MITSUBISHI ELECTRIC
Changes for the Better

Automating the World

Highly Secure HMI/SCADA and Automated Systems

Contents

Copyright and Confidentiality

Authors

Joshua Obal, Senior Product Security Lead

Revision	**11.0**
Issued	10/8/2025

1 Introduction

Mitsubishi Electric Iconics Digital Solutions (also referred to as 'the company') products have a history of installation in mission-critical and highly secure applications. These systems are in use at some of the most secure Defense Department applications, both for the US Department of Defense and for those of other nations. The software products are also routinely installed in FDA regulated sites, regulated utility and national grid installations, and other critical infrastructures. These applications require the products to be designed for, and tested to meet rigid requirements.

Mitsubishi Electric Iconics Digital Solutions uses features such as encryption, certificate authentication, user and system encrypted passwords, and obfuscation to provide the highest level of security demanded by today's systems. Equally important, the system is designed to be extremely flexible for system administrators, so all system-to-system and system-to-client interface parameters can be adjusted to work within a customer's secure infrastructure.

This document will present an overview of the many features and qualities of Mitsubishi Electric Iconics Digital Solutions applications that establish suitability for secure projects.

1.1 Security for Mission-Critical Applications

We have invested millions of dollars in our product technology, including our commitment to maintaining rigorous security standards. As a company that provides customers with products that help them operate their industrial, manufacturing, and mission-critical facilities, Mitsubishi Electric Iconics Digital Solutions utilizes the latest security technologies and protocols, as well as operational best practices, to ensure that our customers' information is handled with care.

1.2 Attention to Detail at Every Step

We employ a multi-step review process across many phases of the software development lifecycle. We utilize a multi-phase development lifecycle that includes unit testing, integration testing, system testing, and performance testing. Each new feature undergoes dedicated security testing, including stress tests to validate security and control mechanisms.

1.3 Restricted Access and Secure Communications

Real-time data can only be accessed by authorized users. At the customer's discretion, only defined clients can communicate to the servers. In addition, access to the system can be controlled by user and group level permission. Mitsubishi Electric Iconics Digital Solutions' extensive use of OPC Unified Architecture security model secures communications, and encryption ensures that data security is held to the highest standards.

1.4 Redundant Operations and Mission-Critical Technology

Our extensive redundant technology is employed at many mission-critical facilities. Redundant servers can be located in the same facility or across the country, offering maximum flexibility. From STIG certified product installation to secure communications and transaction audit trails using proven FDA 21 CFR Part 11 practices, our solutions are deployed in the most business-critical applications.

2 Defense in Depth in Product Development

2.1 Secure Product Development Environment

Mitsubishi Electric Iconics Digital Solutions prioritizes security at every stage of development. We have achieved ISO/IEC 27001:2022 certification, the internationally recognized standard for information security management. This certification validates our efforts to adhere to security best practices, not only for product development, but also for the entire organization. Additionally, our development processes have been certified to meet the IEC 62443 Part 4-1 Secure product development lifecycle requirements. This section highlights some of the security measures employed in the software development process.

2.1.1 Physical Security

Our offices are secure facilities with video surveillance, individual keycard access, and separate locked rooms for all servers, all to ensure that no unauthorized personnel gain access to the development and build environments containing product code and other sensitive information.

2.1.2 Virtual Security

We maintain a secure VPN for our employees. The VPN secures the data within the company and protects the online privacy of our employees. Separate guest networks are required for visitors. Internal access to network resources is appropriately reviewed and restricted.

2.1.3 Secure Build Environment

The company requires the usage of secure software development and project management tools that manage the engineering team and their workflows. The tool covers the entire software development life cycle with built-in security, including authenticated accounts and authorization-based permissions for users and groups. Access to sensitive information such as private keys is highly restricted.

2.2 Security Training

All Mitsubishi Electric Iconics Digital Solutions employees must regularly complete security awareness training. In addition, development and test team members must complete advanced security training on designing, developing, and testing secure products. Team members also receive training on the tools used for secure development and testing.

2.3 Security in the Design Process

2.3.1 Digital Security

The product code repositories are protected digitally, requiring user credentials to access different parts of the code based on the assigned permissions. Users are unable to access code unless approved.

2.3.2 Secure Threat Modeling and Code Reviews

The development team maintains and regularly reviews a security threat model for the company's software. In addition, secure code reviews are performed as needed to look for potential issues that could lead to security holes. Security-related issues are addressed as soon as these are discovered, and a clear history is maintained for all such reviews.

2.3.3 Secure Code Analysis and Penetration Testing

The company uses source code analysis tools to identify potential security vulnerabilities in our source code. These tools detect known vulnerabilities in third-party components as well as insecure coding practices in internally developed code. In addition, we work with third parties to perform penetration tests on our products. Our security validation efforts include for-hire penetration testing companies, feedback from security

researchers via our website or email, and participation in ethical hacking competitions that encourage discovery of potential vulnerabilities in our products.

2.3.4 Open Source and Third-Party Vulnerability Monitoring

Company policy requires that all third-party software be reviewed and approved before use in our products. Factors considered in the evaluation include quality, reputation, security, and licensing terms. We also keep third-party code as up to date as possible to help ensure that known security issues are addressed. In addition, the company continuously monitors all third-party software in its products for potential vulnerabilities.

