Highly Secure HMI/SCADA and Automation Systems

August 2018
An ICONICS Whitepaper
www.iconics.com

CONTENTS

About This Document

Copyright and Confidentiality

Overview

ICONICS products have a history of installation in extremely critical and secure applications. ICONICS systems are in use at some of the most secure Defense Department applications, both for the US Department of Defense, and those of other nations. The ICONICS software products also are routinely installed in FDA regulated sites, regulated utility and national grid installations and other critical infrastructure. These applications require the products to be designed for, and tested to, rigid requirements.

ICONICS uses features such as encryption, certificate authentication, user and system encrypted passwords, and obfuscation to provide the highest level of security demanded of today's systems. Equally important, we make the system extremely flexible for the system administrator, so that 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 ICONICS applications that make them a good fit for a secure project.

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 helps provide customers products that help them operate their industrial, manufacturing and mission-critical facilities, ICONICS utilizes the latest security technologies and protocols, as well as operational best practices, to ensure that our customers' information is handled with care.

Attention to Detail at Every Step

We employ a multi-step code review process across many phases of the software development lifecycle. Fuzz tests are performed, along with internal audits. ICONICS also utilizes a multi-phase development lifecycle that includes unit testing, integration testing, system testing, and performance testing. Security testing is done on a per-feature basis for new functionality, including stress tests for security and controls.

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. ICONICS extensive use of OPC Unified Architecture security model secures communications and encryption ensures that data security is held to the highest standards.

Redundant Operations and Mission Critical Technology

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

Development, Standards, and Certifications

Secure Product Development Process

ICONICS takes security during development very seriously. This section talks about some of the security measures employed in the software development process.

Physical Security

The ICONICS offices are a secure facility, with video surveillance, individual keycard access, and a separate locked room for servers, all to ensure that no unauthorized personnel gain access to the product code.

Digital Security

The product code is protected digitally, requiring specific credentials to access different parts of the code. Developers are only allowed to view code they are specifically responsible for, reducing the chance of unauthorized access.

Security Threat Modeling and Code Reviews

The ICONICS development team maintains and regularly reviews a security threat model for the ICONICS software. In addition, 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 they are discovered.

Timely Hot Fixes

Should there be the discovery of a security vulnerability, the ICONICS development team will work to release a hot fix for the issue as soon as possible. Hot fixes for security issues are released to the public and not protected by a login, ensuring that all customers are able to get the latest security updates.

Binary Signing

Strong Name Signing

ICONICS binaries use strong name signing, which provides versioning and naming protection, along with a strong integrity check. It allows ICONICS to guarantee that the contents of the assembly have not been changed since it was built.

For more information on strong name signing, see this MSDN article:
http://msdn.microsoft.com/en-us/library/wd40t7ad(v=VS.85).aspx

VeriSign

ICONICS Binaries are signed by VeriSign, which ensures that the files being used have not been tampered with or changed without our authentication.

For more information on VeriSign, see their website: http://www.verisign.com/

Obfuscation

ICONICS product binaries are obfuscated, preventing the code from being reverse engineered. Not only does this allow ICONICS to protect its intellectual property, it makes the application harder to hack.

For more information on obfuscation, see this MSDN article:
http://msdn.microsoft.com/en-us/library/ms227226(v=vs.80).aspx

Compatibility with Microsoft Updates

ICONICS' quality assurance labs test with the most recent Microsoft operating systems and updates to ensure compatibility. ICONICS recommends that all customer machines use the latest Windows Updates for the best security protection.

Compatibility with Kaspersky and other Security Scan Software

ICONICS' quality assurance labs has tested the compatibility of the ICONICS products with the Kaspersky Industrial CyberSecurity software package, which is a portfolio of technologies and services designed to secure every industrial layer, including SCADA servers, HMI panels, engineering workstations, PLCs, network connections and people. These tests help ensure there are no adverse impacts on the normal operation of the ICONICS software when the Kaspersky software is installed and used. ICONICS plans to expand this program and include testing with other mainstream anti-virus software. Please contact ICONICS for information of other anti-virus testing or any particular requests.

Product Deliveries are Free from Viruses and Malware

Prior to product release, all ICONICS software packages are thoroughly scanned to ensure that no virus or malware content is incorporated into the delivered software. This halts would-be intruder software components from being installed with ICONICS environments.

