2ND ANNUAL

2025

State of Industrial DevOps Report

Navigating OT Cyber Complexity, Embracing AI, and Accelerating Profitable Growth

COPIA

Building on the work of pioneers like Dr. Suzette Johnson and Dr. Robin Yeman, **Industrial DevOps** is a methodology for applying Lean, Agile, and DevOps principles to the planning, development, manufacturing, and serviceability of cyber-physical systems.

This is achieved through a technical foundation of **Industrial Code Lifecycle Management (ICLM)** — the systematic management of all industrial automation code as a critical asset.

By embedding practices like **automated backup and recovery, version control, and collaborative change management** directly into the operational technology environment, Industrial DevOps increases resilience, de-risks operations, accelerates development velocity, and improves overall system quality."

LETTER FROM COPIA'S CEO & FOUNDER

A year ago, we launched our inaugural report, driven by the conviction that traditional Operational Technology (OT) management was unsustainable against rising complexity and cyber threats. That first report clearly showed the manufacturing and distribution sectors were ready for the transformative power of Industrial DevOps.

This 2nd annual report builds on that foundation. We again surveyed 200 senior leaders and decision-makers, from C-Suite to Management, across diverse industries to gauge progress, identify trends, and understand evolving challenges and opportunities. This year's data reveals not just continued momentum, but significant maturation in the adoption and understanding of Industrial DevOps principles, alongside distinct variations in perspective across organizational hierarchies.

A few key takeaways from this year's report:

- C-Suite respondents report the highest average cost of downtime at $4.29 million/hour.
- Downtime attributed to industrial code remains significant at 45%.
- Cybersecurity breaches are the #1 cause of unplanned downtime for the 2nd year in a row
- 92% are invested or plan to invest in Industrial DevOps within the next 11 months.
- 89% agree that integrating AI into Industrial DevOps platforms will unlock new levels of efficiency, productivity, and innovation.

This report provides industry leaders with the critical data and nuanced understanding necessary to navigate strategic decisions, benchmark progress, and ultimately, accelerate the journey towards a more secure, efficient, and innovative future for industrial operations.

Sincerely,
Adam Gluck
CEO & Founder Copia Automation

Welcome to the 2nd Annual State of Industrial DevOps Report!

Building on the findings of our inaugural report, this 2nd Annual State of Industrial DevOps Report tracks the continued evolution and adoption of Industrial DevOps across the industrial landscape. While benchmarking remains the core focus, this year's report also includes a new dimension based on seniority to provide a richer understanding of how perspectives on challenges, priorities, and solutions differ across organizational levels.

Increased connectivity, the proliferation of smart devices, and the ongoing shift towards software-defined operations present immense opportunities but also **significant challenges related to OT cybersecurity, adoption of AI, and the impact on the workforce**, just to name a few.

The data included in this report reveals that Industrial DevOps offers a crucial bridge between Information Technology (IT) and Operational Technology (OT), enabling better collaboration, governance, and security in the management of the industrial code that powers modern production.

20
25

TABLE OF CONTENTS

EXECUTIVE SUMMARY

There is a critical "perception gap" between senior leadership and operational management. This disconnect in how challenges are viewed, prioritized, and valued creates significant strategic misalignments that can undermine the success of technology initiatives.

This year's data, now analyzed by seniority, uncovers a nuanced and complex landscape. The key findings highlight a fundamental difference in perspective across the organizational chart:

THE COST OF DOWNTIME ESCALATES WITH SENIORITY:

The most compelling finding is that the perceived financial and strategic impact of downtime increases significantly with seniority. C-Suite executives view operational disruptions as a far more costly and enterprise-threatening issue than their operational managers do, leading to different levels of urgency and investment priorities.

DIVERGENT VIEWS ON RISK AND ROOT CAUSE:

This perception gap extends to the root causes of downtime. Senior leaders point to systemic issues like industrial code and cybersecurity as primary drivers, whereas managers on the floor are more focused on immediate hardware failures and human error. This creates a fundamental disagreement on where to focus resources for remediation.

MISALIGNED PRIORITIES ON AI AND SECURITY:

While enthusiasm for AI is universal, leaders are focused on mitigating strategic risks like data security, while managers prioritize tactical, operational efficiencies. Similarly, OT cybersecurity is a top-tier concern for the C-Suite but a much lower priority for managers, exposing a potential blind spot in organizational defense.

This report provides the critical data and nuanced understanding necessary for leaders to identify these internal gaps, foster alignment, and build a unified strategy to accelerate their journey toward a more secure, efficient, and innovative future.

INTRODUCTION

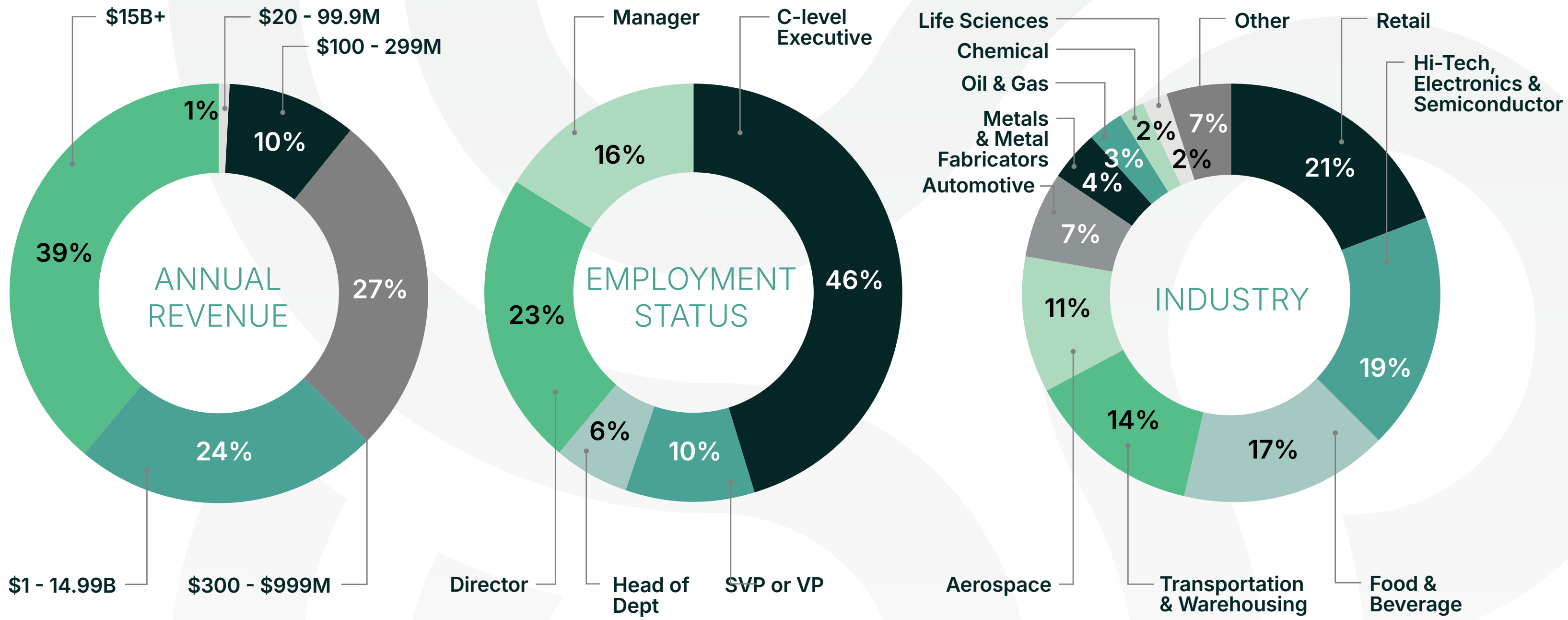
THE INDUSTRIAL DEVOPS IMPERATIVE IN 2025

This industry report from Copia Automation, in association with Sapio Research, is based on a survey of **200 executives and senior managers** actively involved in their organizations' operational technology and industrial automation strategies.

Participants spanned C-Suite (46%), SVP/VP/Head of Department (16%), Director (22%), and Manager (16%) roles.

The companies surveyed are predominantly large enterprises, with **63% reporting over $1 billion in annual revenue.**

Industries represented include **Retail (20%), Hi-Tech/Electronics/Semiconductor (19%), and Food and Beverage (17%).**



Demographic/Firmographic Raw Data

01

INDUSTRIAL DEVOPS: HOW DID WE GET HERE AND WHERE ARE WE GOING?

To understand the future, we must look at the past. We explore how Industrial DevOps evolved from the separate paths of factory automation and modern software development practices.

TIMELINE SUMMARY:
FROM GANTT TO WATERFALL TO INDUSTRIAL DEVOPS

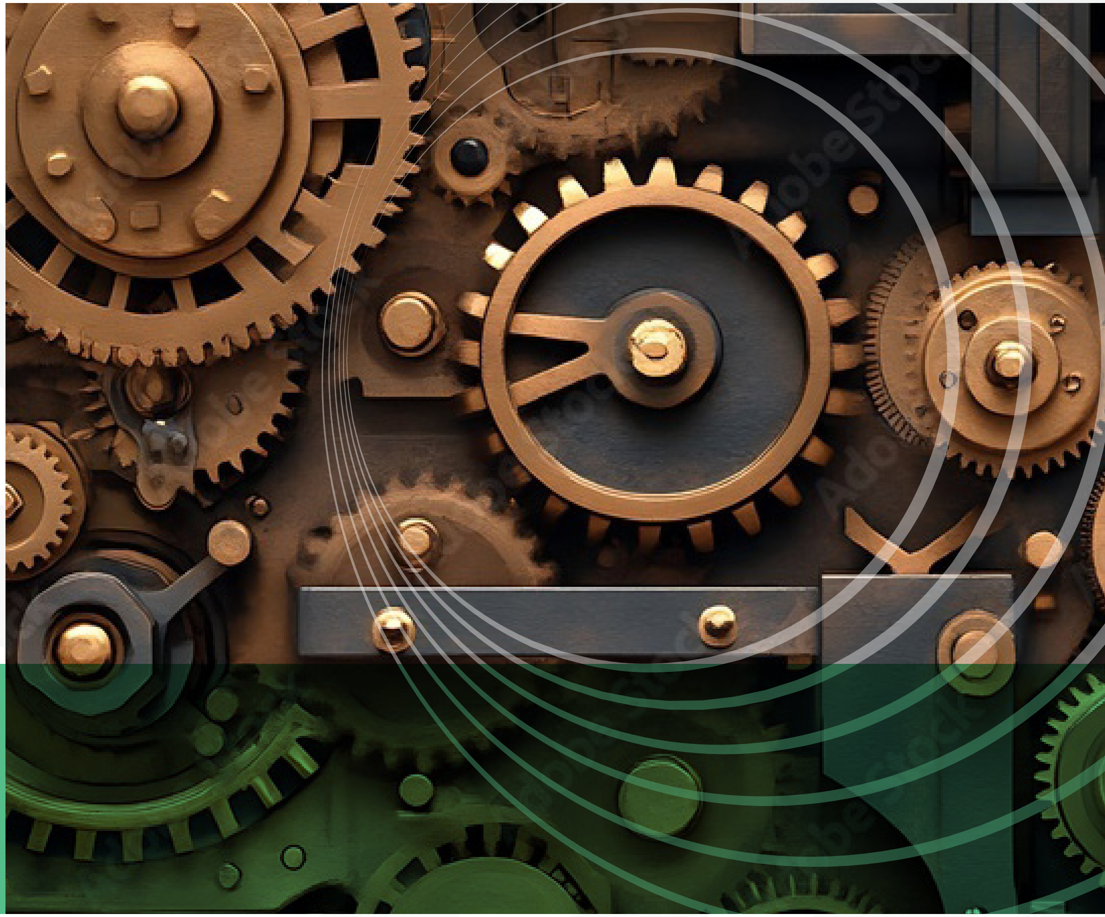
01

Understanding the state of Industrial DevOps requires appreciating a 200-year evolution in process. This journey began with foundational technologies like Eli Whitney's **interchangeable parts (1798)** and early management tools like the **Gantt Chart (c. 1910)**, which sought to visualize and control production. These innovations culminated in Henry Ford's **moving assembly line (1913)**, the ultimate expression of Mass Production — a model that prioritized volume above all.

The first great philosophical shift came in the **1950s** when **W. Edwards Deming** taught Japan's industrial leaders that quality comes from improving the process, not from final inspection. His data-driven, people-centric approach, paired with Toyota's development of **Lean Manufacturing**, created a new model focused on eliminating waste, building in quality, and fostering continuous improvement.

This cycle of innovation then crossed over into the digital realm. Software's initial "Waterfall" methodology adopted the linear model of mass production, using tools like the Gantt chart to plan its rigid, sequential steps. The inflexibility of this approach directly spurred the creation of **Agile (2001)** and **DevOps (2009)**, movements that reintegrated the people-centric, quality-first principles of Lean and Deming.

Today, this journey comes full circle with **Industrial DevOps**, which applies these mature, battle-tested software practices back to the factory floor. Understanding this history — of how we learned to pair people, process, and technology to accelerate production with quality — is essential for contextualizing the trends, challenges, and opportunities presented in this second annual report.



TIMELINE

THE EVOLUTION OF PROCESS AND PRODUCTION

Craft & Early Mechanization

Late 1800s
Craft Production: The dominant model where skilled artisans create custom goods individually. It is slow, expensive, and dependent on individual skill.

