving Detection Tools for Industrial Realities

While advanced detection platforms like Extended Detection and Response (XDR) are common in IT, applying them effectively in OT environments is not straightforward. Visibility in manufacturing is often constrained, and telemetry from industrial devices is non-standard or incomplete.

To succeed, detection systems must integrate across IT, OT, and cloud layers without disrupting critical operations. They should ingest telemetry from industrial protocols like Modbus, DNP3, and OPC-UA, and interpret behaviors from PLCs, HMIs, and SCADA systems. Automated response actions must be context-aware and risk-prioritized to avoid triggering unnecessary shutdowns or alert fatigue.

A key enabler here is intelligent baselining. AI and ML can identify what 'normal' looks like for machines and processes, allowing anomalies to be flagged with greater precision. Coupled with least-privilege communication policies and zero trust segmentation, these strategies reduce the number of events that need to be analyzed, making alerts more relevant and manageable for security teams.

5.4 Adaptive Security Architectures for the Connected Future

The increasing convergence of IT, OT, and cloud requires more than traditional security controls. Static defenses must give way to adaptive security architectures that evolve alongside the threat landscape. In these architectures, telemetry, access control, and response policies are continuously informed by risk signals, behavior, and business context.

Key Elements:

- **Centralized Data Collection:** Centralizing logs and behavioral data from across environments is foundational. AI and analytics tools use this data to detect threats and adjust access policies in real time.
- **Context-Aware Access Control:** Adaptive systems go beyond role- or location-based permissions by considering device behavior, time of access, and current threat conditions to determine connection eligibility.
- **Dynamic Segmentation:** Unusual user or device behavior triggers isolation or communication restrictions to prevent lateral movement and reduce disruption.
- **Virtual Patching:** Rules block exploit attempts without requiring system downtime, enhancing resilience while maintaining uptime.
- **Automated Credential Management:** Adaptive architectures enable automatic credential rotation and policy enforcement, reducing manual effort and closing attack vectors.

The ultimate goal is to create a self-securing environment, rather than relying on human intervention for every decision. This prevention-first approach supports both operational integrity and cybersecurity maturity.

5.5 Defending Automation and Control Logic

As manufacturers automate more processes and deploy intelligent machinery, the integrity of control logic becomes a prime target. Threat actors, both external and internal, may seek to alter logic to disrupt operations, sabotage product quality, or cause physical damage.

To reduce damage, manufacturers should implement:

- **Adopt Zero Trust Access Models:** Implement time-bound, tightly scoped access with continuous, real-time monitoring of user behavior and command sequences.
- **Leverage Behavioral Analytics and Automated Containment:** Automatically contain devices or users that act outside expected parameters, such as unusual access times or anomalous commands.
- **Implement Secure Kill Switches:** Enable systems to be isolated or reverted to known-safe states swiftly in case of compromise.
- **Monitor Performance Metrics for Sabotage:** Track system performance to detect subtle signs of sabotage, like degraded quality or accelerated equipment wear, even without traditional alarms.
- **Maintain Immutable, Cryptographically Signed Logs:** Record all access, commands, and changes securely to support real-time forensics and ensure long-term compliance.

Step	Action	Description
1	Assess and Upgrade Cryptography	Evaluate current encryption (TLS, VPNs, software signing) and migrate to post-quantum cryptographic standards.
2	Secure Key Management	Replace centralized key vaults with distributed vaulting to avoid single points of failure in key storage.
3	Strengthen Defense-in-Depth	Implement strong segmentation, identity-based controls, and encryption-in-use to limit data exposure.
4	Implement Quantum-Resilient Audit Logs	Use tamper-proof, cryptographically protected logs stored in quantum-resilient repositories for long-term integrity and tamper detection.

5.6 Preparing for the Quantum-enabled World

Quantum computing may still be on the horizon, but threat actors are already preparing. Nation-states and advanced adversaries are stockpiling encrypted data today with the expectation that they will decrypt it tomorrow.

Manufacturers, especially those in defense, aerospace, and energy, must begin preparing now. The table on the left demonstrates some steps to prepare manufacturing environments for the challenges posed by quantum-enabled cyber threats.

Key Takeaways from Chapter 5

- Securing the future of manufacturing requires moving beyond traditional defenses to more adaptive, intelligent security architectures.
- AI-driven detection and behavioral analytics are essential for identifying and responding to subtle, emerging threats in real time.
- Quantum-resilient encryption is a critical investment to protect sensitive data against future quantum-enabled cyberattacks.
- Embracing these advanced strategies today ensures operational integrity, safety, and resilience in a rapidly evolving cyber threat landscape.

Advancing OT and IoT Maturity to Defend Manufacturing from the Edge In

Authored by Byos

6.1 Defending Manufacturing from the Edge Inwards

With OT (operational technology) and IoT networks at the heart of manufacturing environments, these Internet-connected devices bring their own set of cybersecurity risks and dangers. As threats become increasingly sophisticated, manufacturers need to move beyond simple monitoring and take action to enhance visibility and control.

This chapter provides actionable advice on enhancing OT/IoT security maturity using network segmentation, vulnerability scanning, zero trust deployment, and readiness of the workforce. The aim is to assist organizations in observing more and responding quicker and more intelligently to protect critical infrastructure.

6.2 Edge Microsegmentation Means Flexibility

Effective segmentation in OT can be achieved without impacting uptime. Microsegmentation at the edge, close to devices, uses plug-and-play tools to isolate systems without changing existing infrastructure. Unlike rigid IT methods, this places policies near individual endpoints, ensuring critical systems stay isolated while allowing necessary communications, preserving performance.

