opentext™

DevOps for manufacturing

Drive secure innovation

Contents

Secure the manufacturing industry with DevOps

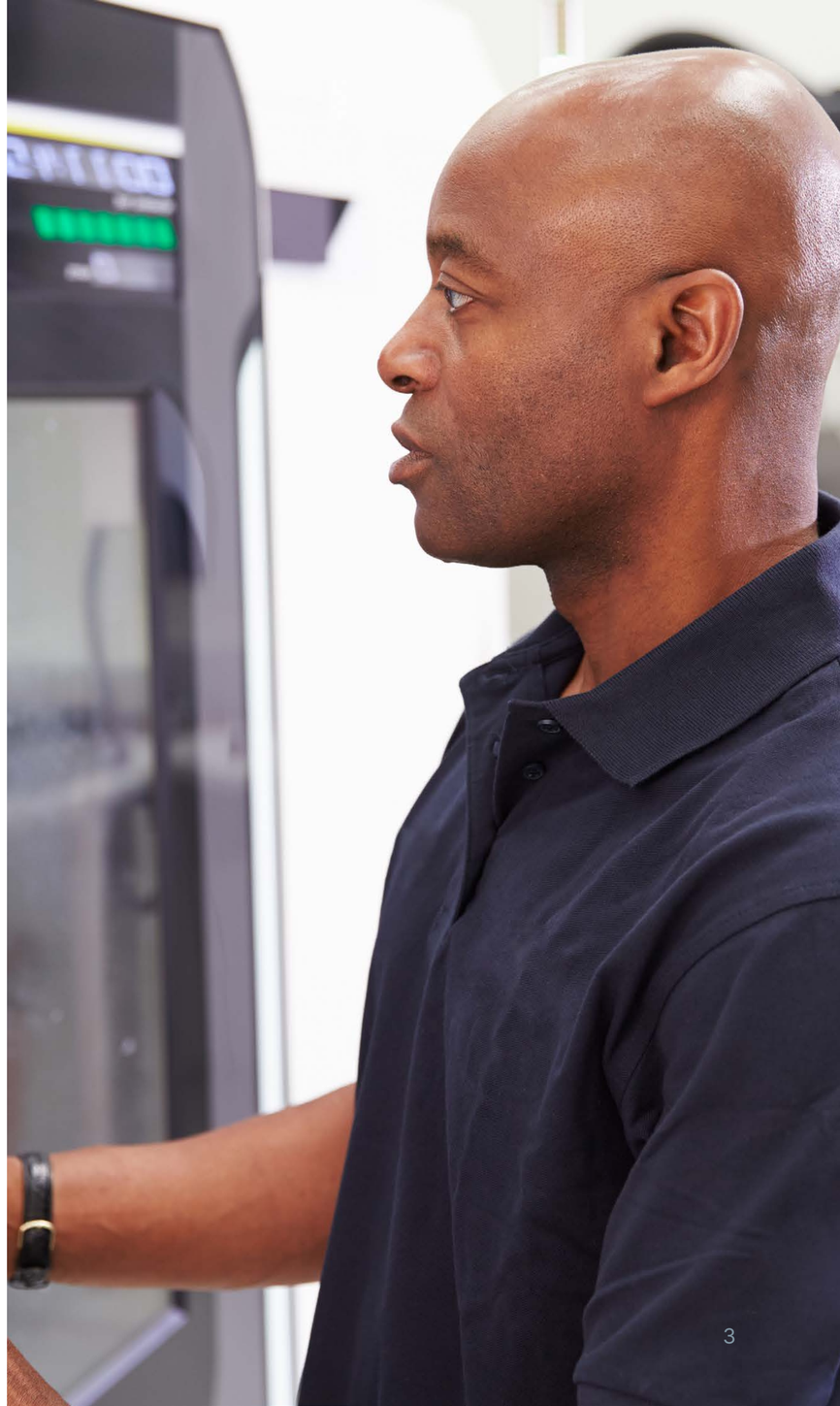
Manufacturing is changing. Again. For example in vehicles evolve from mechanical systems to software-defined platforms containing more than 100 million lines of code, traditional development approaches are no longer sufficient. Today's connected vehicles represent complex cyber-physical systems where software vulnerabilities can directly impact passenger safety, regulatory compliance, and brand reputation.

