Programmable Control Products

VersaMax*

Controllers and Ethernet Network Interface Unit (ENIU)

Secure Deployment Guide, GFK-2955B

June 2016

Warnings, Cautions, and Notes as Used in this Publication **GFL-002**

Warning

Warning notices are used in this publication to emphasize that hazardous voltages, currents, temperatures, or other conditions that could cause personal injury exist in this equipment or may be associated with its use. In situations where inattention could cause either personal injury or damage to equipment, a Warning notice is used.

Caution

Caution notices are used where equipment might be damaged if care is not taken.

Note: Notes merely call attention to information that is especially significant to understanding and operating the equipment.

These instructions do not purport to cover all details or variations in equipment, nor to provide for every possible contingency to be met during installation, operation, and maintenance. The information is supplied for informational purposes only, and GE makes no warranty as to the accuracy of the information included herein. Changes, modifications, and/or improvements to equipment and specifications are made periodically and these changes may or may not be reflected herein. It is understood that GE may make changes, modifications, or improvements to the equipment referenced herein or to the document itself at any time. This document is intended for trained personnel familiar with the GE products referenced herein.

GE may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not provide any license whatsoever to any of these patents.

GE PROVIDES THE FOLLOWING DOCUMENT AND THE INFORMATION INCLUDED THEREIN AS-IS AND WITHOUT WARRANTY OF ANY KIND, EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY IMPLIED STATUTORY WARRANTY OF MERCHANTABILITY OR FITNESS FOR PARTICULAR PURPOSE.

* indicates a trademark of General Electric Company and/or its subsidiaries.
All other trademarks are the property of their respective owners.

If you purchased this product through an Authorized Channel Partner, please contact the seller directly.

General Contact Information

Online technical support and GlobalCare	http://support.ge-ip.com
Additional information	http://www.ge-ip.com/
Solution Provider	solutionprovider.ipatge.com

Technical Support

If you have technical problems that cannot be resolved with the information in this manual, please contact us by telephone or email, or on the web at http://support.ge-ip.com

Americas

Online Technical Support	http://support.ge-ip.com
Phone	1-800-433-2682
International Americas Direct Dial	1-780-420-2010 (if toll free 800 option is unavailable)
Technical Support Email	support.ipatge.com
Customer Care Email	customercare.ipatge.com
Primary language of support	English

Europe, the Middle East, and Africa

Online Technical Support	http://support.ge-ip.com
Phone	+800-1-433-2682
EMEA Direct Dial	+420 239015850 (if toll free 800 option is unavailable or if dialing from a mobile telephone)
Technical Support Email	support.emea.ipatge.com
Customer Care Email	customercare.emea.ipatge.com
Primary languages of support	English, French, German, Italian, Czech, Spanish

Asia Pacific

Online Technical Support	http://support.ge-ip.com
Phone	+86-400-820-8208
	+86-21-3877-7006 (India, Indonesia, and Pakistan)
Technical Support Email	support.cn.ipatge.com (China)
	support.jp.ipatge.com (Japan)
	support.in.ipatge.com (remaining Asia customers)
Customer Care Email	customercare.apo.ipatge.com
	customercare.cn.ipatge.com (China)

Contents

Contents

1 About this Guide

This document provides information that can be used to help improve the cyber security of systems that include VersaMax controllers. It is intended for use by control engineers, integrators, IT professionals, and developers responsible for deploying and configuring VersaMax controllers and Ethernet Network Interface Units (ENIU).

Secure deployment information is provided in this manual for the following catalog numbers.

Product Line	Catalog Number	Description
VersaMax	*IC200CPUE05*	CPUE05 PLC CPU with Embedded Ethernet
VersaMax	*IC200EBI001*	Ethernet Network Interface Unit

2 Introduction

This section introduces the fundamentals of security and secure deployment.

2.1 What is Security?

Security is the process of maintaining the confidentiality, integrity, and availability of a system:

- Confidentiality: Ensure only the people you want to see information can see it.
- Integrity: Ensure the data is what it is supposed to be.
- Availability: Ensure the system or data is available for use.

GE recognizes the importance of building and deploying products with these concepts in mind and encourages customers to take appropriate care in securing their GE products and solutions.

NOTE: As GE product vulnerabilities are discovered and fixed, security advisories are issued to describe each vulnerability in a particular product version, as well as the version in which the vulnerability was fixed. GE product security advisories are available at the following location:

http://support.ge-ip.com/support/index?page=kbchannelandid=S:KB14607.

2.2 I have a firewall. Isn't that enough?

Firewalls and other network security products, including Data Diodes and Intrusion Prevention Devices, can be an important component of any security strategy. However, a strategy based solely on any single security mechanism will not be as resilient as one that includes multiple, independent layers of security.

Therefore, GE recommends taking a "Defense in Depth" approach to security.

2.3 What is Defense in Depth?

Defense in Depth is the concept of using multiple, independent layers of security to raise the cost and complexity of a successful attack. To carry out a successful attack on a system, an attacker would need to find not just a single exploitable vulnerability, but would need to exploit vulnerabilities in each layer of defense that protects an asset.

