GE
Automation & Controls
EmbeddedLinux Products

PACSystems* Controllers with Linux Secure Deployment Guide

GFK-3055
August 2018

For Public Disclosure

Legal Information

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.

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

General Contact Information

Online technical support and GlobalCare	www.geautomation.com/support
Additional information	www.geautomation.com
Solution Provider	solutionprovider.ip@ge.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 www.geautomation.com/support

Americas

Phone	1-800-433-2682
International Americas Direct Dial	1-780-420-2010 (if toll free 800-option is unavailable)
Customer Care Email	digitalsupport@ge.com
Primary language of support	English

Europe, the Middle East, and Africa

Phone	+800-1-433-2682
EMEA Direct Dial	+ 420-296-183-331 (if toll free 800-option is unavailable or if dialing from a mobile telephone)
Customer Care Email	digitalsupport.emea@ge.com
Primary languages of support	English, French, German, Italian, Spanish

Asia Pacific

Phone	+86-21-3877-7006 (India, Indonesia, and Pakistan)
	+86-400-820-8208 (rest of Asia)
Customer Care Email	digitalsupport.apac@ge.com
Primary languages of support	Chinese, English

Table of Contents

PACSystems* Controllers with Linux Secure Deployment Guide GFK-3055

Table of Figures

Chapter 1 About this Guide

GE provides these general recommendations and guidelines to aid the end user in managing security risk associated with the operation of the CPL410. However, it is entirely the owner's responsibility to ensure the security of the Linux OS and any associated applications deployed on the platform.

1.1 Applicable Products

This document provides information that can be used to help improve the cyber security of systems that include Linux Operating Systems supplied by GE Automation & Controls. It is intended for use by control engineers, integrators, IT professionals, and developers responsible for deploying and configuring products with embedded, customer accessible Linux (embedded open Linux).

Product	Catalog #	Description	Provisioning Connection	Data Source Connection	Cloud Connection
CPL410	IC695CPL410	Ubuntu Linux 16.04 embedded in an Industrial Internet Control System running PACSystems*.	• Ethernet LAN	• Virtual LAN through hypervisor • Ethernet LAN	• Ethernet LAN

1.2 Related Documentation

1.2.1 Product Landing Pages

Product	URL
CPL410 with Embedded Field Agent	https://digitalsupport.ge.com/communities/en_US/Article/IC695CPL410-Landing-Page
Mini Field Agent	https://digitalsupport.ge.com/communities/en_US/Article/ICMFA000000-Landing-Page
CPE400 with Embedded Field Agent	https://digitalsupport.ge.com/communities/en_US/Article/IC695CPE400-Landing-Page
Virtual Field Agent	https://digitalsupport.ge.com/communities/en_US/Article/ICVFA000000-Landing-Page

1.2.2 Other Documentation

Document ID	Document Title
GFK-3053	CPL410 Quick Start Guide
GFK-2993	Field Agents User Guide
GFK-3017	Field Agent Upgrade Guide
GFK-3018	Field Agents Registration Guide
GFK-3019	Field Agent Machine Adapters User Guide
GFK-2830	PACSystems RXi, RX3i, RX7i and RSTi-EP Controller Secure Deployment Guide
GFK-2222	PACSystems RX7i, RX3i and RSTi-EP CPU Reference Manual
GFK-2314	PACSystems RX3i System Manual
GFK-2224	PACSystems RX7i, RX3i and RSTi-EP TCP/IP Ethernet Communications User Manual
GFK-2225	PACSystems TCP/IP Ethernet Communications Station Manager User Manual
GFK-2571	PACSystems RX3i & RSTi-EP PROFINET I/O Controller Manual
GFK-2572	PACSystems RX3i PROFINET Controller Command Line Interface Manual
GFK-2904	PROFINET IO Devices Secure Deployment Guide
GEH-6721 Vol I	Mark* VIe and Mark* VIeS Control Systems Volume I: System Guide
GEH-6721 Vol II	Mark* VIe and Mark* VIeS Control Systems Volume II: General-purpose Applications
GEH-6721 Vol III	Mark* VIe and Mark* VIeS Control Systems Volume III: For GE Industrial Applications
GEH-6839	Mark* VIe Control Systems Secure Deployment Guide
GEH-6700	ToolboxST* User Guide for Mark* Controls Platform
GEH-6767	Security Baseline Information for Mark* VIe Control
GEA-S1289	Cyber Security Management System for Mark* VIe Control
GFA-2120B	Mark* VIe UCSC Outcome Optimizing Control for Power Generation Applications
GEH-6851	Control Server – High Availability (HA) Maintenance Guide