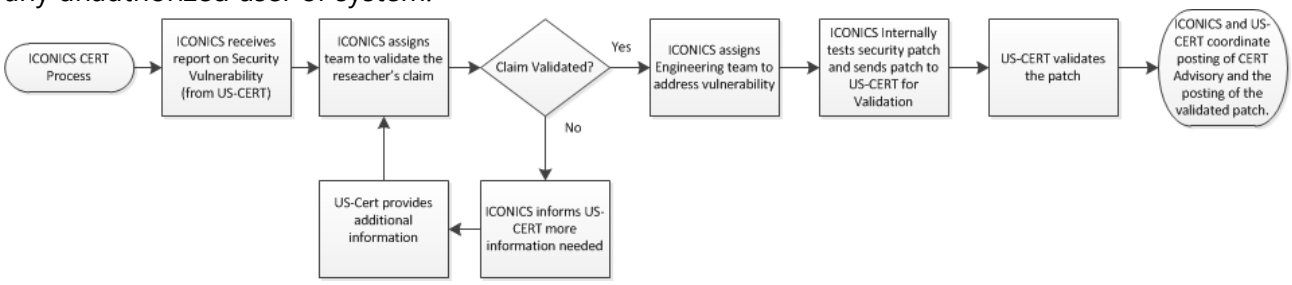
CERT Program with Homeland Security

The United States Department of Homeland Security maintains an Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) that continuously focuses on control system security in collaboration with US-CERT. This team continuously monitors the media, the internet, software researchers globally, and other sources available to it for any indication that vulnerability exists in any current installed or shipping industrial control system. In addition, they have their own testing and analysis capabilities to search for publicly open vulnerabilities.

ICONICS maintains a hotline with ICS-CERT. The ICS-CERT has a direct interface with the ICONICS Vice President of Engineering and ICONICS' fast security response team that is ready to analyze and remedy any possible system exposure.

On a few rare occasions ICS-CERT has contacted ICONICS to make it aware of possible vulnerabilities. These instances have been discovered by both university and private researchers that have focused on discovering software vulnerabilities. In these situations, the ICONICS security response team immediately activates and works with ICS-CERT, to prove or disapprove the suspected issue.
If it is determined to be a real vulnerability the issue is resolved as quickly as possible and a hot fix download is developed, tested internally, tested with the ICS-CERT team, and made available.
We coordinate with ICS-CERT, so that the resolution is available at the time that they issue a public control system advisory describing the occurrence. ICONICS issues notice of the occurrence at the same time as ICS-CERT.

ICONICS is not aware of any instance where an operating ICONICS installation has been penetrated by any unauthorized user or system.



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), checklists and applicable Center for Internet Security (CIS) benchmarks. The guidelines were developed to meet the needs of system administrators. The ICONICS products have gone through several rounds of STIG testing at various DOD sites.

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

For companies that are regulated by the Food and Drug Administration (FDA), ICONICS also provides information on how to achieve validated installations according to the Code of Federal Regulations: Food and Drug Administration Title 21, Chapter I, Part 11.

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

Microsoft Windows Certifications

ICONICS products have been certified for numerous Windows Operating Systems. This means that ICONICS products have been verified not to install components in improper locations, modify the registry in unsafe ways, or otherwise make unsafe or unauthorized changes to the operating system.

- Windows 10 – Compatibility achieved for GENESIS64 in September 2015.
- Windows Server 2012* – Certification achieved for GENESIS64 in September 2012.
- Windows 8 – Compatibility achieved for GENESIS64 in September 2012.
- Windows 7 – Compatibility achieved for GENESIS64 in August 2009.
- Windows Server 2008 – Certification achieved for GENESIS64 in November 2007.
- Windows Vista – Certification achieved for GENESIS64 in September 2006

* Note, Microsoft does not support a application certification program for Windows Server 2016

ICONICS is a Microsoft Gold Partner and has performed security audits and reviews of its products. Achieving Microsoft certification has required that ICONICS follows development practices which allow it to meet these high standards. In achieving Microsoft certification, ICONICS works closely with Microsoft to address any security vulnerabilities which may be discovered during the certification process.

