GEH-6843

Control Server

Dell™ Wyse™ Thin Client HMI System

Secure Deployment Guide

Aug 2016

Public Information

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.

***Public Information** – This document contains non-sensitive information approved for public disclosure.*

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.

For further assistance or technical information, contact the nearest GE Sales or Service Office, or an authorized GE Sales Representative.

Issued: Aug 2016

We would appreciate your feedback about our documentation.
Please send comments or suggestions to controls.doc@ge.com

Contents

Notes

1 Introduction

This document provides information that can be used to help improve the cyber security of systems that include Mark VIe Control System. It is intended for use by control engineers, integrators, IT professionals, and developers responsible for deploying and configuring the thin client within the Mark VIe Control System.

Each site will have its own philosophies, procedures, and audit requirements. In the power generation field many of these will be based on industry standards and practices such as described in ISA-99, IEC-62443, NIST 800, and NERC CIP documents. These standards and practices should be used as guidance while configuring and maintaining the site.

This document describes many tools that are available and concepts that should be followed to help sites meet their security requirements, but tools alone cannot guarantee a site's compliance. The best password policy enforcement tool cannot protect against posting a password on a sticky-note on a computer monitor - an act that is likely to raise issues during an audit. Site procedures (which are outside the scope of this document) must be created, maintained, and followed to meet most audit requirements.

Certain sections of this document include information about optional products, such as the NetworkST 4.0 product with its network hardening capability or the SecurityST product with its wealth of additional security functions. These products are not required to run the Mark VIe control system, but their pre-packaged functionality can be used to strengthen the site security posture. Whether or not these products are used, the concepts presented in this document should be addressed within each site's specific security requirements.

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 supplied with the NetworkST 4.0 option) 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.

Notes

2 Security and Secure Deployment

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.

Different sites will have different needs and requirements surrounding these concepts. Follow the site's requirements when building, deploying, and using systems, keeping in mind the impact that decisions and procedures will have on the site's security posture.

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 Concepts

There are a number of concepts that are used throughout this document that provide many of the building blocks used to improve a site's security posture. This section describes these basic concepts.

Authentication is the act of determining or verifying the identity of a user or element that is requesting access to a resource or requesting that a particular action be taken.

- Example: The Microsoft® Windows® Operating System typically defines a username to establish an identity for a user and a password to verify that the user is in fact who they claim to be.
- Example: Many communications schemes use a Certificate to verify the identity of the endpoint (or endpoints) of that communication. As part of the initiation of the communication link one or both sides provide their certificate to verify their identity.

Authorization is the act of determining what identities are allowed (authorized) to access a resource or perform an action. Most authorization schemes support multiple levels of authorization, such as a distinction between the ability to view an item versus the ability to modify an item.

- Example: The Microsoft Windows Operating System supports multiple levels of access on items (such as ReadOnly versus ReadWrite access to a file) and a set of operating system privileges to control actions that users may take.

Access Control Lists (ACLs) are often used as a method of binding together the requester's identity with the level of access allowed. These ACLs are defined on a per-item basis, so different items may have different ACLs.

- Example: The Microsoft Windows Operating System supports ACLs on files and devices to define which users have what access rights to those items.
- Example: The network switches support ACLs on their administrative interfaces to define which elements of the system have the right to access the administrative functions.

Note When done at the operating system level, ACLs protect an item no matter what tool (program) is used to attempt access - this is called authoritative security. This is a stronger level of protection than when the tool being used determines whether to allow access or not - this is called cooperative or client-based security. Cooperative security can be bypassed by using a different client to access the resource, authoritative security cannot be bypassed as easily.

The concept of **Least Privileges** states that each user should be granted only the access rights and privileges that they need to perform their work function. This protects items and configurations against inadvertent changes by users, possibly because of malware that the user has inadvertently triggered

- Example: the Microsoft Windows Operating System supports the concept of Administrator level access for making changes to the operating system and software running on the computer. If a user is running with administrative access, any malware that they trigger could alter the operating system or any program in any way that it desired. If the user is running in a non-administrative account it is limited in the changes that it can make.
- Example: the ToolboxST subsystem supports a Users and Roles concept to define what operations a user is allowed to take, such as forcing variables, issuing alarm acknowledge and reset commands, or downloading configurations to controllers.

The concept of **Role Based Access Control** (RBAC) is a consolidation of using the user's identity (authentication) and their allowed rights (authorization) in a slightly easier to maintain manor. An intermediate concept of a user's Role is introduced, which defines a collection of users with shared access rights and privileges. This simplifying scheme has a number of benefits:

- Authorization (done on a per-item basis) is done not to a set of user identities, but instead to a Role - it's ACL is not a list of usernames but a (much smaller) list of Roles. As users are added and removed from the system the ACLs on each item do not have to change since they were tied to the Roles and not the users, making updates very fast and efficient.
- Reporting on the members of a single Role is quick and easy compared to having to visit all items and examine their individual ACLs.
- If a user's Role changes (their job requirements change) it is a simpler task to assign them to a new role, and perhaps change it back again if the change was only temporary.
- New roles are typically easy to define as the site's operating procedures change and different classifications of users are required or different sets of privileges are identified.
- Example: the Microsoft Windows Operating System has a single security group that grants Administrative access to computers - the Administrators group. Adding or removing a user to the Administrators group will grant or revoke the user's administrative privileges and the individual ACLs on all files and devices does not have to be changed.
- Example: The ToolboxST subsystem supports a Users and Roles concept, which defines what rights and privileges are given for each Role. If a site decides to change whether the Operators role is allowed to force variables, granting or revoking the Force privilege to the Operators role is all that is required - there is no need to change each user's privileges.