For example, if a system is protected because it is on a network protected by a firewall, the attacker only needs to circumvent the firewall to gain unauthorized access. However, if there is an additional layer of defense, say a username/password authentication requirement, now the attacker needs to find a way to circumvent both the firewall and the username/password authentication.

2.4 General recommendations

The following security practices should be followed when using GE products and solutions.

- The controllers and supervisory level computers covered in this document were not designed for or intended to be connected directly to any wide area network, including but not limited to a corporate network or the Internet at large. Additional routers and firewalls (such as those illustrated in section 6.1, *Reference Architecture*) that have been configured with access rules customized to the site's specific needs must be used to access devices described in this document from outside the local control networks. If a control system requires external connectivity, care must be taken to control, limit, and monitor all access, using, for example, virtual private networks (VPN) or Demilitarized Zone (DMZ) architectures.
- Harden system configurations by enabling/using the available security features, and by disabling unnecessary ports, services, functionality, and network file shares.
- Apply all of the latest GE product security updates, SIMs, and other recommendations.
- Apply all of the latest operating system security patches to control systems PCs.
- Use anti-virus software on control systems PCs and keep the associated anti-virus signatures up-to-date.
- Use whitelisting software on control systems PCs and keep the whitelist up-to-date.

2.5 Checklist

This section provides a sample checklist to help guide the process of securely deploying VersaMax Controllers and ENIUs.

1. Create or locate a network diagram.
2. Identify and record the required communication paths between nodes.
3. Identify and record the protocols required along each path, including the role of each node. (Refer to section 3, *Communication Requirements*.)
4. Revise the network as needed to ensure appropriate partitioning, adding firewalls or other network security devices as appropriate. Update the network diagram. (Refer to section 6, *Network Architecture and Secure Deployment*.)
5. Configure firewalls and other network security devices. (Refer to section 3.5, *Ethernet Firewall Configuration* and section 6, *Network Architecture and Secure Deployment*.)
6. Enable and/or configure the appropriate security features on each VersaMax module. (Refer to section 4, *Security Capabilities*.)
7. On each VersaMax module, change every supported password to something other than its default value. (Refer to section 4.4, *Password Management*.)
8. Harden the configuration of each VersaMax module, disabling unneeded features, protocols and ports. (Refer to section 5, *Configuration Hardening*.)
9. Test / qualify the system.
10. Create an update/maintenance plan.

NOTE: Secure deployment is only one part of a robust security program. This document, including this checklist, is limited to only providing secure deployment guidance. For more information about security programs in general, refer to section 7.3, *Additional Guidance*.

3 Communication Requirements

Communication between different parts of a control system is, and must be, supported. However, the security of a control system can be enhanced by limiting the protocols allowed, and the paths across which they are allowed, to only what is needed. This can be accomplished by disabling every communication protocol that isn't needed on a particular device, and by using appropriately configured and deployed network security devices (for example, firewalls, routers) to block every protocol (whether disabled or not) that doesn't need to pass from one network/segment to another.

GE recommends limiting the protocols allowed by the network infrastructure to the minimum set required for the intended application. Successfully doing this requires knowing which protocol is needed for each system-level interaction.

This section describes how the supported serial and Ethernet application protocols are used by VersaMax controllers and ENIUs, and indicates the role of each participant in the communication. Lower-level Ethernet protocols are not discussed here, but are instead assumed to be supported when needed by the application protocol.

This information is intended to be used to help guide the specification of the network architecture and to help configure firewalls internal to that network, in order to support **only** the required communications paths for any particular installation.

3.1 Protocols Supported

3.1.1 Ethernet Protocols

This section indicates which Ethernet protocols are supported, by VersaMax controllers and ENIUs. Note that some of the supported protocols may not be required in a given system, since the installation may only be using a subset of the available protocols.

Supported Ethernet Protocols

	Protocol	IC200CPUE05	IC200EBI001	IC200EBI001-MH & Later
Link	ARP	✓	✓	✓
Internet	IPv4	✓	✓	✓
	IGMP	✓	✓	✓
	ICMP	✓	✓	✓
Transport	TCP	✓	✓	✓
	UDP	✓	✓	✓
Application	Ethernet Global Data (EGD)	✓	✓	✓
	SRTP Server	✓		
	Remote Station Manager Server	✓		
	Modbus TCP		✓	✓
	FTP		✓	✓
	TFTP			✓

3.1.2 Serial Protocols

In addition to Ethernet communication, VersaMax controllers support communication over RS-232 and RS-485 serial ports. VersaMax ENIUs communicate with the I/O modules in the expansion rack over RS-485 serial ports.

Supported Serial Protocols

	Protocol	IC200CPUE05	IC200EBI001	IC200EBI001-MH & Later
Application	Application-specific	✓	✓	✓
	ASCII Terminal	✓		✓
	Modbus® RTU Slave	✓		
	SNP Slave	✓	✓	✓

NOTE: Some modules can be configured so that one or more of their serial ports is controlled by the user application program that is executing on the controller. Such "Application-specific" protocols are outside of the scope of this document and won't be discussed further.