2.4 Security Features Built into the Product

The company's products include a security system that allows system administrators to restrict access to functions based on the concept of a logged-in user. Features of the security system include the ability to create users and groups or to integrate with Active Directory or Azure Active Directory. The security system allows user permissions to be assigned for controlling applications, data sources, assets, and alarms. More information on the security system and the many other security features included in the company's products can be found below in the sections titled "Product Security Features – Configuration Security" and "Product Security Features – Runtime Security".

2.5 Secure Delivery of the Product

2.5.1 Binary Signing / Strong Name Signing

Mitsubishi Electric Iconics Digital Solutions binaries use strong name signing, which provides versioning and naming protection, along with a strong integrity check. This security process allows us to guarantee that the contents of the assemblies have not been changed since being built.

2.5.2 DigiCert

The company binaries are signed by DigiCert, which ensures that the files being used have not been tampered with or changed without our authentication. For more information on DigiCert, see their website

2.5.3 Product Deliveries are Free from Viruses and Malware

Prior to product release, all the company's software packages are thoroughly scanned to ensure that no virus or malware content is incorporated into the delivered software. This security process helps prevent would-be intruder software components from being installed with our software.

2.5.4 Secure Website Host

We maintain secure websites where the binaries can be downloaded, licenses can be obtained, and online product help can be accessed, in addition to many other useful resources. For the latest information on security, please visit our security webpage.

2.6 Secure Installation

The GENESIS product is designed and installed in a way that helps to secure the system. Out of the box, the product services are installed to run under a Network Service account, limiting the privileges to those that are strictly necessary for standard operations. The post-installation system configuration utility guides users through options that can be used to securely configure SQL Server connectivity.

Users should review the following help topic before deploying the system, to help achieve a secure environment: Security Best Practices in GENESIS Version 11.

2.7 Management of Security Issues

Mitsubishi Electric Iconics Digital Solutions has a defined process for the handling and management of security issues. This process includes guidelines for reporting security vulnerabilities, an established process

for reviewing, analyzing and addressing these issues, and a process for documenting and disclosing these issues.

2.7.1 External Guidelines for Reporting Security Issues

The company guidelines for reporting a security vulnerability are as follows:

If you believe you have discovered a security vulnerability in a company product, we encourage you to:

- Submit information about a potential security vulnerability using the forms provided here, which will guide you through the process.
- Email the details of the potential security vulnerability to secure@iconics.com. Please include details on the product, product version, configuration, and if possible, the steps to reproduce the vulnerability so that we can duplicate the issue being reported. We encourage the use of encryption using our public PGP key which can be found here, Mitsubishi Electric Iconics Digital Solutions values the members of the independent security research community who find security vulnerabilities and collaborate with the company to ensure security fixes are issued to all customers. The company's policy is to credit all researchers in the company Whitepaper on Security Vulnerabilities when a fix for the reported security bug is issued. To receive credit, security researchers need to follow responsible disclosure practices including:
- **Not publish** the vulnerability before the company releases a fix.
- **Not divulge** exact details of the issue, such as exploits or proof-of-concept code.

If vulnerabilities are discovered in third-party software components used in Mitsubishi Electric Iconics Digital Solutions products, researchers should report these using the company's security vulnerability reporting process.

2.7.2 PSIRT

Mitsubishi Electric Iconics Digital Solutions has a Product Security Incident Response Team (PSIRT) as part of its organization. This global team manages the receipt, investigation, and public reporting of security vulnerability information related to the company's products.

2.7.3 Cooperation with CISA and Security Researchers

The United States Cybersecurity & Infrastructure Security Agency (CISA) is responsible for leading the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure. The cybersecurity division of CISA handles vulnerability management to reduce the prevalence and impact of vulnerabilities and exploitable conditions across enterprises and technologies, including through assessments and coordinated disclosure of vulnerabilities reported by trusted partners.

Mitsubishi Electric Iconics Digital Solutions maintains communications with CISA for the coordination of vulnerability disclosures. CISA directly communicates with the company's PSIRT manager or another PSIRT team member assigned to a specific case. We are positioned to promptly analyze and remedy potential security vulnerabilities reported by CISA, including those reported by security researchers.

If and when we address a critical or major security vulnerability that can affect public infrastructure, we coordinate the release of the information on the vulnerability with CISA so that a CISA advisory can be issued to properly inform our customers. T The advisory includes information such as the disclosure date, vendor name, severity (CVSS score), affected product and versions, vulnerability description, and recommended mitigation steps.

2.7.4 Whitepaper on Security Vulnerabilities

The company maintains a whitepaper on the security vulnerabilities in its products. This whitepaper contains information on the known security vulnerabilities and the mitigations that are available for these vulnerabilities. The white paper on security vulnerabilities can be found on the company website here.

3 Product Security Features – Configuration Security

The tools used to configure a GENESIS system include the following built-in security features.

3.1 Workbench Access

User access to the GENESIS Workbench is controlled so that only authorized users can gain access to the Workbench and make system configuration changes.

3.2 Audit Trail of Configuration Changes

The GENESIS Workbench can log all system configuration changes to a database and supports the ability to retrieve, view, and export the configuration changes made over any time period.