Manufacturing organizations must navigate an increasingly hostile threat landscape while meeting stringent regulatory requirements. Since 2019, manufacturing organizations have seen a 300-percent surge in cyberattacks, driven by increased connectivity and digitalization.[1] Additionally, manufacturers face losses of up to $2 million per cyberattack; downtime costs alone can range from $200,000 to $2 million per incident.[2]

DevOps provides the framework to address these challenges by integrating security throughout the software development lifecycle. However, generic DevOps solutions fail to address manufacturing's unique requirements: real-time safety constraints, complex supply chains, legacy system integration, and rigorous compliance mandates.

This ebook guides leaders through the strategic implementation of manufacturing-focused DevOps practices that accelerate innovation while maintaining the security and safety standards that define industry excellence.

1 Hoxhunt, Top Cybersecurity Threats in the Manufacturing Industry 2025, Dec. 20, 2024
2 Tech Informed, Manufacturers face losses up to $2m per cyberattack as IT/OT convergence heightens cybersecurity risks, Feb. 24, 2024



The imperative for secure software development in manufacturing

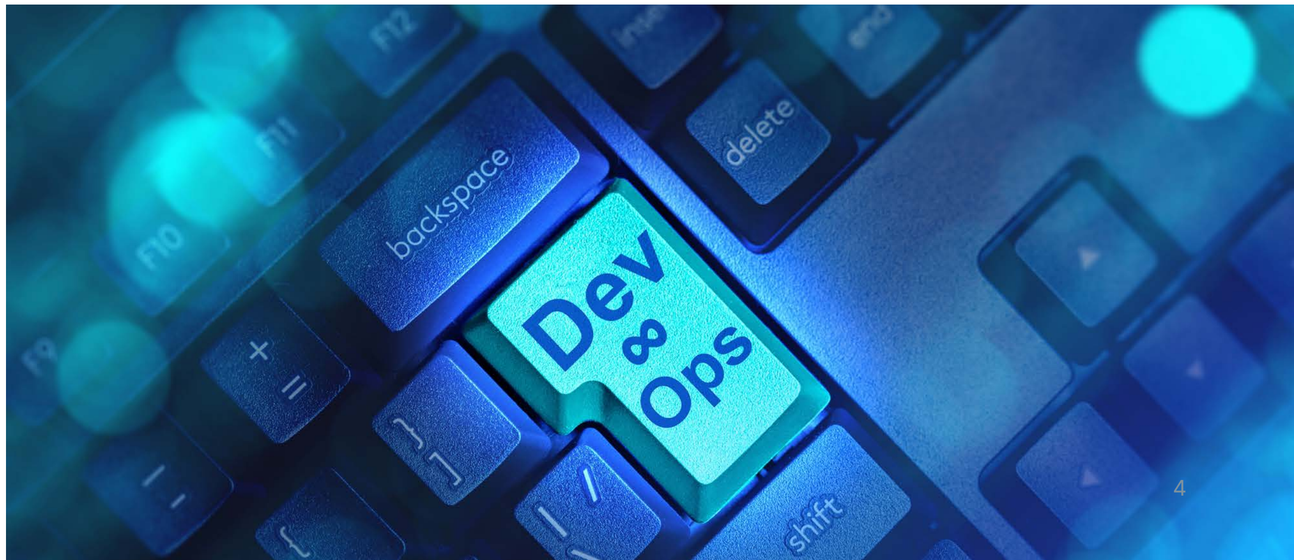
The manufacturing industry stands at a critical inflection point. The threat landscape targeting manufacturing has intensified dramatically. Cybercriminals increasingly view connected vehicles as attractive targets, exploiting vulnerabilities in infotainment systems, telematics, and over-the-air update mechanisms. Recent attacks have demonstrated how adversaries can remotely access vehicle systems, steal personal data, or even compromise critical safety functions.

Specifically for the automotive industry, as vehicles evolve from mechanical systems to software-defined platforms, the traditional boundaries between hardware and software development are disappearing. DevOps—the practice of integrating development and operations teams to accelerate software delivery while maintaining quality—has become essential for manufacturing companies navigating this digital transformation.

