White Paper | Beyond the Factory Floor

Integrating Physical and Cybersecurity for Manufacturing Resilience

Deploying Technologies to Physically and Digitally Secure Production Environments

Executive Summary

How Manufacturers Can Strengthen Operations by Unifying Physical Protection and Digital Defense

Manufacturing operations today face a rapidly expanding threat landscape where physical security risks and cybersecurity vulnerabilities are no longer separate challenges - they are interconnected points of failure. As factories become smarter and more digitally integrated, the convergence of physical and cyber threats creates new avenues for disruption, from unauthorized facility access leading to network breaches, to cyberattacks compromising physical equipment and production lines.

Traditional siloed security models that treat physical and cyber defenses independently are no longer sufficient. In an era where a physical intrusion can trigger a digital shutdown, and a cyberattack can disable physical infrastructure, manufacturers must embrace a unified, integrated security strategy that bridges the gap between these domains.

By combining physical access controls, surveillance analytics, private wireless networking, IoT security, and real-time cyber monitoring into a single, cohesive framework, manufacturers can dramatically strengthen their resilience. Integrated security solutions not only reduce operational risks but also ensure the continuity of production, protect intellectual property, and support long-term business sustainability.

MCA is a trusted technology partner for manufacturers navigating this complex landscape. With deep expertise across voice, data, and security solutions, MCA delivers fully integrated systems that safeguard both the physical and digital realms of modern manufacturing - empowering businesses to protect what matters most and thrive in a future defined by connected operations.

The convergence of physical and cyber threats in smart factories requires a unified security strategy to defend against an increasingly complex and interconnected risk landscape.

To stay resilient in the face of evolving threats, manufacturers must integrate physical and cyber protections, ensuring seamless defense across operational and digital systems.

Introduction: A New Era of Manufacturing Security

The manufacturing sector is undergoing a profound transformation. Traditional production environments, once isolated and manually operated, are evolving into highly connected smart factories powered by automation, AI, IoT, and decentralized systems. While this evolution delivers remarkable gains in efficiency, flexibility, and innovation, it also brings with it an expanded - and increasingly complex - attack surface.

In today's smart factories, the line between physical and cyber vulnerabilities has all but disappeared. A compromised badge reader or unsecured surveillance system can provide an open doorway into critical operational networks. Likewise, a cyberattack against an IoT device, edge gateway, or SCADA system can cause devastating physical consequences - from shutting down assembly lines to disabling critical safety systems. The reality is clear: in the era of Industry 5.0, physical and cyber threats have converged, creating a unified risk environment that manufacturers can no longer afford to treat separately.

To safeguard operations, protect intellectual property, and maintain production resilience, manufacturers must move beyond siloed security models. Instead, they must embrace a unified security strategy that integrates physical protection and cybersecurity into a single, seamless defense framework. As threats grow more sophisticated and interconnected, so too must the solutions designed to counter them.

Chapter 1: The Convergence of Physical and Cyber Threats

In the past, manufacturers could clearly separate their security challenges: physical threats were dealt with by security guards and access control, while cyber threats were the responsibility of IT departments. However, as manufacturing environments become more interconnected through smart devices, cloud platforms, and operational technologies (OT), these once-distinct threat domains have converged into a single, inseparable risk landscape.

Defining the Threats

- **Physical Threats:** These include unauthorized entry into facilities, theft of sensitive materials, physical sabotage of machinery, or tampering with critical infrastructure.
- **Cyber Threats:** These encompass unauthorized access to networks, ransomware attacks, intellectual property theft, and disruptions to automation or control systems through digital means.

The Merging of Physical and Cyber Threats

Today, physical and cyber risks are deeply intertwined. A breach in physical security - such as an intruder accessing an unsecured server room or maintenance port - can lead to massive cyber compromise. Conversely, a successful cyberattack can disable physical safety systems, unlock secure doors, or manipulate automated machinery in ways that endanger personnel and disrupt production.