1.3 Revisions in this Manual

Rev	Date	Description
-	Aug 2018	• Initial Publication

In addition to these manuals, datasheets and product update documents describe individual devices and product revisions. The most recent documentation is available on the GE Automation & Controls support website www.geautomation.com/support.

Chapter 2 Introduction

2.1 What is Security?

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

- Confidentiality: Ensure that only those people whom you want to see certain information can actually 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. As GE product vulnerabilities are discovered and fixed, security advisories are issued to describe each vulnerability in each product version as well as the version in which the vulnerability was fixed. GE Product Security Advisories can be found at the following location:

https://digitalsupport.ge.com/communities/en_US/Article/GE-Intelligent-Platforms-Security-Advisories?Type=Alert

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 such as 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*

Adopting the following security best practices should be considered when using GE products and solutions.

- Care must be taken when connecting hardware to a wide area network including but not limited to a corporate network or the Internet at large. The network segmentation and firewall rules at each network interface must be carefully considered to reduce the allowed traffic to the bare minimum needed for operation. 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. Care must be taken to control, limit, and monitor all access, using, for example, virtual private networks (VPN) or Demilitarized Zone (DMZ) architectures. If a device is being used in a manner that does not require wide area network access, it is strongly recommended that the device not be connected to any wide area network to reduce attack surface.
- Harden system configurations by enabling/using the available security features, and by disabling unnecessary ports, services, functionality, and network file shares.
- Apply the latest GE product security updates, SIMs, and other recommendations.
- Apply 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 *Sample Checklist*

This section provides a sample checklist to help guide the process of securely deploying GE products.

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.
4) Revise the network as needed to ensure appropriate partitioning, adding firewalls or other network security devices as appropriate. Update the network diagram.
5) Configure firewalls & other network security devices.
6) Enable and/or configure the appropriate security features on each GE product.
7) On each GE product, change every supported password to something other than its default value.
8) Harden the configuration of each GE product, disabling unneeded features, protocols and ports.
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 the checklist above, is limited to only providing secure deployment guidance.

Chapter 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 device, and by using appropriately configured and deployed network security devices (e.g. firewalls, routers) to block every protocol (whether enabled or disabled) 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 chapter describes how the supported serial and Ethernet application protocols are used in embedded and indicates the role of each participant in the communication. 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 to support only the required communications paths for each installation.

3.1 Serial Communication

This section indicates which serial interfaces are supported by **Linux** on each Product.

Available Serial Interfaces

Interface	CPL410
RS-232	No
RS-485	No
CAN	No
SDIO (microSD)	No
USB	Yes

3.1.1 Application Layer Protocols

The table below indicates the serial protocols supported by each embedded open Linux Controller type by default. Additional protocols may be installed but are not listed here.

Available Serial Protocols

Interface	CPL410
USB	Yes (Storage, HID, …) USB access not limited, All Devices supported by Ubuntu 16.04 Server
RS232	No

3.2 Ethernet Communication

This section indicates which Ethernet protocols are supported by each embedded open Linux product by default. As access to Linux is not limited, additional protocols can be installed, but are not listed here.