3.3 Configuration Database Security

GENESIS natively supports SQL Server security, allowing both NT and SQL authentication to access databases. Local as well as remote secure database access is supported. GENESIS also supports Entra ID (formerly Azure Active Directory) Security to grant secure connections to Azure SQL Databases.

3.4 Project Deployment Security

GENESIS project management and deployment are managed with the “Pack and Go” feature. Pack and Go files created with the GENESIS Workbench can be optionally password-protected, ensuring these files cannot be tampered with.

3.5 Certificate Management

GENESIS Workbench allows users to configure secure connections via certificates for MQTT, IoT Hub, BACnet with SC, and OPC UA connectivity. When configuring connections to OPC UA servers, users can accept or reject the server’s certificate. To ensure security, all communications between FrameWorX Server, clients, and remote FrameWorX servers should use HTTPS connectivity.

Workbench supports the configuration of the OPC UA certificates used by the FrameWorX Server and data historian for providing OPC UA connectivity to third party clients and for connecting to other OPC UA servers.

4 Product Security Features – Runtime Security

The runtime environment of a GENESIS system includes several built-in security features.

4.1 Security Server and User Access Controls

The Security Server provides restricted access to functionality based on the concept of a logged-in user. A security system administrator configures the system by adding users and assigning specific privileges to these.

4.1.1 User and Group Access and Authentication Controls

The Security Server includes the ability to control user access and privileges for individual users or entire groups of users within the system. Password strength and renewal requirements may be enforced, as may auto-logouts due to inactivity. Additionally, user access can be restricted based upon time of day, or for individually cited critical points.

The Security Server also provides the capability to enforce a configurable limit on the number of consecutive invalid access attempts by any user during a configurable time period and provides the capability to deny access for a specified time period or until unlocked by an administrator when this limit has been exceeded. Additionally, it can support a supervisor manual override of the current human user authorizations (which can be accomplished by a different user log in which does not close the current session).

The Security Server offers nearly identical security options for user accounts and for groups. Security permissions can be granted at the group level, the user level, or both.

Items that can be secured include application actions, data points, alarms, files, stations (limiting what machines a user may log into), methods, assets, reports, transactions, mobile layouts, and custom security tokens. Each of these security-controlled items is defined further in the product documentation.

4.1.2 Microsoft Active Directory Integration

The Security Server can retrieve its list of validated users from a specified domain or a group within that domain either from the Active Directory or from the Entra ID (formerly Azure Active Directory). The validated user account is granted permission by the Security Server to access various capabilities within the GENESIS system. If a user account is removed from the active directory domain, this change will be reflected in the Security Server and unauthorized access will be prevented.

The Security Server can also be configured to automatically log in or out when a matching Windows user logs in or out. When this feature is enabled, the user is logged into GENESIS Security automatically using either NTLM or Kerberos authentication.

4.1.3 Use of External Identity Providers and MFA

GENESIS Security can be configured to forward user authentication to an external web page using either the OpenID Connect or SAML 2.0 protocol. The external authentication web page can then perform Multi-Factor Authentication (MFA) per its capabilities. The GENESIS Security does not support MFA.

4.2 Data Security

4.2.1 SCADA Visualization Password Security

GraphWorX displays can be optionally password-protected, securing project work and ensuring that no unauthorized users can change displays.

4.2.2 Data At Rest Security

GENESIS natively supports SQL Server security, allowing both NT and SQL authentication to access databases. Local as well as remote secure database access is supported.

Recommendation: Secure the SQL Server database(s) used in the system by encrypting the databases. Additionally, apply the best practices as defined in the Microsoft article: SQL Server security best practices - SQL Server | Microsoft Learn.

4.3 Security Event Logging

4.3.1 Runtime Application Audit Trail

Many of the GENESIS applications and servers, including the Alarm Server, Reporting, Bridging, GraphWorX64, and others may be configured to log detailed operator changes to the GENESIS audit log. This tracking provides audit support for discovering the person that made system changes, including details of the changes and when these changes were made.

I In many SCADA applications, maintaining a detailed audit trail of system changes is essential for diagnosing issues and ensuring accountability. Industries such as pharmaceuticals, water and wastewater, and other mission-critical operations require this level of auditing to meet compliance and operational standards. GENESIS includes a built-in feature that allows users to easily enable audit logging.

4.4 Communication / Data in Motion Security

Communication over a network has always carried potential security risks. GENESIS employs the following methods to keep data safe and applications secure when communicating between two or more machines.

4.4.1 OPC Unified Architecture

OPC UA security is concerned with the authentication of clients and servers, the authentication of users, the integrity and confidentiality of their communications, and the verifiability of claims of functionality. This security is achieved through the Discovery and Session Establishment of the connections as well as the encryption of the data transport layer.

Recommendation: Do not use classic OPC communications since classic OPC servers do not provide any security.

4.4.2 OPC UA Discover and Session Establishment

Application-level security relies on a secure communication channel that is active for the duration of the application session and ensures the integrity of all messages that are exchanged.