1798
Interchangeable Parts: Eli Whitney champions the concept of standardized, interchangeable parts, providing the technological foundation for mass production

The Mass Production Age

1901
The Stationary Assembly Line: Ransom E. Olds pioneers the use of a stationary assembly line, where workers with specialized tasks move from one station to the next

c. 1910s
The Gantt Chart: Henry Gantt develops his chart to visually manage schedules, bringing a new level of predictability to complex projects in the craft and early industrial era

1913
The Moving Assembly Line & Mass Production: Henry Ford introduces the moving assembly line, bringing the work to the worker and perfecting the high-volume, low-variety model of mass production

The Lean & Quality Revolution

c. 1930s
The 5 Whys Technique: Sakichi Toyoda at Toyota develops the 5 Whys, a root-cause analysis tool that empowers people to solve problems and becomes a cornerstone of Lean

c. 1950s-1970s
Lean Manufacturing & The Toyota Production System: Influenced by Deming and internal innovators, Toyota perfects its production system, creating the Lean philosophy focused on eliminating waste, ensuring quality, and increasing flexibility

1950s
Dr. W. Edwards Deming in Japan: Dr. Deming introduces his philosophy of statistical process control, quality improvement, and the Plan-Do-Check-Act cycle to Japanese industry, becoming a key catalyst for their manufacturing miracle

Software-Defined Operations

Late 1980s-1990s
Global Adoption of Lean: After decades of Japanese success, Western companies begin studying their methods. The term "Lean" is coined in 1988, and the 1990 book "The Machine That Changed the World" exposes these principles to a mass global audience, sparking widespread adoption.

c. 1970s
The Waterfall Methodology: The software industry formalizes the Waterfall model, mirroring the linear, sequential mindset of the mass production assembly line

2001
The Agile Manifesto: Reacting to Waterfall's rigidity, software developers formalize principles of iterative development, collaboration, and responding to change

DevOps Era Begins

c. 2010s-Present: DevOps principles are adapted back to the manufacturing and industrial world to manage complex cyber-physical systems, completing the 200-year cycle of innovation

2009
The Birth of DevOps: The DevOps movement begins, aiming to bridge the gap between software development and IT operations by applying Agile and Lean principles to the entire delivery pipeline

THE DEVOPS ERA BEGINS

2009
DevOps is born. Allspaw and Hammond give their talk at Velocity and Patrick Debois launched the very first DevOpsDays Conference

2013
The Phoenix Project by Gene Kim, Kevin Behr, and George Spafford further builds the case for widespread DevOps adoption

2013
The State of DevOps Report is first published

2016
Gartner predicts mainstream adoption of DevOps

2017
Forrester calls this "the year of DevOps"

2020
Copia founded to bring DevOps practices to Industrials, establishing the first company dedicated to Industrial DevOps

2023
Industrial DevOps: Build Better Systems Faster by Dr. Suzette Johnson and Robin Yeman is published on the practice and impact of Industrial DevOps

2024
Frost & Sullivan include Industrial DevOps in Top 15 Growth Opportunities in Industrial Automation

2024
The 1st Annual State of Industrial DevOps Report is released

2025
Industry Analyst community begins to recognize Industrial DevOps as necessary for OT Cyber resilience

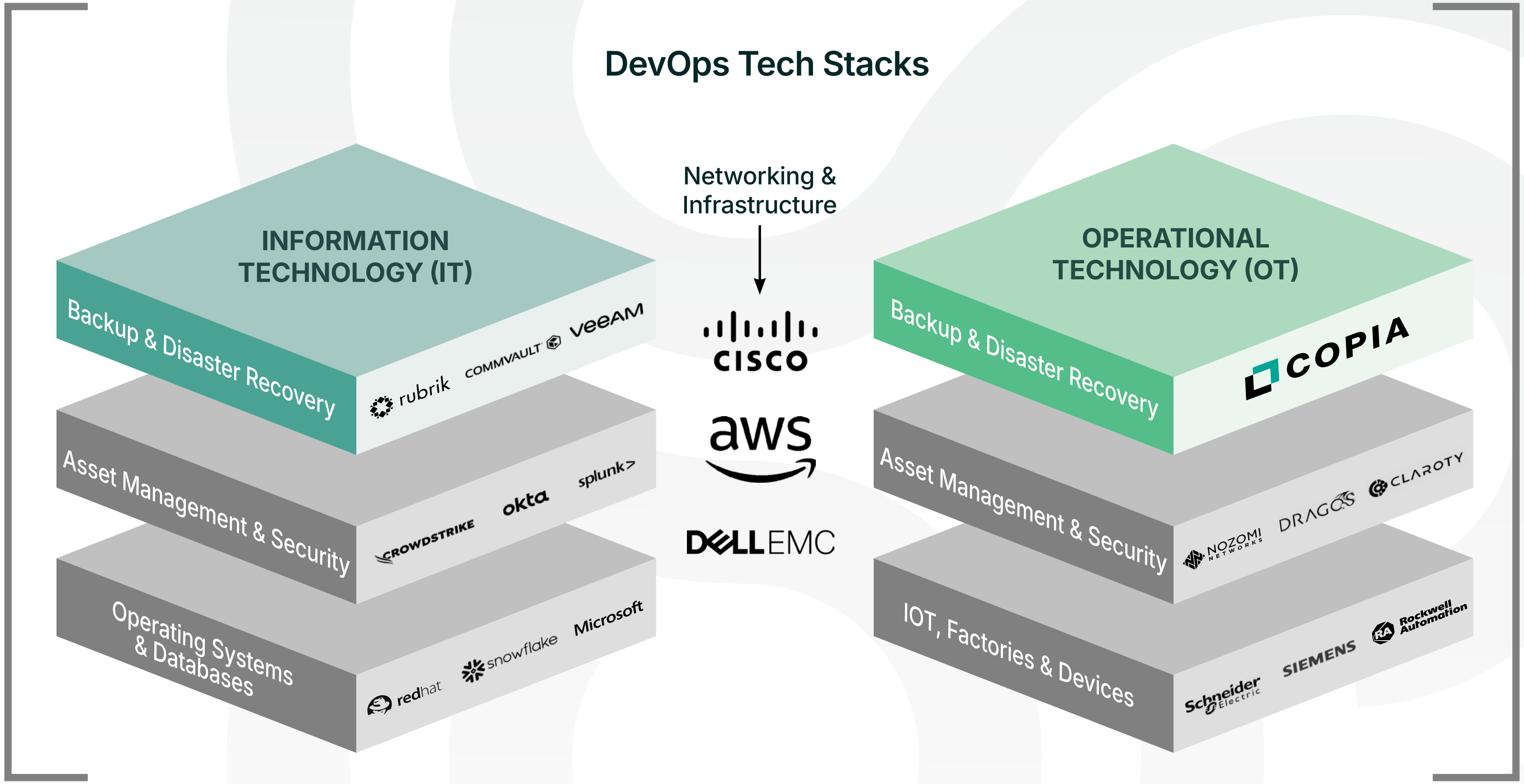
2025
The 2nd Annual State of Industrial DevOps Report is released

2025
Frost & Sullivan publishes 1st ever competitive benchmark guide and market analysis reports for Industrial DevOps

TO UNITE IT AND OT, IT’S IMPORTANT TO UNDERSTAND THEIR TECHNOLOGY STACKS

To unite IT and OT, it’s important to understand their technology stacks because, in essence, **they are speaking two different languages.** IT speaks a language of dynamic scalability and rapid deployment, fluent in cloud, containers, and CI/CD pipelines. OT speaks a language of unwavering reliability and physical safety, rooted in the deterministic logic of PLCs and HMIs.

Without a **universal translator**, requests for ‘more agility’ from IT can sound like ‘more risk’ to OT. Industrial DevOps acts as that translator, **creating a shared vocabulary and toolset** that allows both teams to work toward the common goals of efficiency and security.



DevOps Tech Stacks

INFORMATION TECHNOLOGY (IT)

Backup & Disaster Recovery

Asset Management & Security

Operating Systems & Databases

Networking & Infrastructure

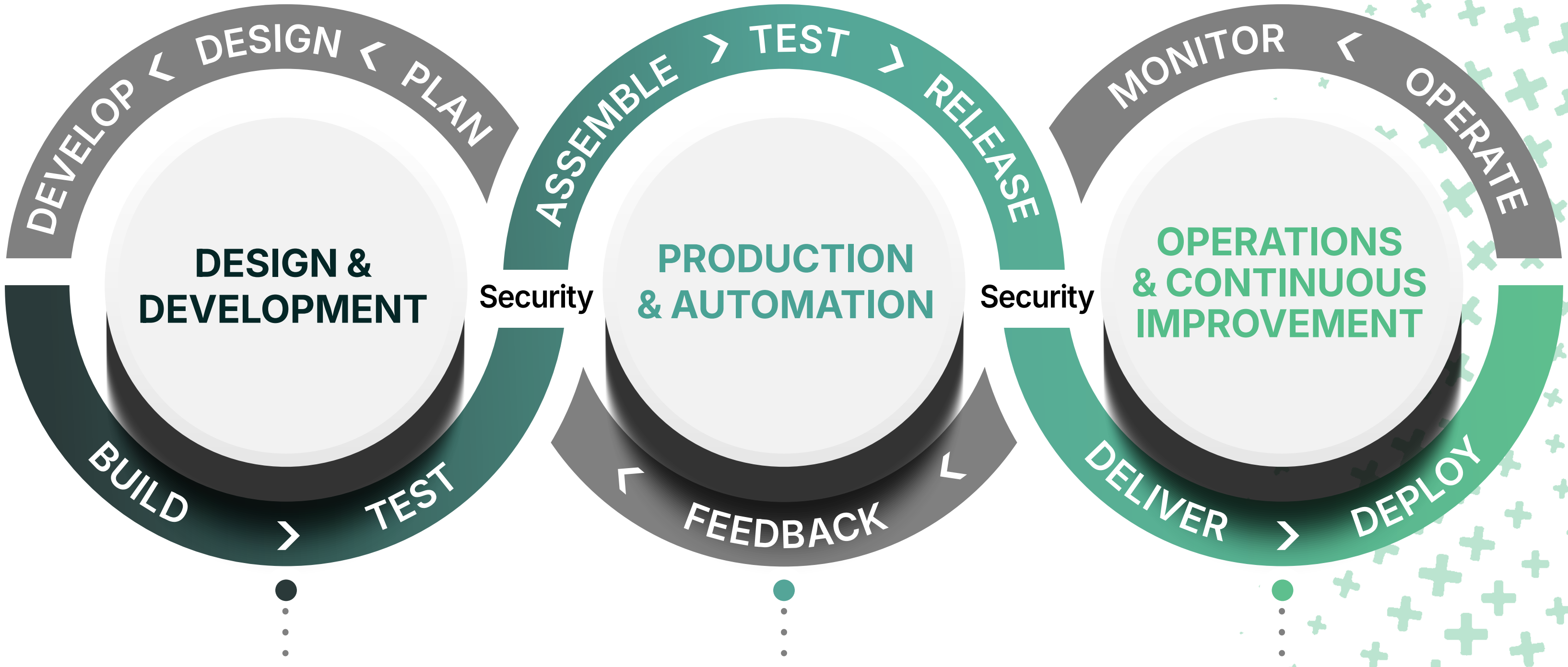
OPERATIONAL TECHNOLOGY (OT)

Backup & Disaster Recovery

Asset Management & Security

IOT, Factories & Devices

INDUSTRIAL DEVOPS PROCESS



The start and end of success in automation and what everything else is built upon.

Automate only where it makes sense. If a person can beat the automation, have a person do it.

Refine the approach through data analysis, trial and error, and willingness to adapt the process based on the outcomes.

> In traditional DevOps, the feedback loop is about data and application performance. In Industrial DevOps, that loop runs through a factory. The process is fundamentally altered to manage the immense responsibility that comes when digital changes have direct, physical consequences on the plant floor.

Dr. Suzette Johnson, Robin Yeman (PhD)
co-author of Industrial DevOps: Build Better Systems Faster

INDUSTRIAL CODE LIFECYCLE MANAGEMENT (ICLM): MOVING FROM ACCEPTANCE TO ACTION

01

Today's Reality

18 Locations

- ~2079 PLCs
- ~2114 Associated Devices
- **28 Controls Engineers / 75 Technicians**

PLC Vendors in Use:

- **Siemens (60%)** → TIA Portal v14 - v19
- **Rockwell (30%)** → Logix500, v16 - v33
- **Codesys (5%)**
- **Ladder Logic: 98%**

Manual Backups and Ad Hoc Version Control

3rd party issues (if one exists)

- Some auto-backups, but primarily Version Control

OT Cyber Vulnerability

- Incomplete asset inventories
- Unknown code changes
- Outdated backups
- Limited or no recovery plan

Today's Possibility

Cyber Resilience & Rapid Recovery

- **Live Asset Inventory:** A complete, accurate, and always-on view of every device and its status, supporting your...
- **Automated Backups:** A complete collection of automated cloud backups enabling your...
- **Rapid Recovery Plan:** Reduce Mean Time to Recovery (MTTR) from days or weeks to **minutes with files you can trust from a place you can access**

Centralization

- **18 Locations, ~4200 Devices, 103 Team Members** → All operating from a **single, centralized platform with...**
- **Automated Git-based Version Control:** Every code change is automatically backed up, versioned, and documented, giving you...
- **Golden Backups:** The latest and the correct version of code is always available for every single device.

Vendor-Agnostic Access & Control

- **Siemens, Rockwell, Codesys, etc.** → Seamlessly manage all projects in one environment, regardless of vendor or software version. Engineers have the right tools without the chaos, along with...
- **Modern Tools for All Code:** Empower engineers and technicians with visual code comparisons (diffs), streamlined code reviews, and a complete audit history for all IEC 61131-3 languages, including your 98% Ladder Logic!

