



Product Manual 35124
(Revision -, 10/2018)
Original Instructions

Digital Valve Positioner (DVP) Cyber Security Manual

Cyber Security Manual



General Precautions

Read this entire manual and all other publications pertaining to the work to be performed before installing, operating, or servicing this equipment.

Practice all plant and safety instructions and precautions.

Failure to follow instructions can cause personal injury and/or property damage.



Revisions

This publication may have been revised or updated since this copy was produced. To verify that you have the latest revision, check manual **26455**, *Customer Publication Cross Reference and Revision Status & Distribution Restrictions*, on the *publications* page of the Woodward website:

www.woodward.com/publications

The latest version of most publications is available on the *publications* page. If your publication is not there, please contact your customer service representative to get the latest copy.




Proper Use

Any unauthorized modifications to or use of this equipment outside its specified mechanical, electrical, or other operating limits may cause personal injury and/or property damage, including damage to the equipment. Any such unauthorized modifications: (i) constitute "misuse" and/or "negligence" within the meaning of the product warranty thereby excluding warranty coverage for any resulting damage, and (ii) invalidate product certifications or listings.



Translated Publications

If the cover of this publication states "Translation of the Original Instructions" please note:

The original source of this publication may have been updated since this translation was made. Be sure to check manual **26455**, *Customer Publication Cross Reference and Revision Status & Distribution Restrictions*, to verify whether this translation is up to date. Out-of-date translations are marked with . Always compare with the original for technical specifications and for proper and safe installation and operation procedures.

Revisions— A bold, black line alongside the text identifies changes in this publication since the last revision.

Woodward reserves the right to update any portion of this publication at any time. Information provided by Woodward is believed to be correct and reliable. However, no responsibility is assumed by Woodward unless otherwise expressly undertaken.

Contents

WARNINGS AND NOTICES.....	2
CHAPTER 1. PURPOSE.....	3
1.1 Related Documents.....	3
CHAPTER 2. DEFENSE IN DEPTH.....	4
CHAPTER 3. SYSTEM ACCESS.....	5
3.1 System Access Points.....	5
3.2 Achieving a Secure Environment.....	5
3.3 Additional Safety Features.....	5
CHAPTER 4. CONFIGURING AN EXTERNAL PC.....	6
CHAPTER 5. NERC CIP v6 COMPLIANCE.....	7
5.1 CIP-2.....	7
5.2 CIP-3.....	7
5.3 CIP-4.....	8
5.4 CIP-5.....	8
5.5 CIP-6.....	8
5.6 CIP 7.....	9
5.7 CIP 8.....	9
5.8 CIP 9.....	9
5.9 CIP 10.....	10
5.10 CIP 11.....	10
REVISION HISTORY.....	11

The following are trademarks of Woodward, Inc.:

ProTech
Woodward

The following are trademarks of their respective companies:

Modbus (Schneider Automation Inc.)
Pentium (Intel Corporation)

Illustrations and Tables

Figure 2-1. Graphical Representation of the Purdue Model and Location of DVP.....	4
---	---

Warnings and Notices

Important Definitions



This is the safety alert symbol used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

- **DANGER** - Indicates a hazardous situation, which if not avoided, will result in death or serious injury.
- **WARNING** - Indicates a hazardous situation, which if not avoided, could result in death or serious injury.
- **CAUTION** - Indicates a hazardous situation, which if not avoided, could result in minor or moderate injury.
- **NOTICE** - Indicates a hazard that could result in property damage only (including damage to the control).
- **IMPORTANT** - Designates an operating tip or maintenance suggestion.

Chapter 1.

Purpose

This manual provides information on implementation of security over CANopen with the following DVP models: 24V, Classic, DVP 5000, DVP 10000, and DVP 12000. The manual discusses and is applicable to the CANopen protocol when used to control the DVP. The non-routable nature of the CAN protocol used by CANopen makes it a good choice for security sensitive environments.

1.1 Related Documents

26773 Digital Valve Positioner DVP5000/DVP10000/DVP12000
26329 Digital Valve Positioner 24V and Classic

Chapter 2. Defense in Depth

The primary network used for commands and response is CANopen. This is a non-routable network. The attack surface requires physical access to the network to inflict an attack vector. This document assumes no Ethernet to CAN gateway on the CAN network, which could grant access by outside actors to the CAN network.