Supported Ethernet Protocols

OSI Layer	Protocol	CPL410
Link	ARP	Yes
Network	ICMP	Yes
	IGMP	Yes
	IPv4	Yes
	IPv6	Yes
Transport	TCP	Yes
	UDP	Yes
Application	DHCP Client	Yes
	DNS Client	Yes
	HTTP Server	Yes
	HTTPS Server	Yes
	OPC® UA Client	Yes
	SSH	Yes
	SCP/SFTP	Yes

3.2.1 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 #
ICMP	0x0800	1
ICMP	0x0800	2
IPv4	0x0800	N/A
IPv6	0x86DD	N/A

Transport Layer Protocols

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

Note: Each of these lower-level protocols is required by one or more of the supported Application protocols.

3.2.2 Application Layer Protocols

Embedded open Linux can act as a server, responding to requests sent through any of several different protocols. It can also act as a client, sending requests to other servers using any of several different protocols. The following table, *Application Layer Protocols*, lists the protocols supported by embedded open Linux, along with any TCP or UDP ports that are leveraged by those protocols. This table could aid in configuring a firewall between embedded Linux Controller and any clients or servers it communicates with. This table lists which of these protocols are communicated with, when in a client or server role.

Application Layer Protocols

Protocol	Server TCP Port	Destination UDP Port
DHCP		67 on server 68 on client
DNS	53	53 on server >1023 on client
HTTP	80	
HTTPS	443	
OPC UA	4840, 4841	
SSH	22	
SCP/SFTP	22	

Chapter 4 Security Capabilities

This chapter describes the embedded Linux capabilities and security features that can be used as part of a defense-in-depth strategy to secure your system.

Security Capability	CPL410
Predefined set of Subjects & Access Rights	Yes
Access Control List	Yes
Secure Remote Operations	Yes
Firmware Signatures	Yes
Software Firewall	Yes
Hardware Entropy Source	Yes
Hard Disk Encryption	No
Secure Boot	Part[1]

[1] Partially: Real Time PLC is part of the Secure Boot chain, but Linux is not.

4.1 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).
2) Enforcement – Approving or rejecting access requests.

This section describes the Access Control capabilities supported by Linux, which includes its Authorization capabilities.

4.1.1 Authorization Framework

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

Functionality	Application Protocol	Subjects Available	CPL410
Web Page	HTTPS	None	Yes[1]
Web Page	HTTPS	“admin” user	No
Remote Login	SSH	“admin” user	Yes[2]

1) Default pages are implemented for demonstration purposes only and do not provide authentication; Web Server user management is strongly recommended to be used for production pages.
2) Default user.

4.1.2 Enforcement

Linux enforces the access rights for the data and services that it provides. An unprivileged user account “admin” is leveraged by default to allow login. This account provides sudo privileges to allow complete system accommodation. GE recommends adding less privileged users for non-administrative tasks.

4.2 *Authentication*

Linux provides password-based authentication for most server protocols. The following tables provide a summary of authentication mechanisms supported by embedded Linux for each protocol.

Authentication supported by default Servers

Functionality	Application Protocol	Authentication Supported	CPL410 default
Web Server	HTTPS/HTTP	Username and Password	No
Remote Login	SSH	Username and Password	Yes[1]
File Transfer	SCP/SFTP	Username and Password	Yes

1) Password change enforced at first login

Authentication supported by default Clients

Functionality	Application Protocols	Authentication Supported	CPL410
Lookup IP addresses by hostname	DNS	None	No
Read data from an OPC UA server	OPC UA	Username and Password, Certificates	Yes

4.2.1 *Privileged Users*

In Linux the superuser root has all rights and permissions to all files and programs.

As root therefore potentially can cause great damage to a Linux system, it is common use not to allow root to log in. Instead ordinary users are provided with additional rights via the “superuser do” (sudo) mechanism. This, powerful tool, can be configured (/etc/sudoers.d) to assign privileges fine-granularly to users on a per program basis. To execute a command requiring privileges, a sudo user needs to prepend “sudo” to the command.
GE recommends providing users only with the minimum privileges required for their tasks.