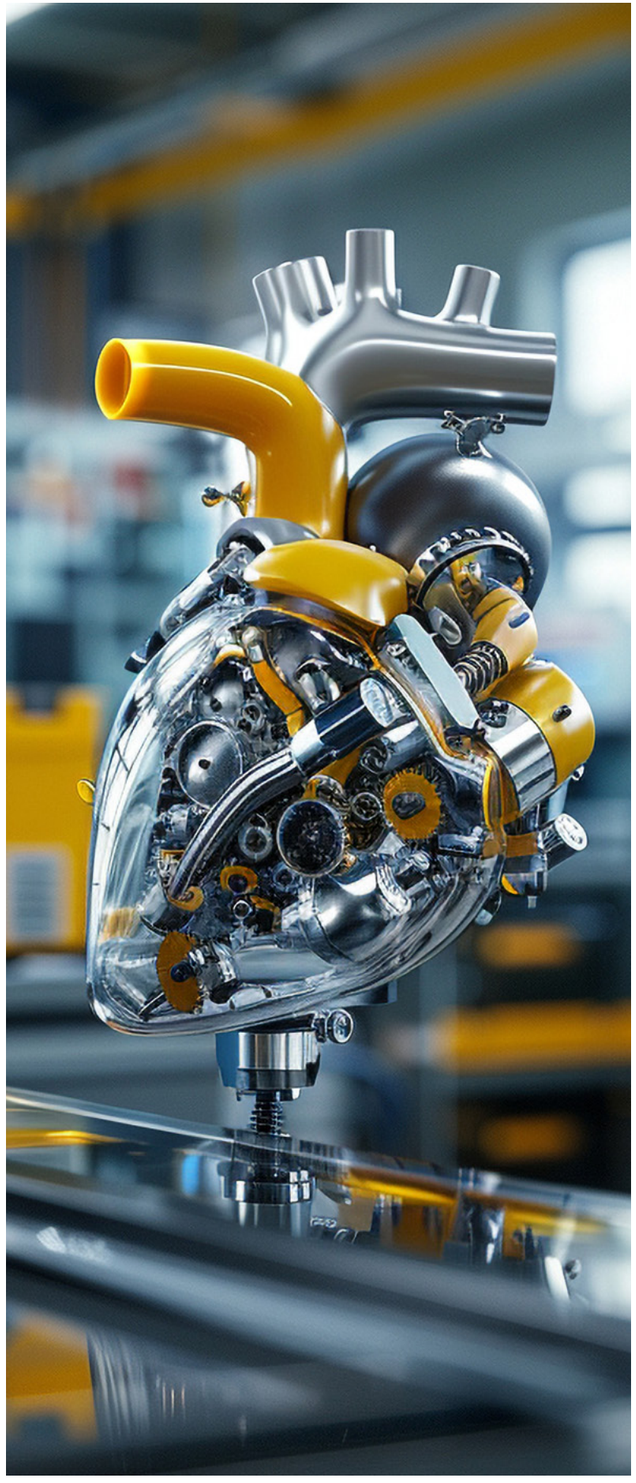
Separating segmentation from the network infrastructure through secure overlays or software-defined networking simplifies implementation and reduces complexity. Insight: Manufacturers should begin by segmenting high-value or legacy assets lacking embedded security, minimizing attack surfaces while maintaining continuity.

Edge microsegmentation also increases manufacturing flexibility, enabling quick, secure network reconfiguration to meet changing production demands. This ensures security evolves alongside operational needs without sacrificing efficiency.

Additionally, it supports secure wireless connectivity for industrial devices, allowing more flexible and scalable networks without extra cabling, simplifying device deployment in OT environments.

6.3 OT Asset Visibility Begins with Passive Discovery

Risk-based OT vulnerability assessments should account for technical flaws and operational context. Passive monitoring tools are preferred to avoid disrupting sensitive systems. By combining passive asset discovery with contextual risk scoring, based on device criticality, known issues, and exposure, teams can maintain updated inventories and prioritize remediation effectively.



Visibility into asset behavior is foundational for effective vulnerability assessments. Passive network discovery tools that map services and ports on devices, especially legacy systems, can help organizations identify potential exposure without disrupting operations.

These tools complement vulnerability management platforms by adding enforcement layers that prevent unauthorized access to critical assets. Prioritizing assets with known exposure and limited patchability ensures assessments remain risk-driven and focused on the most vulnerable points in the environment. Furthermore, involving cross-functional teams across IT, OT, and engineering environments ensures that vulnerability data is interpreted with operational implications in mind.

6.4 Protect OT Systems with Layered Zero Trust Controls

Zero trust security can strengthen OT environments by applying policies that are context-aware and minimally disruptive. Rather than relying solely on perimeter controls, manufacturers can adopt a more granular, phased approach that maintains operational continuity while enhancing security.

Key Elements:

- **Proximity of Enforcement:** Apply policies close to devices or applications through secure gateways or protocol-layer agents.

- **Context-Aware Authorization:** Authenticate and authorize traffic based on port, protocol, device identity, and operational context.
- **Phased Implementation:** Start with visibility-only policies to monitor normal traffic patterns before gradually enforcing rules.
- **Protocol-Specific Policies:** Tailor policies to the predictable, deterministic nature of industrial communications with fixed endpoints and protocols.
- **Layered Controls:** Begin with encrypted connections, then implement zone routing and port-level allow lists to enforce least-privilege access.
- **Legacy Device Support:** Restrict communications only to approved paths to ensure legacy devices run without interruption.
- **Edge Enforcement:** Enforce zero trust at the network edge, supporting legacy protocols and minimizing latency to maintain security and operational continuity.

By adopting a thoughtful, phased zero trust approach tailored to OT environments, manufacturers can significantly reduce risk without disrupting critical operations.

