

# WHAT A SECURE HMI SCADA PLATFORM REALLY LOOKS LIKE:

10 Principles That Define a Cyber-Resilient Platform



- Comprehensive protection across users, data, and systems

- Layered resilience against evolving cyber threats

- Granular control over users and critical operations

- Continuous assurance through ongoing vulnerability management

- Verified security backed by recognised industry standards

- Secure architecture for resilient operations

# WHEN HMI SCADA SECURITY FAILS

An operator logs into the system and sees normal conditions. Behind the scenes, unauthorized changes have already been made. Data has been altered, alarms suppressed, and system configurations modified without detection. By the time the issue is discovered, the impact is already operational, financial, and potentially safety-related.

Many organizations still approach HMI SCADA security primarily as a perimeter defense challenge, relying on firewalls, passwords, and network segmentation while overlooking the security capabilities built into the platform itself.

A secure HMI SCADA platform protects not only networks, but also users, identities, communications, data, applications, and system integrity throughout the operational lifecycle. Achieving this level of protection requires security to be designed into the platform, enforced across operations, and continuously strengthened over time.

Cybersecurity has evolved beyond protecting operational technology from cyber threats. Organizations increasingly face regulatory obligations such as the EU Cyber Resilience Act (CRA), NIS2 Directive, Digital Operational Resilience Act (DORA), GDPR, and emerging AI governance frameworks. These evolving regulations are raising expectations for secure software development, cyber resilience, operational transparency, and risk management across critical infrastructure. Building secure HMI and SCADA systems therefore supports both operational resilience and regulatory readiness.

The following principles define what a secure system really looks like in practice.

1

## SECURITY BEGINS AT THE PLATFORM

Security cannot be layered onto a solution after deployment. Secure design, development, and testing must be embedded throughout the platform lifecycle to establish a foundation for long-term protection. Secure development practices, rigorous testing, and continuous validation establish the foundation for long-term resilience and cybersecurity.

2

## DEFENSE IN DEPTH STRENGTHENS RESILIENCE

No single control is sufficient. Secure SCADA environments rely on multiple layers of protection across people, physical infrastructure, networks, hosts, applications, and data. This layered approach reduces risk and limits the impact of a breach.

3

## GRANULAR IDENTITY AND ACCESS CONTROL PROTECTS CRITICAL OPERATIONS

Access to systems, data, and functionality is tightly controlled through role-based access, group-level permissions, and integration with enterprise identity providers like OAuth 2.0 and OpenID Connect (OIDC), including support for multi-factor authentication where required.

4

## DATA PROTECTION EXTENDS ACROSS THE SYSTEM

Data protection extends across both data at rest and data in motion. Encryption, secure transport protocols, and certificate-based authentication maintain confidentiality, integrity, and authenticity throughout the system.

5

## SECURE COMMUNICATION UNDERPINS MODERN SCADA

Modern SCADA environments rely on communication frameworks that support authentication, encryption, and trusted session management across distributed systems, helping protect data and operations as connectivity expands.

6

## BUILT-IN AUDITABILITY SUPPORTS ACCOUNTABILITY

Every action is traceable through detailed logging and audit trails. This visibility strengthens accountability, supports compliance requirements, and enables faster investigation of anomalies, operational issues, or security incidents.



## 7 SECURITY EXTENDS ACROSS THE LIFECYCLE

Security spans development, delivery, installation, configuration, and ongoing operations. Continuous validation and improvement sustain a strong security posture over time and through future upgrades.

## 8 SECURE ARCHITECTURE REDUCES EXPOSURE

Secure platforms align with network architectures that support segmentation, DMZ strategies, and secure connectivity across distributed environments, reducing exposure while supporting operational resilience.

## 9 VULNERABILITY MANAGEMENT IS ONGOING

Security evolves over time. Effective platforms come from vendors that support structured vulnerability reporting, coordinated disclosure, and timely response to emerging threats before risk becomes operational impact.

