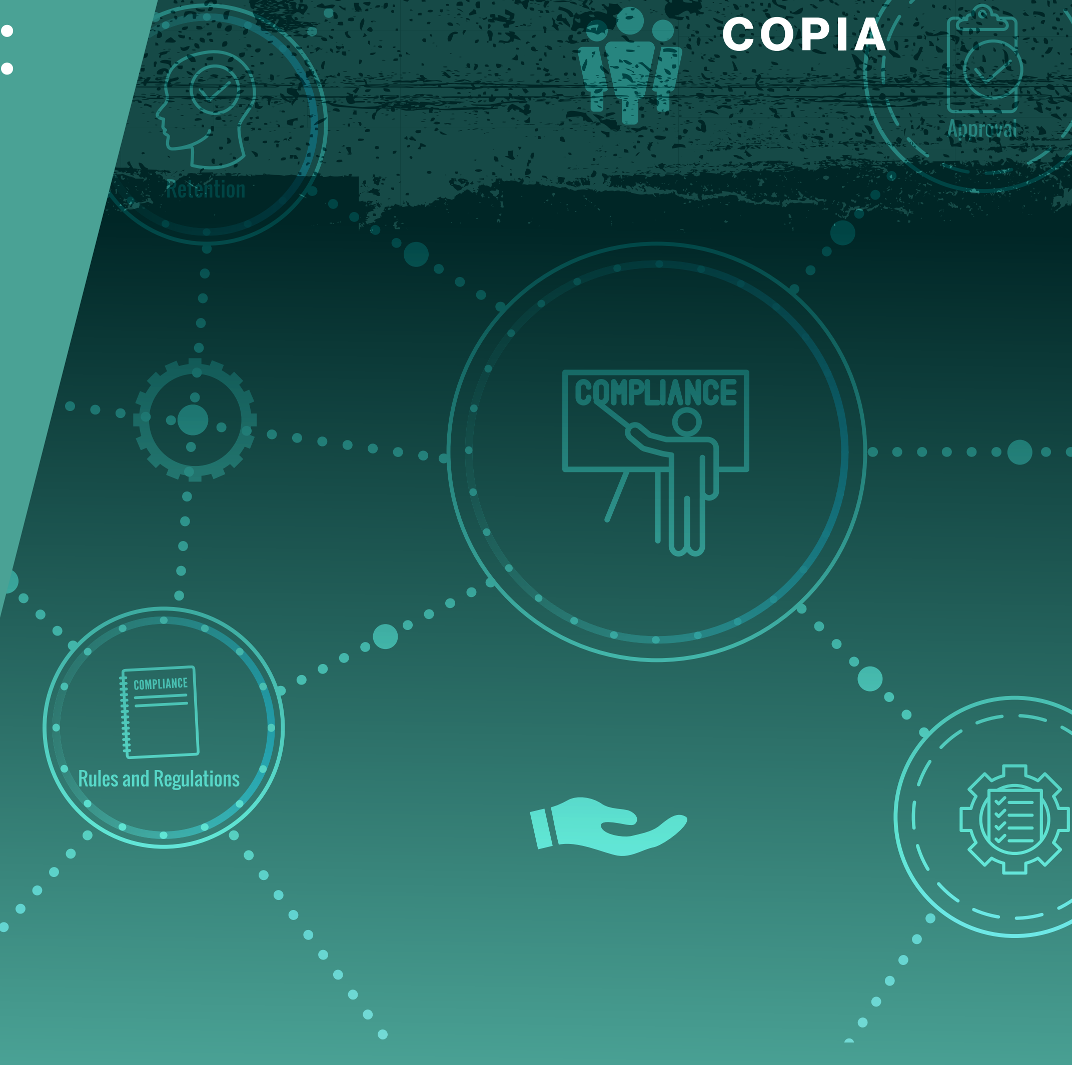
EBOOK

Copia Automation: A Strategic Ally in Achieving ISA/IEC 62443 Compliance

COPIA



Introduction:

Copia Automation's Industrial DevOps platform provides a robust framework and a suite of powerful tools that directly support and enable broader adherence to the ISA/IEC 62443 standards for Industrial Automation and Control Systems (IACS) security. By integrating Git-based version control, automated backup and recovery, and comprehensive change management capabilities, Copia enables organizations to systematically address the stringent requirements of the world's leading industrial cybersecurity standard.

