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.

Revised: Aug 2019
Issued: March 2017


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

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

<table>
<thead>
<tr>
<th>Revision</th>
<th>Location</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Throughout the document</td>
<td>All graphics have been replaced to reflect the controller Primary and Secondary domain and certificate authority replacement of WinServer 2012 R2 with WinServer 2016</td>
</tr>
</tbody>
</table>

Acronyms and Abbreviations

- CMS: Configuration Management System
- EGD: Ethernet Global Data
- EWS: Engineering Workstation
- HA: High Availability
- HMI: Human-machine Interface
- IIA: Industrial Internet Applications
- SSD: Solid State Drive
- VFA: Virtual Field Agent
- VM: Virtual Machine

Related Documents

<table>
<thead>
<tr>
<th>Filename</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>GEH-6839</td>
<td>Mark Vle Control Systems Secure Deployment Guide</td>
</tr>
<tr>
<td>GEH-6840</td>
<td>NetworkST 3.1/4.0 for Mark Vle Controls Application Guide</td>
</tr>
<tr>
<td>GEH-6841</td>
<td>Control Server – Thin Client Dell™ Wyse™ Enhanced SUSE® Linux™ Enterprise Thin Clients User Guide</td>
</tr>
<tr>
<td>GEH-6842</td>
<td>Control Server Dell Wyse Thin Client HMI System Support and Maintenance Guide</td>
</tr>
<tr>
<td>GEH-6843</td>
<td>Control Server Dell Wyse Thin Client HMI System Secure Deployment Guide</td>
</tr>
<tr>
<td>GEH-6845</td>
<td>Control Server — Domain Services Maintenance Guide</td>
</tr>
<tr>
<td>GEH-6846</td>
<td>Control Server Installation and Startup Guide</td>
</tr>
<tr>
<td>GEH-6847</td>
<td>Control Server Dell Wyse Windows® Embedded Standard 7 Thin Client HMI System Secure Deployment Guide</td>
</tr>
<tr>
<td>GEH-6848</td>
<td>Control Server Handover Guide</td>
</tr>
<tr>
<td>GEH-6849</td>
<td>Control Server Dell Windows Embedded Standard 7 Thin Client HMI System Support and Maintenance Guide</td>
</tr>
<tr>
<td>GEH-6850</td>
<td>Control Server Dell Wyse Windows Embedded Standard 7 Thin Client User Guide</td>
</tr>
<tr>
<td>GEH-6851</td>
<td>Control Server Core — High Availability (HA) Maintenance Guide</td>
</tr>
<tr>
<td>GEH-6852</td>
<td>Control Server Core — Simplex Maintenance Guide</td>
</tr>
<tr>
<td>GEH-6721 Vol I</td>
<td>Mark* Vle and VleS Controls Volume I: System Guide</td>
</tr>
</tbody>
</table>
1 Introduction

The Control Server, part of GE’s Industrial Internet Control System, is an integrated computing platform designed to optimize plant and asset performance, enhance control system security, and simplify the maintenance of traditional SCADA computers. Utilizing a centralized server-based architecture, the Control Server integrates multiple functions traditionally provided by discrete workstations into a server-based platform using virtualization technologies. Customers can design, deploy, and maintain their control system from one central location.

The Control Server’s modular design includes a Domain Services module, a Thin Client HMI module, and a Virtual Field Agent (VFA)* using GE’s Predix* engine.

The Domain Services module implements policies to harden the Control Server and Thin Clients to minimize the attack surface against cyber threats. The primary and secondary domain controller Virtual Machines (VMs) provide role-based access control to the Control Server platform, Thin Client terminals, and other thick client computers on the control network. The Certificate Authority VM provides security certificates for placing controllers into, and out of, Secure State.