When a session is established, the client and server applications negotiate a secure communications channel and exchange software certificates that identify the client and server and the capabilities that these entities provide. Authority-generated software certificates indicate the OPC UA profiles that the applications implement and the OPC UA certification level reached for each profile. Certificates issued by other organizations may also be exchanged during session establishment.

4.4.3 OPC UA Transport

Transport level security can be used to encrypt and sign messages. Encryption and signatures protect against disclosure of information and protect the integrity of messages. Encryption capabilities are provided by the underlying communications technology used to exchange messages between OPC UA applications.

4.4.4 FrameWorX

FrameWorX is the GENESIS secure communications platform service that provides data transport between application servers, clients, and network applications. It allows for communication between machines that are

on different subnets, domains, or even across the Internet. FrameWorX utilizes WebSockets by default for its transport layer and supports HTTPS encryption and Integrated Windows Authentication for achieving secure communications.

FrameWorX is fully compatible with firewalls and DMZs and can be configured to comply with IT administration security policies.

FrameWorX supports secure communications for the following types of data sources:

- Real-Time Data Sources (OPC UA, BACnet, SNMP, Sparkplug B, and more)
- Database Access

Workbench supports the configuration of OPC UA certificates used by FrameWorX Server and data historian for providing OPC UA Connectivity to third party clients and for connecting to other OPC UA servers.

4.5 Other Data Communications Security

4.5.1 Allowed Clients

Client access to FrameWorX Server can be restricted by explicitly defining their IP addresses and computer names in the Platform Services Configuration dialog (in Workbench -> Tools -> Access Restrictions tab). Only clients whose IP addresses match the specified range(s) and whose computer names match the allowed name(s) will be allowed to connect.

Note that the address range uses IPv4 and IPv6. Allowed computer names may use wildcard character notation. By default, all IP addresses and all computer names are allowed.

4.5.2 Password-Based Protection

FrameWorX Server contains built-in runtime security checking. Use the Password tab in the Platform Services Configuration dialog to specify usernames and passwords for various applications that need to securely connect to FrameWorX Server.

4.5.3 Port Security

GENESIS communicates over multiple ports, and each one can be configured. Allowing the port numbers to be changed means that a malicious user cannot be sure what port to listen on or attack. We strongly recommend closing ports which are not necessary on machines in order to help maximize the security of the system against malicious attacks.

4.5.4 HTTPS/SSL

GENESIS communications can be configured to use SSL to encrypt communication over the web. For details, please see the following help topics:

- Setting Up the Connection to the FrameWorX Server
- Creating a Certificate
- Direct and Reverse FrameWorX Connection Overview
- Creating an OPC UA Connection

5 Defense in Depth in Automation System

This section describes the implementation of a layered approach for adding security protection to automation systems such as those based on GENESIS. The approach is called Defense in Depth.

Adding Defense in Depth is not a simple exercise where certain technologies are deployed to counter specific risks but requires a comprehensive, system-wide approach to protect all assets. The strategy considers interconnections and dependencies and uses available resources to build effective layers of monitoring and protection. Additionally, Defense in Depth is not a single aspect but a combination of many, including people, technology, operations, and adversarial awareness, all working together to strengthen overall security.

5.1 Defense in Depth Layers

To help with the understanding and implementation of Defense in Depth, it is beneficial to look at it as a set of definable layers. The idea of this layered approach is to provide multiple redundancies if the event systems and data are compromised. If one security layer is breached, Defense in Depth means that many more security layers lie before the attacker to increase the difficulty of a complete breach. Although there is no universally agreed upon standard list of layers, many of the Defense in Depth models include most if not all the layers listed in Table 1 below:

Table 1 – Defense in Depth Layers

	Layer Name	**Examples**
6	Human Layer	Policies and procedures, training
5	Physical Layer	Physical security, ID cards, CCTV, fences
4	Network Layer	Firewalls, VPNs, monitoring, alerting
3	Host Layer	Timely security patching, restricting unwanted services
2	Application Layer	Secure coding, deployment, patching, roll-based access
1	Data Layer	File and data encryption, enterprise rights management

Another way of showing the Defense in Depth layers is provided in Figure 1 below. The idea is that if an attacker gets by the first layer of defense (The Human Layer), they then will need to get past the second layer of defense (physical), and so on.

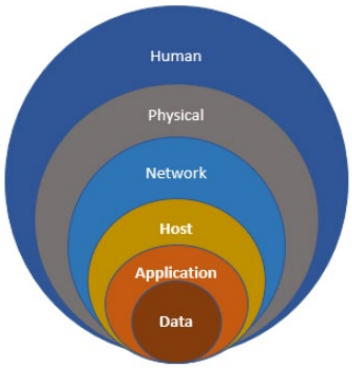

Figure 1 – Defense in Depth Layers

5.2 Risk Management

The attack surface for an automation system includes all the ways an attacker could gain access to the systems or equipment considered critical to business operations. To reduce the likelihood of an attack, an organization must implement controls to reduce the attack surface for critical assets. Determination of what controls are needed, and the implementation of such controls are all part of a process called Risk Management. The Risk Management process typically includes the steps listed in Table 2 below:

Table 2 – Risk Management Steps

	Risk Management Step
1	Inventory assets
2	Determine criticality of each asset
3	Identify the security risk for each asset
4	Determine the potential impact
5	Identify security controls needed
6	Implement security controls

To begin the Risk Management process, an organization must first identify the subsystems and components that are considered business or mission critical (Steps 1 and 2).The organization then performs a cybersecurity risk analysis (Step 3) to identify current threats, vulnerabilities, and risks to the system or operations, as well as the potential impact if a threat is realized (Step 4) Once these steps are completed, the organization identifies the security measures to counter the risks (Step 5) and puts those measures in place (Step 6).The remainder of this section provides insights and recommendations for Risk Management Steps 3–6, with a focus on automation systems based on GENESIS. These insights and recommendations are organized according to the Defense in Depth layers mentioned above.