User	Authentication	Programs	Sudo	Sudo Auth.	CPL410
admin	Username and Password	ALL	Yes	No	Yes
root	Disabled	ALL	NA	NA	Yes

Embedded Linux default users

If, in the default sudo configuration, the “admin” user is allowed to execute all privileged commands without authentication (see table above) it is recommended to change configuration to that effect that sudo authentication is enforced in a production environment. Additionally, consider adding users with sudo privileges for determined tasks respectively commands only.

4.2.2 Authentication Recommendations

GE strongly recommends that authentication be used for every enabled protocol that supports authentication, and that all default passwords be changed. Whenever protocols are used with no authentication mechanism, or when authentication is disabled or relies on sending credentials in plaintext across the network, it is critical to control physical and electronic access to the network to prevent unauthorized messages from being sent and acted upon.

The following table provides recommended actions to mitigate the risk of external or internal entities accessing a facility network and sending unauthorized messages.

Item	Recommendations
Personnel Security Protection	All individuals with permission to physically access end customer systems should have background checks and be trained in the proper use and maintenance of the systems.
Physical Security Perimeter Protection	1) Whenever possible, there should be no physical network path from a facility network to the Internet. It should not be possible for an attacker to reach a facility network from any Internet-facing computer.
	2) Networks should always be physically segmented as suggested in the Reference Network Architecture diagram (Figure 1) to avoid exposure to facility network.
	3) Each asset should be visibly labeled by a unique identifier, with all expected asset identification compiled into an access-controlled list.
Electronic Security Perimeter Protection	1) All external access to a facility network should be managed through a Virtual Private Network (VPN) or similar technology leveraging two-factor authentication.
	2) Next-Generation Firewalls should be properly configured and deployed at each conduit between physical networks that deny all but the specifically allowed protocol families, source addresses, and destination addresses, and specific application-level commands between the two adjacent networks. For example, a Next-Generation Firewall could prohibit write operations across networks while allowing read operations.
	3) If one network node such as MDI servers uses unauthenticated protocols to exchange information or commands with another network node on the same physical network, a Next-Generation Firewall could be deployed between the two network nodes. This Next-Generation Firewall should be configured to explicitly whitelist all expected messages between the two network nodes and deny all other unexpected messages.
	4) To detect and alert for unexpected, unauthenticated messages on a given network, an Intrusion Detection System (IDS) could be configured and deployed. Consider configuring the IDS to log all events to a Security Information and Event Management (SIEM) system that aggregates all security information on the ICS network.
	5) To detect and actively prevent unexpected, unauthenticated messages on a given network from reaching a given network node, an Intrusion Prevention System (IPS) could be configured and deployed. Consider configuring the IPS to log all events to a Security Information and Event Management (SIEM) system that aggregates all security information on the ICS network.
	6) To limit the impact of the compromise of any single user account, it is recommended to divide administrator privileges into several user accounts, each for its own operational function.
	7) To limit the impact of the compromise of any single set of credentials (user name, password) for any end customer equipment, it is recommended to never re-use credentials for different tools or purposes.
	8) Carefully protect sources of and access to credentials (user names, passwords) for all end customer equipment, including switches, routers, firewalls, IDS, IPS, etc.
	9) Enforce a policy of rotating credentials for end customer equipment periodically and after personnel changes. Note that products with no support for enforcement of unique passwords over time should be compensated for with policies and procedures that require a history of unique passwords.

Item	Recommendations
Passwords	Recommendations on password complexity and management can be found in NIST 800-118, Guide to Enterprise Password Management.

4.3 Password Management

Each instance of a server has its own instances of the predefined subjects. Therefore, passwords for each subject must be separately managed for each instance of a given kind of server.

GE strongly recommends the use of long (10 characters or more), complex passwords wherever passwords are used for authentication. Recommendations on password complexity and management can be found in NIST 800-118, *Guide to Enterprise Password Management*.