02

DOWNTIME IN 2025: THE PERSISTENT AND EVOLVING TRILLION-DOLLAR CHALLENGE

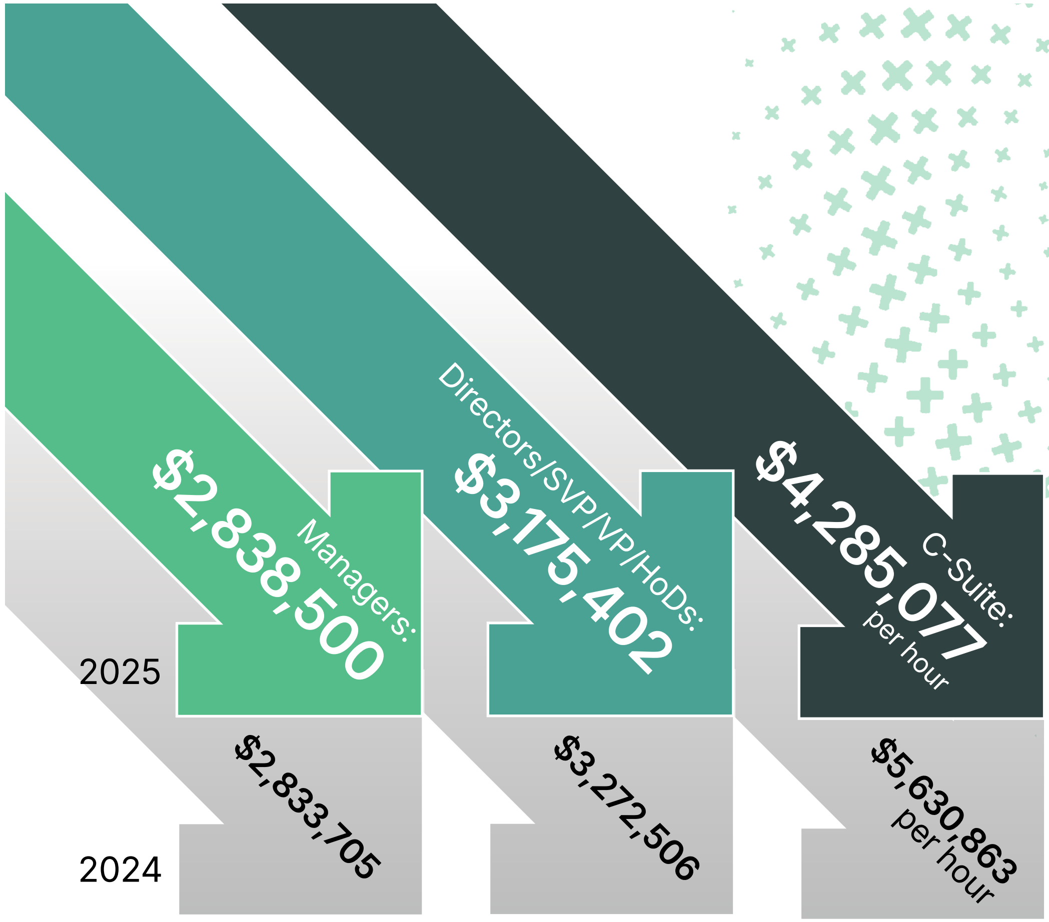
Downtime remains one of the most significant threats to profitability and operational stability. This section examines its current financial impact, primary culprits, and recovery practices, highlighting how perceptions and experiences differ across seniority levels.

THE SIGNIFICANT COST OF STOPPAGES: THE C-SUITE IS IN A DIFFERENT REALM

Divergence on the cost of downtime remains a critical finding, with C-Suite executives reporting 50% higher than Directors and Managers.

While a gap persists, the data shows a 23% year-over-year reduction in downtime costs from the C-Suite. This may indicate a reduction of **indirect costs** driven by investments in operational resilience and cybersecurity — core to Industrial DevOps — that are mitigating the financial fallout of disruptions.

Conversely, the stability of downtime costs at the operational level underscores their focus on **direct costs** like production loss and local repair costs, which are less susceptible to broad market or strategic changes.



17% SAID DOWNTIME COSTS

$10+ MILLION per hour

2025 average cost of downtime:
$3,627,053

2024 average cost of downtime:
$4,181,997

Q1. What do you estimate is the cost to your organization per hour of downtime? Select one. Base: 200

YOUR DOWNTIME PROBLEM? LOOK TO YOUR INDUSTRIAL CODE

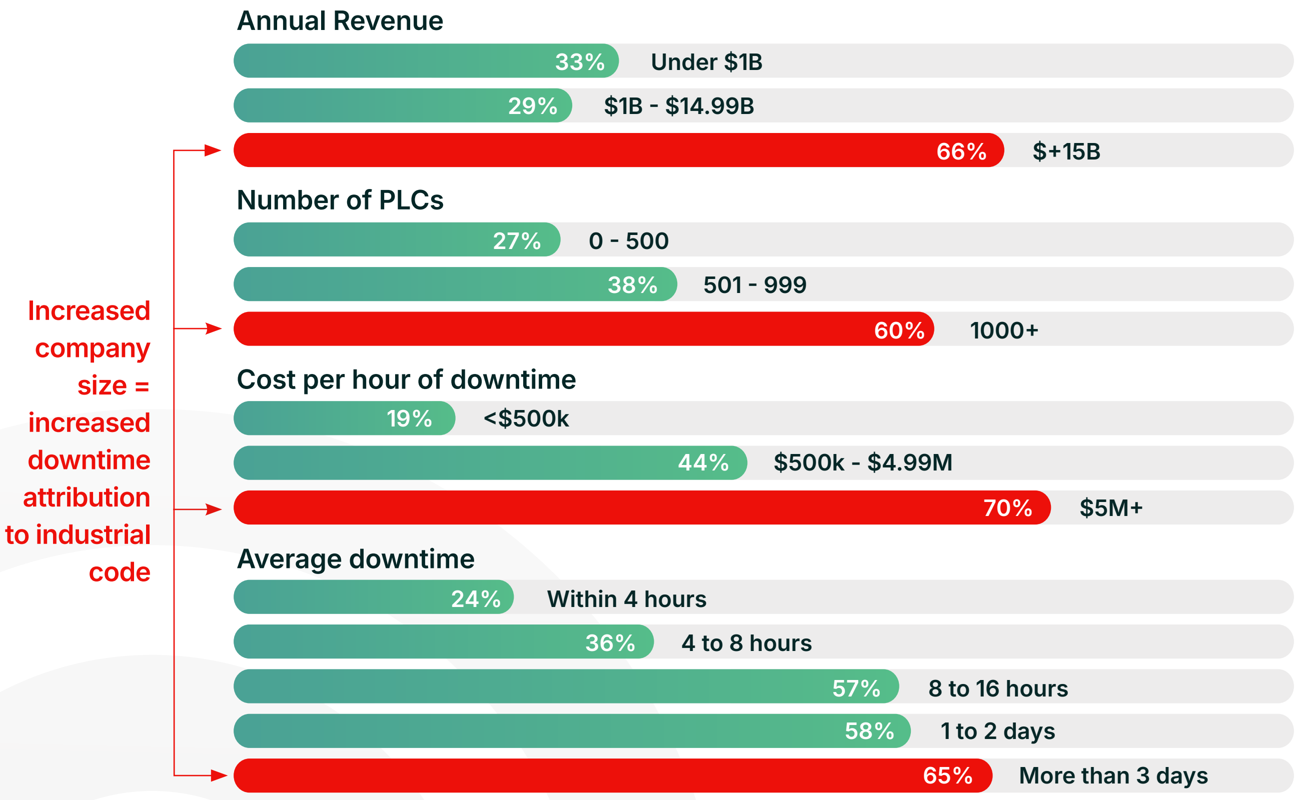
Industrial code remains a major factor in operational disruptions as 45% of total downtime (planned and unplanned) is attributed to issues related to industrial code. How is this possible?

Deeper in the data, we see that size and complexity is crippling large organizations within their operational technology environments. The largest organizations (+15B in revenue) say that industrial code factors into **a whopping 66% of downtime incidents.** This is repeated as we look at the highest amount of PLCs (60%), average duration of downtime (65%), and highest cost per hour of downtime (70%).

Based on this data, it can be inferred that complexity extends downtime incidents and places a greater attribution to industrial code management, testing, and deployment.

An additional divide here is by seniority, with C-Suite attributing 52% of downtime to industrial code vs. 30% cited by managers.

Percentage of Downtime Attributed to Industrial Code (Response by Segment and Size)

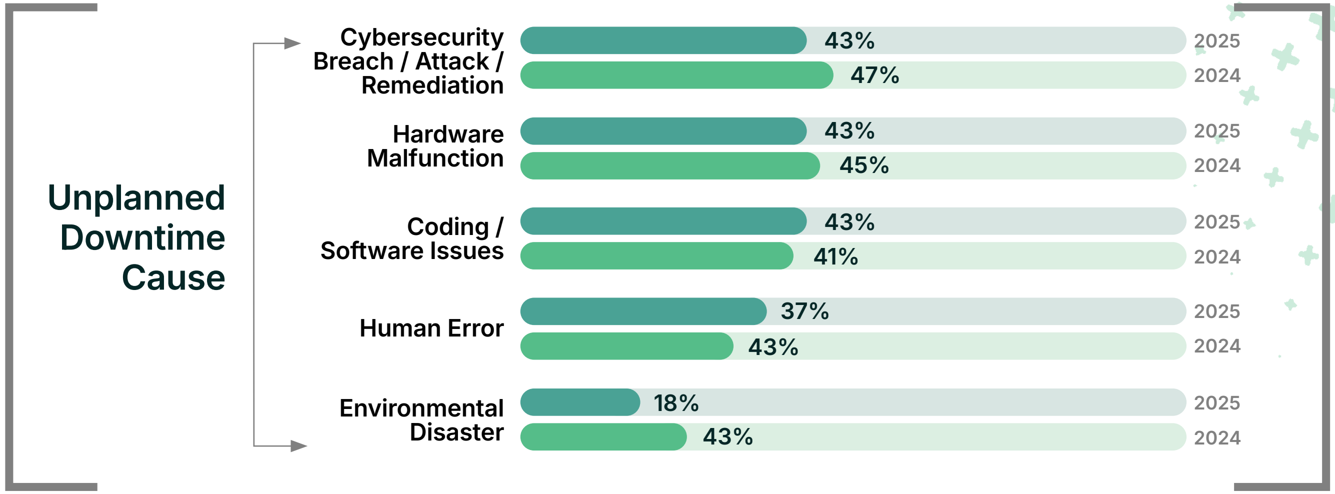


Q2. In the past year, what do you estimate is the percentage of your total downtime attributed to industrial code? Select one. Base: 200

CYBERSECURITY ISSUES INCREASE UNPLANNED DOWNTIME

For the 2nd year in a row, **cybersecurity** ranked as the #1 cause of **unplanned** downtime, although this year it tied with **hardware malfunction** and **coding / software issues**. While it's not surprising to see these as the top causes, it is surprising to see the extremely different perspectives of managers vs. C-Suite executives, ranking cybersecurity at 22% vs. 45% respectively.

This aligns with senior executives' broader responsibility for enterprise risk. Managers highest responses focused on daily operations and control, citing human error (50%) and hardware malfunction (50%) as the top areas of unplanned downtime.



Q3. Looking at periods of unintended downtime in the last year, what were the most common causes? Select up to two. Base: 200

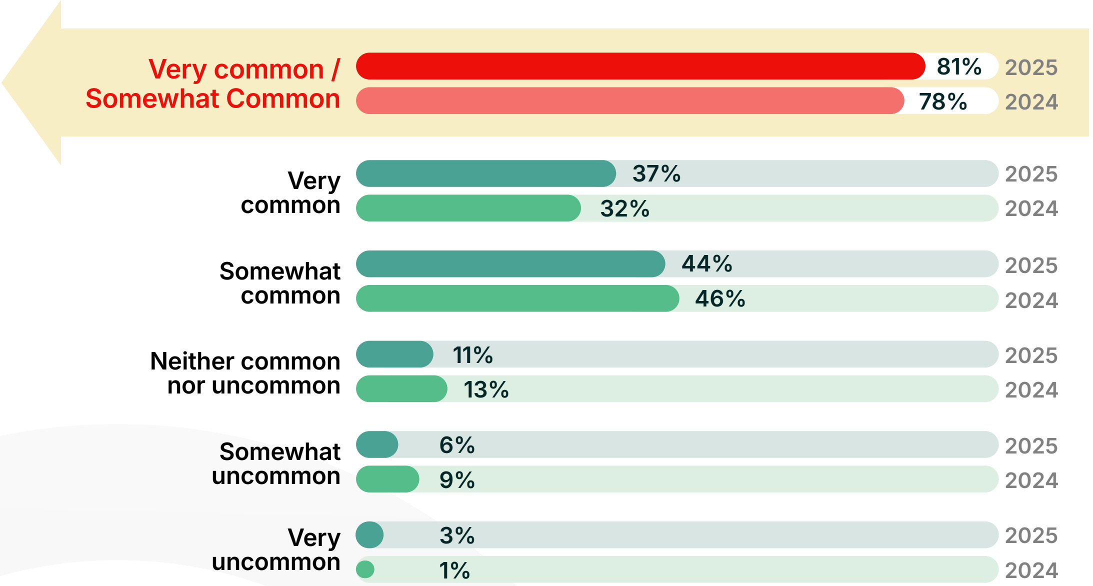
> Security leaders can no longer afford to treat OT as a black box they don't understand, or believe in mythical air-gaps from the internet protecting them from any potential threat. **Threat actors are investing time and resources into the targeting and exploitation of weaknesses in OT."**
>
> Claroty, Team82
>
> State of CPS Security 2025: OT Exposures

CAUSES OF TECHNICAL DEBT: QUICK FIXES VS. VALUE FIXES

While downtime numbers vary, every organization can agree on one thing: the less downtime the better. But at what cost?

This high number of ad hoc fixes year-over-year is a signal that organizations leaning into the "quick fix" are increasing their technical debt by not addressing the core problem.

How common are Ad Hoc Fixes?



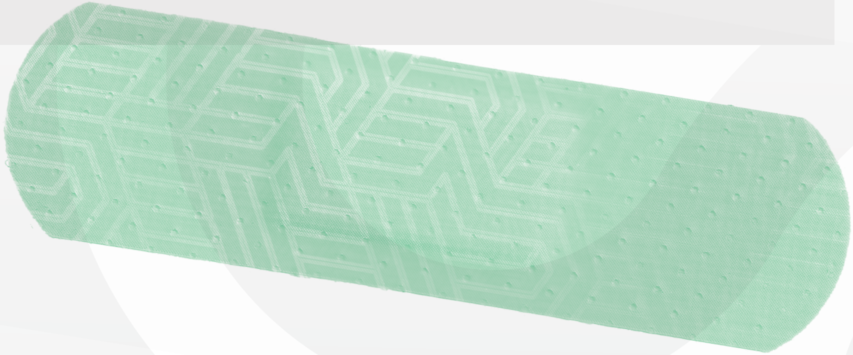
Q4a. In your estimation, how common are ad hoc fixes to industrial code on the factory floor that are aimed at minimizing or recovering from downtime? Select one. Base: 200

PERCEPTION VS. REALITY:
DOES AD HOC FIX FOLLOW-UP REALLY HAPPEN?