5.2.1 Defense in Depth – Human Layer

As noted in the recommended practices on Defense in Depth Strategies by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)[1], organizations face many challenges in managing the human factor within their organizations. Large and complex systems are susceptible to mistakes made by inexperienced or untrained personnel, as well as the activities of malicious insider threats.

According to ICS-CERT, organizations should have the following measures in place to address these concerns:

1. Policies - Clear, actionable policies are necessary to lay the framework for rigorous controls that secure ICS technologies and also provide the governance needed to manage human factors.
2. Procedures – Procedures that state how personnel should conduct a particular process or configure a particular system are necessary to ensure secure functioning and provide a standard, repeatable means to accomplish a task in a safe manner.
3. Training and Awareness – Specialized security training for automation systems is necessary. Operators and IT personnel should know what the indicators of potential compromise look like and what steps they should take to ensure that a cyber investigation succeeds. Management should also know what they can do to make the system more secure, so they can make informed decisions regarding the costs and benefits of the protection measures they put into place.

5.2.2 Defense in Depth – Physical Layer

As noted in the recommended practices on Defense in Depth Strategies by ICS-CERT[1], physical security measures reduce the risk of accidental or deliberate loss or damage to organizational assets and the surrounding environment. The assets being safeguarded include physical assets such as tools and plant equipment, the environment, the surrounding community, and intellectual property including proprietary data such as process settings and customer information. Organizations should tailor physical security controls, like technical controls, to the type of protection needed.

Physical security controls are any physical measures, either active or passive, that limit physical access to any information assets in the automation system. Per ICS-CERT[1], organizations should employ the following measures to prevent undesirable system impact such as the following:

- Unauthorized physical access to sensitive locations.
- Unauthorized physical modification, manipulation, theft or other removal, or destruction of existing systems, infrastructure, communications interfaces, personnel, or physical locations.
- Unauthorized observation of sensitive information assets through visual observation, note taking, photographs, or other means.
- Unauthorized introduction of new systems, infrastructure, communications interfaces, or other hardware
- Unauthorized introduction of devices intentionally designed to cause hardware manipulation, communications eavesdropping, or other harmful impact such as a universal serial bus (USB) memory device, wireless access point, or Bluetooth or cellular device.

Physical measures that can be applied to an automation system include those listed in Table 3 below[1]. Along with the physical measures listed, information on possible GENESIS system support is provided.

Table 3 – Physical Measure Applicable to Automation Systems

	Layer Name	**Examples**
1	Facility access controls	GENESIS monitoring of the third-party facility access control system (via standard industry communications protocols) may be possible and advantageous.
2	Control and server room access	GENESIS monitoring of the third-party facility access control system (via standard industry communications protocols) may be possible and advantageous.
3	Multi-Factor Authentication for physical access (e.g., key card, biometric)	GENESIS supports the option to integrate with 3rd party Multi-Factor Authentication products.
4	Facility monitoring using cameras, motion detectors, access control and environmental sensors, etc.	GENESIS supports the integration of video signals into its system.
5	Alerting for device manipulations such as power removal, device resets, etc.	The GENESIS Alarming capabilities can be used for implementing alerts.
6	Visitor escort requirements and procedures	

[1]Recommended Practice: Improving Industrial Control System Cybersecurity with Defense in Depth Strategies – Industrial Control System Cyber Emergency Response Team, September 2016 -

https://www.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

5.2.3 Defense in Depth – Network Layer

The recent convergence of once-isolated automation networks with modern IT networks has created new attack surfaces and expanded opportunities for cyberattacks. To help reduce the attack surfaces of automation systems at the network layer, both ICS-CERT[1] and NIST[2] have made recommendations for network architectures for Industrial Control System / Automation Systems.

One important recommendation is a network architecture that is based on zones with firewalls strategically placed between the various zones. Figure 2 shows a network architecture recommended by ICS-CERT[1], one which divides the network layer into zones.