2.5 What is Hardening?

Hardening a system includes taking steps to reduce attack surfaces that may be used in an attack on the system. These steps include removing functions that are not essential and changing system settings to help deter attacks. Each section in this manual includes information on how to help harden each component, but the following concepts apply to most all products:

- Disable unused Servers and Services on each device.
- Create and maintain the list of users and their rights. Disable or remove a user's account as soon as the person is no longer granted access rights to the equipment.
- Implement the site's password policies, where possible by configuring the equipment to reject passwords that don't meet the standards automatically.
- Remove all as shipped accounts or (if the account is to remain) change all passwords as soon as feasible during the site commissioning process. Implement strict site policy and controls to limit the exposure of passwords.

2.6 General Recommendations

The following general recommendations should be used to improve the security posture at the site:

- Provide physical security for all devices - many, if not most devices can be compromised by an attacker that has physical access to the device at startup/boot time or direct access to the non-volatile media that the device boots from (hard drive, flash memory, etc.). Access to network equipment (switches, routers) can allow for introduction of new devices onto the networks, including network monitoring equipment.
- Disable unused services on devices to reduce the mechanisms available for attacks.
- Wherever possible, configure the site's password requirements (length, complexity…) into the devices or operating systems to have each device enforce them automatically. If it cannot be automatically enforced it must be done procedurally.
- Implement Role Based Access Control wherever available, and keep the list of users and roles current.
  - Some system components allow for logging (auditing) failures, use these if available - preferably logging to a centralized site SIEM (if available) for both convenience and pattern analysis across devices.
- Implement a site-wide scheme for applying software patches, especially those defined as security patches.

Limiting visibility to the control system is a strong defense-in-depth approach to help prevent attacks. This is accomplished by using separate communications networks (Virtual Local Area Networks or VLANs) to isolate different types of equipment, then tightly controlling the network traffic that can cross from one VLAN to another. There are various schemes and recommendations (ISA-99, IEC-62443) that include network segmentation and they should be followed when making any networking changes or while introducing new equipment to the control system.

- Consider using a dedicated point-to-point link instead of a shared network for dedicated functions within the same network zone. Never bridge network zones using a dedicated link, always go through a router that provides controlled access (and optional logging).
- Consider using an additional firewall even within a network zone to add additional constraints on traffic, especially if the traffic includes a protocol that does not support authentication.

3 Thin Client

3.1 Security Capabilities

3.1.1 User Authentication and Authorization

Under normal operation, users should log into the Thin Client terminals using their domain credentials. This establishes their identity to the Thin Client terminal, and that identity is typically forwarded as part of the connection request to a host computer.

- Logging in to a Thin Client terminal using domain credentials will grant user mode access to the Thin Client terminal. If administrative access to the Thin Client terminal is required, a local account must be used.

Local accounts exist in the Thin Client terminals to handle local administrative level (configuration) changes and to provide for operation at times when a domain controller cannot be contacted for domain authentication.

- Maintain local account passwords according to the site policy. Complexity and reuse rules are not enforced by the equipment, they must be addressed procedurally.
- Users should be provided with local account passwords according to their roles and responsibilities. Administrative level accounts to the Thin Client terminal should only be provided to those who require them to perform their job function.
- If local passwords are disseminated to handle a period where domain controllers are unable to provide domain level user authentication, consider changing the local account passwords once domain authentication has been reestablished.
- Make sure to change all local account as shipped passwords as soon as feasible during the site commissioning process.

3.1.2 Access Control Mechanisms

Thin Client terminal local accounts are granted different levels of access to the Thin Client terminal. The privilege levels assigned control the level of access to Thin Client terminal subsystems, including the ability to view and change the Thin Client terminal configuration.

- The local administrator account provides administrative access to the Thin Client terminal, it can be used to change the configuration of the Thin Client terminal. Use of this password should be limited to those with the requirement to reconfigure or troubleshoot the Thin Client terminal.
- The local user account provides normal user level access to the Thin Client terminal. It should be used whenever a local account must be used and administrative access is not required.
- Domain level accounts are granted user level access to the Thin Client terminal.

3.2 Communication Requirements

3.2.1 Network Connectivity

Thin Client terminals have a single Ethernet connection to the Plant Data Highway (PDH) network. The PDH is used to establish a connection and open a session on a host computer.