In the modern, connected vehicle ecosystem, a single line of code can impact passenger safety, regulatory compliance, and brand reputation. Manufacturing software now controls everything from engine management to autonomous driving systems, making security not just a feature but a fundamental requirement.

The stakes are higher than ever: a cybersecurity vulnerability in a vehicle's software can affect millions of cars globally, potentially leading to recalls, regulatory penalties, and safety incidents.

This reality demands a new approach to software development—one where security is embedded throughout the entire software development lifecycle (SDLC), not bolted on as an afterthought. DevOps provides the framework to achieve this integration, enabling manufacturing organizations to deliver secure, compliant software at the speed required by today's competitive market while maintaining the safety standards that define the industry.



How DevOps transforms manufacturing software development

The manufacturing sector presents unique challenges that distinguish it from traditional software industries. Understanding these distinctions is crucial for successfully implementing DevOps in manufacturing environments.

Legacy system challenges compound these complexities. Manufacturing companies must modernize decades-old ECU-based architectures while maintaining backward compatibility and security. This often involves integrating new DevOps practices with existing development tools, testing frameworks, and deployment systems that weren't designed for continuous integration and delivery.

Vehicle connectivity has fundamentally changed the software development paradigm. Modern vehicles contain dozens of electronic control units (ECUs) running millions of lines of code, with infotainment systems, vehicle-to-everything (V2X) communication protocols, and cloud-connected services creating an expanded attack surface. DevOps practices must account for this distributed architecture, ensuring secure communication between components while maintaining real-time performance requirements.

Cyber-physical risks elevate the importance of secure software development beyond typical IT security concerns. In manufacturing, software vulnerabilities can directly impact passenger safety—a reality that demands rigorous testing, validation, and deployment practices.

DevOps pipelines must incorporate safety-critical testing methodologies and fail-safe mechanisms that traditional web development rarely requires.

Compliance requirements add layers of complexity that generic DevOps solutions often overlook. Standards like UNECE WP.29 mandate cybersecurity management systems throughout the vehicle lifecycle, while ISO/SAE 21434 requires systematic approaches to cybersecurity engineering. Manufacturing DevOps platforms must provide automated compliance checking, audit trails, and documentation generation to meet these evolving regulatory frameworks.

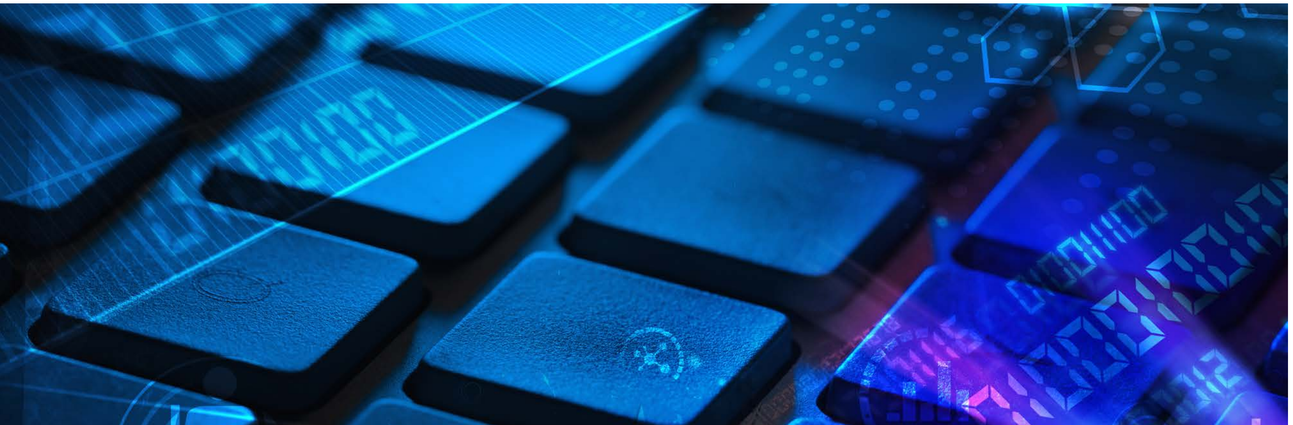
The transformation requires manufacturing organizations to rethink their entire software development approach, from initial design through production deployment and ongoing maintenance.