The Thin Client HMI module provides virtualization of the traditional Human-machine Interface (HMI) computers. The module includes VM options for the following:

- Engineering Workstation (EWS)
- Operator Workstation (OP WKS)
- Communication Gateway (GTW)
- Historian
- Application Server (APP)
- Windows Server

The Engineering Workstation (EWS) VM contains the configuration tools and services for the Mark VIe control system. It also hosts the EGD Config server, the IIS web server, the Thin Client support files, and the licensing servers for the Microsoft and Proficy licensing.

The Operator Workstation (OP WKS) VM provides the traditional Operator interface through the Thin Client terminals for controlling the plant using CIMPLICITY* HMI, WorkstationST, viewing alarms, and trending.

The Communication Gateway (GTW) VM includes WorkstationST* features to allow communication to 3rd party devices through various protocols.

The Historian VM is a Proficy Historian that stores data and provides web based access to view and trend the historical data.
The Application Server (APP) VM includes the ToolboxST and WorkstationST applications and is used when a dedicated server for Configuration Management System (CMS), Alarm Server, or Device Management is required.

The Windows Server VM is a Windows Server 2012 R2 VM that can be used for other 3rd party software such as Triangle Microworks®, GE Power’s Performance Monitoring or Boiler Stress Monitoring.

The Virtual Field Agent (VFA) module is a Linux operating system VM used as a platform for applying Predix Applications. The VFA provides the infrastructure for developing, testing, debugging, and deploying Industrial Internet Applications (IIA). The IIAs leverage data from the control system as well as adjacent non-control data sources such as weather to create new customer facing applications such as life models, operations prediction, and asset level part-life/revenue optimizations.
The base system elements use commercial off the shelf (COTS) parts and are available in several configurations of Simplex (single server) and High Availability (redundant servers) for application-specific needs. The Simplex and High Availability (HA) Server hardware is scalable from very low capacity to high capacity. Each capacity level increases the number of CPU cores, RAM, and disk storage. The Control Server platform offers easy expansion by adding client terminals or server hardware as needed. Server-based architecture and the small footprint of the client hardware allows for easy installation and maintenance. The platform hardware uses rack-mounted servers with high performance solid state drives (SSD). The Control Server can be supplied in a rack-based cabinet with redundant power feeds and roof-mounted cooling fans with ample space for network switches, patch panels, and other equipment.

Example High Availability Hardware System:
Each server has multiple Ethernet connections to support redundant connections to multiple networks.

The Host servers have dual redundant power supplies. The servers can operate with both power supplies simultaneously as well as with one power supply being disconnected. This configuration provides power redundancy to the server.

**Note** High Availability VMs hosted in the cluster are monitored, and in the event of a failure, the VMs on a failed host are restarted on the alternate host. The VM configuration shown in this document is representative of the initial configuration that may change over time.
3 Architecture and Platform Hosting

The Control Server platform provides hosting capabilities for a variety of applications on various operating systems. This is accomplished through virtualization technology that distributes computing and storage resources from one or more hosts to VMs that are running on the host(s). In this environment, a host is defined as a physical server or computer that is sharing at least some of its resources with a VM. In modern virtual technology, this is achieved using a software layer called a **hypervisor**. The hypervisor is the base level software that connects the host’s physical resources, such as processing power, memory, or disk storage space, to the VMs per the VM’s need and configuration.

### 3.1 Legacy HMI Architecture

The following figure displays a traditional control system architecture that uses standalone HMI desktop computers (thick clients) to provide the physical interface to the system. Control system software processes are distributed across the HMIs on the network.

**Traditional Thick Client Control System Architecture**

Legacy systems used a quantity of discrete workstations to host the same HMI functions throughout the geographical locations of a system. The impact of this is that each HMI workstation must be purchased, built, and maintained individually.

With the Control Server platform, all the software for the equivalent of these multiple discrete workstations is loaded on the two redundant servers and can be administered and maintained on the servers without the need to go to each geographical location of operator displays.