Runtime Security

This section describes some of the security features that are built into ICONICS products.

ICONICS Security Server and User Access Controls

The ICONICS 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 them specific privileges. In addition, administrators may associate users with certain administrator-defined groups that also have assigned privileges. Thus, a user has the effective rights of all the groups to which he or she belongs plus his or her own private rights.

User and Group Access and Authentication Controls

The ICONICS Security Server includes the ability to control user access and privileges for individual users or entire groups 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 offers nearly identical security options for user accounts and for groups. You can apply security restrictions at the group level, the user level, or both. The Security Server uses the following rule for determining whether a privilege is extended or denied to a user based on his or her security:

1. Within a single user or group, denials take precedence. If a policy states the user has access to A, B, and C, then is denied access to B, the sum of that policy is that he has access to only A and C.
2. If any policy applied to the user – including his own user policy, any group he is in, or the Default Group – grants access to a feature, the sum is that the user has access. If the user's policy states he has access to A, B, and C, and is denied access to B, but then his group grants him access to B, he will have access to A, B, and C.

Group or user accounts are defined by using the several tabs available when you define or edit the group or user. 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. These are defined further within the Product documentation.

Encryption

The Security Server uses RSA and RC2 encryption. RSA is used for session key encryption and supports 512 or 1024 bit encryption and RC2 is used for encryption of the credentials and supports 40 or 128 bit encryption. The system relies on Microsoft's Basic Cryptographic Provider and Enhanced Cryptographic Provider for all these encryption. Depending on the number of encryption bits, we use either the basic or the enhanced encryption.

More information on the security technology can be found at:
http://msdn.microsoft.com/en-us/library/Aa386986

The bit length that can be specified in the configurator reflects the RC2 part of our encryption process. If a user chooses 40 bits, the session key is encrypted with 512 bits RSA encryption and the credentials are encrypted with 40 bit RC2 encryption.

Microsoft Active Directory Synchronization

The Security Server can retrieve its list of validated users from a specified domain or a group within that domain. The validated user account is granted permission by the ICONICS Security Server to access various capabilities within the SCADA and analytics products. If a user account is removed from the active directory domain, this change will be reflected in the ICONICS 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 Login Dialog will check the logged in Windows user and see if there is an ICONICS user with a matching domain name and user name. If a matching user is found, that user is logged into ICONICS security automatically.

Other Security-Related Capabilities

These are some other features of ICONICS products that help increase the security of projects.

Configurator Audit Trail and Logs

Many of the ICONICS application servers, including the AlarmWorX64 Server, ReportWorX, BridgeWorX, GraphWorX64 and others may be configured to log detailed operator changes to the GenEvent log. This provides audit support for discovering who made particular changes.

In addition, the ICONICS Workbench can log all system configuration changes to a database, and supports the ability to retrieve, view, and export the configuration changes mode over any time period.

In many SCADA applications it is important to have an audit trail of system changes in the event that issues arise. Industries such as pharmaceutical, and water-wastewater and other mission-critical operations require this level of auditing of SCADA systems. This is now a built-in capability with the ICONICS product suites.

Microsoft SQL Server Security

ICONICS products natively support SQL Server security, allowing both NT and SQL authentication to access databases. Local as well as remote database security access is supported.

SCADA Visualization Password Security

GraphWorX32 and GraphWorX64 display technologies can be optionally password-protected, securing project work and ensuring that no unauthorized users can change displays.

Project Deployment Password Security

ICONICS project management and deployment is managed with the “Pack and Go” feature. Pack and Go files created with the GENESIS32 Workbench or with the GENESIS64 Workbench can be optionally password-protected, ensuring they cannot be tampered with.

Passwords in Our Database

When GENESIS64 Security is set to Database mode, the passwords are hashed using the PBKDF2 function. The hash is 48 bytes long, uses 12 bytes of salt and, when starting GENESIS64 V10.95, is hashed using 10,000 iterations.

When GENESIS64 Security is set to Active Directory mode, no user passwords are stored, but the password for the connection from the security server to Active Directory is stored. This password is obfuscated.

Storing this password in the database can be avoided altogether by leaving the AD connection username and password blank. In this case, the security will use the Windows-integrated authentication to connect to the AD. For the Windows-integrated authentication to work, the FrameWorX server must run under a domain account.