The UNECE World Forum for Harmonization of Vehicle Regulations (WP.29) is a unique worldwide regulatory forum within the institutional framework of the UNECE Inland Transport Committee.

Challenges of implementing DevOps in the manufacturing industry

Adopting DevOps in manufacturing environments presents distinct obstacles that require strategic planning and executive commitment to overcome.

Cultural shift represents perhaps the most significant challenge. Manufacturing organizations have traditionally operated with clear boundaries between hardware and software teams, with development cycles measured in years rather than weeks. DevOps demands cross-functional collaboration, shared responsibility for security, and acceptance of iterative development approaches. Engineering leaders must champion this cultural transformation, demonstrating how DevOps principles can enhance rather than compromise the rigorous quality standards that define manufacturing excellence.



Resource constraints particularly affect cybersecurity expertise. While manufacturing companies excel at mechanical and electrical engineering, many lack deep cybersecurity knowledge specific to software development. The shortage of professionals who understand both manufacturing requirements and modern security practices creates bottlenecks in DevOps implementation. Organizations must invest in training existing staff or recruiting specialized talent—both expensive and time-consuming propositions.

Complex infrastructure adds technical challenges that pure software companies rarely encounter. Manufacturing DevOps must seamlessly integrate hybrid cloud environments with on-premises systems and embedded platforms. This tri-modal architecture requires sophisticated orchestration, monitoring, and security controls that maintain performance while ensuring compliance across diverse computing environments.

Regulatory compliance introduces constraints that can seem antithetical to DevOps speed and flexibility. Manufacturing software must meet strict documentation requirements, undergo extensive validation testing, and maintain detailed audit trails. Balancing these compliance needs with DevOps principles requires careful platform selection and process design to automate compliance activities without sacrificing development velocity.

These challenges are surmountable with proper planning, but they require manufacturing-specific solutions rather than off-the-shelf DevOps platforms designed for general software development.

Key features of a manufacturing-focused DevOps platform

Manufacturing organizations require specialized DevOps capabilities that address the unique security, compliance, and operational requirements of the industry.

Automated security testing forms the foundation of manufacturing DevOps platforms. Static analysis tools must understand embedded C/C++ codebases, real-time operating systems, and safety-critical software patterns common in industrial environments. Dynamic analysis capabilities should simulate attack scenarios specific to manufacturing systems, such as manipulation of industrial communication protocols, wireless communication interception, and sensor spoofing. These tools must integrate seamlessly with existing manufacturing development environments and provide actionable remediation guidance.

CI/CD **integration** for manufacturing requires specialized pipeline configurations that accommodate lengthy testing cycles, hardware-in-the-loop validation, and phased deployment strategies. Pipelines must support parallel testing across multiple vehicle configurations, automated regression testing for safety-critical functions, and controlled rollout mechanisms that can halt deployments if anomalies are detected. Integration with manufacturing-specific tools like MATLAB/Simulink, industrial automation software, or proprietary testing frameworks is essential to ensure a smooth workflow.

Supply chain security addresses the complex ecosystem of third-party components that comprise modern vehicle software. Platforms must provide software bill of materials (SBOM) generation, vulnerability scanning for open-source components, and license compliance checking. Given the long lifecycle of industrial equipment and software, these tools must track component vulnerabilities across years of deployment and provide automated alerts when new threats emerge.

End-to-end encryption capabilities must protect sensitive data throughout the development and deployment lifecycle. This includes securing update mechanisms, protecting diagnostic data, and ensuring secure communication between cloud services and vehicle systems. Encryption implementations must meet manufacturing-specific standards while maintaining the performance requirements of real-time systems.

Threat intelligence provides manufacturing-specific vulnerability monitoring and incident response capabilities. These systems should track emerging threats targeting industrial control systems, provide early warning of attacks affecting similar platforms, and offer forensic capabilities for security incident investigation.

Regulatory compliance tools are essential for automating the documentation and audit processes required by manufacturing standards. These capabilities should generate compliance reports, maintain audit trails, and provide dashboard visibility into compliance status across the entire software development lifecycle.