Configuration tool access is provided by the RS-232/RS-485 ports. The only tools that communicate on this port are the official Woodward service tools for DVP. No other protocols are allowed. When not in use, a plug or physical blocking device should be attached to the DB-9 service connector.

Referencing the Purdue model, this device could be considered a Level 0 device. Protections around this device include physical (locked cabinets, physical network protections, access alarms).

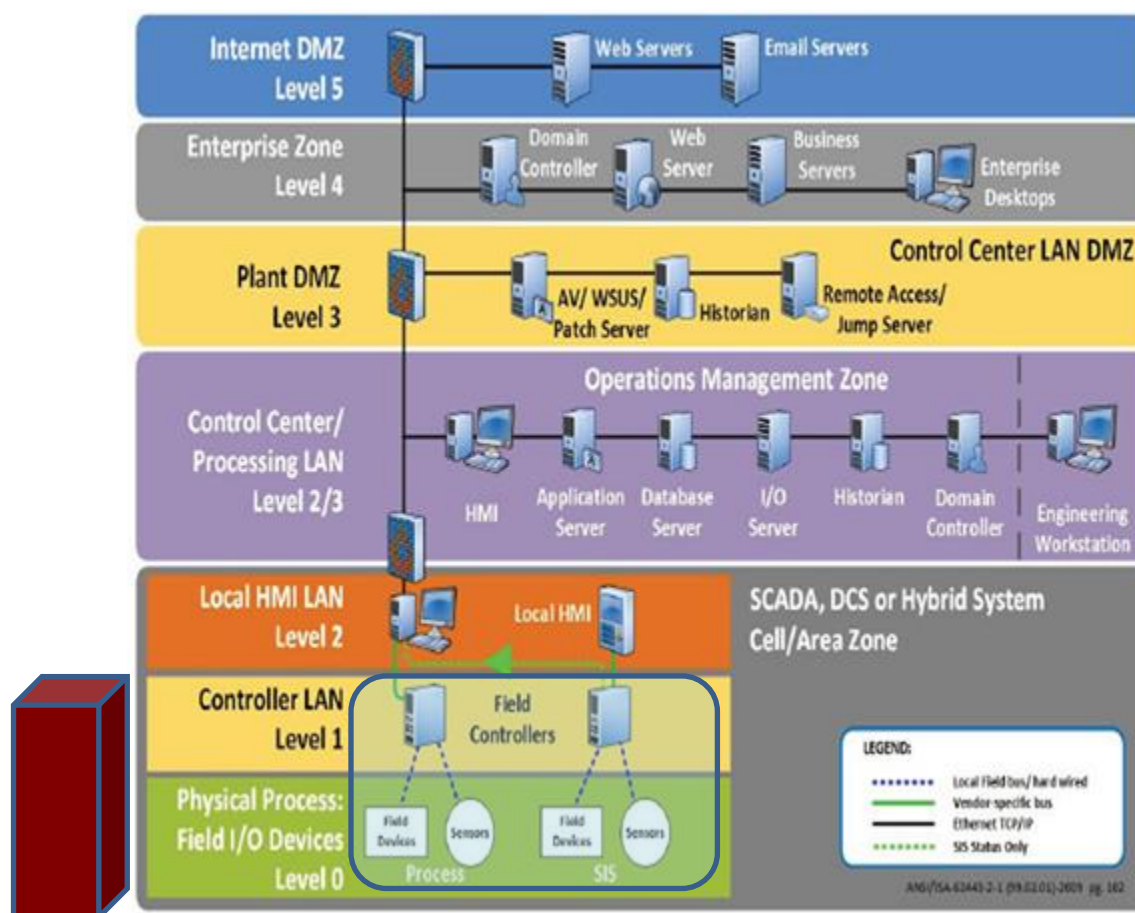


Figure 2-1. Graphical Representation of the Purdue Model and Location of DVP

The DVP does not have a default username/password to control access. Access control is handled by devices higher in the model (the service tool computer, PLC communication to DVP).

