RUNSAFE SECURITY

Securing Industrial Software in Design & Operation

HOW RUNSAFE SUPPORTS IEC 62443-4 FOR ENERGY SYSTEM MANUFACTURERS

Energy infrastructure operates as an essential service where uptime, safety, and reliability are non-negotiable. Industrial systems run continuously for years, often with limited ability to patch or update software. At the same time, cyber threats are evolving, and create exposure to vulnerabilities that impact operations. To maintain uninterrupted operation of the infrastructure, these systems must remain secure and safe while in-service and throughout their lifecycle.

IEC 62443-4: WHAT MANUFACTURERS MUST DEMONSTRATE

Manufacturers supplying industrial control systems to energy infrastructure must align with **IEC 62443-4** to ensure products are designed with security as a foundation — not an afterthought. Manufacturers must demonstrate end-to-end security maturity across four core areas:

- **Secure Software Design** — Define how software is built and proactively designed against threats
- **Embedded Security** — Ensure products include the required security protections for operation
- **Visibility & Risk Awareness** — Understand software composition and where vulnerabilities exist
- **Lifecycle Vulnerability Management** — Remediate and respond to vulnerabilities throughout the lifecycle

HOW RUNSAFE SUPPORTS IEC STANDARDS

RunSafe strengthens how manufacturers meet IEC 62443 Series 4 by improving software resilience, visibility, and vulnerability management—without disrupting system operation or requiring code changes.

SECURE SOFTWARE DESIGN

Security designed into software architecture to reduce real-world exploit paths

- Identifies memory corruption vulnerabilities and exploitability using Risk Reduction Analysis, showing potential threats and attack feasibility
- Verifies software composition with build-time SBOMs to ensure no known vulnerable components are included
- Enables risk-informed design decisions based on actual exploitability, not just vulnerability presence

EMBEDDED SECURITY

Built-in runtime protections that defend software during operation

- Makes vulnerabilities non-exploitable by randomizing memory layouts and relocating functions at runtime
- Protects runtime software from memory-based attacks, even if vulnerabilities exist

VISIBILITY & RISK AWARENESS

Clear understanding of software composition and vulnerability exposure

- Provides automated build-time SBOM generation with full visibility into components and dependencies
- Identifies where vulnerable components exist across applications and systems
- Uses Risk Reduction Analysis to assess exposure to CVEs and zero-days, prioritizing patching based on exploitability

LIFECYCLE VULNERABILITY MANAGEMENT

Continuous risk reduction while patches are developed and deployed

- Monitors for new vulnerabilities and compares SBOM differences between builds to track changes
- Analyzes exposure to CVEs and potential zero-days to determine which vulnerabilities are exploitable
- Makes vulnerabilities non-exploitable at runtime, allowing systems to remain secure while patches are developed
- Supports lifecycle updates and triage through integrations with tools like GitHub, GitLab, and Bitbucket

A STRONGER CYBERSECURITY POSITION

RunSafe provides technical evidence and reporting that supports these elements.

Component	Supported by RunSafe
Secure Development Lifecycle Governance	**
Threat Modeling and Secure Design	✓
Software Component Visibility and Vulnerability Assessment	✓
Component Security Capabilities	✓
Vulnerability Response and Patch Management	✓

*** Subject to RunSafe customers' practice*

WHY RUNSAFE?

Industrial systems can't always be patched on demand — yet vulnerabilities exist. RunSafe helps manufacturers by making vulnerabilities non-exploitable at runtime and providing build-time SBOMs for full software visibility, strengthening in-service resilience and aligning with IEC 62443-4 across the full product lifecycle.

ABOUT RUNSAFE SECURITY, INC.

RunSafe Security proactively protects embedded software for both commercial and defense deployments across critical infrastructure, with comprehensive risk identification, protection, and monitoring, ensuring robust, continuous security without affecting performance. Headquartered in McLean, Virginia, with an office in Huntsville, Alabama, RunSafe Security's customers span the aerospace, defense, energy, industrial, and national security verticals. Learn more at: **RunSafeSecurity.com.**