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.

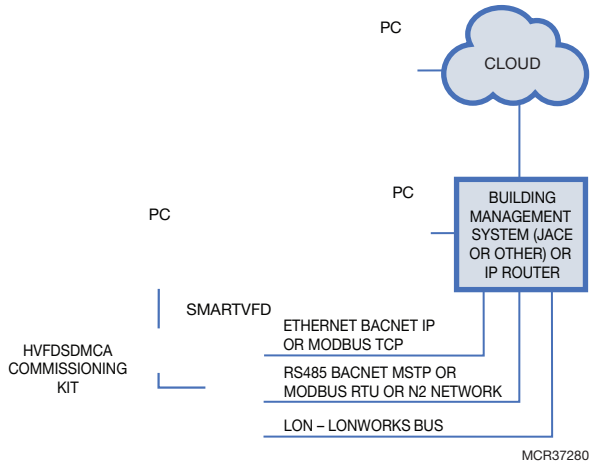

Fig. 1.

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