Common Vulnerabilities Driving Convergence

- **Unsecured Access Points:** Traditional badge systems, if not integrated with cybersecurity protocols, can be exploited to gain entry to critical network hardware such as routers, control servers, or industrial PCs.
- **IoT Devices and Industrial Sensors:** Connected sensors, cameras, and control panels often operate over private networks but are frequently overlooked in security planning. Without proper encryption and access controls, these devices can serve as easy entry points for cyberattacks targeting OT environments.

- **Physical Sabotage of OT Networks:** Access to manufacturing floor devices - such as programmable logic controllers (PLCs) or SCADA terminals - allows bad actors to physically disrupt production lines, alter product quality parameters, or even shut down entire facilities.

Real-World Case Examples and Sector Parallels

- **Vendor Breach via HVAC System Access:** In a well-known incident outside the manufacturing sector, attackers exploited vulnerabilities in a building's HVAC system controls to gain entry into a company's broader corporate network. This breach, while not involving a manufacturing facility, highlights a critical risk that manufacturing environments increasingly share as they connect HVAC, energy management, and operational controls to private networks. If left unsecured, these systems can serve as an unexpected backdoor into manufacturing OT and IT systems.
- **Physical Access Leading to Malware Introduction:** Industrial organizations have seen incidents where third-party contractors or visitors, granted physical access to secured areas without stringent cybersecurity controls, have inadvertently introduced malware through personal devices. Manufacturing facilities - where maintenance contractors and equipment vendors are common - face the same risk if physical access is not tightly managed and network segmentation is not enforced.
- **Exploitation of IoT Surveillance Systems:** Across multiple sectors, attackers have leveraged unprotected or poorly secured surveillance cameras to penetrate network environments. Given manufacturing's heavy reliance on surveillance for facility security, similar vulnerabilities can be exploited to gain unauthorized access to critical operational or safety systems if IoT devices are not properly secured

Chapter 2: Identifying the Weak Points in Manufacturing Facilities

The convergence of physical and cyber threats has exposed new vulnerabilities across manufacturing environments. As factories integrate smart technologies, decentralized production models, and cloud-connected systems, traditional assumptions about facility security are no longer sufficient. To build true operational resilience, manufacturers must first recognize and address the most common weak points where modern threats are likely to strike.

Unsecured Access Points and Network Infiltration

Physical access points such as loading docks, maintenance doors, server rooms, and utility areas have historically been secured through traditional means - locks, badges, or basic surveillance. However, without integration with cybersecurity protections, these access points can now serve as direct conduits for network infiltration.

For example, a bad actor gaining physical access to a network switch, unprotected server, or unsecured IoT device can bypass perimeter firewalls entirely, moving laterally through critical operational technology (OT) systems. In many facilities, access control systems are not fully linked to digital network protections, leaving physical and cyber domains dangerously isolated.

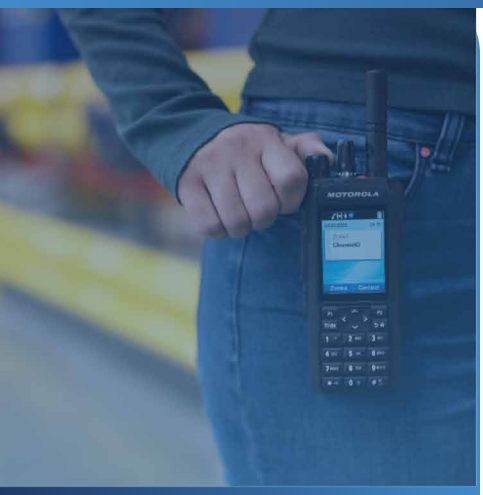
Key Risk: **Physical intrusion can immediately escalate into network compromise, especially when critical infrastructure is accessible from unsecured areas.**

IoT Devices and Industrial Sensors as Attack Vectors

The explosion of Internet of Things (IoT) devices in manufacturing - environmental sensors, surveillance cameras, smart lighting, automated machinery controllers - has brought major operational benefits but also introduced new vulnerabilities. Many IoT devices lack robust encryption, regular firmware updates, or proper segmentation from sensitive networks.