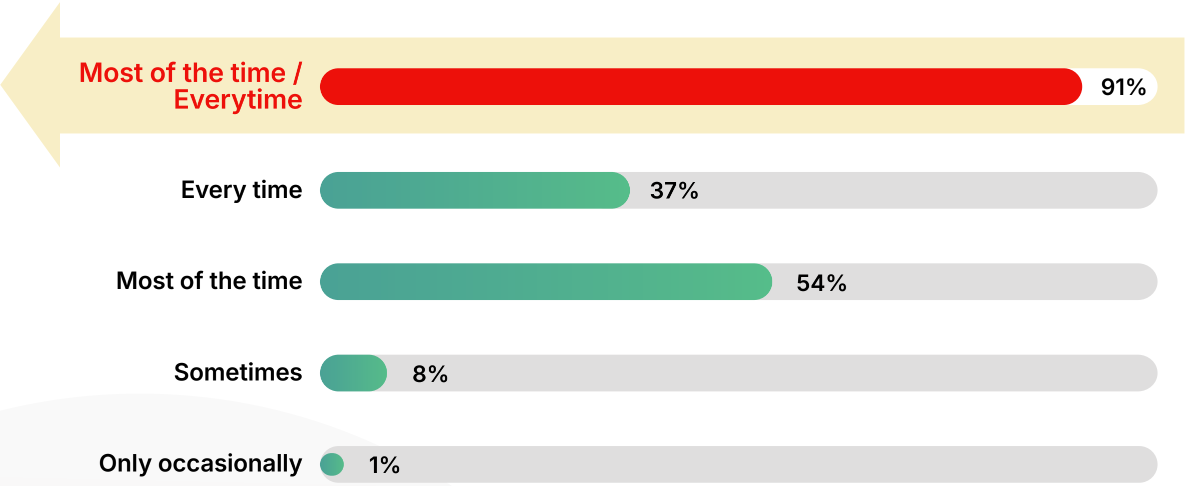
This year's survey added a new question to understand how frequently those ad hoc fixes received follow-up.

When asked how often respondents followed up to fix the problem addressed by the ad hoc fix, 37% said that they do it every time and another 54% said most of the time.

This is surprising when looking at other data like the time to recover from downtime incidents (**28hrs**), time spent debugging code each month (**48hrs**), and percent of time spent remediating cybersecurity issues (**69%**).



Frequency of follow-up to permanently fix problem Ad Hoc fix addressed



Q4b. How frequently do you or the responsible team follow up on these ad hoc fixes to fully address and fix the problem? Select one. Base: 200

Q5. On average, how long does it typically take to resolve a downtime event attributed to industrial code changes, confusion over code, lack of visibility into industrial code, and issues with PLC programming? Select one. Base: 200

Q10. On average, how much time do you estimate that you and your team spend debugging code per month? Select one. Base: 200

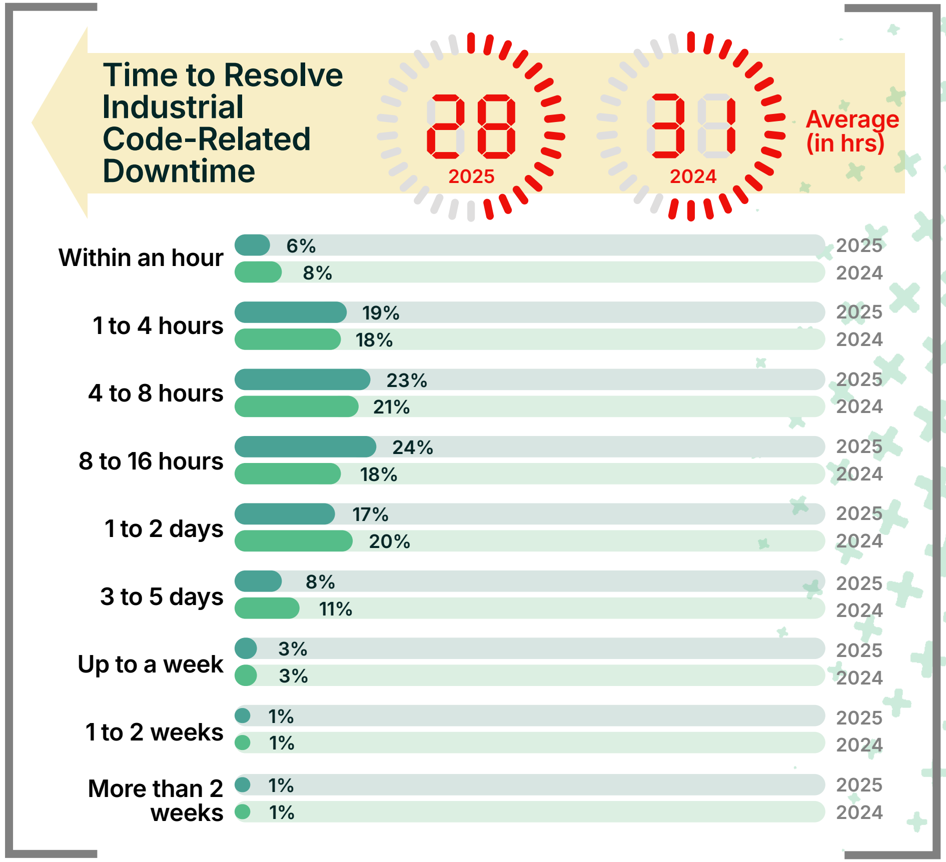
Q20k. In your opinion, how frequently do teams that adopt Industrial DevOps practices spend time on the following activities? Base: 200

COMPOUNDING CODE AND CASCADING FIXES

02

With the increase of devices in operational technology (OT) environments, the code that runs those devices has triggered a compounding effect.

Once an industrial code downtime event happens, the time to recover (28hrs) shines a light on the reality of industrial code management practices and **the barrier they pose to rapid recovery.**



Q5. On average, how long does it typically take to resolve a downtime event attributed to industrial code changes, confusion over code, lack of visibility into industrial code, and issues with PLC programming? Select one. Base: 200

> **A quick win adds value; a quick fix adds time.**
>
> **Invest in solutions that enhance, not just extend."**

Jeff Winter

Industry 4.0 & Digital Transformation Enthusiast

“

This 50% perception gap on the cost of downtime is critical. If those holding the purse strings see a much larger fire, their willingness to invest in comprehensive solutions like Industrial DevOps will differ significantly from those who, while still seeing a costly problem, might underestimate its total strategic impact.

Adam Gluck, CEO & Founder of Copia Automation

03

REDEFINING THE PLANT FLOOR: THE IMPACT OF AI AND CYBERSECURITY ON OT

We analyze how teams are leveraging AI for new efficiencies while building critical defenses to protect the newly intelligent and connected factory from emerging cyber threats.

THE EXPLODING ATTACK SURFACE: A CRISIS OF SCALE

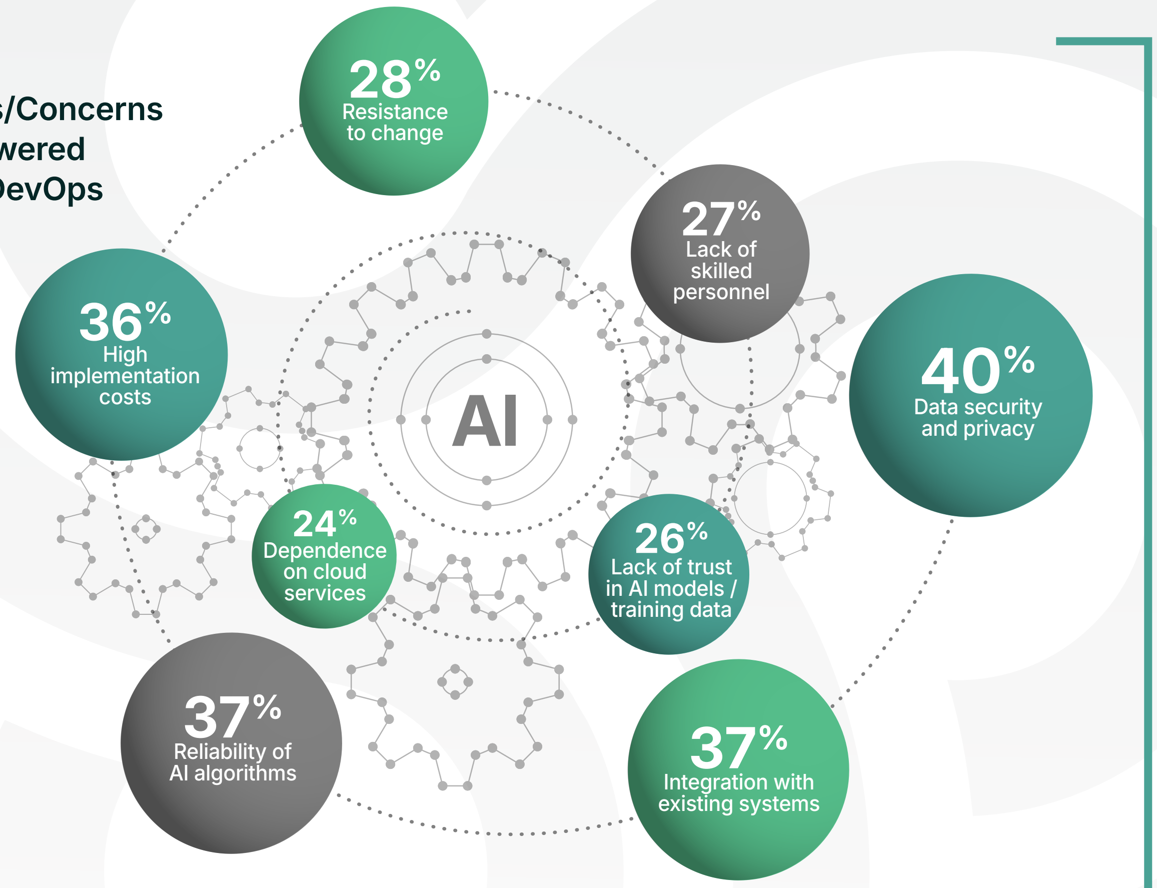
While leaders are optimistic about AI, their enthusiasm is dwarfed by the scale of the risk they now face.

The modern plant floor is a sprawling digital ecosystem, with the average enterprise organization managing over 2,000 PLCs and another 2,100 associated devices like cameras, sensors, and drives.

With this number nearly doubling every five years according to IoT Analytics, the attack surface is expanding at an unmanageable rate. This is why data security and privacy (40%) is the top concern in AI adoption. It's no longer a theoretical risk; it's the mathematical certainty of trying to secure thousands of interconnected points of failure.

The promise of an intelligent factory is entirely dependent on the ability to first see, and then defend, this vast and complex asset inventory from a legion of emerging threats.

Challenges/Concerns with AI-Powered Industrial DevOps



S8. In your best estimation, how many PLCs do you have? Select one. Base: 200

S9a. How many associated devices do you have with those PLCs ? Select one. Base: 200

Q24. What potential challenges or concerns do you foresee with the adoption of AI-powered Industrial DevOps? Select all that apply. Base: 200

MANUAL OVERSIGHT IS OBSOLETE: DEMANDING MODERN SYSTEMS FOR CYBER DEFENSE

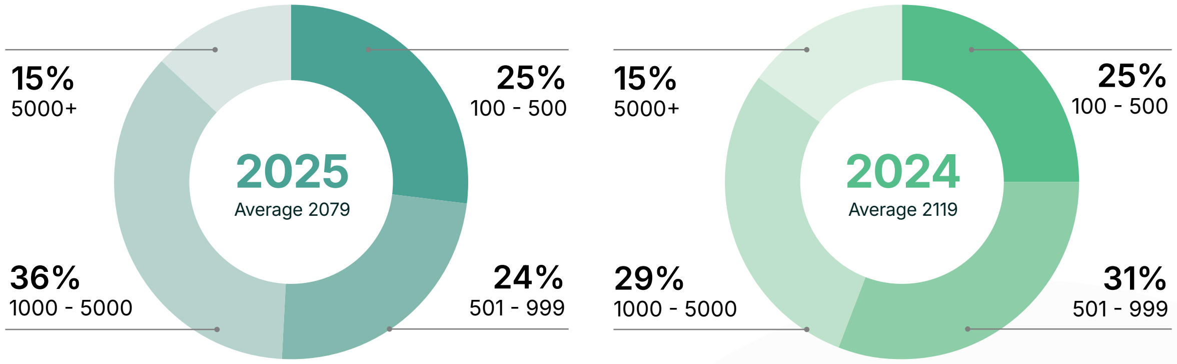
In an environment with over 4,000 devices from an average of **6 different PLC vendors**, manual asset tracking and security oversight is no longer feasible.

This operational reality is precisely why teams are demanding modern tools equipped with AI as their first line of defense. The most-valued AI feature is not about efficiency; it's a plea for control: **AI-driven version control with change detection and anomaly alerts (49%)** (data and more on next page).

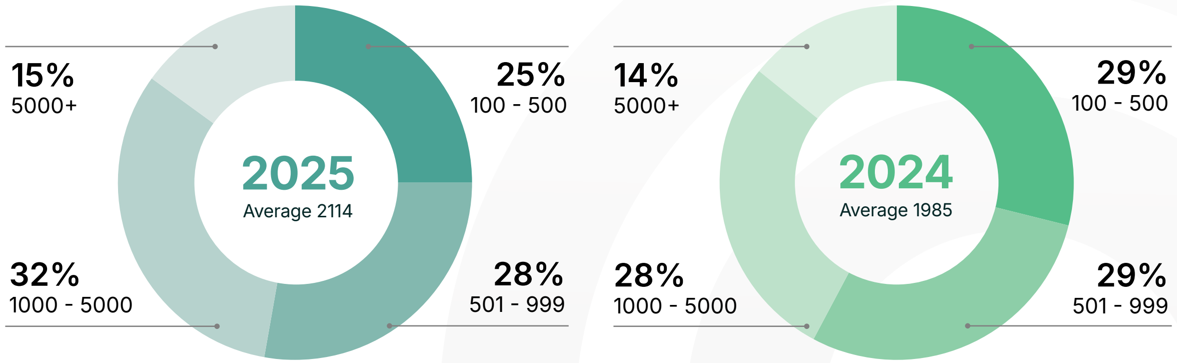
It's impossible for human teams to manually monitor every code change across thousands of PLCs or vet every new device. They need intelligent systems to act as a vigilant, automated guardian that can spot a single unauthorized change or a new vulnerability across a complex, multi-vendor landscape.