3.2 Service Requests

The VersaMax Service Request protocol is a proprietary, media-independent application protocol that provides access to services supported by the VersaMax controller. This is the primary protocol used by Proficy Machine Edition: Logic Developer – PLC when communicating with a VersaMax CPU. It supports many different operations, including:

- Upload / download the user application and configuration to the controller
- Start/stop the controller
- Read, write, verify, or clear Flash/EEPROM memory
- Clear controller memory
- Gather diagnostic information from a controller
- Verify equality
- View and, in some cases, set the target controller's operating parameters: device information, memory usage, date and time, reference points/words, access levels, passwords and OEM key, and sweep information
- View and optionally clear a log of any faults that have occurred in the controller

The Service Request protocol is transported over a specific media by encapsulating it within a media-specific protocol. Specifically, SRTP is used for transporting it over an Ethernet network and SNP is used for transporting it over a serial channel. Almost all SRTP and SNP transmissions contain at least a portion of a Service Request/Reply embedded within them.

Supporting communication between any two nodes using Service Requests requires that the system support communicating using either SRTP or SNP between those two nodes.

3.2.1 SRTP

SRTP is used to send Service Requests to a controller via an Ethernet network, and to convey the results back to the client. The VersaMax controller supports only SRTP Server (processing service requests) functionality.

SRTP Server

SRTP Server functionality is enabled at all times on the modules that support this protocol.

3.2.2 SNP

SNP is used to send Service Requests to a Controller via a serial connection, and to convey the results back to the client. Support for SNP Slave functionality is enabled whenever a VersaMax Controller's serial port is configured to support either SNP Slave or Modbus RTU Slave. This is because the Controller's serial ports will auto-switch from Modbus RTU mode to SNP mode when an SNP packet is received.

Firmware Update

The SNP protocol is also used to support updating the firmware on the VersaMax controller or on an installed module that supports having its firmware updated over the backplane. This is accomplished through the use of Service Requests that are only supported when received via a serial port. Firmware updates are not supported over Ethernet using the SRTP protocol.

VersaMax ENIU uses SNP for updating the firmware on an installed module that supports having its firmware updated over the backplane.

- VersaMax ENIUs prior to IC200EBI001-MH revision support firmware upgrade over Ethernet using FTP protocol.
- VersaMax ENIUs IC200EBI001-MH and later use the SNP protocol.

Supported Firmware Upgrade Protocol in VersaMax Controller

Protocol	WinLoader.exe (Windows PC)	IO device
SNP	Master	Slave

Supported Firmware Upgrade Protocol in VersaMax Ethernet Network Interface Unit

Protocol	WinLoader.exe (Windows PC)	IO device
SNP	Master	Slave
FTP*	Client	Slave

* Only revisions prior to IC200EBI001-MH support firmware upgrade through FTP.

3.3 Server

This section summarizes the available communication-centric functionality, where the communication is initiated by some other device or PC.

VersaMax Controller Server Capabilities

	Functionality	Required Application Protocols	Example Clients
Ethernet	Service Requests	SRTP	Proficy Machine Edition HMI Other controllers
	EGD Consumption	Ethernet Global Data	Other controllers
	Ethernet Station Manager	Remote Station Mgr	stamgr24.exe on PC Other Ethernet interface
Serial	Service Requests	SNP Slave	Proficy Machine Edition HMI Other controllers
	Firmware Update	SNP Slave	WinLoader.exe on PC
	Modbus RTU Slave	Modbus RTU	HMI Other controllers 3rd-party Masters
	Serial Station Manager	ASCII Terminal	Terminal emulator on PC

VersaMax ENIU Server Capabilities

	Functionality	Required Application Protocols	Example Clients
Ethernet	EGD Consumption	Ethernet Global Data	Other controllers
	Modbus TCP Server	Modbus TCP	Other controllers
	Versamax ENIU Firmware Update	FTP*	Host PC
	Versamax ENIU Programmer Interface	FTP	PME, Versa Pro & Remote I/O Manager.
Serial	Versamax ENIU & I/O module Firmware Update	SNP Slave	WinLoader.exe on PC

* Only revisions prior to IC200EBI001-MH support firmware upgrade through FTP.

3.4 Client

This section summarizes the available communication-centric functionality, where the communication is initiated by the VersaMax CPU or Ethernet Network Interface Unit. The servers involved in these communications are selected by the user application and/or configuration.

VersaMax Controller and ENIU Client Capabilities

	Functionality	Required Application Protocols	Example Servers
Ethernet	EGD Production	Ethernet Global Data	Other controllers

3.5 Ethernet Firewall Configuration

Network-based and host-based firewalls should be configured to only allow expected and required network traffic. This section identifies the EtherTypes and the TCP/UDP ports used by the protocols supported on VersaMax controllers and ENIUs.

This information should be used to help configure network firewalls, in order to support **only** the required communications paths for any particular installation.

3.5.1 Lower-level Protocols

Ethernet communication is typically described using four layers, each with its own set of protocols. At the top of that hierarchy is the Application layer. Below the Application layer are the Transport, Internet, and Link layers.