The ISA/IEC 62443 standards are a series of documents that define a comprehensive framework for securing IACS environments. They address people, processes, and technology, and are structured to manage cybersecurity throughout the entire lifecycle of the system. Copia's platform aligns with the core principles of these standards by providing the necessary mechanisms for visibility, control, and documentation of all changes within the industrial control system environment.

> Copia enables organizations to systematically address the stringent requirements of the world's leading industrial cybersecurity standard.

Mapping Copia’s Features to Key ISA/IEC 62443 Requirements

Copia’s platform offers tangible solutions to many of the foundational requirements outlined in the various parts of the ISA/IEC 62443 series of standards:

Foundational Requirement 1: Identification and Authentication Control (IAC)

- Copia provides robust access control features, including Single Sign-On (SSO) and Multi-Factor Authentication (MFA), to ensure that only authorized personnel can access and modify control system code. This aligns with the IAC principle of verifying the identity of all users and processes seeking access to the IACS.

Foundational Requirement 2: Use Control (UC)

- Through granular user permissions and role-based access control, Copia allows organizations to enforce the principle of least privilege. This ensures that users only have access to the specific code and systems necessary for their roles, a key tenet of the UC requirement. Approval workflows further enforce that changes are reviewed and authorized before deployment.

Foundational Requirement 3: System Integrity (SI)

- At its core, Copia is designed to maintain the integrity of industrial control system programming. Its Git-based version control system creates an immutable history of all code changes, providing a complete audit trail. The platform’s visual differencing tools allow for a clear and immediate understanding of what has been changed, by whom, and when. Furthermore, Copia’s DeviceLink™ product automates the backup of device programs and provides a “single source of truth,” supporting rapid restoration to a known good state in the event of a system compromise or failure. This directly supports the SI requirement for protecting the IACS from unauthorized manipulation.

Foundational Requirement 4: Data Confidentiality (DC)

- While the primary focus is often on system integrity and availability in IACS, data confidentiality is also a crucial component of the standard. Copia helps protect sensitive intellectual property embedded in control logic by securing the code in a centralized, access-controlled repository.

Foundational Requirement 5: Restricted Data Flow (RDF)

- By providing a structured and auditable method for deploying code changes, Copia helps organizations manage the flow of information to and from the control system. This structured approach, with clear approval gates, mitigates the risk of unauthorized or malicious code being introduced into the IACS environment, supporting the RDF principle of network segmentation and controlled communication.

Foundational Requirement 6: Timely Response to Events (TRE)

- In the event of a cybersecurity incident or an operational issue, a swift and effective response is critical. Copia's detailed audit trails and version history are invaluable for forensic analysis, allowing teams to quickly identify the source of a problem. The ability to rapidly compare the running code on a device with the last known good version in the repository accelerates troubleshooting and reduces downtime. The platform's disaster recovery capabilities, powered by automated backups, support a timely return to normal operations.

Foundational Requirement 7: Resource Availability (RA)

- The ultimate goal of IACS security is to ensure the availability and reliability of the industrial process. By preventing unauthorized changes, enabling rapid recovery from failures, and streamlining troubleshooting, Copia's platform directly contributes to maximizing system uptime and ensuring resource availability.

Empowering a Secure Development Lifecycle (IEC 62443-4-1)

The ISA/IEC 62443-4-1 standard specifically addresses the requirements for a secure product development lifecycle. Copia's Industrial DevOps platform provides the foundational tooling to implement such a lifecycle for industrial automation code:

- **Change Management:** The platform's structured workflows for proposing, reviewing, approving, and deploying changes are central to a secure development process.
- **Version Control:** A complete and unalterable history of all code versions ensures that every change is tracked and auditable.
- **Testing and Validation:** By providing a sandboxed environment for code development and testing before deployment, organizations can validate the security and functionality of changes without impacting the production environment.
- **Documentation:** The inherent documentation capabilities of Git, combined with Copia's user-friendly interface, ensure that the "why" behind every change is recorded, providing invaluable context for future maintenance and security reviews.

In conclusion, for organizations in the manufacturing and distribution sectors seeking to align with the ISA/IEC 62443 standards, Copia Automation's platform is not merely a tool but a strategic asset. It provides the essential process and technology underpinnings to build a robust and auditable industrial cybersecurity program, moving from manual, error-prone processes to a modern, automated, and secure Industrial DevOps methodology.

Connect with the Copia Team

Schedule a demo now or reach out to us directly at contact@copia.io for a personalized consultation.