Changing Passwords

Functionality	Authenticated Subjects	How Passwords Are Assigned
SSH remote login	"admin" user	Auto-prompted upon first login using the default password (admin).

4.4 Firewall

A firewall is a network security mechanism filtering network traffic according to predefined firewall rules. With a firewall the user can, for example, limit Linux access to specified IP Addresses or services (ports).

To minimize the surface area for attacks on the Local Area Network, GE strongly recommends evaluating the possible security impact of each port to be opened, and only opening the minimum set of ports required to support the deployed applications and Machine Adapters. Furthermore, GE strongly recommends limiting the protocols used to the minimum set required for the intended application and adding additional compensating security controls whenever using insecure protocols that cannot be otherwise removed from the deployment.

4.4.1 CPL410 Firewall

CPL410 Ubuntu Linux comes with a Kernel built in firewall configurable with the *iptables* utility. The rules (i.e. the tables) you need to define with *iptables* are complex. Ubuntu therefore also provides the “uncomplicated firewall” tool *ufw,* which is a more straightforward frontend to *iptables*.

A detailed description on how to create rules is beyond the scope of this guide. Please refer to the Ubuntu home page to learn more about *ufw* and *ipables* (https://wiki.ubuntu.com/UncomplicatedFirewall, https://help.ubuntu.com/community/IptablesHowTo).

As changes to the firewall tables can have a large impact on the security of a device, the firewall tools have been enhanced to log table access to the file /var/log/iptables.log.

To give users unlimited access, CPL410 does not implement any *iptable* rules. All active Linux services are therefore accessible via network without protection. Although CPL410 instantiates only a minimum set of network services, the user may wish to limit access to those services by a set of firewall rules (e.g. limit access to a range of IP Addresses).

Note: Security requirements vary considerably from one application to another. Predicting the required level of security or the appropriate configuration for tools in place is nearly impossible. CPL410 therefore implements only some basic security rules, but additional to the mechanism mentioned here, Linux has built-in features and installable tools to assist the user in securing the Open CPL410 Platform. Please follow the numerous security “best practices” guides to achieve the level of security you wish for the Linux side.

CPL410 default Network Services

A network service is a program running in background, monitoring network connections from remote clients and providing data services to those clients. Only the bottom Ethernet Port of the CPL410 (ETH) is assigned to Linux. All services listed below, therefore only listen on this port for incoming remote traffic.

The default setup of CPL410 Linux instantiates a minimal set of network services:

Service	Protocol	Accepted Addresses	Port	Program
SSH	TCP IPV4/IPV6	From all	22	sshd
HTTP	TCP IPV4/IPV6	From all	80 Redirected to HTTPS	apache2
HTTPS	TCP IPV4/IPV6	From all	443	apache2
DHCP Client	UDP IPV4		68	dhclient
ICMP	IPV4/IPV6	From all	N/A	Kernel IP Stack

Every network service offered to remote clients also may be an attack vector by exploiting bugs in the implementation of this service. To minimize the attack surface of your CPL410, only start as few services as necessary and limit access to the remaining services by firewall rules or appropriate service configuration.

4.5 Confidentiality and Integrity

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 it was malicious.

Following are the communications protocols supported by GE embedded Linux provide either of these features, as detailed in the table below. Therefore, compensating controls may be required to meet an installation’s security requirements for protecting data in-flight.

Protocol-Provided Security Capabilities

Protocol	Data Encryption	Message Authentication Codes
DHCP	No	No
DNS	No	No
HTTPS	Yes	Yes
OPC UA	Yes	Yes

4.5.1 Secure Boot

The Secure Boot mechanism ensures that only verified Controller components can be loaded and executed.

CPL410 Secure Boot

For CPL410 the Controller real time engine, the bootloader and the Hypervisor are part of the secure boot chain and therefore can neither be accessed by customers, nor be tampered with by attackers.