Information on the supported protocols from these three lower layers is summarized here.

Link Layer Protocols

Protocol	EtherType
ARP	0x0806

Internet Layer Protocols

Protocol	EtherType	IP Protocol #
IPv4	0x0800	(n/a)
ICMP	0x0800	1
IGMP	0x0800	2

Transport Layer Protocols

Protocol	EtherType	IP Protocol #
TCP	0x0800	6
UDP	0x0800	17

Each of these lower-level protocols is required by one or more of the Application protocols supported on VersaMax Controllers and ENIUs.

3.5.2 Application Layer Protocols

The following is the list of TCP and UDP port numbers for the Application layer protocols supported by VersaMax Controllers and ENIUs.

Application Layer Protocols

Protocol	TCP Port	UDP Port	IC200CPUE05	IC200EBI001	IC200EBI001-MH & Later
Ethernet Global Data (EGD)		18246	✓	✓	✓
SRTP (Server only)	18245		✓		
Remote Station Manager		18245	✓		
Modbus TCP	502			✓	✓
FTP	20 and 21			✓	✓
TFTP		69			✓

4 Security Capabilities

This section describes VersaMax controller and ENIU capabilities and security features, which can be used as part of a defense-in-depth strategy to secure your control system.

4.1 Capabilities by Product

This section provides a summary view of the supported security capabilities.

Security Capabilities

Security Capability	IC200CPUE05	IC200EBI001	IC200EBI001-MH & Later
Predefined set of Subjects and Access Rights	✓	✓	✓
Plaintext Login	✓	✓	✓
Secure Login (SRP-6a)			
Access Control List	✓	✓	✓
Firmware Signatures			✓

4.2 Access Control and Authorization

The Access Control process can be divided into two phases:

1. Definition – Specifying the access rights for each subject (referred to as **Authorization**), and
2. Enforcement – Approving or rejecting access requests

This section describes the Access Control capabilities supported by VersaMax controllers and ENIU, which includes its Authorization capabilities.

4.2.1 Authorization Framework

Defining the access rights for each subject implies that the system must have some means to identify each subject. The most familiar way this is achieved is by assigning a unique User ID to each person who will access the system.

VersaMax controllers and VersaMax ENIUs, however, don't provide such a facility – there is no support for creating User IDs. In many cases, a User ID doesn't even have to be specified to authenticate. In such cases, authorization is based on the functionality being used and the password that is provided for authentication. However, the authentication features supported on VersaMax Controllers and ENIUs implicitly define a fixed set of subjects, which are identified here.

The set of implicitly defined subjects will vary depending on the server protocols that are supported, which depends on what modules are installed and how they are configured. Each kind of server has its own set of predefined subjects – there are no subjects that apply across multiple servers (other than "anonymous"). Further, each instance of a server has its own instances of the predefined subjects – access rights for each subject must be separately managed for each instance of a given kind of server.

For example, each VersaMax controller acts as a Service Request server. Therefore, access rights for each VersaMax controller in the system must be independently managed. Similarly, Ethernet Interface supports the Ethernet Station Manager server. Therefore, access rights for Ethernet Interface must be individually managed.

The subjects defined and supported by each server protocol are indicated in the following table.

Subjects Available on VersaMax Controllers

	Functionality	Application Protocol	Subjects Available
Ethernet	Service Requests	SRTP	Anonymous PRIV Level 1 user PRIV Level 2 user PRIV Level 3 user PRIV Level 4 user OEM user
	EGD Consumption	Ethernet Global Data	Anonymous
	Ethernet Station Manager	Remote Station Mgr	Anonymous STA Modify-level user
Serial	Service Requests	SNP Slave	Anonymous PRIV Level 1 user PRIV Level 2 user PRIV Level 3 user PRIV Level 4 user OEM user
	Firmware Update	SNP Slave	Anonymous
	Modbus RTU Slave	Modbus RTU	Anonymous
	Serial Station Manager	ASCII Terminal	Anonymous STA Modify-level user

Subjects Available on VersaMax Ethernet Network Interface Unit

	Functionality	Application Protocol	Subjects Available
Ethernet	EGD Consumption	Ethernet Global Data	Anonymous
	Modbus TCP Server	Modbus TCP	Anonymous
	Versamax ENIU Firmware upgrade	FTP*	Fixed user login and password
	Versamax ENIU Programmer Interface	FTP	Fixed user login and password
Serial	Versamax ENIU & I/O Firmware upgrade	SNP Slave	Anonymous

* Only revisions prior to IC200EBI001-MH support firmware upgrade through FTP with Fixed user login and password.

4.2.2 Specifying Access Rights

For each subject, VersaMax controllers and ENIUs provide predefined access rights. In some cases those access rights can be partially restricted, while in other cases they either cannot be changed at all, or can only be revoked by disabling the associated server/protocol.