6.5 Secure OT by Enforcing at Device First

Zero trust enforcement in OT works best across multiple layers. The table below shows key tiers and how each helps balance security with operational needs. *See table below.*

Enforcement Tier	Description	Key Benefits	Considerations
Device Level	Enforcement begins at the device, focusing on high-value or high-risk assets like PLCs, HMIs, and legacy systems without built-in security.	Prevents lateral movement and limits breach blast radius	Critical for protecting vulnerable devices directly
Subnet Level	Applies segmentation to groups of devices organized by function or zone, using layer 2-4 controls that are protocol-agnostic.	Contains threats within subnets, requires no full re-architecture	Practical, balances security with operational continuity
Application Layer	Finer-grained control at the application or protocol level, typically where legacy constraints and protocol diversity allow.	Enables detailed security controls	Often challenging in OT; best applied in mature environments

6.6 Build OT Readiness with Scenario-based Training

Workforce training should be grounded in real-world scenarios that reflect specific devices, protocols, and workflows present in an organization's environment. Rather than generic cybersecurity awareness modules, training should:

- Include simulated incident response exercises involving OT systems
- Hands-on labs using digital twins or emulated ICS environments
- Cross-training between IT and OT personnel to build shared understanding

Scenario-based training, such as ransomware targeting an HMI or unauthorized PLC reconfiguration, helps staff recognize anomalies and respond appropriately. Training must be ongoing and updated regularly to reflect emerging threats and lessons learned from industry incidents.

6.7 Predictive Detection Requires Smarter Visibility

Mature visibility is defined by the ability to:

- Continuously discover and classify all OT and IoT assets on the network
- Map communication patterns and baseline normal behavior
- Correlate anomalous activity with threat intelligence and contextual data
- Track policy compliance and segmentation integrity in real time
- Enable cross-domain visibility across IT and OT networks

Transitioning to predictive detection requires the integration of machine learning-based analytics, which can detect subtle deviations from established baselines. This includes anomaly detection at the protocol and device behavior level. Pairing this with contextual threat intelligence helps prioritize alerts and guide proactive responses.

Insight: Manufacturers should invest in unified monitoring platforms that bridge IT and OT, and use architectural designs that enable security observability without relying solely on traditional inline appliances.

Key Takeaways from Chapter 6

- Establishing mature OT/IoT visibility requires continuous effort, ongoing investment, and a clear strategy.
- Inter-functional cooperation is essential to maintain effective visibility and security.
- Prioritizing network segmentation helps contain threats and protect critical assets.
- Regular vulnerability assessments identify and address emerging risks promptly.
- Strong access controls reduce the likelihood of unauthorized system access.
- Empowering the workforce with training and awareness strengthens overall resilience.

Together, these steps build a resilient, future-proof manufacturing environment.

Embedding Security into ICS by Design

Authored by Paul Veeneman, Securisect

7.1 Introduction: From Integration to Resilience

As industrial systems become increasingly interconnected, the challenge of securing OT environments grows more complex. Integrating IT and OT environments has introduced operational efficiencies, but added cyber risks that threaten safety, productivity, and reliability. In this landscape, cyber resilience must be built into the design of systems, not as an added afterthought.

Security-by-design is the principle of embedding cybersecurity considerations into every phase of system architecture, implementation, and operation. This chapter explores practical approaches to implementing resilience by design within manufacturing and industrial control system (ICS) environments.

7.2 Barriers to Effective OT Security

Securing OT environments presents unique challenges that differ from traditional IT security. Manufacturers face obstacles ranging from incomplete asset visibility to organizational silos and resource limitations. Understanding these key challenges is essential for developing effective, resilient cybersecurity strategies in industrial settings.

Key Challenges:

- **Incomplete Asset Visibility:** Many organizations lack a comprehensive asset inventory, making it difficult to classify systems, monitor behavior, or assess vulnerabilities. This blind spot undermines downstream security processes and operational integrity. Comprehensive asset visibility is essential for detecting anomalies, responding to incidents, and meeting regulatory compliance.
- **Siloed Organizational Structures:** Cybersecurity responsibilities are often split between IT, OT, engineering, and operations teams. These silos slow coordinated responses, delay decisions, and lead to inconsistent security controls. Site-level autonomy can further fragment security postures, even in large organizations.
- **Static Architectures in Dynamic Environments:** Industrial systems often use static IPs, hard-coded protocols, and outdated control logic. While operationally simple, these configurations expose systems to persistent reconnaissance and exploitation through publicly available intelligence tools.
- **Budget and Resource Constraints:** Many manufacturing facilities, especially small to mid-sized, have limited cybersecurity budgets. This restricts the adoption of enterprise-grade monitoring tools, leaving critical systems vulnerable to threats that more mature security programs would detect.

7.3 Lessons from the Field

Improving visibility is a critical step toward securing industrial environments. Cost-effective and scalable monitoring solutions help manufacturers detect risks early, gain better control over network activity, and strengthen their defenses without disrupting operations.

Key Elements:

- **Lightweight monitoring stack:** Use open-source tools like Zeek, Elasticsearch, and Kibana on low-cost, energy-efficient hardware.
- **Integration method:** Deploy via switch mirror (SPAN) ports to gain deep network visibility without adding latency or disrupting systems.
- **Scalability and flexibility:** This model scales easily and serves as a secondary source of truth for asset validation and anomaly detection.
- **Traffic pattern analysis:** Centralized dashboards visualize network traffic to spot unauthorized protocols, communications, and early compromise indicators.
- **External monitoring:** Deploy nodes outside the firewall to simulate an attacker's perspective, revealing external scanning activity and threat exposure.
- **Threat pattern identification:** Detect persistent scans from specific geographies or automated adversaries, improving threat intelligence.

By implementing these cost-effective monitoring strategies, manufacturers can enhance network transparency and proactively identify vulnerabilities, key steps toward resilient and secure industrial operations.

7.4 Recommendations and Best Practices

To build robust OT security, organizations must adopt a proactive and layered approach that addresses both technology and operational challenges. The following key actions provide a practical roadmap for reducing risk and enhancing resilience in complex industrial environments.