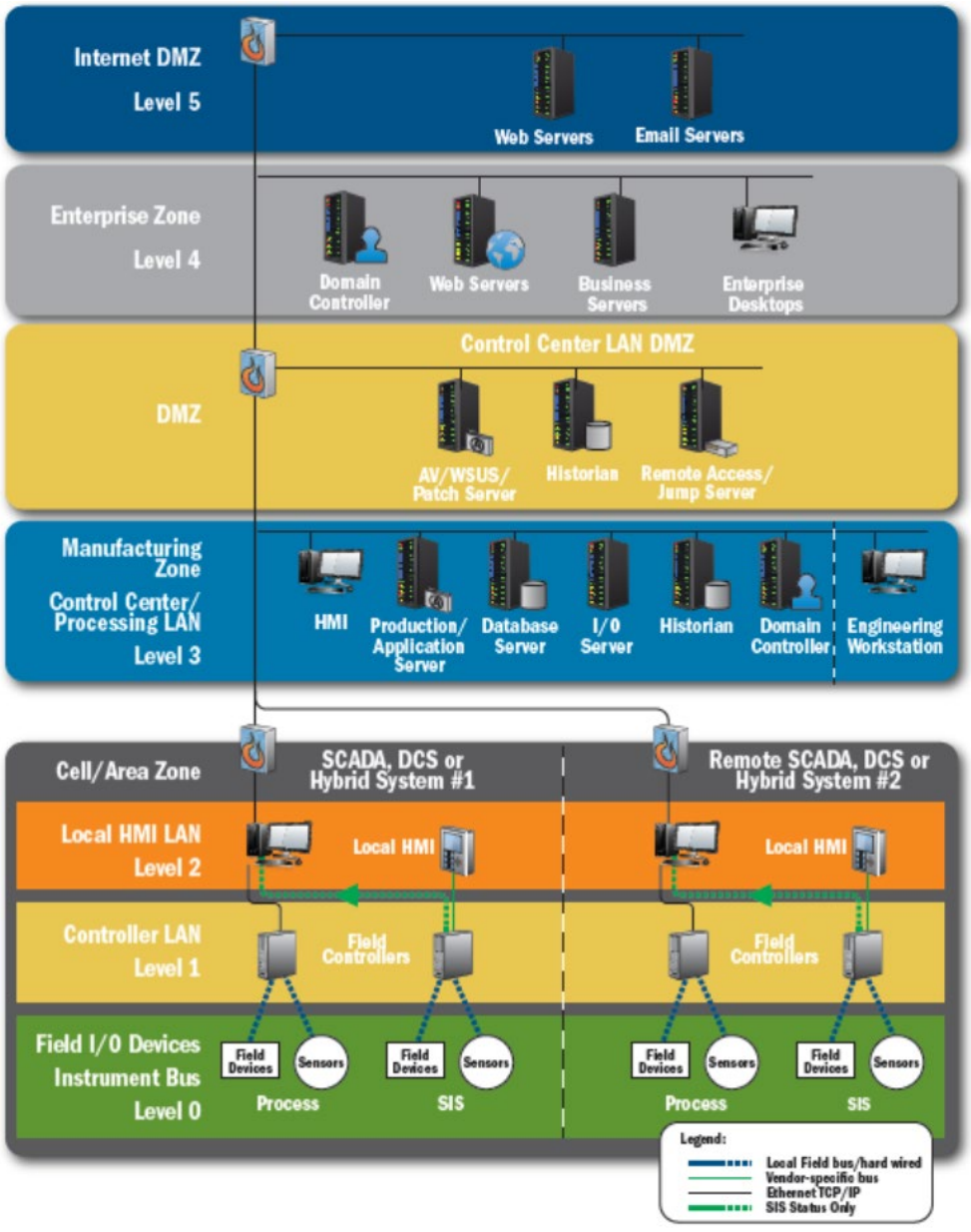

Figure 2 – Zone Segmentation recommended by ICS-CERT[1]

Notably, the architecture and design of GENESIS make it an excellent fit with the network architecture recommended by ICS-CERT[1] and by NIST[2] in their Guide to Industrial Control System (ICS) Security. Figure 3 shows a GENESIS system architecture diagram with zone segmentation, illustrating how GENESIS fits into the network architecture model recommended by ICS-CERT and NIST.

