Honeywell

SmartVFD Security Guide

OPERATING GUIDE

INTRODUCTION AND INTENDED AUDIENCE

This manual contains security-related information to guide the contractor install, operate, and securely maintain it.

SYSTEM OVERVIEW

The following is a system diagram of the SmartVFD in an example installation.

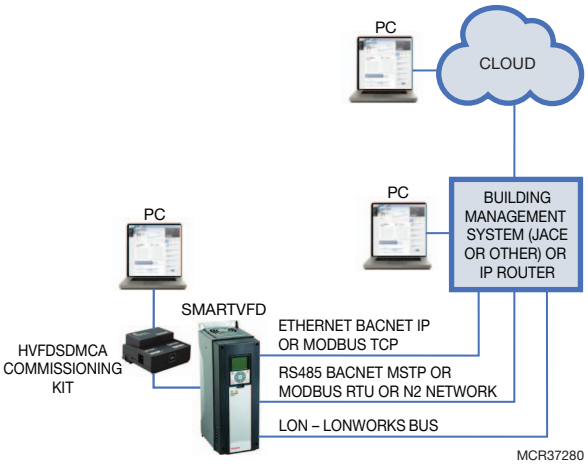

Fig. 1.

Some key elements of the diagram are:

Lonworks network: Lonworks (LON) network provides access to the Honeywell SmartVFD controller so it can communicate and share information.

BACnet network: The BACnet MS/TP or BACnet IP network provides access to the Honeywell SmartVFD controller.

Modbus RTU or N2 network: Modbus RTU or N2 bus networks provide access to the Honeywell SmartVFD controller so it can communicate and share information.

HVFDCDMCA Commissioning Kit: Required for direct access commissioning of the SmartVFD. Connects to PC via USB and connects to SmartVFD via RJ45 using a communication bus.

Drive Care Tool: PC software designed to allow user access to all of the VFD parameters. It is used in conjuction with the HVFDCDMCA Commissioning Kit hardware to connect a PC to the SmartVFD.

Building Management System: The Building Management System is not specifically defined, but can be any management system that accepts one of the communication types already described and used by the SmartVFD.

The SmartVFD has multiple communication protocol options. Typically only one communication protocol is chosen to interface with the SmartVFD in any given installation.

SYSTEM DESIGN AND PLANNING

This section contains information on activities that need to happen when the system is being planned by the contractor.

Physical Security of Components

It is important to have a plan for physical security of system components. It is recommended that the contractor identify the security needs of the building owner and provide guidance for implementation in addition to the requirements of the building owner.

It is recommended that the organization responsible for providing security for network assets be involved in the planning. The Building owner/Customer's IT groups needs to approve and connect the SmartVFD to the system so that the IT system will work with the SMARTVFD.

Physical security controls, such as a locked cabinet or equipment room that restricts physical access to the SMARTVFD are necessary to prevent system tampering, power interruption, and other security issues.

Ensure that SMARTVFD components requiring high reliability are protected with secure power sources and emergency power systems. Honeywell recommends

31-00140-01

strongly that you consider reliable power for the SmartVFD control system. System reliability is an important security issue and following these requirements and recommendations allows continuous monitoring and ensures HVAC control system reliability.

IT Network

Typically a static IP address is used for accessing the BACnet/IP to MS/TP router. Refer to your user manual to access the configuration menu in the MS/TP router.

See additional notes in “APPENDIX 1 - IT NETWORK NOTES” on page 3.

See additional notes in “APPENDIX 4 - SMARTVFD PC SECURITY INFORMATION” on page 4 for Installation Security Issues.

Lon/ BACnet/Modbus/N2 Communications Bus

It is required that physical security access to SMARTVFD communications bus wiring be accomplished by:

1. Installing wiring in physically inaccessible locations that restricts physical access to the Lon or BACnet communications bus.

Or

2. Installing wire in conduit.

This required physical security access protection is important to prevent security threats to the control system. Failure to protect the Communication bus can lead to critical security issues. For example, data loss or corruption could result due to not following the required protection for the Lon or BACnet communication bus.

See “APPENDIX 2 - INSTALLATION BEST PRACTICES” on page 3.

Secure and Unique Passwords

User-level parameter access to the SmartVFD via the keypad can be restricted to monitoring only through the use of an access code settable on the keypad, parameter P8.1 and P8.2.

Access to the SmartVFD directly by PC via the Drive Care Tool software (and the HVFDCDMCA hardware kit) requires no password.

Any PC application accessing the SmartVFD via the BMS or router should be protected with a robust password.