The Control Server can be added to an existing traditional system and existing computers can be added to the Control Server domain to provide additional security.
3.2 Virtual HMI Architecture

A Virtual Machine (or virtualized computer) is a copy of a normal standalone computer running within a server environment. From an operator point of view, there is no difference between a normal standalone computer and a virtualized one in presentation and any other user processes. For example, the operation of any software within the VM and the use of peripherals (mouse, keyboard, and monitor) is the same as in a standalone computer.

From a hardware point of view, a VM is completely different from a standalone computer. A VM’s processing power does not need to reside next to the operator or have direct peripheral connectivity to the server itself. Instead, access to the VM can be achieved by remotely connecting to the VM and exporting its user interface to the operator. This connection can be simply achieved by means of a Thin Client computer, or another standalone computer, over the local network.

**Simplex Control Server**

**High Availability One-to-One Control Server**
(one Thin Client connected to one VM)
High Availability Many-to-One Control Server
(many Thin Clients connected to one VM)

Simplex

The Control Server is available in a single server configuration called Simplex. In all Simplex configurations, the disk drives are configured in RAID for data redundancy, and the network interfaces (NICs) are redundant for up to three networks. On the higher-end servers, there are also dual power supplies. The physical server that participates in the main Control Server infrastructure is denoted Host Server 1 (HS1). This server uses VMware’s vSphere ESXi operating system as the hypervisor layer.

High Availability

The Control Server is also available in a configuration called High Availability (HA). In an HA configuration, the two main hosts (HS1 and HS2) are formed into a cluster (refer to the description of Virtual SAN in the following section). When formed into a cluster, the hosts work together to improve the availability of the VMs that are running on them.

The cluster has a Witness server that continually communicates with the two host servers. If communication is lost to one server, the remaining server becomes the master. With the loss of communication to the Witness, the first server goes into a read-only state, but continues operating. When communication is re-established, the first server synchronizes with the second server since the second server was the master during the communication loss.

The HA function works on multiple levels. VMs can be migrated between hosts with no impact on the clients. If a host fails (HS1 or HS2), the VMs that are running on that host are automatically restarted on the running host and the clients can reconnect.

Several things should be noted and are defined as follows:

1. Physical servers that participate in the main Control Server infrastructure are denoted Host Server 1 (HS1) and Host Server 2 (HS2). These servers use VMware’s ESXi as their hypervisor layer.

2. The physical servers that make up the Control Server platform are managed through vCenter appliance (HC1). vCenter is a VM that operates on one of the Control Server hosts and manages rules, assesses health, and provides a central console for all hosts and VMs that make up the Control Server.

3. HS1 and HS2 participate in a physical storage sharing and protection scheme called Virtual Storage Array Network (SAN). Virtual SAN is a method native to VMware vSphere that pools storage resources from multiple hosts into a single storage array that is shared by participating hosts and protected from a single host or disk failure.

4. MC2 is an ESXi host that does not participate in the Virtual SAN and hosts a Witness virtual machine (HW1) that assesses the health of the Virtual SAN and reports this health to vCenter.
Virtual SAN

The Virtual SAN is VMware’s way of providing shared storage. Virtual SAN is unique in that it uses the on-board storage from the hosts in a software RAID cluster rather than a separate, external, network storage device. It integrates the storage available in each host to create a cluster-wide storage that maintains multiple copies of each VMs data. If a disk or host fails, no data is lost and the systems continues to operate, possibly with a reduction in performance. Once the failed hardware is replaced, the system can rebuild the disk storage with minimal downtime and no data loss. The Virtual SAN uses a dedicated high-speed network between the two servers (HS1 and HS2) to maintain data synchronization.

3.2.1 Thin Client Visualization

The HMI Client shown in the previous diagrams is a remote connected unit allowing access to a VM computer. It is called a Thin Client because it does not provide any of the processor functions in a normal computer, but instead acts as an interface (keyboard/mouse/monitor) to the multi-media, peripherals, networking, and communication ports of the machine to which it is connected. The user must connect to a VM, log in, and run the desired application. For information on how to configure and download the Thin Client, refer to the Control Server Dell Wyse Thin Client HMI System Support and Maintenance Guide (GEH-6842).