1. Maintain a dynamic asset inventory: Accurate asset identification is the foundation of effective security. Use both passive and active discovery methods to build and continuously update a living inventory. Track device classifications, firmware versions, communication patterns, and lifecycle data. Combine open-source tools with commercial platforms to ensure comprehensive and redundant asset intelligence.

2. Reduce the value of single points of failure: Design resilient systems that can absorb disruptions. Identify mission-critical functions and remove dependencies on single components. Implement redundancy where possible, such as backup power supplies, failover communication paths, and replicated control logic. This limits operational impact and enhances recovery capabilities.

3. Implement automated moving target defense: Static IP addresses are vulnerable to tracking and scanning. Regularly rotate public IP addresses to disrupt attacker reconnaissance. Use DHCP with scheduled renewals and programmable UPS-controlled modem restarts. This approach has shown to reduce external scanning by over 90% and nearly eliminate visibility on platforms like Shodan and Censys.

4. Design with the adversary in mind: Attackers exploit predictable systems. Disable unnecessary services and ports, remove unused protocols, and enforce strict least-privilege access. Review all communication paths with operational questions: Is this necessary? Can it be segmented? Is this system unnecessarily exposed?

5. Monitor proactively and reactively: Effective security combines pre-incident intelligence with post-incident response. Deploy monitoring across internal, external, and edge layers to detect deviations from normal behavior. Use dashboards to identify anomalous traffic, unauthorized devices, and unusual protocol use. Integrate these insights into incident response workflows to reduce detection and response times.

Together, these measures enable manufacturers to create resilient, adaptive OT environments that reduce vulnerabilities, limit attack impact, and support continuous operational integrity.

Key Takeaways from Chapter 7

- Building resilience in industrial systems requires rethinking traditional assumptions about connectivity, control, and security to meet modern threats.
- Organizations must move beyond reactive defenses and adopt a proactive, security-by-design approach that integrates continuous visibility, segmentation, and unpredictability into their environments.
- Security-by-design is not a one-time project but an ongoing process of evaluating systems, understanding adversary tactics, and adapting controls to emerging risks.
- Practical strategies such as deploying low-cost network monitoring solutions, rotating IP addresses to reduce attack surfaces, and minimizing the value of exposed assets make industrial resilience both achievable and cost-effective.
- These proactive measures force attackers to repeatedly reset and reevaluate their approaches, slowing their progress and reducing the risk of successful breaches.
- Ultimately, resilience by design empowers organizations to maintain operational continuity, protect critical assets, and stay ahead in an increasingly complex and dynamic cyber threat landscape.

Manufacturing Resilience Begins with Proactive Strategies

Authored by Salvador Technologies

8.1 Proactive Strategies Must Go Beyond Response Plans

Growing connectivity within manufacturing environments increasingly results in exposure to various cyber threats and attacks that can lead to a detrimental effect on organizational operations and safety. Developing organization-wide incident response and recovery plans is no longer a luxury; it has become a business and risk imperative that enhances incident preparedness and drives operational continuity.

This chapter explores how organizations can enhance preparedness, incorporate real-time monitoring, and collaborate with external cybersecurity agencies to reduce downtime and effects. When it comes to building a resilient system, organizations must adopt advanced scenario planning and simulation exercises to facilitate quick and enable decision-making when it counts most.

8.2 Building Cyber Resilience Takes More than a Playbook

Manufacturers can no longer afford to rely on outdated or fragmented response protocols. In an environment where a single ransomware incident can freeze production, put employees at risk, and cause long-term financial damage and compliance related risks, a reactive stance falls short.

To build true readiness, organizations should prioritize:

- Real-time monitoring to detect abnormal activity, flag unauthorized access, and identify system failures before they escalate
- Clear internal protocols with defined roles, escalation paths, and communication strategies that activate immediately during an incident
- Cross-functional involvement across IT, OT, operations, and executive teams to ensure alignment and speed in response
- External collaboration with cybersecurity agencies and industry bodies that provide threat intelligence, incident support, and recovery resources
- Routine simulation exercises to stress-test plans, identify weak spots, and build the muscle memory needed to respond quickly under pressure

These simulation exercises should go beyond theoretical tabletop drills. They need to reflect real-world scenarios, challenge assumptions, and expose gaps that may otherwise remain hidden. The goal is not to check a compliance box, but to transform incident response from a static plan into a tested, adaptable capability. This will also bring out organizational weaknesses before they are exploited by adversarial hackers.

Resilience is not a one-time achievement. It is a continuous process that demands commitment, coordination, and constant refinement.
Those who invest in it today will be far better positioned to recover tomorrow.

8.3 Real-time Recovery as a Standard, Not a Backup Plan

Manufacturing organizations must adopt a layered approach with the assumption that cybersecurity breaches are inevitable and build layers of defense accordingly. This means segmenting critical OT networks, implementing zero-trust policies, maintaining IT and OT assets comprehensive visibility, and ensuring there is a real-time recovery solutions or tools for quick recovery to ensure operational continuity.

As for responsibility, it is broader than just the CISO. While the CISO should spearhead cybersecurity strategies, true resilience requires cross-functional collaboration across plant managers, site managers, IT, OT, operations, engineering, finance, and human resources. The leadership team needs to understand and prioritize resilience as a fundamental part of risk management, business and operational continuity planning.

8.4 Manufacturers Strengthen Defense Through Shared Response

Collaboration is essential in the OT cybersecurity landscape, especially across manufacturing environments, where supply chains are deeply interconnected. Manufacturers should proactively build relationships with public agencies like CISA or local CERTs and participate in industry-specific Information Sharing and Analysis Centers. These organizations offer critical threat intelligence, joint exercises, and coordinated response protocols that strengthen awareness and resilience.

Practically, collaboration means more than just information sharing. It involves aligning incident response playbooks, defining roles in joint response scenarios, and setting up secure communication channels in advance. Including supply chain partners in tabletop exercises has proven beneficial in enabling coordinated, end-to-end response and synchronized recovery.