This isn't just a feature request; **it's a fundamental requirement for operating securely at scale.**

PLCs per Organization



Associated Devices Per Organization



PLC Brands in Operation Per Organization

2025
Average
6.02

2024
Average
5.61

S8. In your best estimation, how many PLCs do you have? Select one. Base: 200
S9a. How many associated devices do you have with those PLCs ? Select one. Base: 200
S10. In your best estimation, how many different brands of PLCs do you have in your organization? Select one. Base: 200
Q23. Which of the following AI-driven features in Industrial DevOps would be most valuable to your operations? Select all that apply. Base: 200

THE INTEGRITY PARADOX: DISTRUSTING THE TOOLS YOU NEED THE MOST

The challenge of securing the plant floor is magnified by its complexity in the dangerously fragmented operational technology (OT) space, and this fuels the top concerns around AI: the **reliability of its algorithms (37%)** and a fundamental **lack of trust in its models (26%)**.

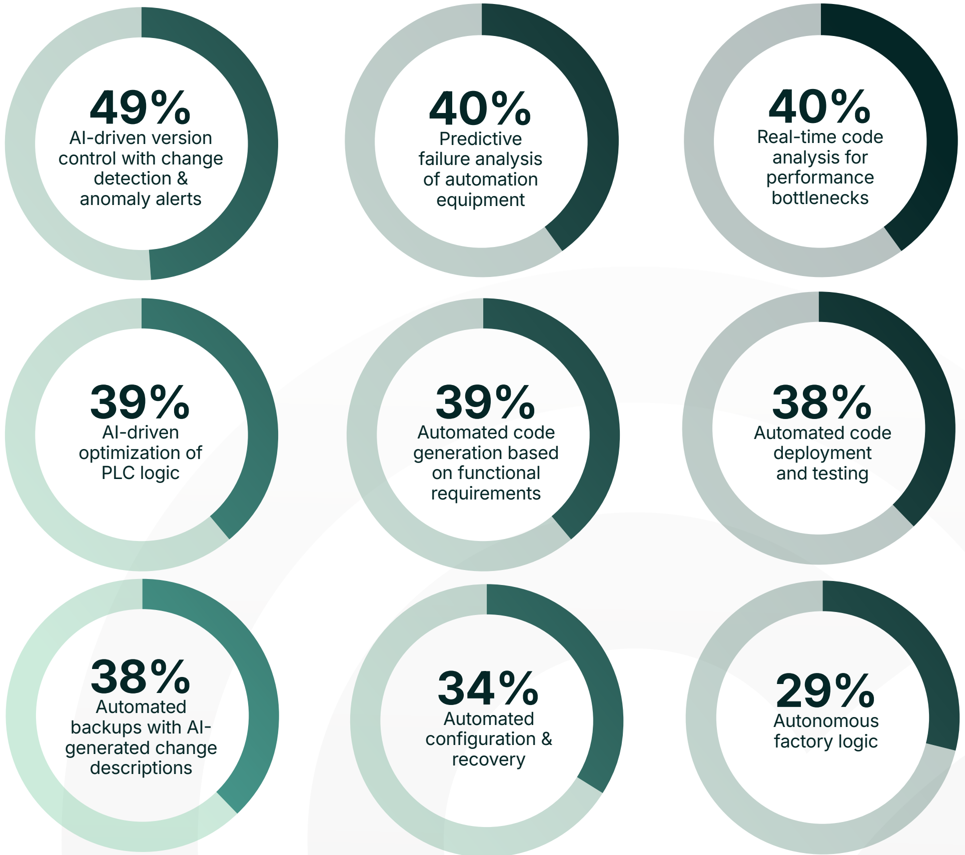
If a human engineer struggles to master this complexity, how can a single AI be trusted to do so without error?

And yet, herein lies the integrity paradox. Despite this deep-seated concern, teams are simultaneously demanding AI features that require an intimate understanding of their most critical systems.

A remarkable **40% want AI for real-time code analysis**, and **39% seek AI-driven optimization of PLC logic**. They are asking AI not just to stand guard at the perimeter, but to enter the inner sanctum and actively improve core production code.

This reveals that the "crisis of trust" is not a wholesale rejection of AI, but an **urgent demand for trustworthy AI** — one that is transparent, reliable, and proven to master the multi-vendor reality of the modern plant floor.

Most Valuable AI-driven Industrial DevOps Features for Operations



Q23. Which of the following AI-driven features in Industrial DevOps would be most valuable to your operations? Select all that apply. Base: 200

DROWNING IN DATA: FIND THE THREAT WITHIN

With thousands of devices generating millions of data points, the biggest security threat is no longer just an external attacker; it's a critical event getting lost in the noise, which can enable infiltration across your operational technology (OT) environment.

An accidental misconfiguration by an untrained employee — a major concern cited as **lack of skilled personnel (27%)** — is nearly impossible to find in a sea of routine alerts.

This is the new reality of internal risk: a single line of flawed code on one of 2,000 PLCs can halt production or open an external door to your "secure" environment, but finding it is like searching for a needle in a haystack.

This makes AI-powered anomaly detection indispensable. It provides the only practical way to filter that noise, instantly flagging the one event that deviates from the established baseline, whether it's a malicious instruction or a costly human error.

Q24. What potential challenges or concerns do you foresee with the adoption of AI-powered Industrial DevOps? Select all that apply. Base: 200

> **Weaponizing PLCs to Achieve Initial Access.** Currently, there are hundreds of thousands of ICS devices exposed to the internet, as determined by most public internet scanning services, including Shodan and Censys. These internet-facing devices usually lack security and allow anyone to access them, modify parameters, and even alter their behavior and logic via download procedures."

Claroty,
Evil PLC Attack: Weaponizing PLCs | Claroty

THE CONFIDENCE PARADOX:
HIGH CONFIDENCE MASKS HIDDEN RISKS

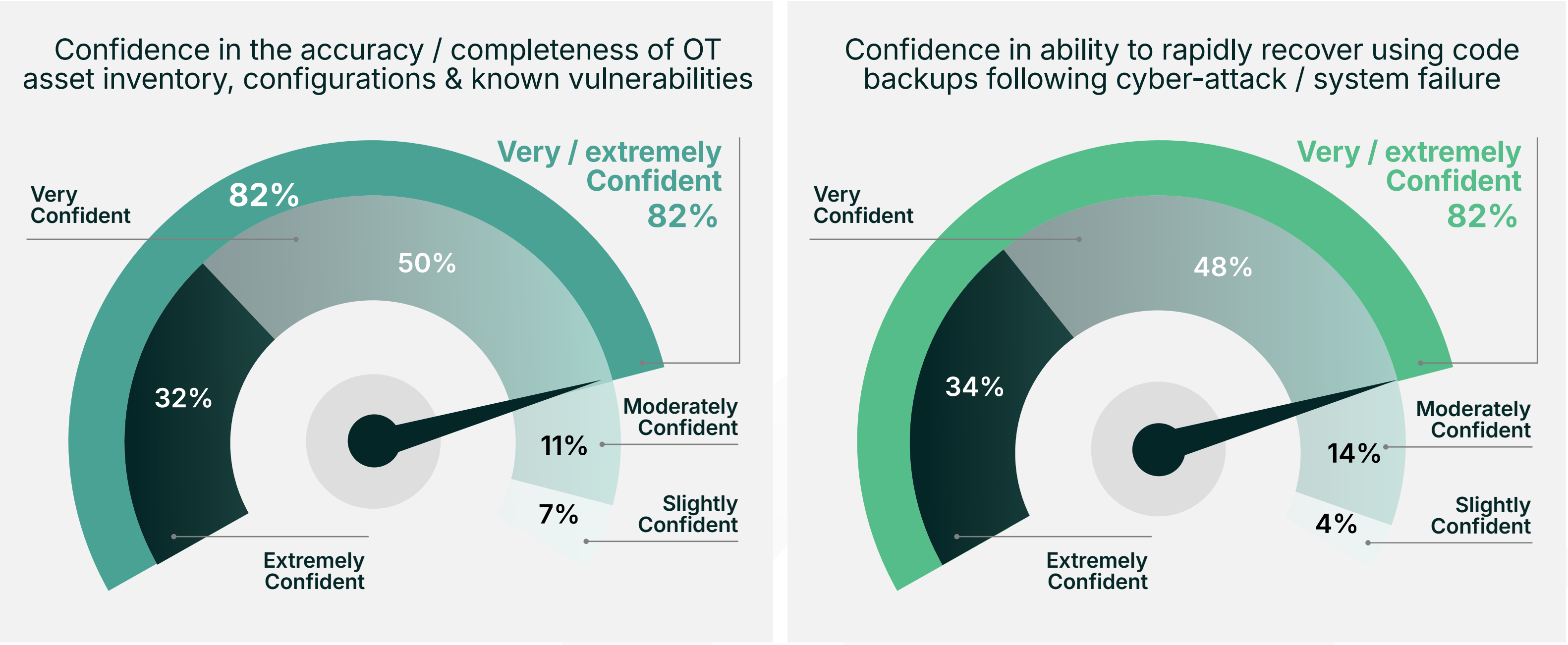
Despite the massive scale and complexity of the modern OT environment, a remarkable **82% of organizations** are very or extremely confident in the accuracy of their asset inventories.

Similarly, **82% are highly confident** in their ability to recover from a major cyberattack using code backups.

While this confidence is encouraging, it presents a potential paradox, particularly when only **50% of organizations believe that cybersecurity collaboration between IT and OT teams is very effective.**

Given the reality of managing thousands of devices from an average of six different vendors, **is this confidence justified, or does it mask underlying risks?**

Confidence Level



Q13. How would you rate the effectiveness of collaboration between your IT and OT teams specifically regarding cybersecurity policies and managing changes to industrial control systems? Select one. Base: 200

Q14 How confident are you in the accuracy and completeness of your organization's current inventory of operational technology (OT) assets , including details like configurations and known vulnerabilities? Select one. Base: 200

Q15. How confident are you in your organization's ability to quickly and reliably recover critical operational technology (OT) operations using code backups following a significant cyberattack or system failure? Select one. Base: 200

THE UNIFYING MANDATE:
INTEGRATING CODE, SECURITY, AND OPERATIONS

The challenges of scale, complexity, and AI adoption all point to a single, undeniable conclusion. When asked how important it is to integrate OT cybersecurity tools with industrial code management tools, the answer is a resounding 87% who state it is very or extremely important.

It is clear that siloed approaches — where cybersecurity, code management, and operations exist in separate spheres — are no longer seen as viable in the face of modern threats.

This demand for integration is the very definition of Industrial DevOps. It is the recognition that a secure plant floor can only be achieved when security policies are embedded into the tools that manage code, when asset inventories are automatically tied to change logs, and when IT and OT teams collaborate through a unified platform.

The industry is no longer just identifying problems; it is explicitly asking for the solution.

> **An organization cannot control whether it suffers a ransomware attack, but it can align investments to three critical controls: back up and restore, business continuity and phishing training."**
>
> Gartner
>
> What is Cybersecurity? Key Topics, Strategies, and Insights

Q16. How important do you believe it is for your organization to integrate operational technology (OT) cybersecurity tools with industrial code management tools? Select one.
Base: 200

> The more organizations use both industry-adopted standards and ICS-specific threat intelligence, the more mature their overall cyber capabilities are.

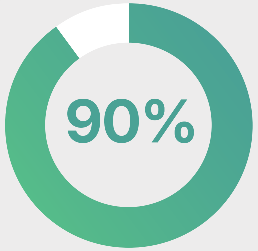
SANS 2024 State of ICS/OT Cybersecurity

04

THE TIPPING POINT: HOW INDUSTRIAL DEVOPS IS BECOMING AN INDUSTRY STANDARD

Driven by urgent needs for security and efficiency, the data shows a market tipping point where Industrial DevOps is actively becoming the new standard.

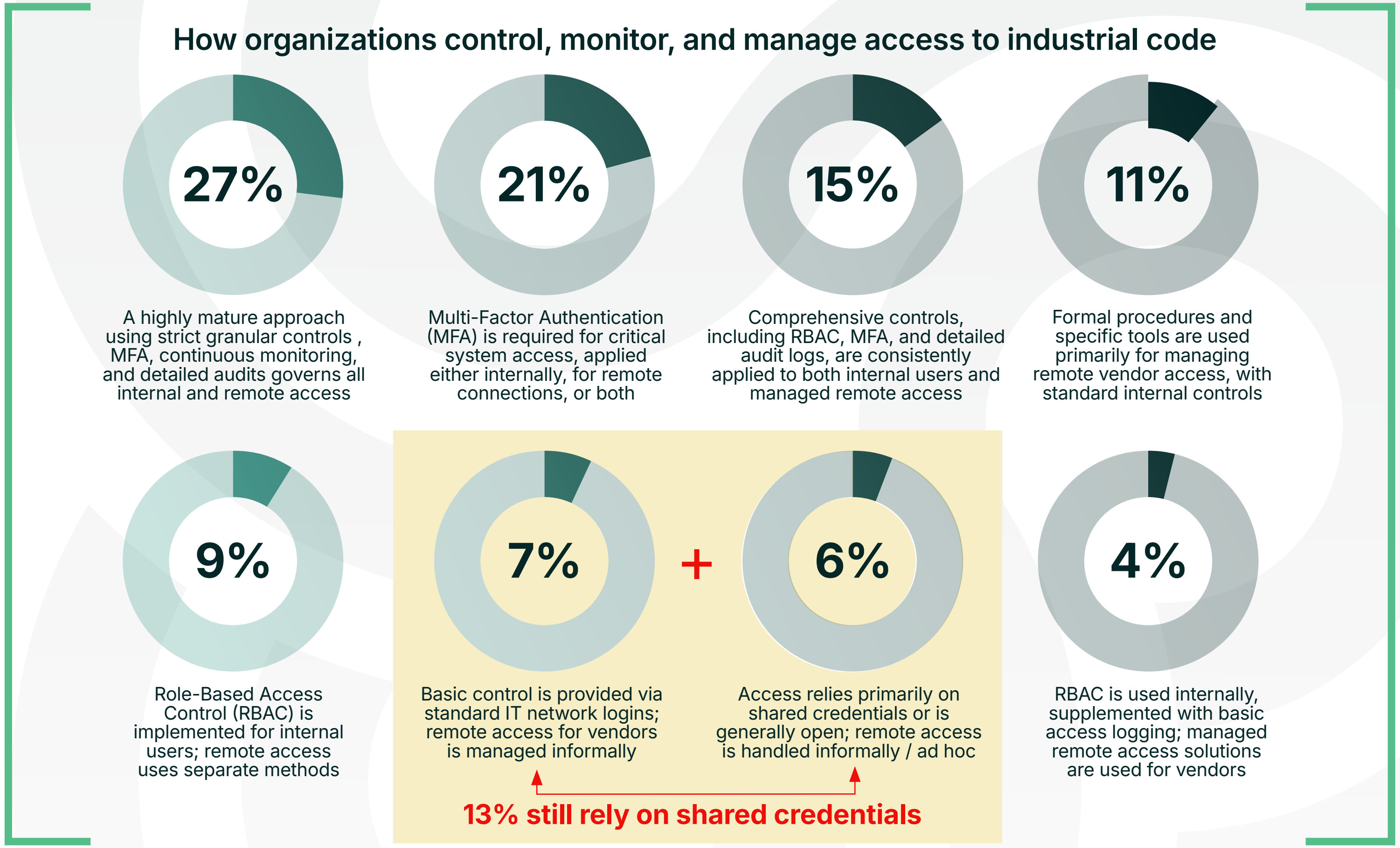
Faced with the risks of a fragmented and insecure operational landscape, the industry is not just showing interest in a new solution; it is demanding it.