Best practices for selecting the right DevOps platform

Choosing an appropriate DevOps platform requires careful evaluation of manufacturing-specific requirements and organizational readiness factors.

Assess development workflows by conducting a comprehensive audit of existing software development processes, security practices, and compliance procedures. Identify specific gaps where manual processes create bottlenecks, security vulnerabilities go undetected, or compliance requirements add unnecessary overhead. This assessment should map current toolchains, integration points, and skill gaps to inform platform selection criteria. Document quantitative metrics like deployment frequency, lead time for changes, and mean time to recovery to establish baseline measurements for improvement.

Industry expertise should be a primary selection criterion when evaluating DevOps platform vendors. Manufacturing requirements differ significantly from general software development, and platforms designed for web applications often lack critical manufacturing-specific features. Prioritize vendors with demonstrated experience in manufacturing cybersecurity, understanding of industry standards and existing integrations with manufacturing development tools. Evaluate vendor case studies, customer references, and technical documentation to verify manufacturing domain expertise.

Compliance alignment requires detailed evaluation of each platform's ability to support current and emerging regulatory requirements. Verify that platforms provide built-in support for UNECE WP.29 cybersecurity management systems, automated compliance checking, and documentation generation for regulatory audits. Consider future regulatory trends and ensure selected platforms can adapt to evolving compliance requirements without requiring complete replacement.

Scalability considerations must account for the unique scaling patterns of manufacturing software development. Unlike web applications that scale primarily through increased transaction volume, manufacturing software must scale across industrial equipment models, geographic markets, and regulatory jurisdictions. Evaluate platforms' ability to support diverse deployment targets, multi-region compliance requirements, and the long-term maintenance needs of software that may remain active for decades.

Developer-friendly tools ensure successful adoption by engineering teams accustomed to manufacturing-specific development environments. Platforms should integrate seamlessly with existing IDEs, testing frameworks, and version control systems. Evaluate learning curves, documentation quality, and the availability of training resources to minimize disruption during platform adoption.

"DevOps adoption in manufacturing is accelerating, with organizations reporting up to a 30% reduction in deployment times and a 40% improvement in collaboration and process efficiency when platforms are tailored to manufacturing's unique needs." - Veritis, 2025

Case study: Major Automotive Systems Manufacturer

Challenge

This major manufacturer must ensure that its twice-yearly releases of PLM software are non-disruptive and bug-free for users.

Solution

This major automotive systems manufacturer implemented OpenText™ DevOps Cloud:

- Delivers applications faster
- Prioritizes quality
- Optimizes experience
- Boosts collaboration

Outcomes

- Automated more than 90% of functional tests
- Enabled significant reuse of testing components
- Saved time and effort while providing complete visibility of status

“Working with OpenText technologies enables me to meet my primary requirements: I can automate the GUI, execute tests, analyze root causes, quickly identify where I have issues, and create good dashboards. The key thing is that I never lose visibility.”