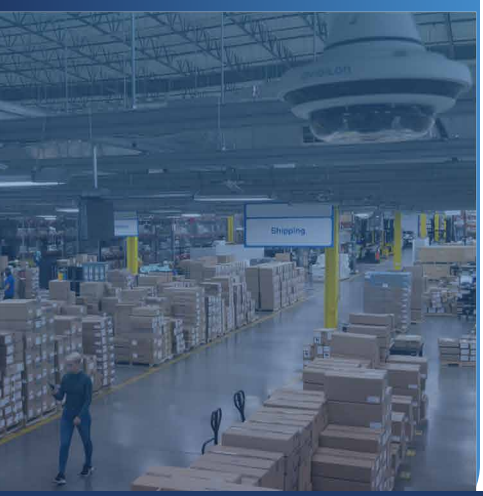
Unsecured physical access points and poorly protected IoT devices create direct conduits for attackers to bypass firewalls and infiltrate critical OT systems.

Weak physical and cyber integration leaves manufacturers vulnerable to risks, allowing exploitation of access points, IoT sensors, and third-party interactions, compromising operations.



Unsecured IoT and IIoT devices create entry points for attackers, enabling operational disruptions, intellectual property theft, or even catastrophic sabotage.

The intersection of physical and cyber vulnerabilities in manufacturing demands an integrated security framework to safeguard both production efficiency and operational resilience.



In many manufacturing facilities, thousands of devices continuously transmit operational data across shared wireless or IP-based networks. If even one connected device is exploited, attackers can use it as a foothold to access SCADA systems, modify production processes, or disrupt automated controls.

Real-World Parallel: In 2021, a water treatment plant in Oldsmar, Florida was hacked, and the intruder remotely increased the levels of sodium hydroxide (lye) in the water supply to dangerous levels before a plant operator noticed the unauthorized change and reversed it. Although this attack did not occur in a manufacturing facility, it illustrates how the exploitation of small, seemingly isolated operational systems - such as a sensor or control interface - can cause potentially catastrophic consequences when proper security measures are not in place.

Key Risk: **IoT and IIoT devices, if unsecured, provide low-hanging fruit for attackers targeting both operational disruption and intellectual property theft.**

Physical Sabotage Impacting Operational Technology (OT) Networks

While cybersecurity threats often dominate conversations today, physical sabotage remains a potent and often under-appreciated risk. An insider or external actor physically tampering with control systems - disabling PLCs, corrupting local server firmware, unplugging critical gateways - can cause immediate and catastrophic impacts on production.

Because many OT devices, such as industrial controllers or on-site SCADA units, are not hardened against physical tampering, even brief unauthorized access can result in downtime, data loss, safety system failures, or cascading production errors.

Key Risk: **Physical breaches at the equipment level can cause damage or downtime on par with the worst cyberattacks, especially if detection systems are not in place.**

The Hidden Fragility of Smart Manufacturing

Manufacturing facilities today are not just at risk because they are more connected - they are at risk because critical systems often lack seamless protection across both physical and cyber domains.

- **Physical gaps** (like unsecured access points) now have direct cyber consequences.
- **Digital vulnerabilities** (like unprotected IoT devices) can expose physical assets to remote manipulation or sabotage.
- **Operational systems** (such as SCADA or PLCs) sit at the intersection of these threats, often without adequate monitoring for hybrid attack patterns.

Recognizing these weaknesses is the first step. In the next chapter, we will explore how manufacturers can proactively build an integrated security framework that closes these gaps, protects both their people and their data, and ensures operational resilience in an era of blended threats.