Backup and recovery play a unique role in this ecosystem. By ensuring all parties and roles can easily restore systems rapidly and securely utilizing OT specific tools or platforms, manufacturers create a shared baseline of resilience.

8.5 OT Security Rises with Realistic Attack Scenarios

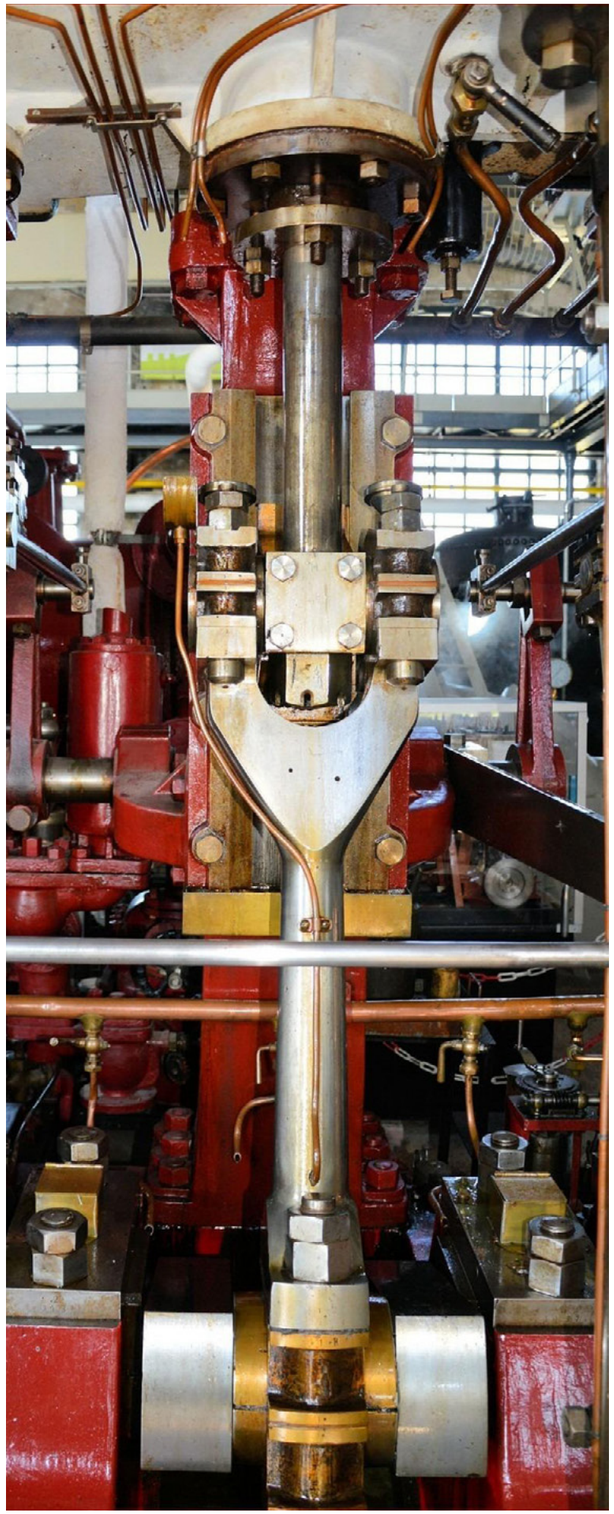
Manufacturing environments, with their mix of legacy systems and real-time operations, are especially vulnerable to ransomware and cyber threats. Running simulations is a proactive way to uncover weaknesses before a real attack strikes.

Key benefits of simulation exercises:

- **Reveal technical and procedural gaps:** Simulations help identify vulnerabilities in both systems and workflows that may not be obvious during routine operations.
- **Strengthen incident response:** Exercises clarify team roles, communication channels, and escalation paths, such as who to contact and in what order during a crisis.
- **Measure response speed:** Simulations help determine how long it takes to isolate compromised segments and activate backup systems.
- **Validate full recovery lifecycle:** They ensure backup integrity, data can be restored promptly, and normal operations can rapidly resume without knock-on disruptions.

8.6 Cyber Resilience Requires Precision

While RTO (Recovery Time Objective) and RPO (Recovery Point Objective) originated in IT, they are just as critical, if not more so, in OT cybersecurity. In industrial settings, these metrics must reflect not only data loss but also physical safety, operational continuity, and environmental risk.



Key Adjustments for OT Contexts:

- **RTO (Recovery Time Objective):**
  - IT focus: Time to resume system access
  - OT focus: Time to restore safe and stable operations
  - Example: On an oil rig, RTO must be measured in minutes to prevent pressure build-up or environmental harm.
- **RPO (Recovery Point Objective):**
  - IT focus: Amount of data loss acceptable
  - OT focus: Precision of state restoration in control systems
  - Consideration: Control systems must resume with consistency, timing and state misalignments can be dangerous.

In OT, recovery is not just about speed, it is about restoring safely, with precision, and without endangering people or the environment. Traditional IT metrics must be reinterpreted through the lens of physical risk.

Key Takeaways from Chapter 8

- Cyber resilience is now a core operational necessity, not just a technical concern.
- Organizations must evolve from static, reactive plans to proactive, tested strategies and industry specific tools.
- True resilience relies on coordinated action across teams and functions.
- Recovery processes and platforms should be regularly tested and used, not just reserved for times of crisis.
- Leadership must treat cyber risk as business risk, aligning cybersecurity with operational priorities.
- The most resilient manufacturers will be those who prioritize preparedness, precision, and collaboration ahead of time.

7 Steps to Strengthen OT Cybersecurity in Manufacturing

Authored by Chris McLaughlin, CISO, Johns Manville

9.1 Introduction: From Visibility to Resilience in OT Security

In the evolving industrial landscape, cybersecurity in OT environments has become a foundational element of business continuity and safety. As manufacturers increasingly converge IT and OT systems, cyber threats that once targeted enterprise networks now reach deep into production environments, threatening uptime, safety, and operational integrity.