Access Rights on VersaMax Controllers

Subject	Application Configuration	Application Logic (while in STOP)	Application Logic (while in RUN)	Application Data	Application Data Overrides/Forces	Fault Tables	Controller Status (e.g. RUN/STOP)	PRIV Level Passwords	Module Firmware
OEM user	A	A	-	-	-	-	-	-	-
PRIV Level 4 user	RWD	RWD	RW	RWD	RWD	RD	RW	WD	W
PRIV Level 3 user	RWD	RWD	R	RWD	RWD	RD	RW	-	-
PRIV Level 2 user	R	R	R	RW	R	RD	RW	-	-
PRIV Level 1 user	R	R	R	R	R	R	R	-	-
Anonymous (SRTP, SNP)	Same as highest "PRIV Level user" that currently has no password.								
Anonymous (EGD, Modbus RTU)	-	-	-	RW	RW	-	-	-	-

Key: A=access control, R=read, W=write, D=delete/clear

The *OEM user* has the ability to prohibit any subject from reading or writing the Application configuration or logic. That subject does **not** have the ability to grant additional access rights to any of the subjects.

Access Rights on VersaMax Ethernet Network Interface Unit

Subject	Application Configuration	Application Logic (while in STOP)	Application Logic (while in RUN)	Application Data	Application Data Overrides/Forces	Fault Tables	Controller Status (e.g. RUN/STOP)	PRIV Level Passwords	Module Firmware	Fatal Error Info
Anonymous (EGD, Modbus TCP)	-	-	-	RW	-	RD	-	-	-	-
Anonymous (SNP)	Same as highest "PRIV Level user" that currently has no password.									-
FTP	RWD	-	-	-	-	-	-	-	W	-
TFTP	-	-	-	-	-	-	-	-	-	RD

Key: A=access control, R=read, W=write, D=delete/clear

Physical Access

The VersaMax controller supports a configuration setting that can be used to require physical access to the controller in order to change the application configuration, application logic and/or overrides/forces of application data. This is controlled using the "Memory Protection Switch" setting in the hardware configuration that is downloaded to the controller.

When the Memory Protection Switch setting is enabled and the RUN/STOP switch is physically in the RUN position, then the predefined Access Rights are changed to the following.

Access Rights VersaMax Controllers with Memory Protection ENABLED and Physical Switch in RUN Position

Subject	Application Configuration	Application Logic (while in STOP)	Application Logic (while in RUN)	Application Data	Application Data Overrides/Forces	Fault Tables	Controller Status (e.g. RUN/STOP)	PRIV Level Passwords	Module Firmware
OEM user	A	A	-	-	-	-	-	-	-
PRIV Level 4 user	R	R	R	RW	R	RD	RW	WD	W
PRIV Level 3 user	R	R	R	RW	R	RD	RW	-	-
PRIV Level 2 user	R	R	R	RW	R	RD	RW	-	-
PRIV Level 1 user	R	R	R	R	R	R	R	-	-
Anonymous (SRTP, SNP)	Same as highest "PRIV Level user" that currently has no password.								
Anonymous (EGD, Modbus RTU)	-	-	-	RW	R	-	-	-	-

Modbus-specific Limitations

Access to Application Data via the Modbus RTU server is limited to only those data items that have been mapped into the Modbus address space. This mapping is fixed and cannot be altered.

4.2.3 Enforcement

The VersaMax controller enforces the access rights for the data and services that it provides. Thus, the VersaMax controller ensures that the Application Configuration can only be updated by a user with the access rights to write/delete the Application Configuration. Similarly, the VersaMax Ethernet Interface ensures that only the *STA Modify-level* user can execute Ethernet Station Manager commands that are capable of modifying the operation of the module.

4.3 Authentication

The VersaMax controller or ENIU provides password-based authentication for some, but not all, of its server protocols. For each unauthenticated protocol that is enabled, compensating controls may be needed to satisfy a particular installation's security requirements.

NOTE: The default configuration for all Server protocols is for no authentication, or for authentication using well-known default values.

4.3.1 Summary

This section summarizes the authentication mechanisms supported by VersaMax controllers for each protocol.

Authentication Available on VersaMax Controller Servers

	Functionality	Application Protocol	Authentication Options
Ethernet	Service Requests	SRTP	Plaintext login Disabled
	EGD Consumption	Ethernet Global Data	None
	Ethernet Station Manager	Remote Station Mgr	Plaintext login
Serial	Service Requests	SNP Slave	Plaintext login Disabled
	Modbus RTU Slave	Modbus RTU	None
	Serial Station Manager	ASCII Terminal	Plaintext login

Authentication available on VersaMax Ethernet Network Interface Unit Servers

	Functionality	Application Protocol	Authentication Options
Ethernet	EGD Consumption	Ethernet Global Data	None
	Modbus TCP Server	Modbus TCP	None
	Versamax ENIU Firmware Upgrade	FTP*	Plaintext Login
	Versamax ENIU Programmer Interface	FTP	Plaintext Login
Serial	VersaMax ENIU & I/O module Firmware Upgrade	SNP	None

* Only revisions prior to IC200EBI001-MH support FTP with plaintext login.