4.5.2 CPL410 Linux Integrity

The Secure Boot Chain is built on static signatures and hashes. Since CPL410 embedded Linux is open to customer modifications signatures and hashes can vary. Therefore, they cannot be integrated into the Secure Boot chain. GE A&C therefore cannot guarantee security or integrity of the Linux components. It is the responsibility of the user to ensure that Linux files are trustworthy and cannot be corrupted by attackers.

One possibility to ensure the integrity of Linux is to regularly create hashes of monitored files and compare them with externally stored reference values.

Factory Reset files

The same applies to the factory reset files, which are located on partition 12 (/dev/sda12). These files are used to restore Linux to the delivery state (see also CPL410 Quick Stat Guide) in case Linux is inoperable. Partition 12 is not mounted by default but is fully accessible by Linux and therefore may be tampered by malware.

4.5.3 SSH

SSH allows secure transfer protocols using encryption only. Encryption keys are therefore automatically exchanged between server and client. So, if establishing a SSH client connection for the first time, user will be asked to accept the remote host public key. Accepted public keys are stored in a client database to be used in future communications. If a fake server tries to masquerade as a known server whose public key is already stored in the client database, SSH tools will warn about a key change, thus enabling the user to identify the fraud.

CPL410 SSH

CPL410 SSH-Host-Key-Pairs (public and private) are stored in the directory /etc/ssh. These keys are not populated at the time of delivery. Therefore, new SSH-Keys are generated automatically during the first boot or whenever Linux detects missing keys during a boot up. Users may use these generated keys or create new ones with the ssh-keygen command.

Chapter 5 Configuration Hardening

This chapter is intended to assist in reducing the potential attack surface by providing information that can be used to harden the configurations that are present in an embedded Linux installation. Configuration Hardening should be considered in addition to enabling and using security features such as Authentication, Access Control, and Authorization.

In general, GE recommends disabling all services and protocols that are not required for the intended application.

5.1 Linux Hardening

5.1.1 Harden Access to each Industrial Data Source

When implementing applications consuming industrial data from a data source like an OPC UA Server it is important to configure the visibility of variables or registers such that only those tags that are expected to be consumed are readable by the application and other network nodes. For example, OPC UA variables in the PACSystems CPUs can be left unpublished, published internally to other components of the User Application, published as External Read-Only, or published as External Read/Write. Variables should not be published as External Read-Only unless they need to be read by an embedded Linux application or another network node. Variables should not be published as External Read/Write unless they need to be read and written to by a Field Agent or another network node. Refer to the User Guide or Secure Deployment Guide for the specific industrial data source to learn how to restrict the visibility of available variables and registers.

GE strongly recommends that all published variables and registers be only published as read-only. If applications need also to write OPC UA variables published as read/write, GE strongly recommends limiting the variables and registers published as read/write to the minimum set needed by the application.

As an additional layer of security, GE strongly recommends enabling authentication for read and write operations on industrial data sources wherever supported. For example, PACSystems CPUs should have Enhanced Security enabled with passwords protecting PRIV Levels 2, 3, and 4. With this set, an attacker on the network would be unable to, for example, write to any OPC UA variables that are accidentally published as read/write on a PACSystems OPC UA Server without knowing the PRIV Level 2 password.

If more granular control of specific read and write operations to industrial data sources is required, an application level firewall with knowledge of industrial protocols (like the Wurldtech OpShield*) can be placed in-line between the industrial data source and Field Agent. The firewall can be configured to enforce policies that whitelist specific devices from reading or writing to specific OPC UA variables.

5.2 CPL410 Hardening

5.2.1 CPL410 Linux Update

Embedded Linux is installed during production of the device. In the time that passes until the initial operation, most probably new security threats have been discovered and mitigated. To integrate such mitigations update Linux by using the standard Ubuntu update mechanisms.

Depending on the software repositories configured in /etc/apt/sources.list file and in the /etc/apt/sources.list.d directory, new software packages are typically downloaded from external repositories. A working Internet connection is therefore required to install or update packages.