Thick Client and Thin Client systems are functionally the same. However, the virtualized architecture of the Control Server with Thin Clients provides many benefits, including:

- An improved mechanism is provided for managing and updating the HMIs.
- Critical processes run only on the server.
- The Server can be in an environmentally safe and physically secure environment with controlled access.
- Only inexpensive and easy-to-replace Thin Client terminals are located in the potentially harmful plant environment and are accessible by users.
- Thin Clients are centrally managed from the server, which makes commissioning new Thin Clients and replacing damaged ones a plug-and-play operation at the physical Thin Client location.
- HMI functionality and the user experience continue to be completely controlled by the HMI configuration. The Thin Client configuration only determines what HMI VMs the Thin Client is allowed to communicate with on the network.
3.2.2 Control Server System Architecture
4 Control Server Modules

4.1 Domain Services

In addition to the VMware vSphere infrastructure and physical hardware, the Control Server contains an optional Domain Services layer. The VMs supporting Domain Services are illustrated in the following figure.

Domain Services consists of three VMs: DC1, DC2, and CA1. Their functions are described as follows:

1. Centralized User Account and Group Security Policy Management through Windows Active Directory (DC1 and DC2)
2. Domain-Host Connection Protocol (DHCP) servers for connection management (DC1 and DC2)
3. Domain Name System (DNS) servers for name resolution (DC1 and DC2)
4. Certificate authority for managing secure connections (CA1)

The Control Server infrastructure and security layers contain various default and reference user names and passwords for Control Server administration and to support hosted applications such as Thin Client. These are managed in a separately controlled document that is shared at the time of handover.
4.2 Thin Client HMI

The HMI VM is a virtual machine that is hosted on and managed by the Control Server platform. The operating system running on the HMI VM is Windows Server 2012 R2 and fulfills Engineering Workstation (EWS), Operator Workstation (OP WKS), Communication Gateway (GTW), Historian, Application Server (APP), or some combination of these functions. All control system configuration and user interface infrastructure is built on the HMI VM.

There are many ways to access the HMI VMs. The primary method in the Thin Client architecture is through a Thin Client device. A Thin Client is a small form-factor, limited purpose computer that brokers remote sessions into the HMI VMs and provides a physical interface connecting the user to the HMI VM. This simplifies management of the access model for the system and ensures that users can only access the computers and roles granted to them from the system administrators.

The client accesses the HMI VMs through connections. Connections are configured centrally through initialization (INI) files. Refer to the Thin Client Maintenance Guide for more information on how to configure the Thin Client initialization.

Depending on the Thin Client and the architecture chosen, the client accesses the HMI VM through either Remote Desktop Protocol (RDP) or PC-over-IP (PCoIP). Refer to the Thin Client User Guide for more information on how to launch a connection to an HMI VM.

There are a couple of other ways to access an HMI VM if a client is not available. You can use a laptop with VMware View Client for Windows or the Remote Desktop Connection feature built into Windows. The vSphere Web Client also has a console feature built into it that you can use to access a HMI VM. Log into vCenter appliance using its web client, locate the VM, and select Launch Remote Console.

HMI Functions

One of the primary functions of the HMI VM is to provide an interface between the user, the controls, and ultimately, the physical machine. Other available HMI functions include:

- Operator screens
- ToolboxST* troubleshooting and control system configuration (including controls software changes)
- Setting up and viewing live and historical trends
- Viewing and analyzing historical data (through recorder or historian)
- Alarm Viewer
4.3 Virtual Field Agent (VFA) for Predix Applications

Customers can use the GE Predix software running on the VFA VM to deploy asset monitoring and optimizing Apps from GE or develop their own.
Notes
Glossary of Terms

Certificate Authority (CA) A trusted entity that issues digital certificates that certify the ownership of a public key by the subject of the certificate.