Chapter 3: Building a Physical and Cybersecurity Framework

As manufacturing facilities become more interconnected and technologically advanced, safeguarding operations requires more than isolated security upgrades. True resilience demands an integrated security framework - one that unifies physical protection and cybersecurity into a single, seamless defense system. Integration strengthens threat detection, accelerates incident response, and protects both people and production from the rising convergence of risks

Principles of Integration

1. Unified Threat Monitoring and Detection

Physical breaches, network anomalies, and equipment tampering must no longer be treated as separate security events. Unified monitoring systems can correlate physical access events (such as unauthorized door entries) with network activities (like unusual login attempts or device traffic spikes). By centralizing threat data, manufacturers can detect and respond to coordinated or multi-layered attacks before they escalate into major disruptions.

2. Common Alerting and Response Protocols

Integrated security frameworks establish a single playbook for all types of incidents, whether physical, cyber, or hybrid. Alarm triggers from access control systems, surveillance analytics, and cybersecurity sensors should funnel into a centralized command center, ensuring that dispatch, IT, operations, and executive teams can coordinate a unified, immediate response.

3. Centralized Management Dashboards

Rather than managing security information from fragmented platforms, integrated systems provide a single dashboard view. Operators can monitor physical facility security (cameras, badges, motion detectors) and network health (device performance, unauthorized access attempts, traffic anomalies) from a single, streamlined console - dramatically reducing blind spots and decision-making delays.

Best Practices for Physical and Cyber Integration

Encrypted Private Wireless Networks (4G/5G/CBRS)

Physical breaches, network anomalies, and equipment tampering must no longer be treated as separate security events. Unified monitoring systems can correlate physical access events (such as unauthorized door entries) with network activities (like unusual login attempts or device traffic spikes). By centralizing threat data, manufacturers can detect and respond to coordinated or multi-layered attacks before they escalate into major disruptions.

Network Segmentation for IoT and SCADA Systems

Rather than allowing production and administrative networks to overlap, modern manufacturing facilities should segment operational technology (OT) environments from corporate IT infrastructure. Critical systems - such as IoT sensors, PLCs, and robotic controllers - should operate on their own protected, monitored subnetworks to prevent lateral movement by attackers.

Smart Access Control Systems Tied to Cybersecurity Monitoring

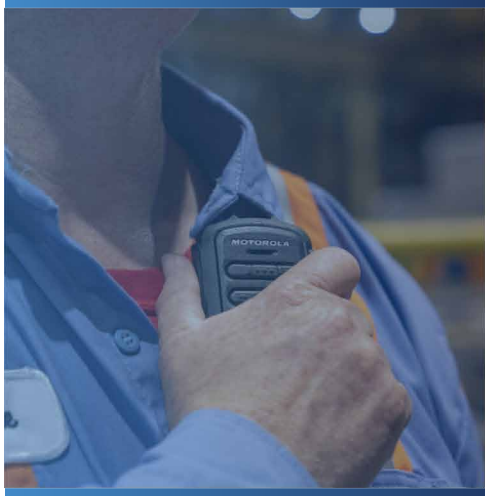
Badge systems, biometric readers, and mobile credentials should not operate in isolation. Instead, physical access events must feed directly into cybersecurity analytics platforms. Unauthorized entry to a control room, for instance, should trigger real-time alerts to IT security teams, not just physical security personnel.

The Business Case for Integrated Security

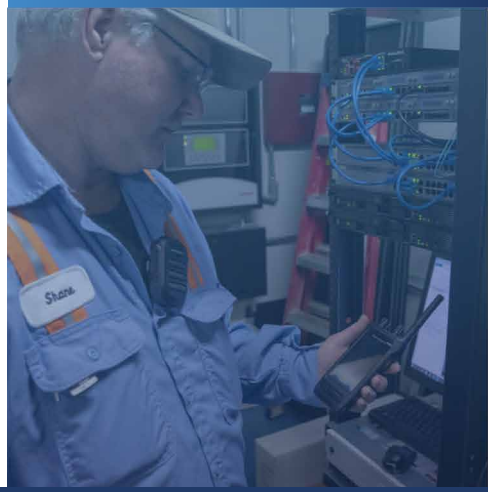
Beyond risk reduction, integrated security delivers tangible operational and financial benefits:

- **Faster Incident Response:** Unified systems allow teams to diagnose and contain threats in minutes, not hours.
- **Reduced Operational Downtime:** Early threat detection prevents small events from becoming large-scale disruptions.
- **Improved Compliance and Reporting:** Integrated logs and real-time monitoring simplify regulatory compliance audits for safety and data protection standards.
- **Enhanced Business Continuity:** Facilities that detect, isolate, and recover from hybrid threats quickly are better positioned to maintain customer trust and operational momentum.

