WHITE PAPER

Copia Automation and NIST Compliance in Industrial Settings

Achieving Cybersecurity and Operational Resilience

COPIA

Introduction

Industrial facilities face increasing cybersecurity threats that can disrupt operations, compromise safety, and lead to significant financial losses. The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) provides a widely recognized set of standards, guidelines, and best practices to help organizations manage and reduce these risks. This white paper outlines how Copia Automation's Industrial DevOps platform can support manufacturers in achieving and maintaining NIST CSF alignment, enhancing both their cybersecurity posture and operational resilience.

This white paper outlines how Copia Automation's Industrial DevOps platform can support manufacturers in achieving and maintaining NIST CSF alignment, enhancing both their cybersecurity posture and operational resilience.

Understanding the NIST Cybersecurity Framework (CSF)

The NIST CSF offers a structured approach to cybersecurity risk management, applicable to organizations of all sizes and across various sectors, including manufacturing. It is composed of three main components:

- **Core:** A set of five functions—Identify, Protect, Detect, Respond, and Recover—that organize cybersecurity activities.
- **Implementation Tiers:** Describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the Framework.
- **Profiles:** Align standards, guidelines, and practices to organizational needs and objectives, and risk appetite.

The NIST CSF helps organizations to:

- Identify their assets, systems, and data.
- Protect these assets through the implementation of appropriate safeguards.
- Detect cybersecurity events in a timely manner.
- Respond effectively to contain the impact of incidents.
- Recover operations and restore capabilities after an incident.

The Challenge: Cybersecurity in Industrial Automation

Industrial automation systems, including PLCs, HMIs, and other control devices, are critical to manufacturing operations. However, they were not designed using a secure by design methodology, making them vulnerable to cyberattacks.

Key challenges include:

- **Legacy Systems:** Many industrial facilities rely on outdated systems with known vulnerabilities and limited patching capabilities.
- **Lack of Visibility:** Organizations often lack a comprehensive inventory of their OT assets and their configurations, making it difficult to assess and manage risk.
- **Connectivity & Automation:** The increasing connectivity between OT and IT networks, driven by Industry 4.0 initiatives, expands the attack surface and increases the potential for cyberattacks to disrupt operations.
- **Change Management Risks:** Improperly managed changes to OT systems can lead to production disruptions, safety incidents, and security vulnerabilities.

How Copia Automation Supports NIST CSF Alignment

Copia Automation's Industrial DevOps platform provides capabilities that directly support the NIST CSF functions, helping manufacturers improve their cybersecurity posture and achieve alignment with this critical framework.

1 Identify

- **Asset Identification:** While Copia is not an asset discovery tool, its Industrial DevOps Platform does provide a centralized repository for all connected automation code and configurations, enabling organizations to maintain an inventory of their OT software assets. This includes code running on PLCs, robots, and other industrial devices.
  - By maintaining a clear record of all software assets, Copia helps organizations establish a strong foundation for their cybersecurity program, as recommended by the NIST CSF.

2 Protect

- **Access Control:** Copia enforces granular access control to automation code and configurations, allowing organizations to define roles and permissions and restrict access to authorized personnel.
  - This aligns with the NIST CSF's emphasis on access control policies and procedures to protect sensitive information and assets.
- **Change Management:** Copia's version control system provides a structured approach to managing changes to OT software, ensuring that all changes are authorized, tested, and documented.
  - This helps organizations implement robust change management processes, a key safeguard recommended by the NIST CSF to prevent unauthorized modifications and reduce the risk of cyber incidents.
- **Backup and Recovery:** Copia automates the backup of PLC data and automation code, enabling organizations to quickly recover from cyberattacks or other disruptive events.
  - This supports the NIST CSF's guidance on implementing backup and recovery plans to ensure business continuity and minimize the impact of incidents.

3 Detect

- **Change Detection:** Copia's version control features enable organizations to detect unauthorized or unexpected changes to automation code, which may indicate a cyberattack or other security incident.
  - By providing visibility into code changes, Copia helps organizations to quickly identify potential security breaches, aligning with the NIST CSF's focus on implementing detection processes.

4 Respond

- **Incident Response:** Copia's version control and rollback capabilities enable organizations to quickly restore OT systems to a known good state after a cyberattack, minimizing downtime and disruption to operations.
  - This supports the NIST CSF's guidance on developing and implementing incident response plans to contain the impact of incidents and restore normal operations.

5 Recover

- **Recovery Planning:** Copia's backup and recovery features facilitate the development and implementation of recovery plans for OT systems, ensuring that organizations can restore operations in a timely manner following a cyber incident.
  - This aligns with the NIST CSF's emphasis on recovery planning to restore systems and assets affected by cybersecurity incidents.

Copia Automation and Specific NIST CSF Functions

The table below summarizes how key functionalities of the Copia Automation platform align with the core functions of the NIST Cybersecurity Framework:

NIST CSF Function	Copia Automation Functionality	How it Supports the Function
Identify	Centralized Code Repository, Asset Inventory	Provides a single source of truth for OT software assets, aiding in comprehensive identification.
Protect	Granular Access Control, Version Control, Automated Backups	Enforces secure access, manages changes systematically, and ensures data/code availability.
Detect	Change Detection (via Version Control)	Alerts to unauthorized or unexpected modifications in automation code.
Respond	Version Control (Rollback Capabilities), Automated Backups	Enables rapid restoration of systems to a known good state after an incident.
Recover	Automated Backups, Version Control (Recovery Planning Support)	Facilitates the restoration of operations and systems using reliable backups and history.

Conclusion

The cybersecurity landscape for industrial automation is increasingly complex and challenging. As manufacturers embrace digital transformation and connect their operational technology (OT) systems, the need for robust security measures aligned with recognized standards like the NIST Cybersecurity Framework becomes paramount. Copia Automation's Industrial DevOps platform offers a powerful solution to help organizations navigate this challenge. By providing essential capabilities across asset identification, access control, structured change management, automated backups, and change detection, Copia directly supports the core functions of the NIST CSF — Identify, Protect, Detect, Respond, and Recover.

Implementing a platform like Copia not only aids in achieving alignment with NIST guidelines but fundamentally enhances an organization's cybersecurity posture and operational resilience. It provides the necessary visibility, control, and recovery mechanisms to minimize risk, respond effectively to incidents, and ensure business continuity in the face of cyber threats. For manufacturing and distribution facilities seeking to strengthen their defenses and build a more secure and reliable operational environment, adopting a comprehensive Industrial DevOps solution like Copia Automation is a strategic imperative in today's interconnected world.

Take the Next Step in Your Journey

Don't let outdated tools and processes hold you back. Discover how Copia Automation can revolutionize your PLC code development workflow. Contact us today for a personalized demo and embark on your journey towards Industrial DevOps.

You can also reach out directly by emailing contact@copia.io.