Password During Communication

If authenticating over an untrusted network, it is recommended that the network communications be secured using HTTPS in order to provide protection on the password that is transmitted.

Data Communications

Communication over a network has always been a potential security risk. Below are some of the methods ICONICS uses to keep your data safe and your applications secure when communicating between two or more machines.

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 is achieved through the Discovery and Session Establishment of the connections as well as the encryption of the data transport layer.

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 they 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.

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.

Data Communication Security

FrameWorX

FrameWorX is the ICONICS 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 the Windows Communication Foundation (WCF) to generate secure transports with certificate authentication. Consult ICONICS for detailed information about the processes necessary to configure WCF certificates.

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 industry standards:

- OPC UA
- Database Access
- Web Services support

Windows Communication Foundation (WCF)

Windows Communication Foundation (WFC) can use various transport protocols including:

- NET.TCP
- HTTP
- HTTPS (Hypertext Transfer Protocol Secure)
- WS-HTTP (WS-Secure Conversation)

FrameWorX Server exposes its API on several endpoints. Each endpoint is bound with a transport protocol. The endpoints are defined in a WCF configuration file in a standard way. By default, FrameWorX server allows communication on all protocols – both secured and non-secured. For secured systems it is recommended to disable the unsecured endpoints and leave only the secured ones.

For secure systems it is recommended to use the WS-HTTP protocol with certificates, where available. For Silverlight and MobileHMI clients, which do not support WS-HTTP, it is recommended to use the HTTPS protocol.

Documents describing the procedure of setting up the WS-HTTP or HTTPS communication protocols are listed in the References section.

Modules that leverage FrameWorX communication are the ones that benefit from the above security, most notably:

- GENESIS64
- Hyper Historian Loggers
- Hyper Historian Collectors
- Cloud Connector
- MobileHMI

NOTE: The ICONICS Workbench system configuration tool is currently being enhanced to support Viewing, Importing, Creating, and Configuring certificates on the Server. Starting in version 10.95.2, look for new support for securing IoTWorX communications, and starting in version 10.96 for new support for securing FrameWorX Server, OPC UA and Hyper Historian communications.

ICONICS GenBroker

GenBroker is a simple, secure alternative to DCOM for setting up communication between two remote machines. It can allow communications between machines that are on different subnets, domains, or even across the Internet.

GenBroker has a number of optional security components, including the ability to choose between TCP/IP, SOAP/XML, and DCOM communication channels.

Clients can be limited by GenBroker to only have read only access, and they can be limited to only certain forms of data, such as Data Access, Alarms and Events, tag browsing, security, licensing, etc. Furthermore, user access can be limited to specified machines and IP addresses.

Other Data Communications Security

Allowed Clients

You may restrict what clients are allowed to connect to FrameWorX Server by explicitly defining their IP addresses and computer names in Platform Services Configuration dialog (in Workbench -> Tools -> Allowed Clients 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.

Password Manager

In GENESIS64 V10.95, every FrameWorX Server checks runtime security. Use the Password tab in the Platform Services Configuration dialog to specify user names and passwords for various applications that need to connect to FrameWorX Server.

Port Security

ICONICS products use a number of ports for communication, and all of them are configurable. Allowing the port numbers to be changed means that a malicious user cannot be sure what port to listen on or attack. ICONICS strongly recommends closing ports which are not necessary on machines in order to help maximize the security of the system against malicious attacks.

HTTPS/SSL

WebHMI pages for GENESIS64 can be configured to use SSL to encrypt communication over the web. Please see the Whitepaper entitled “Securing GENESIS64 Communications using HTTPS”.