A staggering **90% of industrial professionals agree that their team would directly benefit rom using Industrial DevOps technology and practices.** This overwhelming consensus represents a clear mandate for change.

It is a direct response to the deep divisions in security maturity, where **27% of organizations have advanced access controls, but 13% still rely on shared credentials.**

The desire for Industrial DevOps is the desire for a standard of excellence that can close this gap, professionalize industrial code management, and provide the consistent, secure, and efficient foundation that is currently missing.


How organizations control, monitor, and manage access to industrial code

Q17. Which statement best describes how your organization controls, monitors, and manages access to industrial code? Select one. Base: 200

Q21. Based on your experience, to what extent do you agree with the following statement: 'My team would benefit from using Industrial DevOps technology and practices for industrial code management'? Select one. Base: 200

THE BREAKING POINT: WHY A PATCHWORK OF TOOLS IS NO LONGER TENABLE

04

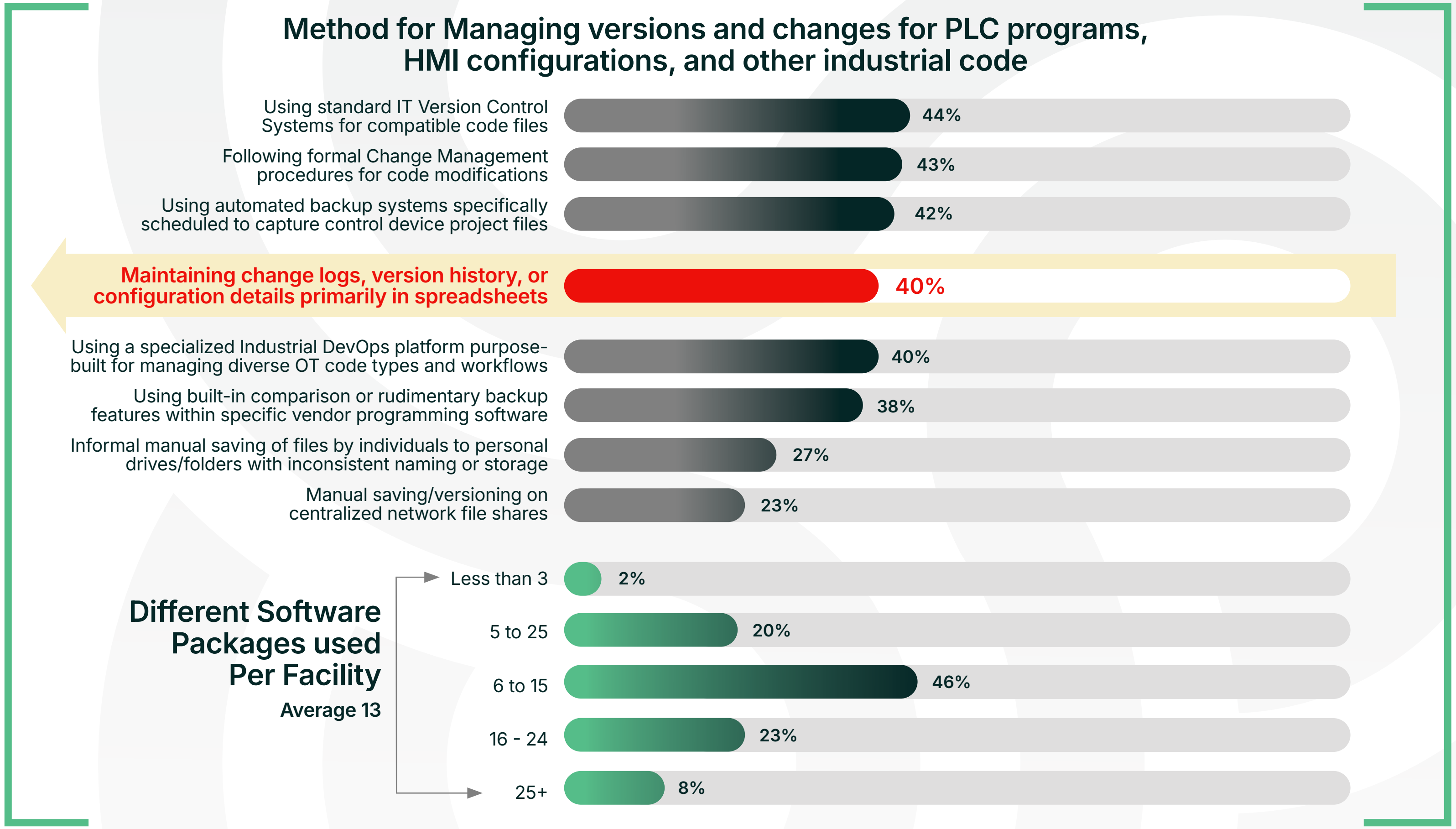
The modern plant floor is drowning in complexity.

The average facility is not running on a single, unified system, but is instead managed by nearly **13 different software packages.**

This software sprawl has created a chaotic and unsustainable environment for managing critical industrial code. With no single standard, teams are left with a patchwork of conflicting processes: **44% use IT version control systems**, while an equal **40% still rely on manual spreadsheets.**

A further **27% admit to informal, ad hoc saving of files on personal or local drives**. This fragmented approach is the direct cause of inefficiency, poor visibility, and critical security gaps.

The old way of working has reached its breaking point, forcing organizations to seek a more unified and resilient strategy.



Q18. In your best estimation, how many different software packages are being used per facility to manage controls / operations ? Select one. Base: 200

Q19. Which of the following methods does your organization currently use to manage versions and changes for PLC programs, HMI configurations, and other industrial code? Select all that apply. Base: 200

FROM EARLY ADOPTION TO MAINSTREAM MOMENTUM

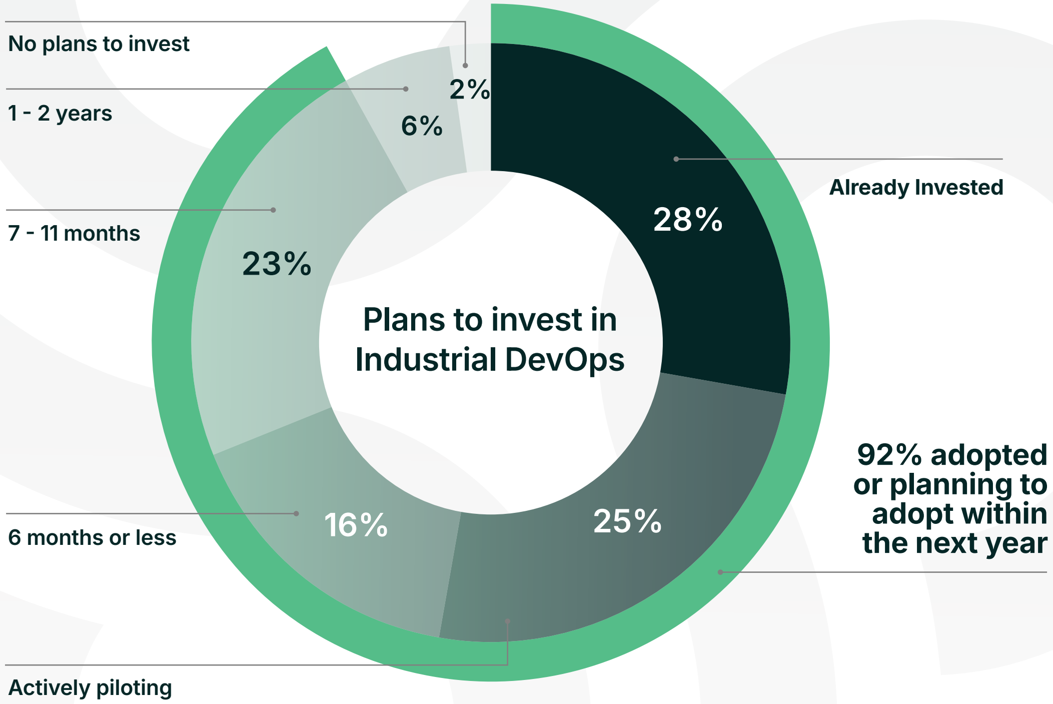
The adoption of Industrial DevOps is no longer a future trend; it is a present-day reality that has reached a market tipping point.

The data shows the market is already in rapid motion, with over half of organizations (53%) either having already invested in or actively piloting Industrial DevOps solutions.

The momentum is accelerating, with a total of **92% of companies having already adopted or planning to invest within the next year.**

This is not a gradual shift but a rapid realignment of the industry. The window for gaining an early adopter advantage is closing fast.

For the few organizations with no immediate plans, the risk of being left behind with outdated, insecure, and inefficient processes is becoming more acute with every passing quarter.



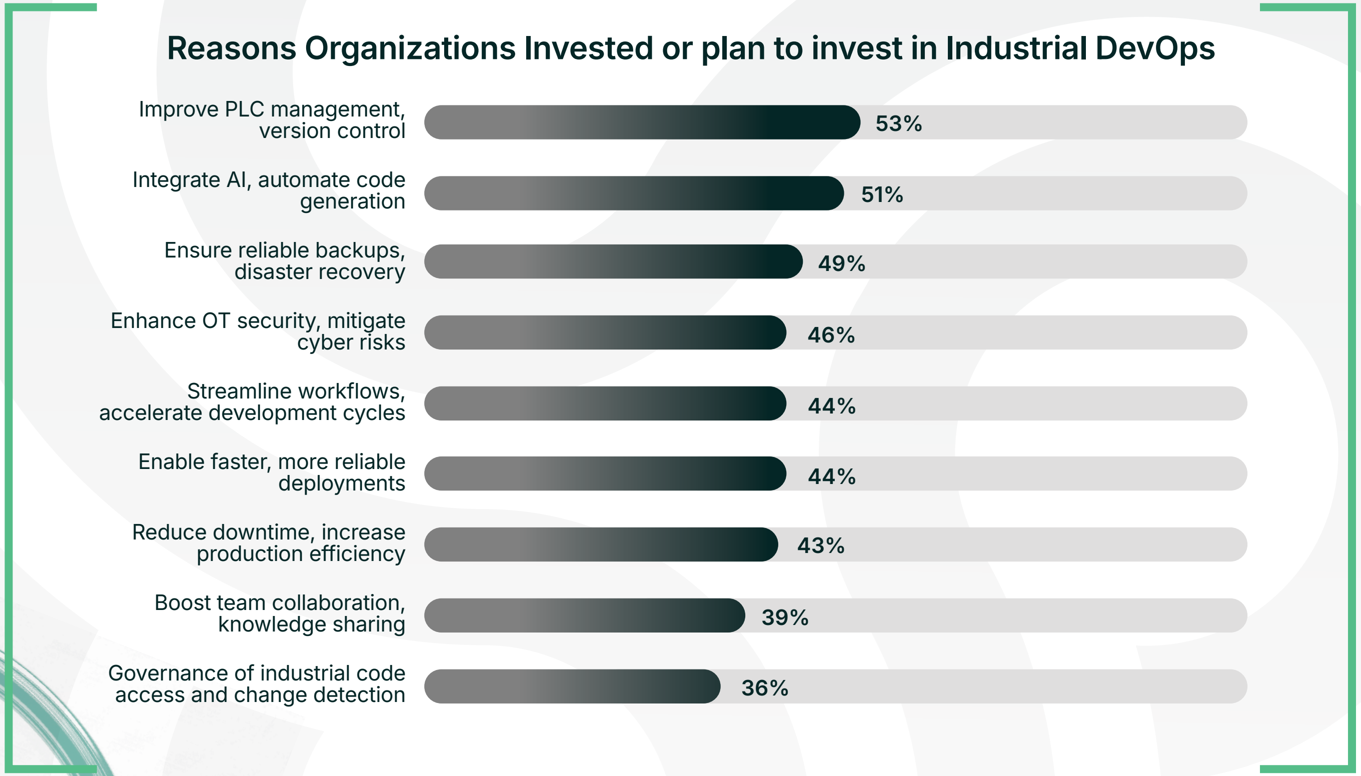
Q25. When do you plan to invest in Industrial DevOps? Select one. Base: 200

THE BUSINESS CASE: UNPACKING THE DRIVERS OF INVESTMENT

When asked why they are investing, leaders point to a multi-faceted business case. The top driver is operational stability: **53% seek to improve basic PLC management and version control.**

This is closely followed by future-proofing, with **51% aiming to integrate AI and automate code generation.** Foundational security and resilience are also key, with **49% focused on ensuring reliable backups and disaster recovery**, and **46% looking to enhance OT security.**

This blend of stability, security, and innovation creates a compelling value proposition that justifies investment by promising to both protect current operations and accelerate future growth.



Reasons Organizations Invested or plan to invest in Industrial DevOps

Q26. Which of the following are reasons you invested or plan to invest in Industrial DevOps? Select all that apply. Base: 138

With the technological need established and market momentum in full force, the greatest barrier to realizing the benefits of Industrial DevOps is not budget or tools — it's people.

An overwhelming **43% of organizations cite change management resistance as the primary challenge to adoption.** This is significantly higher than competing priorities (32%) or lack of budget (26%).

The core challenge is cultural and success hinges on effective leadership. It's imperative to champion this new way of working, accompanied by investment in upskilling teams. As with any initiative, clear and regular communication of the benefits of moving away from the risky, ad hoc processes of the past to a more secure and collaborative future is needed.

It's also crucial to point out — the percent of organizations with no challenges has doubled year-over-year.