## 10 STANDARDS AND COMPLIANCE DEMONSTRATE SECURITY MATURITY

Adherence to recognized standards such as IEC 62443, ISO/IEC 27001, CMMC, and ISO 9001 demonstrates a commitment to security, quality, and industry best practices. Compliance with established standards also provides greater confidence for customers, stakeholders, and regulated industries while helping organizations support evolving cybersecurity and regulatory requirements.

## SECURITY IS THE STANDARD, NOT A FEATURE

Secure HMI SCADA is not defined by a checklist of features. Security is defined by how a platform is designed, deployed, operated, and continuously improved throughout its lifecycle.

Organizations that rely on fragmented solutions or outdated approaches increase exposure to operational and cybersecurity risk. A resilient security strategy requires a platform that unifies protection across systems, data, users, and infrastructure.

GENESIS, the intelligent HMI/SCADA platform from Mitsubishi Electric Iconics Digital Solutions, was designed around these principles, combining secure development practices, built-in protections, and support for layered security architectures to help organisations strengthen cybersecurity across manufacturing, buildings, infrastructure, and industrial environments.

GENESIS helps organizations implement the principles required for secure, mission-critical operations across manufacturing, buildings, infrastructure, and industrial environments.

# BUILD A MORE SECURE HMI SCADA ENVIRONMENT

Download the

***Highly Secure HMI SCADA and Automation Systems Whitepaper***

To explore the architecture, development practices, and cybersecurity principles behind a modern secure HMI SCADA platform.

OR

Connect with a

**GENESIS Expert**

To see how these principles apply in real-world environments.



## ABOUT MITSUBISHI ELECTRIC ICONICS DIGITAL SOLUTIONS

Mitsubishi Electric Iconics Digital Solutions, headquartered in Foxborough, Massachusetts, is a global leader in industrial automation, smart and sustainable buildings, and digitalization software. Our advanced HMI, SCADA, and Smart Building solutions enable businesses to visualize, monitor, and optimize their most critical assets and spaces. With installations in over 100 countries and adoption by more than 70% of Global 500 companies, we drive operational efficiency and continuous improvement across industrial manufacturing, infrastructure, and built environment sectors. Backed by cutting-edge technology and deep industry expertise, we deliver flexible, scalable, and high-performance software solutions. As a testament to our excellence, Mitsubishi Electric Iconics Digital Solutions has been recognized as a seven-time winner of the Microsoft Partner of the Year award.

### Mitsubishi Electric Iconics Digital Solutions Sales Offices

**World Headquarters**  
2 Hampshire Street  
Foxborough, MA, USA, 02035  
+1 508 543 8600  
info@iconics.com

|                                            |                                           |                                              |                                               |                                       |
|--------------------------------------------|-------------------------------------------|----------------------------------------------|-----------------------------------------------|---------------------------------------|
| <b>Australia</b><br>australia@iconics.com  | <b>France</b><br>france@iconics.com       | <b>Japan</b><br>japan@iconics.com            | <b>Philippines</b><br>philippines@iconics.com | <b>UK</b><br>uk@iconics.com           |
| <b>Brazil</b><br>brazil@iconics.com        | <b>Germany</b><br>germany@iconics.com     | <b>Malaysia</b><br>malaysia@iconics.com      | <b>Singapore</b><br>singapore@iconics.com     | <b>Vietnam</b><br>vietnam@iconics.com |
| <b>Canada</b><br>canada@iconics.com        | <b>India</b><br>india@iconics.com         | <b>Mexico</b><br>mexico@iconics.com          | <b>South Korea</b><br>southkorea@iconics.com  |                                       |
| <b>China</b><br>china@iconics.com          | <b>Indonesia</b><br>indonesia@iconics.com | <b>Middle East</b><br>middleeast@iconics.com | <b>Taiwan</b><br>taiwan@iconics.com           |                                       |
| <b>Czech Republic</b><br>czech@iconics.com | <b>Italy</b><br>italy@iconics.com         | <b>Netherlands</b><br>holland@iconics.com    | <b>Thailand</b><br>thailand@iconics.com       |                                       |

## MITSUBISHI ELECTRIC ICONICS DIGITAL SOLUTIONS, INC.

HEAD OFFICE: 2 Hampshire Street, Suite 300, Foxborough, MA 02035