Authentication Supported by VersaMax Controller and Ethernet Network Interface Unit Clients

	Functionality	Required Application Protocols	Authentication Supported
Ethernet	EGD Production	Ethernet Global Data	None

4.3.2 Plaintext Login

Authentication for many of the supported protocols involves sending a plaintext password to the VersaMax Controller or ENIU. In some cases these plaintext passwords cannot be more than seven (7) characters long. When such protocols are required, additional compensating controls may be needed to satisfy a particular installation's security requirements.

4.3.3 Recommendations

GE strongly recommends that authentication be used for every enabled protocol that supports authentication, that all default passwords be changed wherever possible, and that access be appropriately restricted to any PC-based file that includes a plaintext password.

When a choice between a plaintext-based login and a Secure Login is available, GE strongly recommends that the Secure Login feature be used.

4.4 Password Management

As described in the section, *Authorization Framework*, each instance of a server has its own instances of the predefined subjects. As a result, passwords for each subject must be separately managed for each instance of a given kind of server.

For example, each VersaMax controller acts as a Service Request server. Therefore, the passwords for each VersaMax controller in the system must be independently managed. Similarly, the VersaMax Ethernet Interface supports the Ethernet Station Manager server. Therefore, the passwords for Ethernet Interface must be independently managed.

GE strongly recommends the use of long (7 characters or more), complex passwords wherever passwords are used for authentication.

Changing Passwords in VersaMax Controller

Functionality	Authenticated Subjects	How Passwords are assigned
Service Requests	PRIV Level 1 user PRIV Level 2 user PRIV Level 3 user PRIV Level 4 user OEM user	All of these passwords are controlled by the PRIV Level 4 user.
Ethernet Station Manager	STA Modify-level user	Included in plaintext in an AUP file that must be imported into the Ethernet Configuration and downloaded to the VersaMax Controller. **stpasswd=<*newpass*>** Max of 7 characters in password.

For more detailed information on assigning these passwords, refer to the VersaMax PLC User Manual (GFK-1503).

4.4.1 Communications Protocols

Some communications protocols provide features that help protect data while it is "in flight" – actively moving through a network. The most common of these features include:

- **Encryption** – Protects the confidentiality of the data being transmitted.
- **Message Authentication Codes** – Ensures message authenticity and integrity by cryptographically detecting message tampering or forgery. This ensures the data originated from the expected source and was not altered since it was transmitted, regardless of whether or not it was malicious.

Currently, none of the communications protocols supported by VersaMax Controllers and ENIUs provide either of these features, as detailed in the following tables. Therefore, compensating controls may be required to meet an installation's security requirements for protecting data in-flight.

Protocol-provided Security Capabilities on VersaMax Controller

	Protocol	Data Encryption	Message Authentication Codes
Ethernet	Ethernet Global Data	N	N
	Remote Station Manager	N	N
	SRTP	N	N
Serial	ASCII Terminal	N	N
	Modbus RTU Slave	N	N
	SNP Slave	N	N

Protocol-provided Security Capabilities on VersaMax Ethernet Network Interface Unit

	Protocol	Data Encryption	Message Authentication Codes
Ethernet	Ethernet Global Data	N	N
	FTP	N	N
	Modbus TCP	N	N
	TFTP*	N	N
Serial	SNP Slave	N	N

*Supported only from revisions IC200EBI001-MH and later.

4.5 Logging and Auditing

The VersaMax controller and ENIU do not provide a dedicated security log embedded within the controller, nor does it integrate with an external Security Information and Event Management (SIEM) system. However, the VersaMax Controller and ENIU do log operational events into two small (64 entry) fault tables. Each fault entry includes the time and date that the fault was logged, using the date/time maintained on the controller

These fault tables can be read by remote clients as well as by the user application running on the controller. Thus, logged events could be communicated to an external system for persistent storage and auditing, if required by an installation's security policy. For VersaMax controllers Proficy Machine Edition can be used to export the fault tables to an XML file or print them.

Most of the events that are logged in the VersaMax Controller fault tables represent functional issues, such as hardware failures and unexpected firmware operation. While those are not specific to security, they may still provide information that is useful during a security audit.

There are two security-specific faults that can be logged in VersaMax controllers.

1. When an attempt to authenticate using the Service Request protocol fails, a specific fault is logged in the Controller Fault Table and a system variable (#BAD_PWD) is set to signal that a login attempt has failed. The fault text is "Password Access Failure", and the fault extra data encodes information specific to the event.
2. When an attempt to use an access controlled feature fails due to insufficient privileges, a specific fault is logged in the Controller Fault Table. The fault text is "Access Control List violation detected", and the fault extra data encodes information specific to the event.

5 Configuration Hardening

This section is intended to assist in reducing the potential attack surface by providing information that can be used to harden the configuration of the VersaMax products that are present in a particular installation. Configuration Hardening should be considered in addition to enabling and using security features such as Authentication, Access Control, and Authorization.

GE recommends disabling, on each VersaMax product, all ports, services, and protocols that aren't required for the intended application.

5.1 Controller

This section provides information to use when hardening the configuration of a VersaMax controller. These options should be considered when configuring any VersaMax controller that supports them.