Challenges to adopting a more Industrial DevOps-oriented approach to industrial automation

	2025	2024
Change management resistance — people don't want to change their way of working	43%	NA
Competing priorities	32%	44%
Lack of budget to fund an initiative	26%	31%
Lack of need to manage code more effectively	25%	30%
Lack of skills	22%	29%
Lack of interest from management/decision makers	21%	39%
Haven't found a technology that can take an Industrial DevOps-oriented approach	21%	24%
We have no challenges	**20%**	**10%**

Q22. What are the main challenges your organization faces in adopting a more Industrial DevOps-oriented approach to industrial automation? Select all that apply. Base: 200

FROM FIREFIGHTING TO FUTURE-BUILDING: THE NEW FOCUS OF HIGH-PERFORMING TEAMS

04

The ultimate promise of Industrial DevOps is a fundamental shift in how teams spend their most valuable resource: their time. The data shows that organizations making this transition are successfully moving from a reactive posture to a proactive one.

This is most evident in cybersecurity, where teams now spend significantly more time **preventing security issues (79% often/always)** than they do **remediating them (69%)**. This is the very definition of shifting left — building security in, not bolting it on as an afterthought.

This proactive stance on security and operations frees up engineering talent to focus on high-value activities that drive growth, like **learning new technologies (81%)**, while reducing time spent that doesn't, like **unplanned work and/or rework (59%)**.

By automating and standardizing core processes like version control and security testing, Industrial DevOps creates an environment where innovation is not a luxury, but a daily activity.

Where Industrial DevOps Teams Spend Time

	Never	Rarely	Sometimes	Often	Always	Often/Always
Learning and adopting new technologies	2%	3%	14%	46%	35%	81%
Monitoring and troubleshooting applications	2%	4%	15%	40%	39%	79%
Preventing cybersecurity issues	3%	4%	16%	40%	39%	79%
Code review and approval	2%	2%	17%	39%	40%	79%
Security testing and compliance	2%	4%	16%	43%	36%	79%
Documentation and knowledge sharing	2%	3%	18%	46%	32%	78%
Business value-adding work	3%	3%	20%	45%	31%	76%
Version control and configuration management	2%	3%	22%	44%	29%	73%
Remediating cybersecurity issues	2%	6%	24%	38%	31%	69%
Unplanned work and/or rework	2%	9%	30%	35%	24%	59%

Q20k. In your opinion, how frequently do teams that adopt Industrial DevOps practices spend time on the following activities? Base: 200

THE STRATEGIC IMPERATIVE: BEYOND OPPORTUNITY TO NECESSITY

04

The evidence is conclusive.

Given the unsustainable nature of current patchwork processes, the **90% mandate for a new approach**, the rapid market adoption, and the powerful business case — from enhancing security to enabling AI — **Industrial DevOps has moved beyond being an opportunity.** It is now a strategic imperative.

In an era of increasing cyber threats and competitive pressure, relying on informal processes and fragmented toolchains is no longer a viable option. Adopting a unified platform to manage, secure, and streamline the lifecycle of industrial code is essential for protecting critical operations, empowering the workforce, and positioning the enterprise to lead in a new age of manufacturing.

> **C-Suite respondents peg downtime at $4.29 million per hour—almost 50 percent higher than frontline estimates—and blame industrial code for over half of all stoppages. That gap won’t close with meetings alone; it demands a single source of truth that shows every change across thousands of PLCs. Industrial Code Lifecycle Management provides that clarity, turning finger-pointing into fast recovery while freeing engineers to innovate. In a world where minutes cost millions, unified visibility is the new competitive currency.”**

Sebastián Trolli, Research Manager, Global Head of Industrial Automation and Software at Frost & Sullivan

05

LEVERAGING THIS REPORT: A GUIDE TO BENCHMARKING YOUR INDUSTRIAL DEVOPS JOURNEY

This report provides a comprehensive snapshot of the industrial landscape, revealing critical trends, persistent challenges, and the evolving perspectives of leaders across various seniority levels. Now, it’s time to turn these insights into action. This section will guide you on how to leverage the data to benchmark your own organization’s Industrial DevOps maturity, identify areas for improvement, and foster internal alignment for a more secure, efficient, and innovative future.

05

YOUR 5-STEP BENCHMARKING PLAYBOOK

Here’s how to systematically benchmark your organization using the insights from this report:

1. Assess Your Current State Against Key Metrics
2. Identify Perception Gaps and Misalignments
3. Prioritize Areas for Improvement
4. Develop a Tailored Action Plan
5. Monitor Progress and Iterate

Why Benchmark?

Benchmarking allows you to:

- **Identify Strengths and Weaknesses:** Understand where your organization excels and where it lags compared to industry peers.
- **Validate or Challenge Internal Perceptions:** Compare your internal data and anecdotal experiences with the report’s aggregate findings and seniority-specific views.
- **Build a Data-Driven Business Case:** Use objective industry data to advocate for investment, resources, or changes within your organization.
- **Prioritize Initiatives:** Focus your Industrial DevOps efforts on the areas that offer the greatest potential for impact, informed by what’s working (or not working) for others.
- **Foster Internal Alignment:** Initiate crucial conversations across IT, OT, and leadership based on shared data, bridging the perception gaps highlighted throughout this report.

STEP 1 ASSESS YOUR CURRENT STATE AGAINST KEY METRICS

Go through the report's key statistics and tables and honestly evaluate where your company stands for each. Pay close attention to the overall averages and the breakdowns by seniority, as these will provide critical context.

Cost of Downtime (Section 2, Q1):

- What is your organization's estimated hourly cost of downtime & how does this compare to the overall mean of **$3.63 million/hour?**
- Does this align across seniority levels? If not, why? If yes, why?
- ACTION: If your costs are higher, or if there's a significant perception gap, this is a prime area for deeper analysis and strategic investment.

Downtime Attribution to Industrial Code (Section 2, Q2):

- What percentage of your downtime do you attribute to industrial code issues? How does this compare to the **overall 45%**?
- Does this align across seniority levels? If not, why? If yes, why?
- ACTION: A high attribution to code, especially at senior levels, signals an urgent need for robust Industrial DevOps solutions. If your operational teams attribute less, explore why — are quick fixes masking deeper, recurring code issues that impact overall system stability?

Primary Causes of Downtime (Section 2, Q3):

- What are your top 3 causes of unplanned downtime? Do they align with the report's findings of **Hardware Malfunction (43%), Coding/Software Issues (43%), and Cybersecurity Breach (43%)?**
- Are cybersecurity concerns as prominent for your operational teams as they are for your senior leaders? (Report shows Managers at **22%** vs. C-Suite **45%**).
- ACTION: Identify discrepancies. If your operational teams are focusing on hardware but senior leadership sees rising cyber threats, your investment strategy might be misaligned.

Investment in Industrial DevOps (Section 3, Q25):

- Is your organization **already invested (28%), actively piloting (25%), or planning to invest (39%)** in Industrial DevOps within the next 11 months?
- How does your pace of adoption compare to the **92% overall** who are engaged or planning to invest?
- ACTION: If you're behind the curve, leverage the report's data to highlight the industry's clear trajectory towards Industrial DevOps adoption.

Challenges to Adoption (Section 3, Q22):

- What are your primary challenges in adopting Industrial DevOps? Is **change management resistance (43%)** a significant hurdle?
-
- ACTION: Tailor your change management strategies to address specific concerns at each level of the organization.

Code Management Practices (Section 3, Q19):

- Are you primarily using **specialized Industrial DevOps platforms**, spreadsheets (**40% overall**), or informal manual saving?
- ACTION: Understand existing successful adoptions within your organization. Leverage internal champions and their experiences to inform broader rollouts.

AI in Industrial DevOps (Section 4, Q23, Q24):

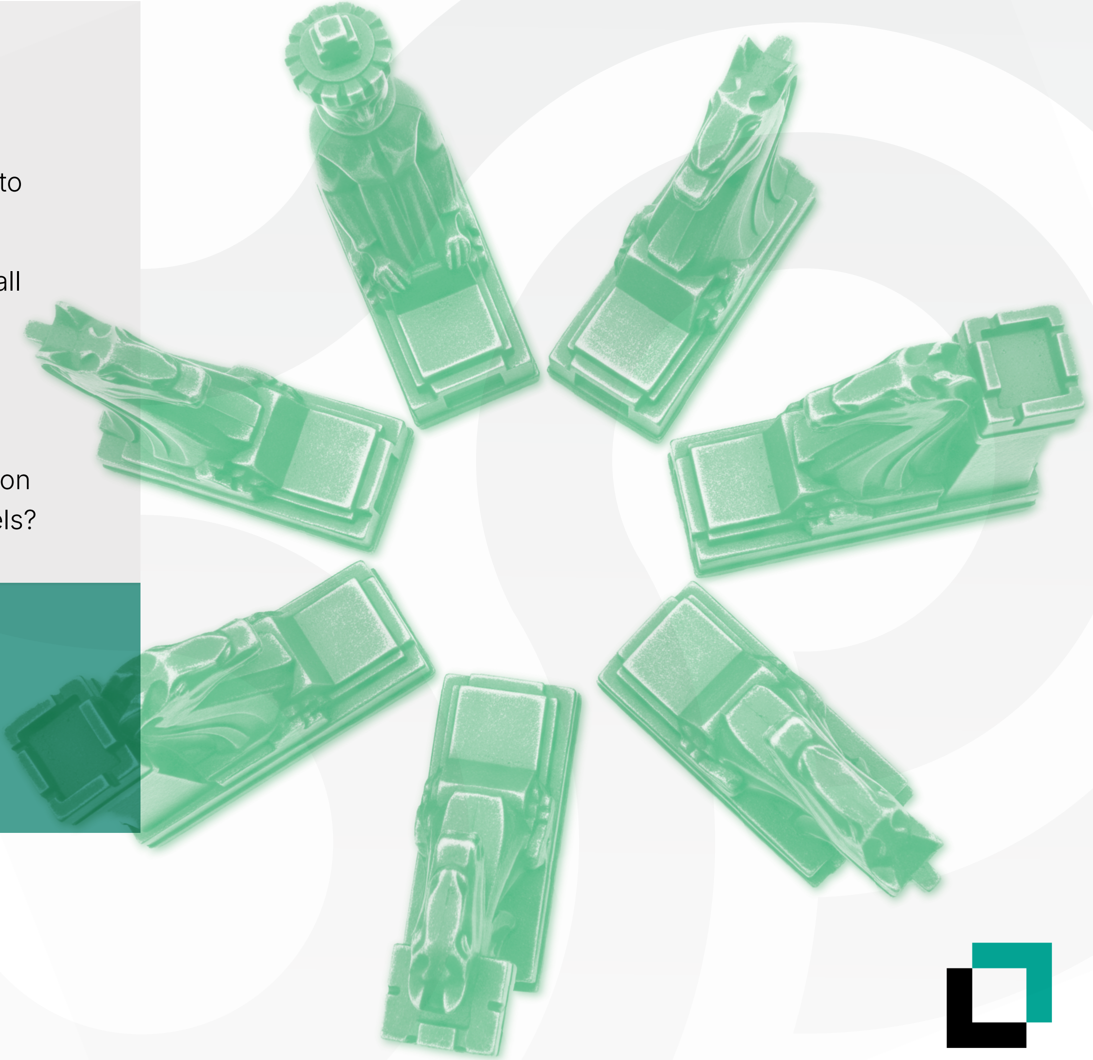
- How enthusiastic are your teams about AI in OT? Which AI features are most valued (e.g., **AI-driven version control, automated code generation, PLC logic optimization**)?
- What are your top concerns regarding AI adoption (e.g., **data security and privacy, integration with existing systems, reliability of AI algorithms**)?
- Do your Managers express fewer concerns about security and reliability, while senior leaders emphasize them more?
- ACTION: Develop an AI strategy that balances operational benefits with strategic risk management, addressing concerns at all levels.

STEP 2 IDENTIFY PERCEPTION GAPS AND MISALIGNMENTS

Identify perception gaps across seniority for internal benchmarking.

- **Downtime Cost & Code Attribution:** Does your C-Suite truly grasp the full financial and operational impact of downtime and the role of code, or do they under/overestimate it compared to operational teams?
- **Resolution Times vs. Debugging Time:** Do your operational teams report quick fixes, while overall debugging hours remain high?
- **Confidence in Inventory vs. Reality:** Are your senior leaders highly confident in asset inventory accuracy, while your Managers are less so? This indicates a potential blind spot.
- **IT/OT Collaboration Effectiveness:** Is there consensus on how effectively IT and OT collaborate on cybersecurity, or are there significant differences in perceived effectiveness across seniority levels?

ACTION: Gaps in perception are fertile ground for internal discussion. Facilitate workshops or focused meetings to explore these differences, sharing the report's findings as a neutral starting point. The goal is to build a shared understanding of realities and priorities.



STEP 3 PRIORITIZE AREAS FOR IMPROVEMENT

Based on your current state assessment and identified perception gaps, determine which areas require the most immediate attention.

- **High Costs/High Code Attribution:** If your downtime costs are high and code is a major contributor, investing in comprehensive code management, version control, and automated testing (core Industrial DevOps tenets) should be a top priority.
- **Cybersecurity Discrepancy:** If senior leaders are concerned about cyber threats but operational teams aren't prioritizing it as a downtime cause, immediate action is needed to raise awareness and integrate cybersecurity awareness and preparedness into daily OT practices.
- **Resolution Time Paradox:** If quick fixes are prevalent but deeper issues persist (high debugging, long recovery from major incidents), focus on implementing root cause analysis, robust change management, and a unified platform for tracking fixes and preventing recurrence.
- **Low Adoption of Specialized Tools:** If your organization still heavily relies on informal methods despite the industry trend towards specialized Industrial DevOps platforms, assess the barriers to adoption and identify champions for piloting modern tools.

ACTION: Develop a roadmap with clear, measurable goals for these prioritized areas.

> **“While AI presents significant opportunities for accelerating development, its effective adoption hinges on a solid technical and cultural foundation. The highest-performing teams are those that strategically integrate AI to augment their existing, well-established practices, rather than using it as a substitute for them.”**
>
> DORA | Accelerate State of DevOps Report 2024

STEP 4 DEVELOP A TAILORED ACTION PLAN

For each prioritized area, outline specific actions:

- **Cross-Functional Communication:** Establish regular IT/OT/Cybersecurity/Leadership syncs.
- **Standardized Metrics:** Define common KPIs for downtime, code quality, and security.
- **Diverse Representation:** Ensure operational voices are heard in strategic decisions.
- **Tailored Change Management:** Address specific concerns of each seniority level.
- **Root Cause Focus:** Incentivize thorough analysis over quick patches.
- **Leverage Internal Successes:** Identify and scale what's already working well.