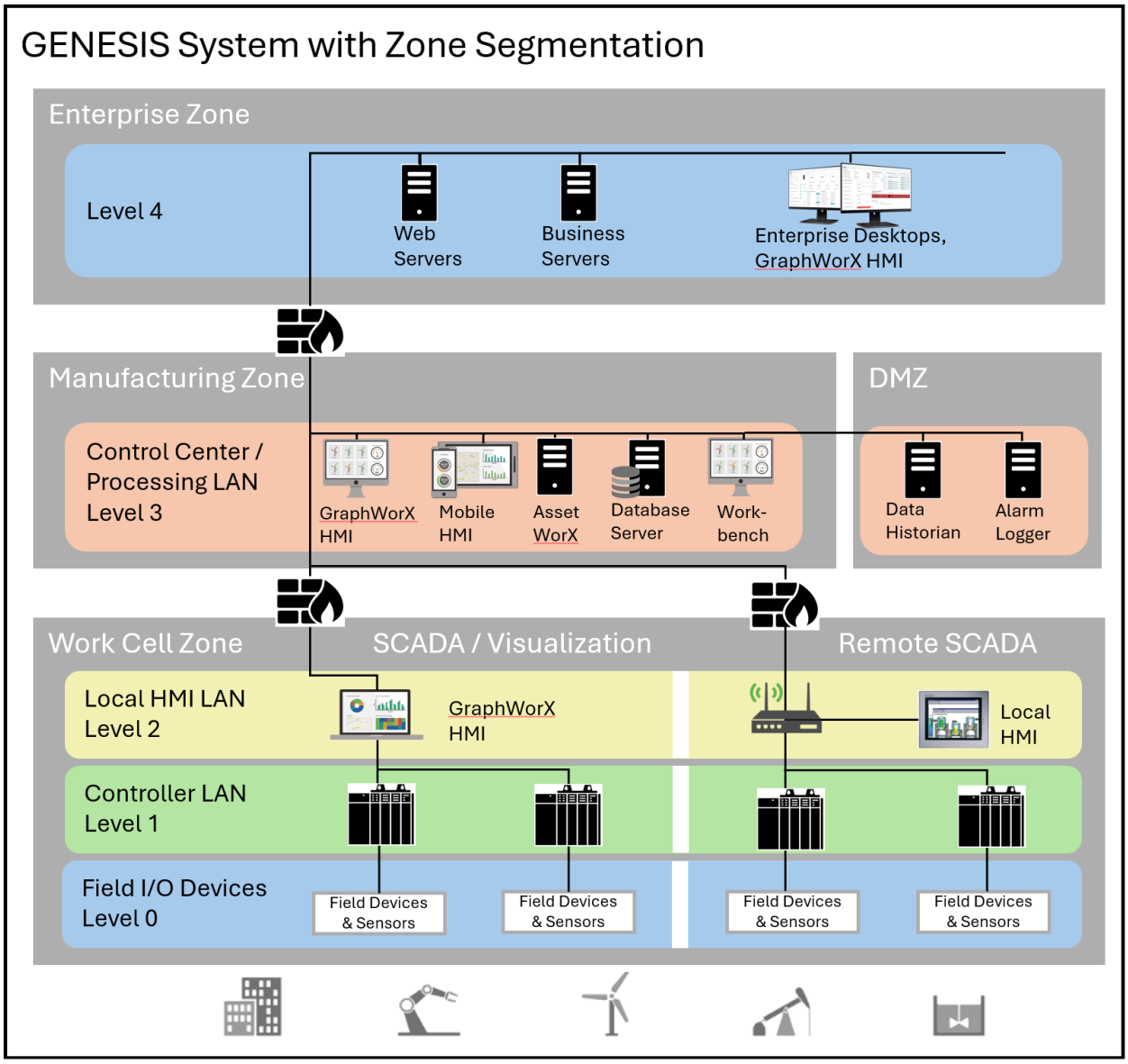

Figure 3 – Example of GENESIS System Architecture with Zone Segmentation

[1]Recommended Practice: Improving Industrial Control System Cybersecurity with Defense in Depth Strategies – Industrial Control System Cyber Emergency Response Team, September 2016 -

https://www.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

[2]NIST Special Publication 800-82 Revision 2 – Guide to Industrial Control Systems (DCS) Security -

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

5.2.4 Defense in Depth – Host Layer

The host or workstation level implements another layer of security. While firewalls protect most devices within a network from intrusion from the outside, a good security model requires multiple layers of defense. This layered approach is especially critical for HMI clients that can connect to the network from outside the trusted automation system network boundary, either via a VPN connection or other means. As a result, to completely secure the network means securing all hosts as well.

The ICS-CERT document "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies"[1] lists several host-level security measures that warrant consideration. Table 4 summarizes key measures and includes notes on how each is supported within a GENESIS system. Note, this table is not the complete list of host security measures. For a complete list, please refer to the ICS-CERT document.

Table 4 – Host Layer Security Measures Applicable to Automation Systems

	Layer Name	Examples
1	Install and configure a host-based firewall.	GENESIS is compatible with / works with firewalls.
2	Choose strong passwords for all accounts on the system and change any default or well-known accounts on the device (preferably, enforce strong passwords and password expiration through operating system capabilities).	The GENESIS Security Server supports integration with Active Directory allowing use of the same passwords and password management used by the host.
3	Change passwords on a pre-defined schedule – usually every 30 days but not more than 90 days.	The GENESIS Security Server supports a password expiration feature, which forces a user's password to expire after a predefined period of time.
4	Install screen savers with short intervals and require a password to log back in whenever possible.	The GENESIS Security Server has the capability to automatically log out the GENESIS user if there is no screen activity for a pre-defined amount of time.
5	Disable unused services and accounts.	GENESIS allows unused services to be disabled so that only the required ones remain enabled.
6	Remove any unnecessary native software from the system that is not needed or used.	GENESIS allows users to select which products are installed, ensuring that only the required components reside on the host.

5.2.5 Defense in Depth – Application Layer

The Application level implements another layer of security. While host- and upper-layer security measures help prevent cyberattacks, built-in safeguards at the application layer provide an additional line of defense. Application Layer security measures built into the GENESIS include those listed in Table 5 below.