These settings are specified within the hardware configuration that is downloaded to the VersaMax controller.

5.1.1 Serial Port Protocols

The hardware configuration for the VersaMax controller includes the ability to modify the operation of the serial ports embedded on the controller, including which server protocols will be supported. This selection is controlled by the "Port Mode" setting, which must be individually specified for each serial port. The protocols that will be supported for each option are summarized here.

Serial Port Configuration for VersaMax Controllers

Port Mode	Supported Protocols
RTU only	Modbus RTU Slave Modbus RTU Master SNP Slave
SNP	SNP Slave
Serial I/O	Application-defined
Disabled	None
Station Manager	Serial Station Manager

Serial Port Configuration for VersaMax Ethernet Network Interface Unit

Port Mode	Supported Protocols
SNP	SNP Slave

To reduce the potential attack surface, configure each serial port using the most restrictive option that still supports the required protocol(s). Setting the "Port Mode" to "Disabled" will disable all protocols for a given serial port, but very low-level handling of data received on that port will still occur.

5.2 Ethernet Interface

This section provides information to use when hardening the configuration of the VersaMax controller's Ethernet Interface. These settings should be considered when configuring any VersaMax Ethernet Interface.

The Ethernet Interface can be configured to disable a number of services. The table below lists those services and indicates the configuration value that will disable each. Note that some of these settings will not entirely close the TCP/UDP port, but they will still reduce the attack surface.

Disabling Ethernet Services

Service	Parameter name	Value
IP Routing	Gateway IP Address	0.0.0.0

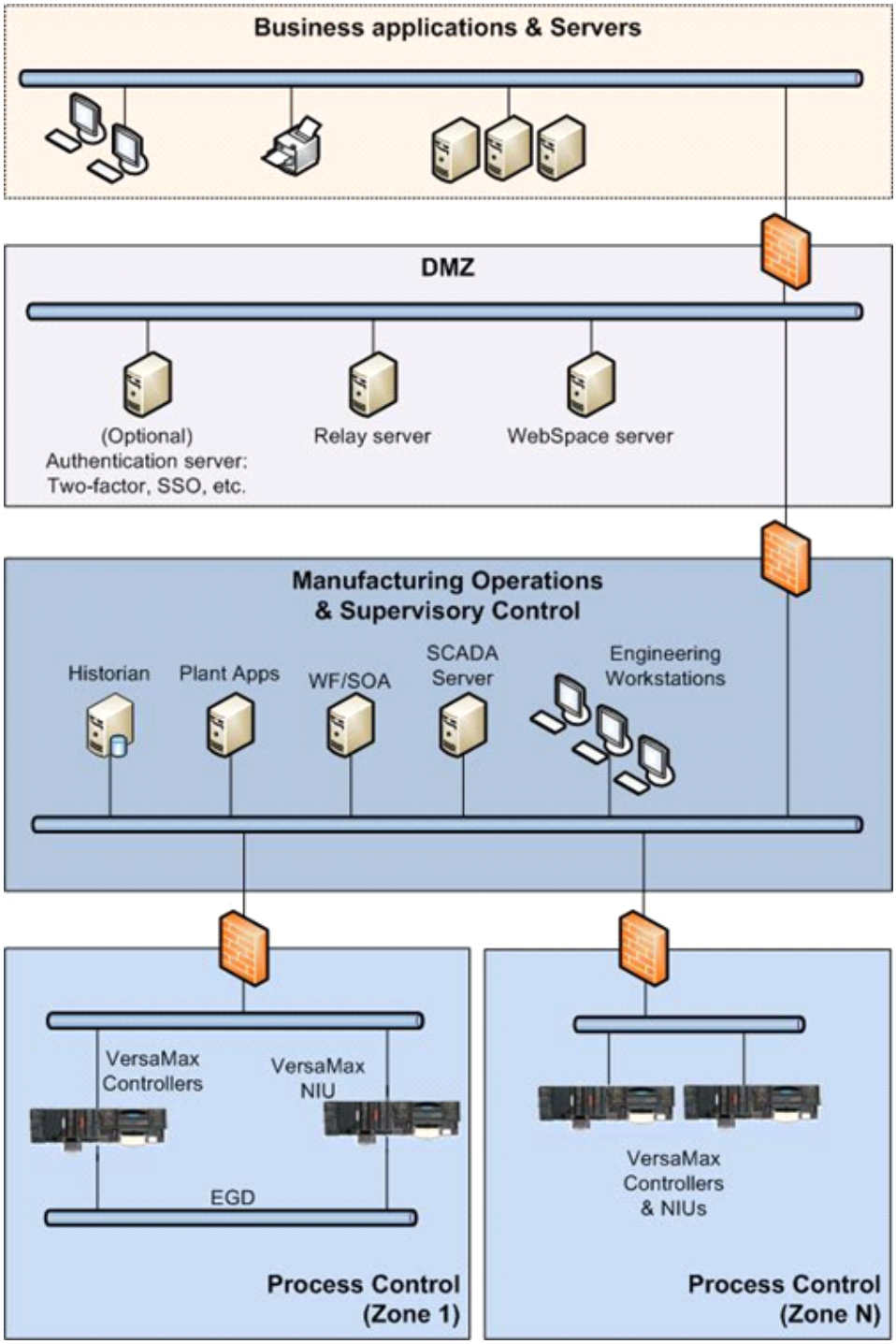
These settings are specified within the hardware configuration that is downloaded to the VersaMax controller or ENIU. For more information on these parameters, refer to the *VersaMax PLC User Manual* (GFK-1503).