Chapter 3. System Access

3.1 System Access Points

3.1.1 RS-232/RS-485

DVP uses an RS-232/RS-485 Service Port. This port is used only for DVP Configuration with the Service Tool.

3.1.2 CANopen Communication Ports

The DVP device can be controlled via CAN communication. Manual 26773 and Appendix A describe the CANopen communication in depth.

3.2 Achieving a Secure Environment

The attack surface is limited to physical access to the device when there is no Ethernet communications module. The RS-232 and CANopen networks are non-routable. This security manual assumes physical connections are used (no protocol converters) to the control. Physical protections (locked cabinet, access alarms) should provide additional layers of protection.

3.3 Additional Safety Features

As another layer of the defense in depth strategy, the DVP does have safety shutdown inputs that are secure and cannot be impacted by malicious code. In addition, there are shutdown contacts that may be used so the Turbine Control System can always shut down the DVP and (if using a spring loaded valve, for example) that the valve will shut down. The safety contacts bypass the processor and firmware so they can block any attack vector that is intended to take control of the DVP.

Chapter 4.

Configuring an External PC

The Service Tool can be used to configure points in the DVP. If this tool is required to be access controlled and audited, the local policy on the computer will need to be configured. This includes the notion of least privilege access on this computer to the DVP service tool. See Manual 26912 for additional information about the Service Tool.

Chapter 5.

NERC CIP v6 Compliance

5.1 CIP-2

Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES.

5.1.1 CIP-2 R1.1 High Impact

The DVP as a generation resource may or may not qualify as a High Impact critical cyber security asset. The DVP reports to other devices in the Cyber Asset and is dependent on the categorization of these devices. If the controlling device is determined to be High Impact, the DVP will fall into this rating.

5.1.2 CIP-2 R1.2 Medium Impact

If the system criticality is not High Impact, CIP-002-5.1a-Attachment 1 Impact Rating Criteria should be reviewed to determine the system category is Medium Impact or Low Impact.

5.1.3 CIP-2 R1.3 Low Impact

All Woodward components not meeting any of the High Impact or Medium Impact requirements above are categorized as Low Impact.

5.2 CIP-3

5.2.1 CIP-3 R1: Cyber Security Policy Review and Approval

CIP-3 R1.1 High Impact and Medium Impact

- CIP-3 R1.1.1 Personnel and Training (CIP-004)
- CIP-3 R1.1.2 Electronic Security Perimeter (ESP) and Interactive Remote Access (CIP-005)
- CIP-3 R1.1.3 Physical Security (CIP-006)
- CIP-3 R1.1.4 System Security Management (CIP-007)
- CIP-3 R1.1.5 Incident Reporting and Response Planning (CIP-008)
- CIP-3 R1.1.6 Recovery Plans (CIP-009)
- CIP-3 R1.1.7 Configuration Change Management and Vulnerability Assessments (CIP-010)
- CIP-3 R1.1.8 Information Protection (CIP-011)
- CIP-3 R1.1.9 Exceptional Circumstances Declaration and Response

CIP-3 R1.2 Low Impact

- CIP-3 R1.2.1 Cyber Security Awareness
- CIP-3 R1.2.2 Physical Security Controls
- CIP-3 R1.2.3 Electronic Access Controls
- CIP-3 R1.2.4 Cyber Security Incident Response
- CIP-3 R1.2.5 Malicious Code Risk Mitigation of Transient Cyber Assets and Removable Media
- CIP-3 R1.2.6 Exceptional Circumstances Declaration and Response

5.3 CIP-4

Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the BES from individuals accessing BES Cyber by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems

5.3.1 CIP-4 R1 Security Awareness Program

CIP-4 R1.1 Reinforce practices

5.3.2 CIP-4 R2 Cyber Security Training Program

- CIP-4 R2.1 Training Content
- CIP-4 R2.2 Training Records Prior to Authorization
- CIP-4 R2.3 Renew Training

5.3.3 CIP-4 R3 Personnel Risk Assessment Program

- CIP-4 R3.1 Identity Confirmation
- CIP-4 R3.2 Background/History Record Check
- CIP-4 R3.3 Background/History Record Check Criteria
- CIP-4 R3.4 Contractor Background/History Record Check
- CIP-4 R3.5 Renew Personnel Risk Assessment

5.3.4 CIP-4 R4 Access Management Program

The DVP does not have user management or authentication. There is no logging of user activity on the DVP.