Spokesperson, Major Automotive Systems Manufacturer

Read their story ›

Prepare for the future of DevOps in manufacturing

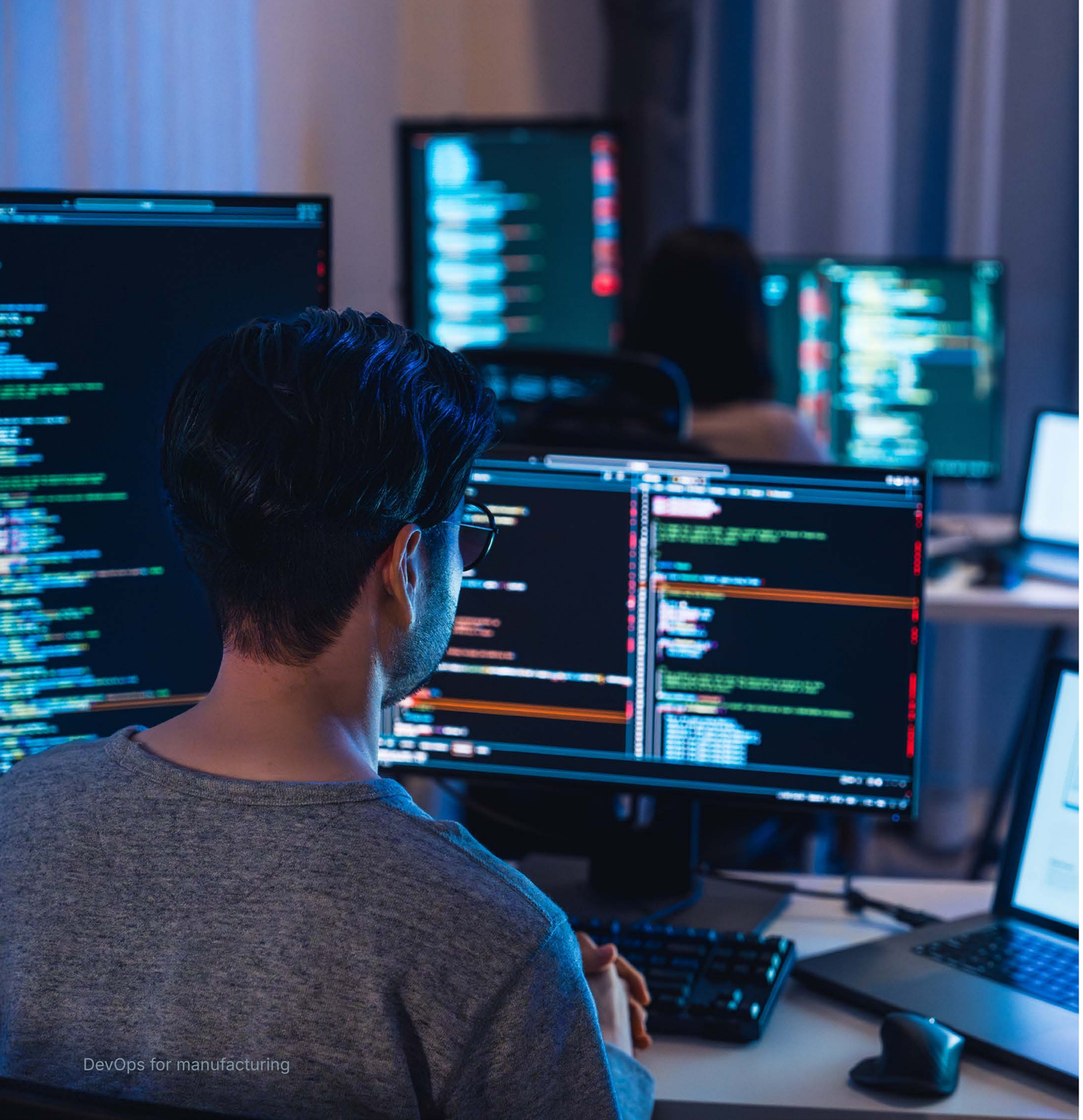
The evolution of manufacturing technology continues to accelerate, demanding forward-thinking approaches to DevOps implementation that anticipate emerging trends and requirements.

AI-driven **security** represents the next frontier in manufacturing cybersecurity. Machine learning algorithms will increasingly analyze code patterns, network traffic, and system behaviors to identify sophisticated threats that traditional signature-based detection systems miss. Manufacturing DevOps platforms will incorporate predictive analytics to identify potential vulnerabilities before they're exploited, automated threat hunting capabilities that continuously monitor systems for anomalous behavior, and AI-powered incident response systems that can isolate and remediate security breaches in real time. However, implementing AI security solutions in manufacturing requires careful consideration of explainability requirements, as regulatory standards often demand clear audit trails for security decisions.

Zero trust **architecture** principles will become fundamental to manufacturing cybersecurity as connectivity expands and attack surfaces grow. Rather than relying on network perimeters for security, zero trust assumes that threats exist both inside and outside traditional boundaries. Manufacturing DevOps must evolve to support continuous authentication and authorization for all system components, micro-segmentation of vehicle networks to limit attack propagation, and real-time risk assessment for every communication between vehicle systems and external services. This shift requires DevOps platforms to integrate identity management, policy enforcement, and continuous monitoring capabilities throughout the software development and deployment lifecycle.