While many organizations have deployed basic security tools, few have implemented a coherent, sustainable OT cybersecurity program. This chapter introduces a practical, experience, based seven, step approach to building and maturing an OT cybersecurity program. The framework supports organizations at any stage of maturity, helping align cybersecurity with operational priorities and business risk.

9.2 Key Objectives of an OT Cybersecurity Program

A mature OT cybersecurity program should extend beyond compliance or technical control. It must ensure operational resilience and foster cross-functional coordination across engineering, IT, and executive teams.

Key objectives include:

- Elevating cybersecurity as a core business risk, not solely a technical issue.
- Building a bridge between IT and OT disciplines to overcome cultural and knowledge gaps.
- Prioritizing protection based on process criticality and safety impact.
- Establishing clear governance frameworks aligned with standards like ISA/IEC 62443.
- Embedding cybersecurity in daily operations and decision-making.

This structured approach emphasizes security as an enabler of safe, reliable, and sustainable industrial performance.

9.3 The 7 Steps to Sustainable OT Cybersecurity

Cybersecurity in manufacturing works best when it is treated as a business issue, not just an IT task. The steps below offer a practical approach to building security into operations from the ground up.

Step 1: Reframe Cybersecurity as a Business Issue

The first step is acknowledging that cybersecurity is a business risk, not just an IT concern. Many manufacturers overlook the

operational consequences of cyber incidents until they experience one. Tabletop exercises can help illustrate these risks and secure stakeholder alignment.

Engage leadership from engineering, operations, safety, property risk, and executive management in these exercises. Simulating scenarios like ransomware, induced downtime fosters a shared understanding of financial, operational, and reputational impacts, building momentum for investment and change.

Step 2: Appoint an OT, IT Translator

Progress often stalls when IT and OT teams operate in silos. Bridging this divide requires a translator, someone who understands both domains and can facilitate collaboration. Many organizations recruit internally, selecting engineers or technicians with shopfloor credibility and providing them with cybersecurity training through ISA/IEC 62443 certification or CISA's ICS programs. Where internal resources are lacking, consider hiring a controls engineer with IT experience. The translator helps align priorities and ensures both teams speak a common language.

Step 3: Understand Critical Business and OT Processes

Effective cybersecurity planning begins with understanding how production actually works. What products are made? What processes are essential? What systems are most vulnerable to disruption?

This requires engagement with plant managers, control room operators, and maintenance teams. By walking the floor and mapping key workflows, security leaders can prioritize protections based on operational importance, rather than simply reacting to asset counts or technology stacks.

Step 4: Inventory and Assess Assets

Once business processes are understood, turn to asset inventory and risk assessment. The focus should be on:

- Identifying internet facing or remotely accessible control systems.
- Mapping data flows between enterprise and industrial networks.
- Categorizing assets by function, criticality, and connectivity.

Use the ISA/IEC 62443 concept of zones and conduits to structure defenses. Zones represent segments of the network grouped by risk, while conduits define controlled communications between them. Avoid high-risk flat networks by designing segmented architectures that limit lateral movement and contain potential breaches.

Step 5: Add IT Value to OT Operations

IT teams can build trust and drive adoption by delivering operational value. This may include identifying and addressing network issues, assisting with backup planning, or advocating for the replacement of obsolete systems.

Collaborating in project design phases ensures new systems are built with cybersecurity in mind. Engineers often appreciate this support, especially as environments grow more complex with virtual machines, remote access requirements, and hybrid control platforms.

Step 6: Make It Real with Tabletop Exercises

Once visibility and trust are established, revisit tabletop exercises with greater operational context. Scenarios should reflect actual plant configurations and incorporate known vulnerabilities or backup limitations.

Use the CIAS model, Confidentiality, Integrity, Availability, and Safety, to frame discussions.

Test isolation strategies, failover procedures, and manual workarounds.

Focus on questions like:

- Can we continue production safely if HMIs go offline?
- Are our safety instrumented systems independently protected?
- Are backups secure from internal or external threats?

These exercises reinforce preparedness and help close gaps in response planning.

Step 7: Implement a Governance Framework

Formal governance is essential for sustaining progress. Many organizations already use ISO 27001 or NIST 800 frameworks for IT; these should be mapped against ISA/IEC 62443 to address OT-specific needs.

Key governance elements include:

- OT, specific access control and authentication policies.
- Secure remote access workflows and vendor management.
- Zone/conduit architecture design and documentation.
- Change control procedures adapted to plant operations.
- Integration with safety systems and emergency shutdown procedures.

Governance structures must scale across sites with varying levels of maturity, supporting consistency without imposing a one-size-fits all model.

With the right structure and collaboration, manufacturers can move from reactive fixes to resilient, secure operations.

9.4 Foundational Capabilities for Maturity

To strengthen their cybersecurity posture, manufacturers should focus on four critical technical capabilities: *See table below.*

These capabilities reinforce the program's ability to withstand, respond to, and recover from cyber threats.

9.5 Looking Ahead: Operationalizing OT Security

Sustainable OT cybersecurity is not achieved through tools alone; it requires alignment with operational strategy, consistent governance, and ongoing collaboration across IT, OT, and business leaders.

As industrial systems become more connected and adversaries more sophisticated, the need for structured, risk-informed OT security programs will only grow. Manufacturers that embed security into operations, treat it as a business enabler, and invest in the right people and capabilities will be best positioned to thrive in a resilient, digital future.

Capability	Description
Immutable Backups	Secure, tamper-proof backups to support recovery from ransomware or data destruction.
OT, Specific Remote Access	Purpose-built solutions that support industrial protocols and granular access control.
Incident Response Plans	Playbooks tailored to OT scenarios, including isolation, manual override, and safety impact.
OT Vulnerability Management	Tools that can safely assess and prioritize risks across legacy and modern control systems.