5.4 CIP-5

Purpose: To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

DVP has non-routable communication through CANopen. The DVP lies within the ESP of the controlling system.

5.5 CIP-6

Purpose: To manage physical access to BES Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

- CIP-6 R1 Physical Security Plan
- CIP-6 R2 Visitor Control Program
- CIP-6 R3 Maintenance and Testing

5.6 CIP 7

Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

- CIP-7 R1 Ports and Services Process Implementation and Documentation. The RS-232/485 port is used for service. When not in use it should be secured by a physical lock or cover. The CANOpen ports are used for field communication. If not used, the ports should not be connected.
- CIP-7 R2 Security Patch Management Implementation and Documentation
The DVP can be updated in the field through the RS-232/485 port. The firmware version is displayed in the configuration tool.
- CIP 7 R3 Malicious Code Prevention Implementation and Documentation
The DVP can be updated in the field through the RS-232/485 port. There are no built in protections to prevent the running of malicious code. It is strongly recommended to load only code downloaded from Woodward.com or provided by authorized Woodward personnel. Code acquired from 3rd party, unauthorized sources should not be used.
- CIP 7 R4 Security Event Monitoring
There is no security event monitoring with the DVP
- CIP 7 R5 System Access Control
There is no system access/user access in the DVP

5.7 CIP 8

Purpose: To mitigate the risk or the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirement

- CIP-8 R1.1 Identification, Classification, and Response
- CIP-8 R1.2 ES-ISAC Notification Process
- CIP-8 R1.3 Incident Response Roles and Responsibilities
- CIP-8 R1.4 Incident Response Containment, Eradication, Recovery, and Resolution
- CIP-8 R2.1 Testing Frequency
- CIP-8 R2.2 Document Test Results
- CIP-8 R2.3 Reportable Incident Record Retention

There is no logging capability for the DVP. No records are retained onboard the device.

5.8 CIP 9

Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

- CIP-9 R1.1 Activation Criteria
- CIP-9 R1.2 Roles and Responsibilities
- CIP-9 R1.3 Recovery Resources - Backup and Storage
There is no user account capability on the DVP. The DVP firmware can be reloaded on the device through the service tool and RS-232/485 port. Firmware version may be recorded using the tool.
- CIP-9 R1.4 Backup Verification Process
There is no documented backup verification process for DVP firmware
- CIP-9 R1.5 Preserve Diagnostic Data
There is no logging on the DVP.

5.9 CIP 10

Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES.

- CIP-10 R1.1.1 OS and Firmware Versions
The DVP firmware cannot be updated in the field. There is only one version of the software.
- CIP-10 R1.1.2 Commercial and Open-Source Application Versions
- CIP-10 R1.1.3 Custom Application Versions
The DVP does not support Custom Application Versions
- CIP-10 R1.1.4 Logical Network Accessible Ports
There are no logical ports on the DVP
- CIP-10 R1.1.5 Security Patches
There are no security patches for DVP
- CIP-10 R1.2 Authorize and Document Deviations from Baseline
DVP cannot vary from baseline, as such no impact assessment is required.

5.10 CIP 11

Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

- CIP-11 R1 Information Protection
No information is stored on the DVP. No account levels are stored on DVP. There are no data destruction procedures.

Revision History

New Manual—

-

THIS PAGE INTENTIONALLY LEFT BLANK

THIS PAGE INTENTIONALLY LEFT BLANK

We appreciate your comments about the content of our publications.

Send comments to: icinfo@woodward.com

Please reference publication **35124**.



B 3 5 1 2 4 : -



PO Box 1519, Fort Collins CO 80522-1519, USA
1041 Woodward Way, Fort Collins CO 80524, USA
Phone +1 (970) 482-5811

Email and Website—www.woodward.com

Woodward has company-owned plants, subsidiaries, and branches, as well as authorized distributors and other authorized service and sales facilities throughout the world.

Complete address / phone / fax / email information for all locations is available on our website.