See “APPENDIX 3 - SECURITY MAINTENANCE TASKS” on page 3.

PCs used to access the SmartVFD

Each PC used for accessing the SmartVFD either via the HVFDCDMCA kit and Drive Care Tool or remotely via a communication bus or ethernet must be protected as a secure platform. Maintaining a secure client platform will involve OS updates, anti-virus software, and protection of local ports from attacks including spam, phishing, and physical compromise.

See “APPENDIX 4 - SMARTVFD PC SECURITY INFORMATION” on page 4 for Installation security issues.

See “APPENDIX 5 - FIREWALL AND NETWORK INTRUSION ISSUES” on page 6 for PC security information.

See “APPENDIX 6 - HARDENING AND COMPUTER ISSUES” on page 7.

MAINTENANCE

This sections contains information for maintaining the SMARTVFD system.

Make sure SmartVFD clients (PCs) are running up to date virus software and comply with Corporate PC security standards.

The Gateway is associated with the building during commissioning and should be inspected periodically for connection. If there is no connection, the connection issues should be resolved in a timely manner.

DECOMMISSIONING

This section contains information for maintaining the SmartVFD system.

There is no specific process for decommissioning the SmartVFD. Simply shutting it off or physically removing the wiring to the device will remove the SmartVFD from the system.

SMARTVFD INSTALLATION SECURITY CHECKLIST

Job Name:

Job Location:

Contractor:

Date:

IT Representative:

Date:

Complete the following security tasks for your installation.

- Design a secure installation considering both software and hardware vulnerabilities.
- Develop a Disaster and Recovery Plan.
- Develop a Backup and Recovery Strategy.
- Install, configure, and keep antivirus software updated on SmartVFD Clients (PCs).
- Securely configure networks and firewalls.
- Set up network intrusion detection.
- Harden the network system to further safeguard against unauthorized access.
- Deliver all required system information upon delivery to the system owner.
- Train end-users on security maintenance tasks at system delivery.
- Assess security risks.

APPENDIX 1 – IT NETWORK NOTES

This section contains information for maintaining the SMARTVFD system.

Businesses with critical Point of Sale infrastructure (POS) or other important assets must use internal network segmentation. Proper network segmentation can be accomplished in a small business with the use of a security gateway or firewall.

Industrial Society of Automation / Industrial Electrotechnical Commission ISA/IEC 62443 Network and system security for industrial-process measurement and control is a recommended security standard that prescribes a clear definition of zones and network segmentation. IEC 62443-Segmentation allows the best control over access and security within an automation network.

An excellent reference for control security topics is NIST Special Publication 800-82 Revision 2: Guide to Industrial Control Systems (ICS) Security available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

APPENDIX 2 – INSTALLATION BEST PRACTICES

This section contains additional Installation best practices for SmartVFD.

SMARTVFD Communication Bus (Lon, BACnet MS/TP, etc):

Security of the bus also means that the bus is electrically reliable for communications. It is important the bus is installed with one wire type consistent throughout the whole gateway to controller connection as to eliminate reflections from bus wire impedance mismatches.

Shielded wire is not recommended for normal installations. See installation instructions for details.

APPENDIX 3 – SECURITY MAINTENANCE TASKS

This section contains additional information on security maintenance tasks for SmartVFD.

It is important to train end-users on documented security maintenance tasks.

Disaster Recovery Planning

Creating, implementing, and maintaining a disaster recovery plan is import for the contractor and customer as the system can be restored in the event of a security breach or equipment failure. As a contractor, you may assist in helping the customer develop a plan or provide services to help implement and maintain the plan. The plan needs to ensure clearly documented procedures, document the person or organization responsible, and provide review of the plan during planned maintenance intervals.

Backup and recovery strategies

Performing backups of operating data is a risk mitigation task to secure your SmartVFD system.

Important configuration information may be lost if there are failures due to a natural disaster, hardware or software failure, or computer virus.

Backup strategies should take into account hard drive failures, user errors, and permanent loss of computer connection, virus infection or other problems.

Do not store backup images on the same computer being backed up. If network drives are not available, store backup images to a connected drive using USB.

Configure your backup software to do full backup's weekly and incremental backups nightly to lower the load and performance impact of backup activities. Ensure that the data was backup up correctly after the backup is complete.

APPENDIX 4 – SMARTVFD PC SECURITY INFORMATION

This section contains additional information on Installation security Issues for SmartVFD.

Software and operating system security

This section includes information to installing and configuring non-SmartVFD software and the operating system.