6 Network Architecture and Secure Deployment

This section provides security recommendations for deploying a VersaMax controller in the context of a larger network.

6.1 Reference Architecture

The following figure illustrates a reference deployment of VersaMax controllers.



The Manufacturing Zone networks (which include the Manufacturing Operations, Supervisory Control, and Process Control networks) are segregated from other untrusted networks such as the enterprise network (also referred to as the business network, corporate network, or intranet) and the internet using Demilitarized Zone (DMZ) architecture. The Process Control networks have limited exposure to traffic from higher-level networks, including other networks in the Manufacturing Zone, as well as from other Process Control networks.

6.2 Remote Access and Demilitarized Zones (DMZ)

DMZ architecture uses two firewalls to isolate servers that are accessible from untrusted networks. The DMZ should be deployed such that only specific (restricted) communication is allowed between the business network and the DMZ, and between the control network and the DMZ. The business network and the control networks should ideally not communicate directly with each other.

If direct communication to a control network is required from the business network or from the internet, carefully control, limit and monitor all access. For example, require two-factor authentication for a user to obtain access to the control network using Virtual Private Networking (VPN) and even then, restrict the allowed protocols/ports to just the minimum set required. Further, every access attempt (successful or not) and all blocked traffic should be recorded in a security log that is regularly audited.

6.3 Access to Process Control networks

Ethernet traffic from the Supervisory Control network to the Process Control networks should be restricted to support only the functionality that is required. For example, since Proficy Machine Edition uses SRTP to download the application to the VersaMax controllers, then SRTP traffic must be allowed through the firewall. However, if a particular protocol (such as Modbus TCP) doesn't need to be used between those regions, then the firewall should be configured to block that protocol. If, in addition to that, a controller doesn't have some other reason it needs to use that protocol, then – in addition to blocking it at the firewall – the controller itself should be configured to disable support for the protocol.

NOTE: Network Address Translation (NAT) firewalls typically do not expose all of the devices on the "trusted" side of the firewall to devices on the "untrusted" side of the firewall. Further, NAT firewalls rely on mapping the IP address/port on the "trusted" side of the firewall to a different IP address/port on the "untrusted" side of the firewall. Since communication to the VersaMax controller or ENIU will typically be initiated from a PC on the "untrusted" side of the Process Control network firewall, protecting a Process Control network using a NAT firewall may cause additional communication challenges. Before deploying NAT, carefully consider its impact on the required communications paths.

7 Other Considerations

7.1 Patch Management

A strategy for applying security fixes, including patches, firmware updates, and configuration changes, should be included in a facility's security plan. Applying these updates will often require that an affected VersaMax controller or ENIU be temporarily taken out of service.

Some installations require extensive qualification be performed before changes are deployed to the production environment. While this requirement is independent of security, ensuring the ability to promptly apply security fixes while minimizing downtime may drive the need for additional infrastructure to help with this qualification.

7.2 Real-time Communication

When designing the network architecture, it is important to understand what impact the network protection devices (such as firewalls) will have on the real-time characteristics of the communications traffic that must pass through them. In particular, the Ethernet Global Data protocol is generally expected to operate with small, known, worst-case bounds on its communications latency and jitter. As a result, network architectures that require real-time communications to pass through such devices may limit the applications that can be successfully deployed.

7.3 Additional Guidance

7.3.1 Protocol-specific Guidance

Protocol standards bodies may publish guidance on how to securely deploy and use their protocols. Such documentation, when available, should be considered in addition to this document.

7.3.2 Government Agencies and Standards Organizations

Government agencies and international standards organizations may provide guidance on creating and maintaining a robust security program, including how to securely deploy and use Control Systems. For example, the U.S. Department of Homeland Security has published guidance on Secure Architecture Design and on Recommended Practices for cyber-security with Control Systems. Such documentation, when appropriate, should be considered in addition to this document. Similarly, the International Society of Automation publishes the ISA-99 specifications to provide guidance on establishing and operating a cyber-security program, including recommended technologies for industrial automation and control systems.

8 Related Documents

VersaMax PLC User Manual (GFK-1503)

VersaMax Modules Power Supplies and Carriers User Manual (GFK-1504)

CPU with Embedded Ethernet Interface (IC200CPUE05) IPI (GFK-1892)

VersaMax PLC Station Manager User's Manual (GFK-1876)

IC200EBI001 - VersaMax Ethernet Network Interface Unit (GFK-1859)

GE Information Centers

Headquarters:
1-800-433-2682 or 1-434-978-5100

Global regional phone numbers
are available on our web site
www.ge-ip.com

GFK-2955B