Domain Controller (DC) A server that responds to security authentication requests (logging in, checking permissions, and so forth) within a Windows® domain.

Dynamic Host Configuration Protocol (DHCP) Dynamic Host Configuration Protocol is a protocol used to automatically assign and manage dynamic IP addresses to devices on a network.

ESXi An enterprise-class, type-1 hypervisor developed by VMware for deploying and serving virtual computers.

Hypertext Transfer Protocol Secure (HTTPS) A protocol for secure communication over a computer network.

High Availability (HA) VMware HA provides high availability for virtual machines by pooling them and the hosts they reside on into a cluster (HS1 and HS2). Hosts in the cluster are monitored and in the event of a failure, the virtual machines on the failed host are restarted on the alternate host.

Hypervisor A piece of computer software, firmware or hardware that creates and runs virtual machines.

Hypervisor Platform A physical server that can support the work of several virtual machines. Each of these virtual machines can potentially have a different operating system and/or purpose.

Initialization (INI) Files The initialization files that hold the Thin Client specific settings that are downloaded to the Thin Client when it boots.

PC-over-IP Protocol (PCoIP) A remote display protocol for delivering remote desktops and applications. For example, this protocol is used by VMware view client.

Plant Data Highway (PDH) The plant level supervisory network that connects the HMI server with remote viewers, printers, historians, and external interfaces. Usually there is no direct connection to the Mark VIe controllers, which communicate over the UDH. Use of Ethernet with the TCP/IP protocol over PDH provides an open system for third-party interfaces.

Remote Desktop Protocol (RDP) A proprietary protocol that provides a user with a graphical interface to connect to another computer over a network connection.

Remote Desktop Services (RDS) Allows a user to operate a virtual machine over a network connection.

Host Server HS1 One of the servers in the cluster used to run VMs. With the High Availability option VMs are able to migrate across servers in the cluster.

Host Server HS2 One of the servers in the cluster used to run VMs. With the High Availability option VMs are able to migrate across servers in the cluster.

Server MC2 A special server (outside the cluster) that is used to host the Witness Appliance (HW1) for the servers that are in the cluster, as well as a special VM used to manage the cluster (MC3).

Stretched Cluster A model of a VMware HA cluster implemented to gain the same benefits that high availability clusters provide to a local site in a model with two data centers (potentially in different locations).

Terminal Services (TS) was renamed Remote Desktop Services in Windows Server 2008 R2. (Refer to the definition for Remote Desktop Services.)

Unit Data Highway (UDH) The network that carries controller to controller data, or controller to HMI data. The UDH is an Ethernet-based network, which provides direct or broadcast peer-to-peer communication between controllers, as well as between controllers and one or more operator or maintenance interfaces.
**Virtual Machine (VM)** An emulation of a particular computer system. Virtual machines operate based on the computer architecture and functions of a real or hypothetical computer, and their implementations may involve specialized hardware, software, or a combination of both.

**Virtual Machine CA1** The CA1 VM serves as the Certificate Authority for the domain. This VM issues certificates to devices (such as the Mark VIe controller) and users to verify identity.

**Virtual Machine DC1** The Domain Controller DC1 serves as the management point for users and computers in the domain. It provides a role-based access control system to manage access to resources and applications, based on the identity and privileges assigned to the user by the administrator.

**Virtual Machine DC2** The Domain Controllers DC2 is the Backup Domain Controller, which supports the domain if the Primary Domain Controller DC1 is unavailable.

**Virtual Storage Array Network (SAN)** Virtual SAN is a distributed layer of software that runs natively as a part of the ESXi hypervisor. Virtual SAN aggregates local or direct-attached capacity devices of a host cluster and creates a single storage pool shared across all hosts in the Virtual SAN cluster.

**Witness Server** The witness is a third instance of a server that acts as an intermediary between the hosts in the cluster (HS1, HS2) to determine when to failover.