Unified threat monitoring enables organizations to detect multi-layered security risks by correlating physical and cyber events through centralized data analysis.



Integrated security frameworks streamline incident response, reduce downtime, and enhance both compliance and business continuity through collaborative, real-time monitoring.



Unlock proactive security with MCA's unified solutions, seamlessly integrating physical and digital defenses to detect threats early and respond decisively.

Empower manufacturing operations with private wireless networks and zero-trust infrastructure, ensuring encrypted, isolated, and resilient protection at every layer.

A Stronger, Smarter Defense

An integrated security framework empowers manufacturers to stay ahead of evolving threats. Rather than reacting after damage has been done, unified systems give operational leaders the tools to detect warning signs early, coordinate swift countermeasures, and protect both the physical and digital heartbeat of their operations.

In the next chapter, we'll explore how MCA's specific solutions - spanning private wireless networking, secure device protection, physical intrusion detection, and cyber monitoring - enable manufacturers to implement these integrated security principles effectively and confidently.

Chapter 4: Integrated Manufacturing Security Solutions

Building an integrated security framework requires more than theory - it demands proven, reliable technologies that can protect manufacturing operations across both the physical and digital domains. MCA delivers precisely this, offering a comprehensive suite of solutions designed to unify communication, surveillance, access control, network protection, and cybersecurity monitoring into a seamless, future-ready defense system.

Our approach enables manufacturers to proactively secure their environments, detect threats early, and respond swiftly across all operational layers - from the factory floor to the cloud.

Private Wireless Networks: The Backbone of Secure Operations

MCA's Private Wireless Solutions - including 4G LTE, 5G, and CBRS platforms - create dedicated, isolated networks for critical operational traffic.

Unlike public Wi-Fi or wired corporate networks, our private wireless infrastructure ensures that voice communications, SCADA data, IoT device transmissions, and video surveillance feeds remain encrypted, isolated, and protected from external threats.

Benefits:

- Complete control over network access and device authentication
- Superior network performance for latency-sensitive automation and monitoring systems
- Reduced exposure to external attacks compared to public cellular and Wi-Fi networks

Secure Device Networks and ZTNA-Compliant Infrastructure

Manufacturing security must extend beyond the perimeter to secure every endpoint and device across operational environments.

MCA deploys industrial-grade routers, edge gateways, and secure connectivity infrastructure built to enforce Zero Trust Network Access (ZTNA) principles across both wired and wireless environments.

Our cellular networking solutions - including public cellular and the aforementioned private wireless architectures - deliver encrypted, isolated communications for production systems, IoT devices, SCADA controls, and mobile assets. In parallel, encrypted facility-wide Wi-Fi networks provide high-speed, isolated connections for non-critical applications while preventing crossover access to critical OT systems.

Capabilities Include:

- Device-level authentication and encryption, ensuring least-privilege access enforcement
- Seamless segmentation between production, administrative, and guest networks

- Encrypted backhaul communication between local facilities and central command centers
- End-to-end data privacy through embedded VPN, traffic segmentation, and secure tunneling technologies

By securing both cellular and parallel Wi-Fi networks with advanced encryption, multi-layer authentication, and dynamic network segmentation, MCA ensures that every device - from IoT sensors to mobile workstations - operates under strict access controls, minimizing exposure and eliminating lateral attack pathways.