Upgrading a system also can include the Linux Kernel and the initial RAM disk, both located in the /boot directory. If a new Kernel or RAM disk has been installed by upgrade, make sure the symbolic links /boot/vmlinuz and /boot/initrd.img are pointing to the latest Kernel (RAM disk version).

Whenever a new Kernel version is active, drivers not provided by Ubuntu need to be recompiled. Two drivers are needed for CPL410 communication with the PLC runtime: these are recompiled on the fly, whenever a new Kernel is detected. Driver archives are located in the /boot/rth folder and must not be deleted.

Note: There always is a risk of damage to the Linux installation when upgrading the system, especially if the Kernel is being updated. Consider performing such an upgrade in a protected environment before attempting such an upgrade on a production system.

5.2.2 CPL410 WEB Server

CPL410 is instantiating an Apache2 Webserver by default. This server is listening to port 80 (HTTP), and 443 (HTTPS), whereas access to port 80 is redirected to HTTPS protocol. The Webserver provides web pages showing information and example applications. Neither the access to the Webserver nor to the pages are protected by default. As these pages are provided for demonstration purposes only, it is recommended to either delete them (/var/www/...) or to protect them by an authentication mechanism.

If a Webserver is not needed for the use case, it is strongly recommended to disable the Apache2 service.

Chapter 6 Reference Network Architecture

The following figure represents a typical deployment of an embedded Linux device for a large industrial application. However, the level of segmentation will vary based on the level of risk assessed for the application.