Virus protection

Although some modern threats can bypass even the best antivirus checks, antivirus software is still an essential element of a comprehensive security strategy.

Installing antivirus software

Install antivirus software on every computer in the network, including the SmartVFD commissioning software, SmartVFD, and computers used for web browser access. After installing antivirus software, check the Windows Event Logs and ensure no errors are reported. If the system starts experiencing failures, the inability to read or write files, the logs show deadlock errors, or the system shows any other unusual behavior, disable the antivirus software to see if the failures continue. Note that some antivirus software may need to be completely uninstalled in order to be disabled.

Ensure frequent updates to antivirus signature files

It is important to update antivirus signature files frequently by subscribing to the updates of your antivirus software vendor(s) and leveraging enterprise antivirus policies and practices when available. Since new viruses are released every day, the system will remain vulnerable to attack if the signature files are not updated at the same rate. Where it is not practical to perform updates daily, monitor reputable web sites that publish information about new virus attacks so that the system can be isolated if a specific threat appears.

Receipt of new signature files generally requires Internet access so that the files can be downloaded from the antivirus software vendor. If possible, set up servers for the controlled distribution of antivirus signature files.

Configuring active antivirus scanning

Adopting an active virus scanning strategy as on-access scanning provides the best real-time protection for your system. Configure the virus scanner to run on-demand scans during regular, scheduled maintenance to catch any malicious files or programs which may be dormant on the computer.

Configure both on-access and on-demand scanning to:
- Scan the boot sectors of all disks.
- Move infected files to a quarantine directory and notify the user that an infected file was found.

Allow the user to clean up the infection.

Regularly review virus scan reports as part of the active scanning strategy.

Tuning antivirus scanning for system performance

When formulating your virus scanning strategy you must take into account the potential impact on critical system resources. For example, if the SmartVFD commissioning software is experiencing problems due to low system resources, you may need to:
- Ensure that antivirus software only runs when system resources on the computer are adequate to meet system needs.
- Limit system resources that are used by antivirus software during scanning.

To find the proper balance between browser workstation performance and virus protection you need to make configuration choices such as disabling scanning on reading of files and changing the default process-based scanning to per-process scanning.

Do not automatically schedule full system scans, as this can result in severe degradation of performance, which could impact the ability of operators to respond to an incident.

Service packs and security updates

An important part of the overall security strategy is to ensure that the operating system is kept up-to date with the latest patches and updates. Before turning the system over to the customer, ensure that you have:
- Installed the latest supported web browser version.
- Updated Windows to the latest service pack supported by SmartVFD (this information is available on the SmartVFD web site or by contacting Technical Support).
- Configured Windows Update to automatically check for updates.

For the SmartVFD primary workstation, discuss with the customer about how to automatically or manually apply updates. The customer may opt to install them manually in order to control when the SmartVFD primary workstation gets rebooted. For client workstation computers, updates should be installed automatically.

User accounts

Securing access to the operating system

The SmartVFD Drive Care Tool does not use Windows user accounts for application security; Windows user accounts are used to secure access to the operating system and still provide a very valuable layer of protection. Ensure that only authorized users have access to computers.

Windows user accounts and passwords

Access is gained to the Windows operating system by logging onto the computer using a user account name and password. This is true for both local and remote terminal services access. Because user accounts may be well known or easily guessed within an organization, the password becomes the prime vehicle for authentication. User account and password policies are therefore important security measures.

User and password policies and settings

Since users are not authenticated using Windows, configure any PC application with access to the SmartVFD so that each user has a unique login name and password. Ensure that when an employee, or any other user with permanent or temporary access, leaves the organization or no longer needs access, their user accounts are disabled. For example, when a subcontractor is on the job working on the SmartVFD HVAC system, they are given access to the system. Monitor their access while the work is in progress and then disable their credentials once the work is complete. In addition, because SmartVFD software is available using a browser, ensure that the SmartVFD user account is also disabled.

Follow Windows user and password policies to secure access to the operating system that has application access to the SmartVFD. As a general rule:

- Review user accounts on a regular basis.
- Disable or delete all unused accounts.
- Disable all anonymous accounts
- Disable all guest accounts.