Physical Intrusion Detection and Intelligent Surveillance

Physical threats remain a major concern, especially in decentralized and automated production environments. MCA's physical security portfolio includes:

- **Video Surveillance with Intelligent Analytics:** Real-time detection of loitering, unauthorized access, perimeter breaches, and equipment tampering.
- **Access Control Systems:** Integrated card readers, biometrics, and mobile credentialing platforms that unify physical access management with cybersecurity monitoring.
- **Intrusion Detection Sensors:** Motion, vibration, and sound sensors designed to detect breaches before attackers reach critical systems.

Benefits:

- Immediate real-time alerts for both physical and cyber teams
- Integration with mass notification and emergency response platforms
- Centralized visibility over facility access and intrusion events

Cybersecurity Monitoring and Threat Detection

In today's manufacturing environments, passive security is no longer enough. MCA provides active, real-time cybersecurity monitoring and threat detection platforms built to safeguard complex, hybrid operational environments.

Capabilities Include:

- Continuous Network Monitoring:
  - Advanced Service and Traffic Management platforms monitor critical services, data flows, and routing behaviors in real-time.
  - DDoS mitigation engines detect and neutralize volumetric attacks before they impact network stability.
  - Secure Access Service Edge (SASE) frameworks enable cloud-native control over user and device access attempts, continuously validating trust before granting network permissions.
- Automated Threat Detection and Behavioral Analytics:
  - Deep Packet Inspection (DPI) technology identifies anomalies in device communications and application traffic patterns.
  - Remote Browser Isolation (RBI) and Intrusion Detection/Prevention Systems (IDS/IPS) safeguard user interactions from advanced web-based and network-layer attacks.
  - Cybersecurity orchestration platforms apply machine learning models to network behavior, detecting emerging threats based on deviations from normal operations.
- Managed Detection and Response (MDR) Services:
  - Threat hunters and automated analytics engines identify, verify, and escalate active threats in real time.

MCA fortifies end-to-end communication channels with advanced encryption, secure tunneling, and multi-layer authentication, ensuring airtight data privacy across all connected devices.

Real-time surveillance, intrusion detection, and unified cyber-physical security systems deliver unmatched protection for decentralized factory environments.

EDA frameworks empower real-time threat containment, rapid remediation, and streamlined policy enforcement across complex manufacturing networks.

Unified Management Systems centralize security operations, combining physical and cyber threat intelligence into a single dashboard for enhanced situational awareness and coordinated response.

- Event-Driven Automation (EDA) frameworks enable real-time containment, remediation workflows, and policy enforcement across entire manufacturing networks.

- **Incident Response Enablement:**
  - Integrated incident management platforms deliver automated threat isolation, device quarantine, forensic analysis, and recovery orchestration, ensuring rapid containment and minimal production impact.

By combining continuous monitoring, intelligent automation, and proactive incident response, MCA ensures that manufacturers can detect, neutralize, and recover from cyber and blended physical-cyber threats before they disrupt operations or cause material harm.

Unified Management Systems and Command Centers

True security integration requires centralized command.

MCA designs and deploys Unified Management Systems that bring together voice communications, video surveillance, access control, IoT telemetry, and cybersecurity data into a single operational dashboard.

Capabilities Include:

- Full-facility situational awareness in real-time
- Correlation of physical and cyber threat indicators
- Streamlined incident response coordination between security, IT, and operations teams
- Scalable architecture for single-site or multi-site manufacturing operations

MCA's Integrated Advantage

MCA's integrated approach to manufacturing security eliminates silos, accelerates detection, and strengthens resilience at every level.

By unifying private wireless networks, secured device communications, intelligent physical security, active cyber monitoring, and centralized management, MCA empowers manufacturers to stay ahead of evolving threats - while protecting the continuity, safety, and success of their operations.

In the next chapter, we will explore how effective incident response planning - rooted in integrated physical and cyber capabilities - can further minimize risks and ensure operational continuity even in the face of complex security events.

Chapter 5: Incident Response in an Integrated Environment

Even with the strongest defenses in place, no security strategy is complete without a robust, coordinated incident response plan. In today's manufacturing environments - where physical security breaches can trigger cyberattacks, and digital intrusions can disrupt physical systems - incident response must evolve beyond traditional IT or facility-based reactions. It must become a fully integrated, proactive, and automated function capable of addressing complex, blended threats at scale and speed.