ICONICS Security Best Practices

- Set up ICONICS Security and enforce a strong password. Note, when GENESIS64 or other ICONICS software is installed, security is not set up by default. This is to simplify the initial setup of the system. Also, set up security to allow only authorized operators to see the Security settings.
- Set up the automatic logout of users to help prevent unauthorized access to the system.
- Use the configurable option "Create a local copy of the configuration on the server" for the configuration databases that are applicable.
- Don't run services that are not necessary. For example, when using a central FrameWorX Server, disable FrameWorX Service on all other computers. Also, disable any unused Point Managers and stop their services, as well.
- Disable all FrameWorX Server endpoints you do not need in the server configuration file (IcoFwxServer.exe.config).
- Disable OPC UA interface, unless you use a third-party OPC UA client in the Platform Services Configuration dialog -> Basic tab.
- Set up security for OPC UA if you do use a third-party OPC UA client with the OPC UA Configuration Tool.
- Set up DCOM permissions for ICONICS.FwxServerOPC properly. This is a Classic OPC interface or FrameWorX Server and it exposes FrameWorX Server via Classic OPC, which relies on DCOM security. It is often set up too open. Note that some GENESIS64 installs may require this interface.
- If using scripts that perform write operations, ensure that the script includes a GenEvent reporting method call to properly log all write operations.
- If using ICONICS Security in Database mode, as opposed to using in conjunction with Active Directory, use binary TCP or HTTPS for the FrameWorX communications protocol, and not HTTP.
- If you require web publishing capabilities, to prevent the possibility of tampering with the GraphWorX display files, configure the FTP server where they are stored to require a user/password for write access to this server. If you do not require web publishing capabilities, ensure FTP access to the website is fully disabled.
- Change out of the box port for GenBroker.
- Configure ICONICS Security to secure configuration and runtime operations.
- When clients are using fixed IP addresses, only allow those clients to connect to FrameWorX.

Conclusion

ICONICS 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, ICONICS will keep abreast of these changes and continue to improve its products to meet future requirements. The ICONICS Applications Solutions Team is 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 on the next page.

References

Application Notes

- GenBroker – Securing Communications with GenBroker
- GENESIS64 – Connecting to Third Party OPC UA Servers
- GENESIS64 Security - Quick Start
- GENESIS64 Security - Retrieving Advanced Security Information
- GENESIS64 Security - Securing Desktop for Operations

White Papers

- Securing FrameWorX OPC UA Communications
- Securing Hyper Historian OPC UA Communications
- Securing GENESIS64 Communications using HTTPS
- Securing GENESIS64 Communications with WS-HTTP
- Securing Hyper Historian Communications with WS-HTTP

Founded in 1986, ICONICS is an award-winning independent software provider offering real-time visualization, HMI/SCADA, energy management, fault detection, manufacturing intelligence, MES, and a suite of analytics solutions for operational excellence. ICONICS solutions are installed in 70 percent of the Global 500 companies around the world, helping customers to be more profitable, agile and efficient, to improve quality, and to be more sustainable.

ICONICS is leading the way in cloud-based solutions with its HMI/SCADA, analytics, mobile and data historian to help its customers embrace the Internet of Things (IoT). ICONICS products are used in manufacturing, building automation, oil and gas, renewable energy, utilities, water and wastewater, pharmaceuticals, automotive, and many other industries. ICONICS' advanced visualization, productivity, and sustainability solutions are built on its flagship products: GENESIS64™ HMI/SCADA, Hyper Historian™ plant historian, AnalytiX® solution suite, and MobileHMI™ mobile apps. Delivering information anytime, anywhere, ICONICS' solutions scale from the smallest standalone embedded projects to the largest enterprise applications.

ICONICS promotes an international culture of innovation, creativity, and excellence in product design, development, technical support, training, sales, and consulting services for end users, systems integrators, OEMs, and channel partners. ICONICS has over 350,000 applications installed in multiple industries worldwide.

World Headquarters
100 Foxborough Blvd.
Foxborough, MA, USA, 02035
+1 508 543 8600
us@iconics.com

European Headquarters
Netherlands
+31 252 228 588
holland@iconics.com

Australia
+61 2 9605 1333
australia@iconics.com

Canada
+1 647 544 1150
canada@iconics.com

China
+86 10 8494 2570
china@iconics.com

Czech Republic
+420 377 183 420
czech@iconics.com

France
+33 4 50 19 11 80
france@iconics.com

Germany
+49 2241 16 508 0
germany@iconics.com

India
+91 265 6700821
india@iconics.com

Italy
+39 010 46 0626
italy@iconics.com

Middle East
+966 540 881 264
middleeast@iconics.com

Singapore
+65 6667 8295
singapore@iconics.com

UK
+44 1384 246 700
uk@iconics.com

Winner
Microsoft Partner
2018 Partner of the Year
Manufacturing Award