Configure password policies so that Windows account passwords are difficult to guess and they are changed often. The following settings are suggested:

- Maximum password age set to 45 to 90 days - this forces the choice of a new password after this time. Configure the setting for the Administrator account shorter than a normal system user. A maximum of 30 days is recommended.
- Minimum password age set to 1 to 5 days- this prevents cycling passwords too rapidly.
- Minimum password length set to 11 characters - This improves encryption and makes guessing harder. Using several words to form a phrase can make a stronger password that is also easier for the user to remember. For example, "My dog Fido has 50 fleas!" is a much stronger password, and much easier to remember, than "X$9d8oc-@Ek".
- Enforce password history set to 24 passwords remembered - This prevents reuse of the same password too quickly.
- Password must meet complexity requirements set to enabled improves encryption and makes guessing harder. Suggest requiring at least three of the following: Uppercase Character, Lowercase Character, Number, and Special Character.
- Store passwords using reversible encryption set to disabled - this prevents passwords from being stored in (the equivalent of) clear-text.
- Account lockout threshold set to 5 invalid logon attempts - this prevents continual password guessing by disabling an account after the specified number of attempts. Consider disabling account lockout for operator (or other user) accounts where denial of service or loss of view would be detrimental to safety or the continued operation of the facility.
- Account lockout duration set to 30 minutes - this specifies the period of time during which a user will not be able to log on following an account lockout. (Note that the administrator can re-enable the account before the expiration of the specified lockout period.)
- Reset account lockout counter after 29 minutes --- this sets the time before the account lockout is reset to zero. For example, with the account lockout set at 10, and the lockout counter set at 29 minutes, lockout will occur if there are 10 invalid logon attempts within 29 minutes. Note that the lockout counter must be less than the lockout duration.

Service and primary workstation accounts

Run Windows services and PC browser required by SmartVFD commissioning software under an account with the lowest possible set of privileges. The following classes of accounts are suggested in order of preference:

- Local service accounts.
- Local accounts with minimum rights.
- Domain accounts with minimum rights.
- The Network Service account.
- Local or domain user accounts belonging to the Local Administrators group.
- The local system account.

Monitoring and logging

System monitoring

Diligent system monitoring will help guard your system against unauthorized access. However, there is always the possibility that an attacker will succeed in circumventing all the safeguards and compromise the system. If this happens, it is important to discover the breach and prevent further damage as rapidly as possible. The earlier a system breach is detected and the more evidence that is captured, then the less damage is likely to occur and the greater the chances of identifying the intruder.

Setting up and analyzing Windows audit logs

Enable the auditing of your file system and registry access. If you suspect that the system is being misused, then Windows auditing provides a useful tool to track who did what and when.

Once Windows auditing is enabled, review the Windows audit logs frequently and take action if unexpected activity is seen.

Restricting access to event logs

By default, anonymous accounts and guest accounts can view Windows Event Logs when logged in to a Windows computer. Restrict this access on the Compass primary workstation, because the System, Application, and Security logs may contain sensitive information about the system and its operations.

IMPORTANT

Back up your system and then back up the registry hive before making any modifications in the Windows registry. If a mistake occurs, you can then recover by reverting back to the backup of the hive-or worse case, revert back to the system backup-to recover and minimize downtime.

⚠ CAUTION

Mistakes made while editing the Windows registry can cause serious issues with your computer. Follow these steps precisely. If you make a mistake you cannot fix, restore your backup and start over.

Question: How do I restrict access to Administrators and system account only?

Answer: To restrict access to administrators and system accounts only.

- Choose Start > Run to open the Run window.
- Type regedit and then click OK.
- Expand the HKEY_LOCAL_MACHINE tree until you open the HKEY_LOCAL_MACHINE\SYSTEM\-CurrentControlSet\Services\EventLog registry key.
- Select the Security sub key.
- Right-click in the right window and then choose New > DWORD Value to create a new registry value.
- Name the new value RestrictGuestAccess.
- Right-click RestrictGuestAccess and then select Modify.
- Type 1 in the RestrictGuestAccess value data field and then click OK.
- Repeat steps 5 through 8 for the Application and System subkeys.
- Close the Registry editor.

APPENDIX 5 – FIREWALL AND NETWORK INTRUSION ISSUES

This section contains additional information on Installation security Issues for SmartVFD.

Configuring the Windows firewall on Windows PCs running the web Browser

The Windows firewall provides another layer of protection and must always be enabled. When the firewall is on, it will reject any incoming connections by default. Exceptions must be put into the firewall to allow incoming connections to succeed. If not manually configured, on first usage the Windows firewall will prompt the user to add a firewall exception. Use the following configuration settings:

- The firewall is on.
- The firewall is on for all network locations (Home or work, Public, or Domain).
- The firewall is on for all network connections.
- The firewall is blocking all inbound connections except those that you specifically allowed.