- Thin Client terminals should never be connected to the UDH.
- Thin Client terminals should never bridge multiple networks - only one network should ever be connected.
- If there are multiple Thin Client terminals located together (such as in a central control room), each Thin Client terminal should be connected to a different network switch - typically one would be connected to each switch in a redundant switch pair.
- Consider pulling two Ethernet cables (one from each switch in a redundant pair) to the location of the Thin Client terminal. In case of network or switch failure, the cable on the Thin Client terminal could quickly be swapped (the existing connection unplugged and the other connection plugged in) to reestablish PDH connectivity. After the network issue is addressed, the connection should be reverted back so that the Thin Client terminals are once again connected to different switches.

Thin Client terminals are designed to be used to establish connections within the local control zone (specifically to hosts on the PDH).

- Do not configure the Thin Client terminals with a default gateway address or router address that would allow communications outside of the local network.
- If external routing is a site requirement, the use of routers and/or firewalls with appropriate rules to limit the addresses and protocols allowed to pass should be implemented.

Thin Client terminals are typically configured to use the DHCP protocol to reserve an IP Address. Since loss of DHCP servers can prevent the Thin Client terminal from obtaining an IP Address, or renewing it when the lease expired, the lease times configured into the DHCP servers is purposefully longer than typical industry standards. The long lease should not cause problems because the number of Thin Client terminals is typically an order of magnitude less than the pool of IP addresses, and Thin Client terminals do not tend to come and go from the site to drain the address pool.

- If the site has many Thin Client terminals joining and leaving the network (an unlikely event) then a reduction in the DHCP lease period may be called for. An option may be to script or manually clean out unused but not-yet-expired device leases if the IP address pool starts to grow low. This would be an unusual condition.
- If changes are made to the DHCP lease time, it may be worthwhile to take into account its relationship to the Windows Cached Credential expiration period (currently 31 days in Microsoft Windows operating systems).
- Static addresses that do not conflict with other site equipment should be available in case manual assignment of Thin Client terminal IP addresses is required during a long term failure of the DHCP servers. These addresses should be outside of the DHCP address pool space in order to prevent conflicts when the DHCP servers are put back into service.

3.2.1.1 Ports and Services List

Port	Protocol	Service	Description
631	TCP	CUPS	Common Unix Printing System server

3.3 Configuration Hardening

Most Thin Client terminals provide USB ports for both local usage (re-flash the local BIOS if needed - the "unbrick" procedure) and for mapping the USB drive through to a host to make it available within the current host session.

- Verify the source and integrity of media before placing it into site equipment.
  - Software distributions should be verified by whatever method the manufacturer supports, such as signed installation files or a separate web site that lists the hashes for the files on the distribution media.
  - Use of password protected media does not ensure that the media is free from malicious software, but it does help prevent the media from being infected while left unattended.
- Consider using hardware USB port locks to prevent access to USB ports, and/or pull the front or rear USB port connectors from the motherboard.
- Consider blocking the use of USB ports on all but one or two Thin Client terminals (often the ones associated with the Engineering Workstation(s)) to limit USB exposure, then use the internal network to transfer the information to computers that need it.
- Make sure the AutoRun option in the host operating system is disabled to help prevent software from being automatically run when the media is inserted or the session connection is established.
- Set secure passwords for each local user account in each Thin Client terminal and limit exposure to only those who require them as described in the section, *User Authentication and Authorization*.

Notes

Glossary of Terms

DHCP Dynamic Host configuration Protocol, a protocol that allows a device to request (lease) an IP address on the network from a DHCP server. The device will have exclusive use of that IP address until it releases the address or the least time expires.

Domain Controller A server that provides identity management functions. It holds a database of the users defined and the groups that those users are members of that are used to control user access to various resources.

Firewall A device that connects between multiple networks in order to limit the types of traffic that are allowed to flow between the networks.

MDH Management Data Highway, a network that contains devices that need to monitor but not control. Traffic from the Monitoring Zone (MDH) to the Control Zone (PDH and UDH) must go through a router with access lists that limit the allowed traffic.

PDH Plant Data Highway, a network that is used to transport non-critical information within the Control Zone. Traffic to the Control Zone (PDH and UDH) from outside the Control Zone must go through a router with access lists that limit the allowed traffic.

SIEM Security Information and Event Management, a server that collects event messages from various other subsystems to provide a central location for analyzing and viewing these events.

Router (Network) A networking device that is typically connected to multiple different networks with rules that define what message traffic is allowed to cross from one network to a different network.

Switch (Network) A networking device that connects multiple devices together to form an Ethernet Network.

UDH Unit Data Highway, a network that is used to transport critical control information within the Control Zone. Traffic to the Control Zone (PDH and UDH) from outside the Control Zone must go through a router with access lists that limit the allowed traffic.

VLAN Virtual Local Area Network (LAN), a mechanism for logically connecting multiple devices into one network within a switch or router. Networking equipment typically support multiple different VLANs within a single switch to provide isolation of network segments within a single switch. VLANs include the UDH, PDH, MDH, MGH, and DMZ

Notes