An effective incident response plan, built on an integrated physical and cybersecurity framework, enables manufacturers to minimize the impact of security events, protect operational continuity, and ensure the safety of people, assets, and production processes.

The Integrated Incident Response Life-cycle

1. Detection: Unified Threat Monitoring Across Domains

The first step in incident response is early, accurate detection. Through integrated monitoring platforms, manufacturers can correlate physical security events (such as unauthorized access attempts, tampering alarms, or perimeter breaches)

with cyber indicators (such as abnormal network traffic, unauthorized device connections, or malware signatures).

Unified detection provides a comprehensive, real-time view of facility and network activity, allowing teams to recognize blended threat patterns before they escalate.

2. Containment: Isolate Physical and Cyber Threats Immediately

Once a threat is detected, rapid containment is critical.

- Physical access can be restricted automatically, locking down sensitive zones or disabling badge credentials in real-time.
- Compromised devices, infected network segments, or suspicious user accounts can be isolated through automated network segmentation, deep packet inspection (DPI) controls, and dynamic quarantine policies.
- Event-Driven Automation technologies trigger predefined workflows that limit lateral movement, halt further spread, and protect critical operational systems while incident investigation begins.

3. Communication: Orchestrated Response Across Teams

Clear, immediate communication between security, operations, IT, and executive leadership is essential during any security event.

Integrated mass notification systems and unified communication platforms ensure that all relevant stakeholders are alerted within seconds of a confirmed incident.

Automated messaging cascades - via radio, desktop alerts, SMS, and mobile applications - ensure consistent, multi-channel delivery of critical information, minimizing confusion and expediting coordinated action.

4. Recovery: Rapid Restoration of Safe Operations

Following containment, manufacturers must focus on restoring safe, normal operations as quickly and securely as possible.

- Physical facilities must be inspected and cleared for operational readiness.
- Network systems must be scanned, remediated, patched, and revalidated.
- Incident logs, forensic data, and behavioral analytics must be reviewed to understand root causes, identify lessons learned, and strengthen defenses.

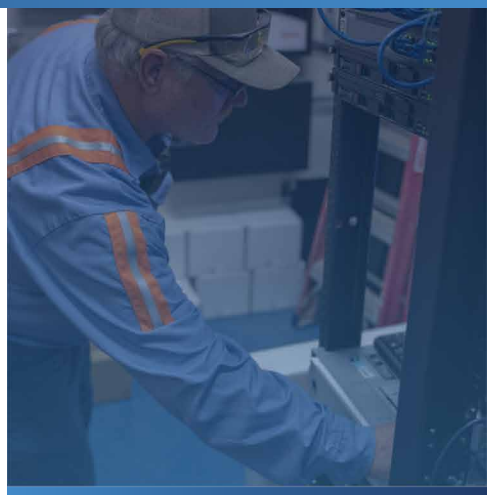
Recovery plans leverage centralized management dashboards, automated incident playbooks, and built-in redundancies across voice, data, and security systems to return to full production with minimal downtime or loss.

Role of Unified Management Systems in Incident Response

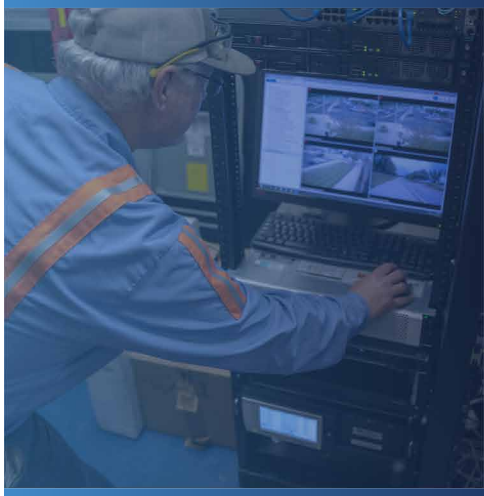
Unified Management Systems provide the centralized command-and-control capabilities required to execute incident response seamlessly across physical and digital environments.