Detecting network

Network Intrusion Detection Systems (NIDS) can take many forms. NIDS can be a dedicated server on the same network branch, freeware software available under GNU or similar licenses (most of these are aimed at UNIX systems), or commercial products aimed specifically at Windows systems.

The purpose of NIDS is to scan incoming network packets and look for unusual traffic or for specific malformed packets known to be associated with attacks. If anomalies are found, NIDS take action such as raising alerts or even disconnecting the computer from the network. The latter is a dangerous option which causes its own denial of service while preventing damage to the system by closing network ports, and so on.

Most firewalls, switches, and routers have reporting capabilities that can report various levels of events varying from debugging to emergency failure. These reports can be viewed using telnet, collected by a central logging server, or emailed to an administrator. For example, the Cisco PIX firewall and Catalyst 4500 switches can be configured to send selected levels of events to a central syslog server where further analysis can occur and significant events can be detected.

Syslog servers are common on Unix systems, and third-party syslog services are available for Windows. They vary in functionality and cost, from freeware, which simply writes to a log file, to sophisticated NIDS that analyze the logs in detail. As well as being able to control the level of severity of events, the PIX firewall allows the suppression of individual messages. This can significantly reduce clutter and also provide some ability to recognize common attack signatures and then raise the appropriate alarms.

When you configure network event logs, maintain a balance between collecting too many events (and missing something important) and filling storage disks and deleting information (which is subsequently needed for an intrusion investigation).

Other forms of intrusion detection will search event logs looking for unusual events, or will compare the current file system to a known good image. Be careful when running such tools to prevent them from using too many resources and interfering with the control system.

Wireless access points

It is generally not advised to allow wireless access to the BAS network.

If a wireless network is part of the existing automation system, follow these guidelines when setting up and configuring a wireless network:

- Do not use the default Service Set Identifier (SSID); configure a unique SSID.
- Disable SSID broadcast.
- Use Wi-Fi Protected Access II (WPA2-Personal) or (WPA2-Enterprise) encryption. Wired Equivalent Privacy (WEP) is not sufficiently secure.
- Use the correct class of network equipment. For example, do not use home or small office equipment for large enterprise jobs.
- Change the default administrator password.
- Ensure access points are running the latest firmware.
- Physically secure access point devices.
- Use a separate access point for public, non-secured access, such as WiFi for guests or customers.
- When feasible, enable media address control (MAC) filtering and enter the MAC addresses for all the wireless devices.

APPENDIX 6 - HARDENING AND COMPUTER ISSUES

This section contains additional information on Hardening and Physical Computer Issues.

Hardening

Hardening involves taking additional actions to make it more difficult to obtain unauthorized access or to circumvent security mechanisms.

Physical computer

Implement additional steps to harden computers against unauthorized access:

- If computers with DVD drives are readily accessible, fit locks or remove the DVD drives. Disable unused USB ports to prevent USB drives or other uncontrolled devices from being connected to the system. Such devices may be used to introduce a virus or other malware. Also disable or physically protect the power button to prevent unauthorized use.
- Set the BIOS to boot only from the operating system's root partition/drive.
- Set a BIOS password (ensure that this does not prevent automatic startup).
- Remove the floppy and CD/DVD drives from the computer.
- Disable USB ports and other ports capable of being used for memory sticks and other portable storage devices.
- Prevent drives, like the DVD drive, from being visible to Microsoft Windows Explorer by using the group policy.
- See Using Group Policy Objects to hide specified drives at http://support.microsoft.com/kb/231289 for more information.
- Note, however, that hiding the drives in Windows Explorer does not prevent those drives from being accessed using a command prompt.

Operating system

Many additional configuration options can be applied to harden the operating system against threats.

Securing the desktop

The following recommendations apply to desktop policy settings:

- Configure Windows to display a warning against unauthorized use of the computer.
- You can configure computers to display a message when someone logs on. A typical message would be "It is an offense to continue without proper authorization."

Historically, legal prosecutions of intruders have failed because no such warning was displayed. The banner can be defined using Group Policy or the local registry.

- Use Group Policy (if the computer is part of a Windows domain) or the local registry to: Hide the last user name on the logon window. By default, the Logon dialog box displays the name of the last user to log on. This saves time if the same user is logging on again but is a security risk.

Home and Building Technologies

In the U.S.:

Honeywell

715 Peachtree Street NE

Atlanta, GA 30308

customer.honeywell.com

Honeywell

31-00140—01 M.S. 01-18
Printed in United States