Key Takeaways from Chapter 9

- OT cybersecurity must be treated as a business risk with operational, financial, and safety implications.
- Appointing an OT IT translator accelerates collaboration and bridges organizational gaps.
- Process understanding is essential to prioritizing protections based on real-world impact.
- Asset inventory and zone conduit architecture enable structured segmentation and defense.
- Tabletop exercises should evolve with the program, incorporating actual plant scenarios.
- Governance frameworks must blend enterprise standards with OT specific controls.
- Foundational capabilities such as immutable backups, secure remote access, incident response, and OT aware vulnerability management are critical to resilience.
- Success lies in integrating cybersecurity into the fabric of operations, not layering it on as an afterthought.

Rethinking Risk and Embedding Cybersecurity in Engineering Culture

Authored by Michelle Govender, Octarity

10.1 Introduction: Engineering a Cyber-Resilient Culture

In today's manufacturing and critical infrastructure environments, insecure remote access, outdated HMIs, and poorly segmented networks can directly impact safety, uptime, and regulatory compliance. Traditional models that position cybersecurity solely as an IT function are failing to keep pace with these realities.

This chapter explores how manufacturers can take practical steps to embed cybersecurity into engineering culture, shift mindsets around risk, and build long-term operational resilience.

10.2 The Case for Cultural Transformation

In the early days of industrial safety, protections were largely reactive, implemented in response to major incidents and driven by compliance requirements. Over time, this evolved into a proactive culture of risk management owned by workers, engineers, and leaders alike. Today, safety is integrated into design specifications, commissioning checklists, and operational KPIs.

Cybersecurity is now on the cusp of a similar transformation. Most organizations remain stuck in a compliance-first posture, with security concentrated in IT departments and minimal influence over plant operations. This siloed approach is no longer sufficient. The complexity of cyber-physical systems, growing threat sophistication, and heightened regulatory scrutiny demand a cultural shift that embeds cyber risk into the very decisions and routines of engineering teams.

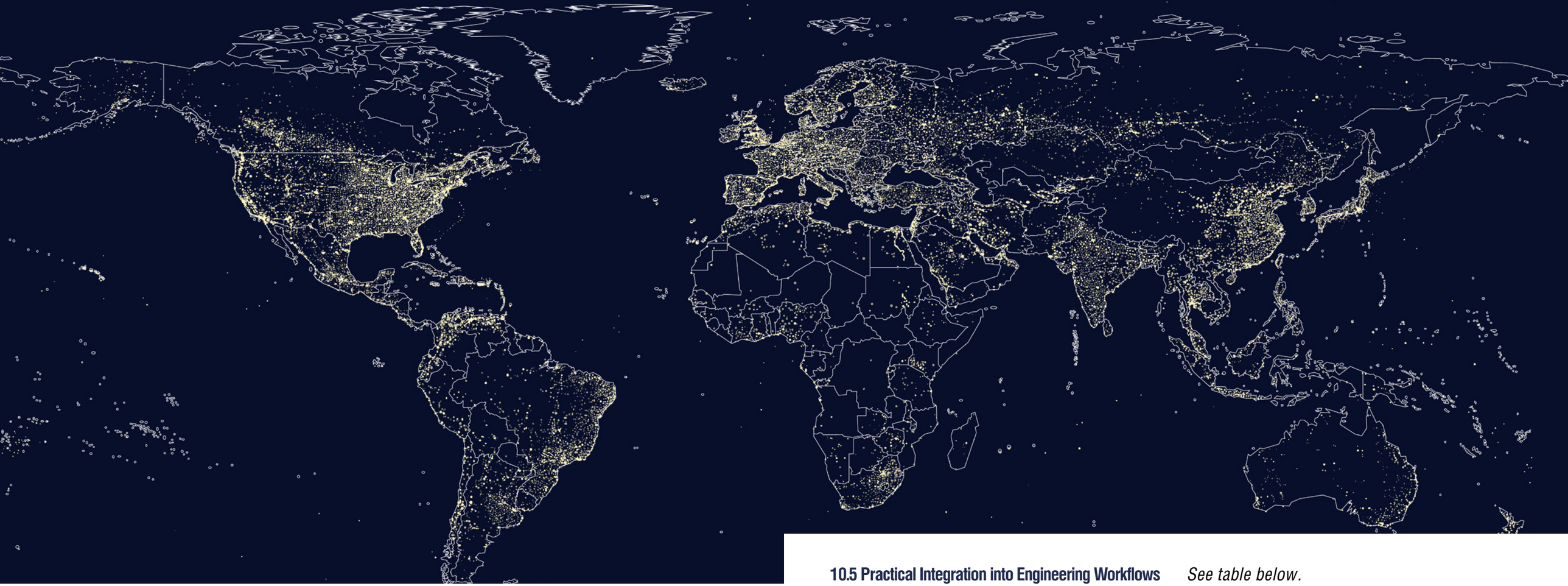
To succeed, cybersecurity must become a shared responsibility, recognized as a condition for safe, reliable operations and integrated into the day-to-day work of those designing, maintaining, and operating critical systems.

10.3 Lessons from the Safety Culture Journey

The evolution of industrial safety culture provides a clear and proven model for embedding risk awareness into operations. Several pivotal moments shaped this transformation: *See table on the right.*

These changes did not rely solely on new policies; they were sustained through leadership modeling, process integration, and the creation of feedback loops that rewarded risk-aware behavior. The result: a dramatic reduction in fatalities and injuries across industries in Europe and beyond.
This same approach can now be applied to cybersecurity.

Safety Culture Milestone	Impact
EU Framework Directive (1989)	Codified behavior-based safety and made risk management part of day-to-day engineering.
Historical industrial incidents (e.g. Chernobyl, Piper Alpha)	Raised global awareness about the consequences of neglecting system-level safety.
KPIs and behavioral indicators	Made safety performance measurable, incentivized frontline participation.
Contractor onboarding and project governance	Extended safety expectations beyond internal teams to partners and suppliers.