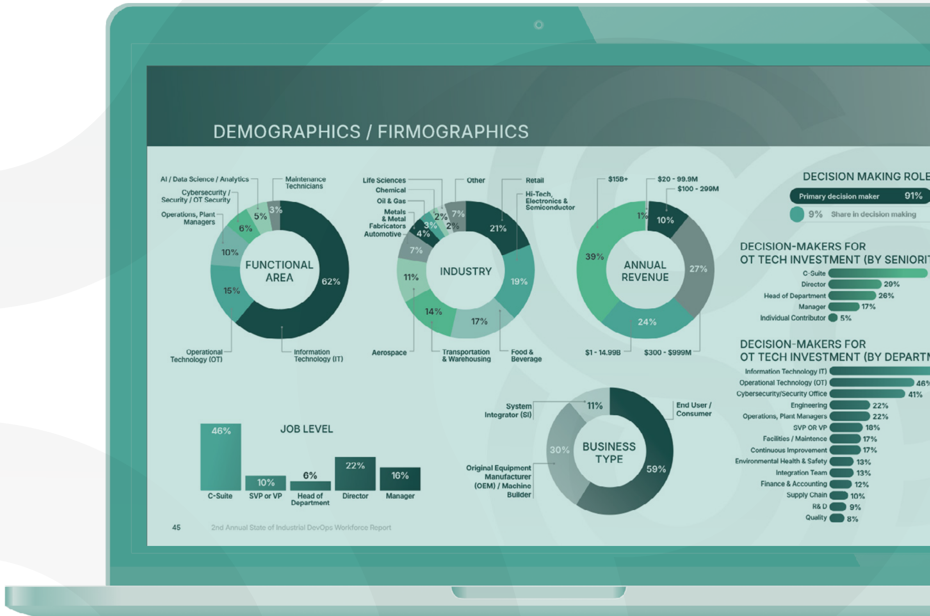
ACTION: Assign owners, set deadlines, and allocate resources. Consider a pilot program for a specific Industrial DevOps initiative, using the report's data as a baseline for measuring success.

STEP 5 MONITOR PROGRESS AND ITERATE

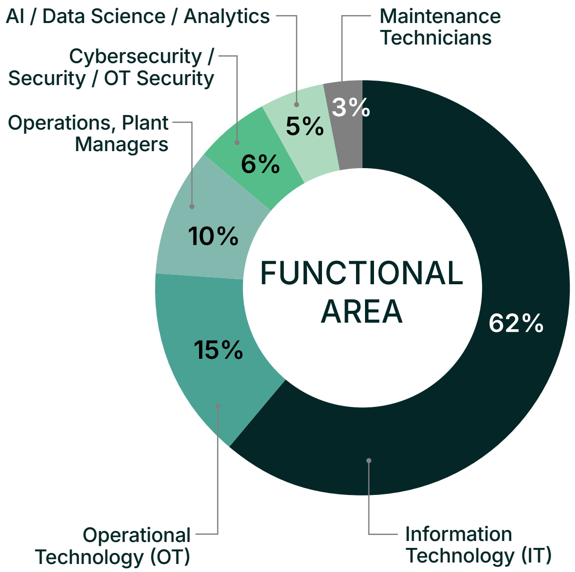
Benchmarking is not a one-time event. Industrial operations are dynamic, and so should be your improvement process.

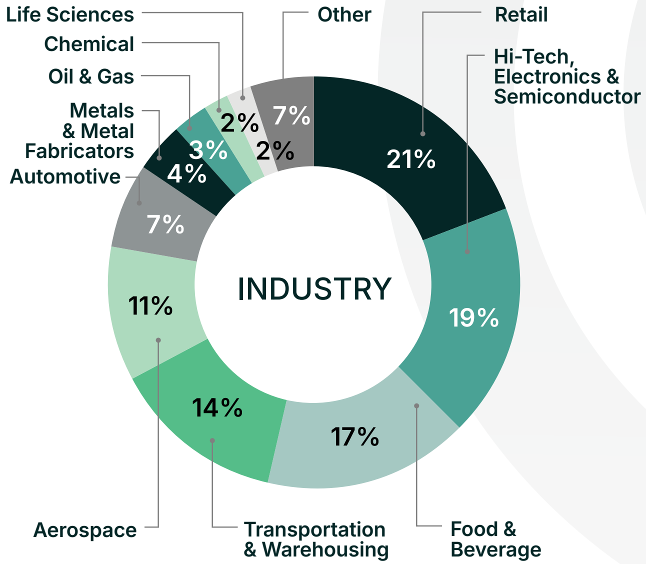
- **Track Your Own Metrics:** Regularly measure your organization's progress against the key metrics identified in Step 1.
- **Revisit the Report:** As the "State of Industrial DevOps Report" is an annual publication, compare your progress year-over-year with the latest industry findings.
- **Adjust Your Strategy:** Be agile. If certain initiatives aren't yielding the desired results, or if new challenges emerge, adapt your approach.

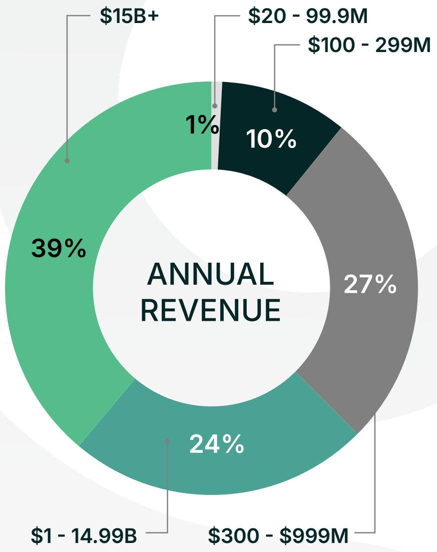
By systematically applying the insights from **The 2nd Annual State of Industrial DevOps Report** to your own operations, you can effectively benchmark your current standing, foster critical internal conversations, and strategically accelerate your journey towards becoming a more resilient, efficient, and innovative industrial enterprise. **The data is here; the transformation is now yours to lead.**
[Book a meeting with Copia to get started now.]


DEMOGRAPHICS / FIRMOGRAPHICS
FUNCTIONAL AREA
AI / Data Science / Analytics
Cybersecurity / Security / OT Security
Operations, Plant Managers
Maintenance Technicians
Operational Technology (OT)
Information Technology (IT)
62%
15%
10%
6%
5%
3%
INDUSTRY
Life Sciences
Chemical
Oil & Gas
Metals & Metal Fabricators
Automotive
Other
Retail
Hi-Tech, Electronics & Semiconductor
Aerospace
Transportation & Warehousing
Food & Beverage
21%
19%
17%
14%
11%
7%
4%
3%
2%
2%
7%
ANNUAL REVENUE
$15B+
$20 - 99.9M
$100 - 299M
$1 - 14.99B
$300 - $999M
1%
10%
27%
24%
39%
JOB LEVEL
46%
10%
6%
22%
16%
C-Suite
SVP or VP
Head of Department
Director
Manager
BUSINESS TYPE
System Integrator (SI)
Original Equipment Manufacturer (OEM) / Machine Builder
End User / Consumer
11%
30%
59%
DECISION MAKING ROLE
Primary decision maker 91%
9% Share in decision making
DECISION-MAKERS FOR OT TECH INVESTMENT (BY SENIORIT
C-Suite
Director 29%
Head of Department 26%
Manager 17%
Individual Contributor 5%
DECISION-MAKERS FOR OT TECH INVESTMENT (BY DEPARTM
Information Technology IT)
Operational Technology (OT) 46%
Cybersecurity/Security Office 41%
Engineering 22%
Operations, Plant Managers 22%
SVP OR VP 18%
Facilities / Maintence 17%
Continuous Improvement 17%
Environmental Health & Safety 13%
Integration Team 13%
Finance & Accounting 12%
Supply Chain 10%
R& D 9%
Quality 8%
45
2nd Annual State of Industrial DevOps Workforce Report

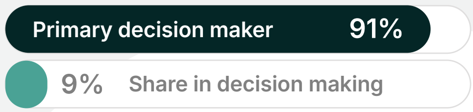
DEMOGRAPHICS / FIRMOGRAPHICS



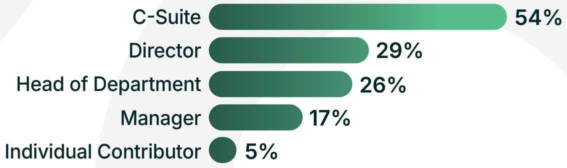




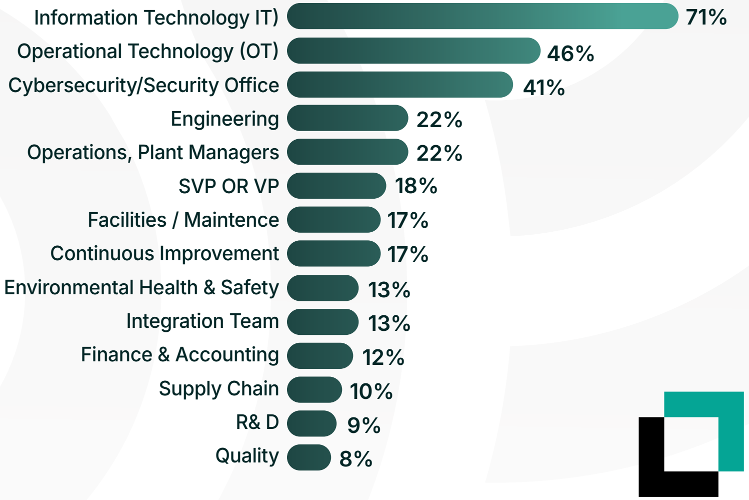
DECISION MAKING ROLE

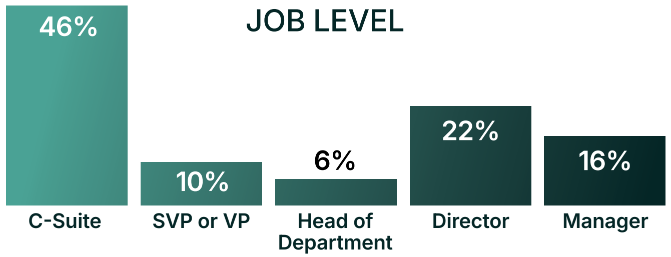


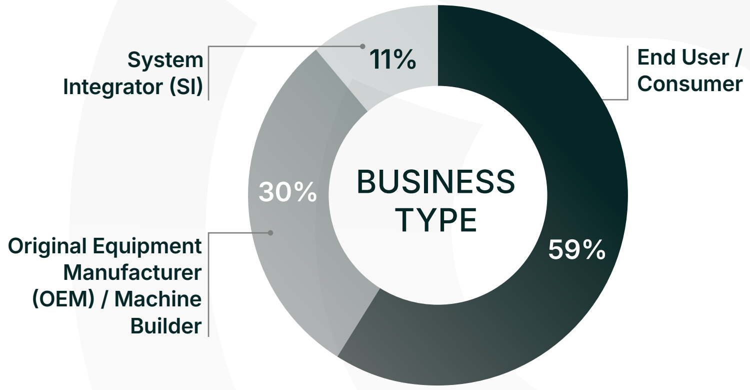
DECISION-MAKERS FOR OT TECH INVESTMENT (BY SENIORITY)



DECISION-MAKERS FOR OT TECH INVESTMENT (BY DEPARTMENT)







ACKNOWLEGEMENTS

This report reflects more than just data; it is a testament to the shared commitment of the Industrial DevOps community to move our industry forward. Its creation was a truly collaborative process, shaped at every stage by the sharp insights of our peers and friends. We extend our sincere gratitude to everyone who lent their time and expertise, making this comprehensive analysis both possible and impactful.

REPORT TEAM:

Copia Automation Team

These reports take a village - thank you, Village!

Friends of Copia:

- Jeff Winter (Contributing Analyst & Editor)
- Dr. Suzette Johnson (Contributor)
- Robin Yeman (Contributor)
- Nathen Harvey (Contributor)
- Harry Koehnemann (Contributor)
- Sebastián Trolli (Contributor)
- The entire Industrial DevOps Community and Industry Analysts that shared time and feedback

COPIA SPONSORSHIPS AND MEMBERSHIPS:

DORA

CSIA CERTIFIED

WORLD ECONOMIC FORUM

2026 SPONSORSHIP OPPORTUNITIES!

Be at the forefront of the AI-powered industrial revolution. Our 2026 report will again deliver the critical insights on automation, security, and efficiency that leaders need. Sponsorship connects your brand directly with the key decision-makers shaping the future of manufacturing. Partner with us and lead the conversation in 2026. Inquire today about our 2026 sponsorship packages! [Submit now to learn more about sponsorship opportunities!]

Tier 1: Bronze - $500

- Logo Placement:
  - Report (prominent placement)
  - Report landing page
  - LinkedIn promotional posts (multiple)
- Early access to the report data and PDF.
- Brand Association: Company name listed as a report sponsor.

Tier 2: Silver - $1500

All Bronze Tier Benefits, PLUS:

- Enhanced Logo Placement: Larger logo placement in the report.
- Social Media Spotlight: Dedicated LinkedIn post highlighting your company.
- Exclusive Webinar Opportunity:
  - Co-host a webinar with Copia Automation to discuss key report findings.
  - Opportunity to present your expertise to a targeted audience.

Tier 3: Gold - $3000

All Silver Tier Benefits, PLUS:

- Premium Logo Placement:
  - Report (Front page, highest visibility)
  - Most prominent logo placement in the report and landing page.
- Strategic Influence & Recognition:
  - Advisory Board Inclusion
  - Press Release Collaboration
  - First Option for Next Year’s Sponsorship

COPIA

copia.io

contact@copia.io

646.389.0222

43 West 24th Street
6th Floor
New York, NY 10010

Copia Automation's Industrial DevOps platform simplifies Industrial Code Lifecycle Management (ICLM). Through automated backups and a central code repository, it builds OT cyber resilience, maximizes uptime, and accelerates growth.