Edge computing will transform how manufacturing software is developed, deployed, and maintained capabilities. DevOps platforms must support distributed deployment models where critical functions execute locally in equipment and products while maintaining secure communication with cloud-based services. This evolution demands new approaches to testing, monitoring, and updating software across thousands of edge devices with varying connectivity patterns and computational constraints.

Increased automation will reduce manual intervention in security processes while improving consistency and effectiveness. Future manufacturing DevOps platforms will feature self-healing systems that automatically patch vulnerabilities, adaptive testing frameworks that evolve based on emerging threat patterns, and autonomous deployment systems that can roll back updates if security anomalies are detected. This automation must maintain human oversight for safety-critical decisions while eliminating routine manual tasks that introduce human error and slow development cycles.



DevOps: A fundamental shift

The manufacturing industry's digital transformation demands a fundamental shift in how organizations approach software development and security. DevOps provides the framework to deliver secure, compliant software at the speed required by today's connected ecosystem while maintaining the safety standards that define manufacturing excellence.

Success requires more than selecting the right technology platform—it demands organizational commitment to cultural change, investment in specialized expertise, and strategic alignment between development practices and business objectives. Manufacturing organizations that embrace DevOps principles while addressing industry-specific requirements will gain competitive advantages through faster innovation cycles, improved security posture, and more efficient compliance processes.

The journey toward manufacturing DevOps maturity is challenging but essential. As cybersecurity threats continue to evolve and regulatory requirements become more stringent, organizations that delay adoption risk falling behind competitors who have successfully integrated security throughout their development lifecycles.

DevOps implementation checklist for manufacturing organizations

Conduct a comprehensive security assessment

- Audit existing development workflows and identify security gaps
- Document current compliance processes and identify automation opportunities
- •Evaluate existing toolchains for DevOps integration readiness
- Assess team skills and identify training requirements

Establish executive sponsorship and change management

- Secure leadership commitment for cultural transformation initiatives
- Define success metrics and ROI expectations for DevOps adoption
- Develop communication strategies to address resistance to change
- Allocate dedicated resources for DevOps implementation and training

Select a manufacturing-focused DevOps platform

- Prioritize vendors with proven manufacturing industry expertise
- Verify compliance support for UNECE WP.29, ISO/SAE 21434, and relevant standards
- Evaluate integration capabilities with existing development tools and infrastructure
- Assess scalability for future software requirements and global deployment needs

Implement phased deployment strategy

- Begin with non-safety-critical systems to minimize risk during initial implementation
- Establish automated testing and security scanning capabilities before expanding scope
- Create detailed runbooks and incident response procedures for production deployments
- Plan for gradual expansion to safety-critical systems with appropriate validation processes

DevOps implementation checklist for manufacturing organizations

Develop ongoing monitoring and improvement processes

- Implement continuous monitoring for security vulnerabilities and compliance status
- Establish regular reviews of DevOps metrics and process effectiveness
- Create feedback mechanisms to capture lessons learned and drive continuous improvement
- Plan for platform evolution to support emerging technologies and regulatory requirements

Build a long-term DevOps maturity roadmap

- Define a multi-year vision for manufacturing DevOps capabilities and organizational maturity
- Plan integration of emerging technologies like AI-driven security and zero-trust architecture
- Establish partnerships with technology vendors and industry organizations for knowledge sharing
- Develop internal expertise through training, certification, and strategic hiring initiatives

Ready to accelerate your manufacturing DevOps journey?

Transform your organization’s software development capabilities with a manufacturing-focused DevOps platform designed specifically for the unique requirements of connected equipment and regulatory compliance.

Start your DevOps journey today! Get a free trial or request a consultation to discuss your specific challenges and explore how DevOps can address your organization’s security, compliance, and innovation objectives.

Additional resources

Take the click tour See DevOps Aviator in action as it helps an engineer using OpenText™ Core Software Delivery Platform generate test cases instantly in just a few clicks.

Read another customer story Find out how others are succeeding with OpenText DevOps Cloud.

About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit opentext.com.

opentext.com | X (formerly Twitter) | LinkedIn | CEO Blog

opentext™