10.4 Envisioning a Cyber-Informed Engineering Culture

A mature cybersecurity culture on the plant floor would include:

- Risk-informed decisions at the point of change, not just post-implementation.
- Engineers trained to recognize cybersecurity red flags during commissioning, procurement, and change requests.
- Shared accountability across IT, OT, and engineering, with cybersecurity treated as a condition for project approval and operational readiness.

For example, commissioning processes would include cybersecurity considerations as standard practice:

- How does this new system connect to the network?
- Who manages logical access after deployment?
- What safeguards are in place for vendor access?
- Are all remote access points auditable and monitored?

These questions are not theoretical; they reflect real-world entry points for attackers and need to become part of everyday engineering decisions.

10.5 Practical Integration into Engineering Workflows

Organizations do not need entirely new frameworks to embed cybersecurity into engineering; they need to enhance existing ones. Many engineering workflows already include gates for safety, quality, and compliance. Cybersecurity can be incorporated through targeted, high-impact interventions:

See table below.

These touchpoints mirror how safety became routine. By aligning cybersecurity with existing forms and sign-off processes, organizations make it easier for teams to incorporate security thinking without increasing administrative burden.

Workflow	Cyber Integration Example
Engineering Change Requests (ECRs)	Add a section with five cybersecurity questions (e.g., connectivity, access control, update procedures).
Project planning and procurement	Require vendors to meet specific cybersecurity requirements or standards (e.g., ISA/IEC 62443).
Preventive maintenance	Include software patching, credential reviews, and access log audits as routine checks.
Commissioning and sign-off	Include cybersecurity validation as a precondition for go-live.

10.6 Shaping Culture Through Leadership and Behavior

Culture is built through repetition, visibility, and reinforcement. Safety leaders long ago recognized the importance of rituals, toolbox talks, walkdowns, and safety "moments" that embedded the importance of risk management into daily operations. *See table below.*

Cybersecurity can follow the same playbook: These approaches help develop a sense of ownership among workers and reinforce the idea that cybersecurity, like safety, is everyone's responsibility.

10.7 Building Tools and Templates that Support Behavior

Sustaining cultural change requires practical tools that reinforce desired behaviors. Instead of building new systems from scratch, organizations can adapt existing resources to integrate cyber considerations.

Key considerations:

- Modify engineering templates (e.g., ECRs, commissioning checklists) to include cyber prompts.
- Add cybersecurity topics to routine training programs and toolbox talks.
- Develop dashboards that track cyber KPIs (e.g., number of assets with validated access controls, percentage of systems with up-to-date firmware).
- Create job aids and one-pagers that help engineers identify common vulnerabilities (e.g., open ports, default passwords, unmanaged remote access).

Simple, consistent prompts in the right places help teams build habits, and habits drive cultural change.

10.8 From Insight to Action

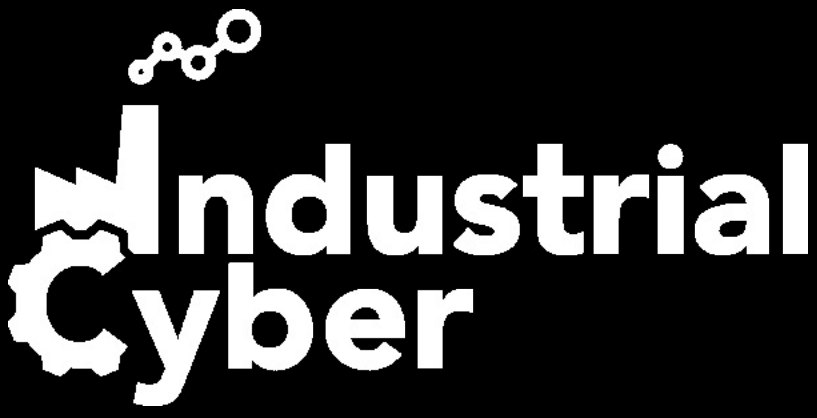
Michelle emphasizes a pragmatic message: "You don't need new frameworks to start, you just need to start. Begin with one process, one form, one team. Pilot a change to an existing commissioning template or introduce a cybersecurity checklist to contractor onboarding. Measure impact, gather feedback, and scale what works".

Cultural transformation is not about perfection, it's about progress. By aligning cybersecurity with the engineering lifecycle, organizations move from isolated controls to sustainable practices. Over time, the norm becomes: "We don't commission it unless it's cyber-safe." Just as engineers today instinctively consider safety implications when designing a system, the next generation will do the same for cybersecurity, if we build the right culture today.

Cultural Tactic	Purpose
Cybersecurity "moments" in team meetings	Normalizes risk conversations and knowledge sharing.
Leadership plant walkdowns that include cyber topics	Demonstrates visible commitment and models expectations.
Shared vocabulary and definitions	Ensures alignment across IT, OT, and engineering disciplines.
Recognition of positive security behavior	Reinforces desired actions and builds momentum.

Key Takeaways from Chapter 10

- Cybersecurity must evolve from a compliance exercise to a core element of engineering culture, mirroring the evolution of industrial safety.
- Historical lessons from safety integration provide a roadmap for embedding cybersecurity into plant operations.
- Cyber risk ownership should shift to the operational level, with engineers trained, empowered, and supported to make secure decisions.
- Integration into existing workflows, ECRs, procurement, commissioning, maintenance, ensures cybersecurity becomes part of routine operations.
- Cultural nudges, leadership visibility, and shared language help reinforce cyber-responsible behavior.
- Practical tools and templates lower adoption barriers and support consistent, sustainable practice.
- Organizations should start small, build momentum, and align security efforts with the real work of running safe and reliable operations.



Manufacturing Cybersecurity Handbook 2025

Industrialcyber.co