Table 5 – Application Layer Security Measures Applicable to Automation Systems

Application Layer Security Measure	Benefit
GENESIS is designed and developed using a secure product development lifecycle. The development process follows the IEC 62443 Part 4-1 standard.	Ensures the product is highly secure.
GENESIS binaries use strong name signing.	Provides versioning and naming protection.
Products are checked for viruses and malware.	Delivers products free from viruses and malware.
User access to the configuration tools can be controlled.	Restricts configuration changes to authorized users.
Users have the option to record / log all system configuration and operational changes.	Traces the history of configuration and operational changes for post-mortem analysis of irregularities.
Users have the option to control user access and privileges for individual users as well as groups of users.	Simplifies the setup of user accounts and access controls for environments with many users.
Users have the option to secure access to many items including data points, alarms, files, stations, methods, reports, and ability to perform command and control actions.	Configures security so users are only given access to what they need.
Microsoft Active Directory and Entra ID are synchronized.	Streamlines security configuration and reduces the number of accounts users must log into.
External identity providers are supported.	Supports Multi-Factor Authentication.
Security events are logged.	Records failed login attempts which can help in detecting attempts to intrude into the system.
Client access can be restricted when necessary.	Helps prevent DoS (Denial of Service) attacks

5.2.6 Defense in Depth – Data Layer

Finally, the Data Layer implements another layer of security. While implementing application layer security measures will help in preventing a cybersecurity attack, having good security measures built into the Data Layer provides another layer of defense. Data Layer security measures built into GENESIS include those listed in Table 6 below.

Table 6 – Data Layer Security Measures Applicable to Automation Systems

Data Layer Security Measure	Benefit
GraphWorX displays (data on display) may be secured.	Allows the system to be set up so that users can only view the real-time data that they need to access to.

Configuration databases may be secured using SQL Server security.	Allows the system to be set up so that users can only access the configuration data that they need to access to.
The system supports OPC UA communications.	Provides secure real-time industrial data transportation that includes support for encryption and signed messaging.
The system supports BACnet/SC communications.	Provides secure real-time building automation data transportation that includes support for authentication and end-to-end encryption.
The system supports FrameWorX Server communications.	Secures GENESIS internal communications with encryption and certificate-based authentication.
The system supports HTTPS/SSL.	Configures GENESIS WebHMI pages to use SSL to encrypt data communications over the web.

6 Standards and Certifications

6.1 ISO 9001 Certified Process

The Mitsubishi Electric Iconics Digital Solutions development processes are ISO 9001 Certified.

6.2 IEC 62443 Certified Process

The Mitsubishi Electric Iconics Digital Solutions development processes have been certified to meet the IEC 62443 Part 4-1 Secure product development lifecycle requirements.

6.3 ISO/IEC 27001 Certification for Information Security Management

Mitsubishi Electric Iconics Digital Solutions has earned ISO/IEC 27001:2022 certification, the internationally recognized standard for information security management.

6.4 Compatibility with Microsoft Updates

The Mitsubishi Electric Iconics Digital Solutions quality assurance labs test with the most recent Microsoft operating systems and updates to ensure compatibility. We recommend that all customer machines use the latest Windows Updates for the best security protection.

6.5 STIG - Security Technical Implementation Guidelines

The U.S. Government's Defense Information Systems Agency (DISA) Field Security Operations (FSO) developed guidelines to assist system administrators in securing systems and applications in accordance with the guidance found in the DISA Security Technical Implementation Guides (STIGs) and Center for Internet Security (CIS) Benchmarks. The guidelines were developed to meet the needs of system administrators. The Mitsubishi Electric Iconics Digital Solutions products have gone through several rounds of STIG testing at various Department of Defense (DOD) sites.

6.6 FDA Code of Federal Regulations (FDA/CFR 21 part 11)

For companies regulated by the Food and Drug Administration (FDA), we provide guidance on achieving validated installations in compliance with the Code of Federal Regulations, Title 21, Chapter I, Part 11.

For more information or a copy of the guidelines, contact a company distributor, sales representative, or technical support.

7 Conclusion

Mitsubishi Electric Iconics Digital Solutions products are designed from the ground up for optimal security and take advantage of industry standards and best practices related to security. As the security needs of the industry continue to evolve, we will keep abreast of these changes and continue to improve our products to meet future requirements. We are happy to work with customers to ensure their applications are inherently secure according to best practices discussed in this white paper.

For more information about any of the features mentioned in this paper, see the references listed below

7.1 Security Best Practices

See the Security Best Practices section of the online help system:

- Security Best Practices in GENESIS Version 11

The Security Best Practices section includes the following information:

- Defense in Depth Measures Expected in the Environment
- Product Security Requirements
- Port Security
- Security Hardening Guidelines
- Industrial Control Systems Security
- Secure Operations Guidelines
- Secure Disposal Guidelines
- Account Management Guidelines

7.2 References

7.2.1 Online Help

The following help topics contain important security-related information:

- System Requirements
- ICONICS Compatible Software and Operating Systems (v10.97.3 and earlier)
- Setting Up the Connection to the FrameWorX Server
- Direct and Reverse FrameWorX Connection Overview
- Creating an OPC UA Connection
- Workbench Security Overview
- Security Server:
    - Security Overview
    - Supported Security Types
    - Enabling Active Directory Security Mode
    - Enabling Entra ID Security Mode

- Connecting to an External Identity Provider for Web Login
- Retrieving Advanced Security Information
- Creating a Certificate
- Providing Security Identity to Third-Party Clients

About Us

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

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

MITSUBISHI ELECTRIC ICONICS DIGITAL SOLUTIONS, INC.
HEAD OFFICE: 2 Hampshire Street, Suite 300, Foxborough, MA 02035

iconics.com

October 2025