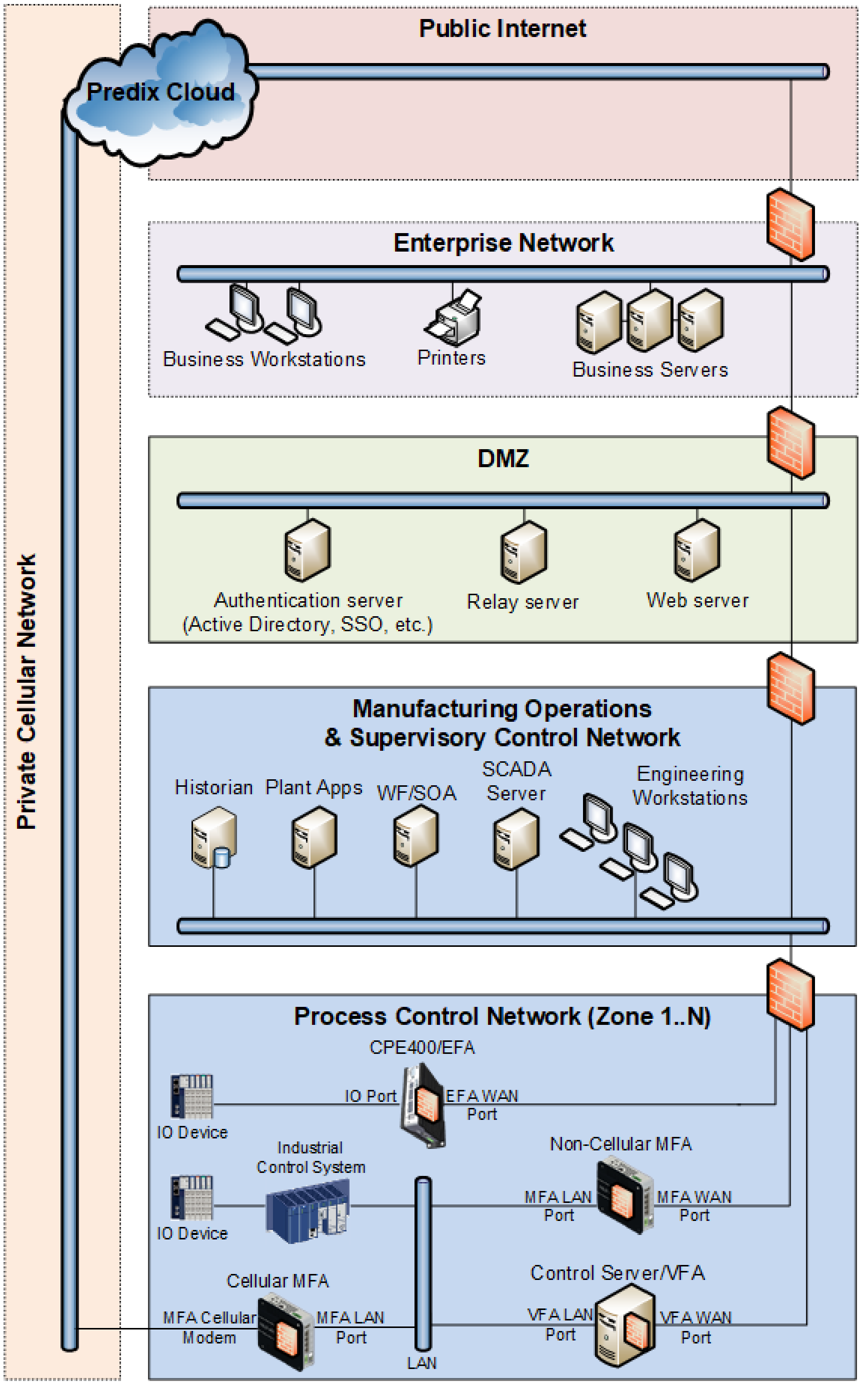

Figure 1: Field Agents SDG Reference Network Diagram

6.1 Remote Access and Demilitarized Zones (DMZ)

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 a 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. The Enterprise network may also reside behind a separate DMZ.

A 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 GE devices and the DMZ, and between the Cloud / Internet and the DMZ.

6.2 Linux to Cloud Communications

Ethernet traffic from the Cloud/Internet to embedded Linux should be restricted to support only the functionality that is required. If a protocol is not needed between those regions, then the firewall should be configured to block that protocol.

Note: Network Address Translation (NAT) and Port Address Translation (PAT) firewalls typically do not expose all the devices on the “trusted” side of the firewall to devices on the “untrusted” side of the firewall. Further, NAT/PAT 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 initial provisioning communication to Field Agents may be initiated from a PC on the “untrusted” side of the Process Control network firewall, protecting a Process Control network using a NAT/PAT firewall may cause additional communication challenges. Before deploying NAT/PAT, carefully consider its impact on the required communications paths.

6.3 Linux to Industrial Data Source Communications

GE recommends avoiding the use of network ports for simultaneous communication with industrial data sources like control systems and Wide Area Networks (Cloud).

However, there may be situations where it is necessary to use a port to communicate with an industrial data source and the Internet. In such situations, GE strongly recommends structuring the network in such a way that does not bridge or otherwise expose the entire Process Control Network to the Manufacturing Operations & Supervisory Control Network and/or DMZ. Special care must be taken to ensure the firewall between the Process Control Network and higher-level networks is configured to block access to any control systems or other industrial data sources from the Manufacturing Operations & Supervisory Control Network.

Chapter 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 may require that an affected device be temporarily taken out of service.

Some installations require extensive qualification to 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 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 Government Agencies & 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 industrial control systems and related equipment. Below is a list of common standards and regulations to consider when designing a system's security policy and architecture. Such documentation, when appropriate, should be considered in addition to this document.

- ISA/IEC 62443 (formerly ISA99) for critical infrastructure
- NIST 800-53 for federal information systems
- ISO 27001 for information security management
- ISO 27002 for information security management
- ISO 27019 for information security management of electric systems
- NERC CIP V5 for critical infrastructure specific to electric systems
- NIST Cyber Security Framework for critical infrastructure

GE Automation and Controls
Information Centers

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

Global regional phone numbers
are available on our web site
www.geautomation.com

Additional Resources

For more information, please visit our web site:

www.geautomation.com