- **Real-time dashboards** integrate alerts from surveillance, access control, IoT telemetry, and cybersecurity monitoring.
- **Automated orchestration** triggers coordinated containment actions across physical locks, network firewalls, device isolation, and service shutdowns.
- **Incident tracking** ensures that all actions, alerts, and resolutions are logged and auditable for compliance and future analysis.
- **Post-incident reporting** simplifies the creation of detailed after-action reports for internal review and regulatory bodies.

By consolidating operational awareness and enabling real-time decision-making, unified management systems dramatically reduce response times and minimize the potential for cascading failures across production environments.



Unified detection and containment strategies are critical for identifying and neutralizing complex threats across both physical and cyber domains before they escalate.



Real-time automation and orchestrated communication ensure rapid, coordinated responses that safeguard operations and prevent prolonged disruptions.

Integrated incident response is the key to safeguarding critical assets, ensuring operational resilience, and defending against today's complex, blended threats.

Unified security strategies empower manufacturers to protect people, processes, and production systems, enabling sustainable growth and future-proofing operations.

Why Integrated Response Matters for Manufacturers

Traditional, disjointed incident responses often result in delayed reactions, duplicated efforts, and greater damage.

Integrated incident response ensures:

- Faster threat isolation and neutralization
- Greater protection of intellectual property and critical operational assets
- Improved compliance with safety, data protection, and industrial security regulations
- Enhanced operational resilience in the face of increasingly sophisticated blended threats

Most importantly, integrated incident response empowers manufacturers to protect what matters most - people, productivity, and brand reputation - while maintaining the agility to adapt quickly to future challenges.

Conclusion: Future-Proofing Manufacturing Security

The manufacturing industry stands at a pivotal crossroads. As facilities embrace smart technologies, automation, and decentralized production models, the convergence of physical and cyber threats has redefined what it means to operate securely.

Traditional approaches - treating physical security and cybersecurity as separate challenges - are no longer sufficient to defend against today's sophisticated, blended risks.

Future-ready manufacturing security demands full integration: a unified defense strategy that protects people, processes, and production systems across both physical and digital environments. Integrated monitoring, intelligent automation, centralized incident response, and proactive risk management are not luxuries - they are essential components of resilient, sustainable operations.

By adopting integrated physical and cybersecurity frameworks, manufacturers can:

- Detect threats earlier across facility and network environments
- Contain and neutralize incidents rapidly before they escalate
- Safeguard intellectual property, critical infrastructure, and production continuity
- Comply more effectively with regulatory requirements and industry best practices
- Build operational resilience that sustains growth in a dynamic, threat-prone world

At MCA, we understand the evolving challenges manufacturers face - and we deliver comprehensive, integrated security solutions designed to meet them head-on.

From encrypted private wireless networks and device-level access controls to intelligent surveillance, active cyber threat detection, and unified command platforms, MCA empowers manufacturers to protect their operations today - and strengthen them for tomorrow.

The threats of the future are integrated. Your defense must be as well.

Partner with MCA to future-proof your manufacturing security and confidently lead the next era of industrial innovation.

About MCA

MCA is one of the largest and most trusted technology integrators in the United States, offering world-class voice, data, and security solutions that enhance the quality, safety, and productivity of customers, operations, and lives.

More than 65,000 customers trust MCA to provide carefully researched solutions for a safe, secure, and more efficient workplace. As your trusted advisor, we reduce the time and effort needed to research, install, and maintain the right solutions to make your workplace better.

Our team of certified professionals across the United States delivers a full suite of reliable technologies with a service-first approach. The MCA advantage is our extensive service portfolio to support the solution life-cycle from start to finish.

MCA Headquarters

135 N Church St #310
Spartanburg, SC 29306

800.596.8205

info@callmc.com

www.callmc.com

MCA