DeltaV™ Firewall-IPD

Firewall Intrusion Protection Device (IPD)

- Provides an additional level of cyber-protection to your DeltaV™ embedded nodes
- Easy, out-of-the-box protection, in a plug-and-play solution
- Enforces physical access requirements when the DeltaV embedded nodes are in 'locked state'
- Layered implementation that can be added to your system at any time
- Purpose-built, fully supported DeltaV security solution

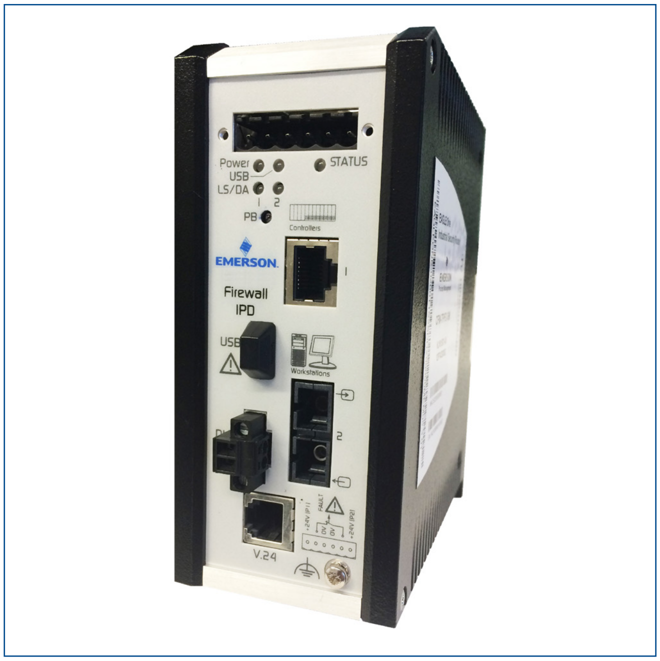


Figure 1 - The DeltaV™ Firewall-IPD provides additional security protection for your DeltaV embedded devices.

Introduction

Network firewalls are used to limit communications traffic between networks so that only permitted messages and a defined level of traffic are allowed to pass between the networks. The DeltaV™ Firewall-IPD is a hardware device that is installed within a DeltaV network between the DeltaV embedded nodes (DeltaV Controllers, EIOC, WIOC, etc.) and workstations. The DeltaV Firewall-IPD provides an additional layer of cybersecurity protection that can be installed within the DeltaV Area Control network. It functions to provide additional protection for embedded nodes installed on the secure side of the firewall against message flooding and denial-of-service attacks originating from the workstation side of the firewall.

Benefits

Even more protection: The Firewall-IPD is highly recommended in any DeltaV system deployment, and moreover if your security risk assessment determines that additional protection is required to prevent automated cyber-attacks on your system, the Firewall-IPD can be economically installed on your system to mitigate these threats.

Easy to deploy: The Firewall-IPD is pre-configured to match the required DeltaV communication rules. Simply install the hardware, hook up the network cables and the protection is in place—right out of the box.

Security layer can be added at any time: The Firewall-IPD can be installed during your initial system implementation or at any later time when you decide you need additional protection for your embedded nodes. It is highly recommended to be installed in Electronic Marshalling-based systems.

The DeltaV Firewall-IPD is a fully supported solution: The firewall is "purpose-built" and is specifically configured and tested to function in a DeltaV network. It is set up to serve the very specific purpose of protecting DeltaV embedded nodes from cyber-attacks. As a fully supported DeltaV product the Firewall-IPD is available only from Emerson.

DeltaV embedded nodes lock feature: Available in DeltaV v13.3.1 and higher, the DeltaV embedded nodes can be locked to prevent unauthorized access to certain functions, and the Firewall-IPD is pre-configured to only allow the unlock command to reach the embedded nodes if the user has physical access to the unit.

Product Description

The DeltaV Firewall-IPD is a 24-volt DIN rail-mounted hardware firewall specifically configured to be installed in a DeltaV system and support DeltaV communication protocols.

The firewall is set up so that the factory default configuration will allow DeltaV communications and deny any other communications not specifically required for the DeltaV embedded nodes to communicate bi-directionally with DeltaV workstations.

The firewall can be installed in a one-to-one configuration in front of each DeltaV embedded node, or it can also be mounted in conjunction with a multi-port switch, with one firewall supporting up to eight DeltaV controllers. Any supported network switch can be used for this purpose.

DeltaV-specific Plug-and-Play Installation

The Firewall-IPD is easy to install in your DeltaV network. Since it comes pre-configured from the factory, installation is as simple as mounting it on the DIN rail, connecting the communication cables and powering up the unit. The unit is configured to begin protecting your controllers on power-up—no additional programming or configuration is required.

Extended Security Functions

In order to make the firewall easy to use in a DeltaV system, the Firewall-IPD is pre-configured and does not require any additional configuration. The only optional security setup of the firewall involves limited adjustments to the default firewall rule set that may be desired to provide additional protection depending on the results of your risk assessment.

Firewall Management

Management of the firewall is not required because it is a plug-and-play device. For increased security, the firewall is delivered without an IP address and with its web interface disabled. Default DeltaV firewall rules are included so that no configuration is required. Alarm contacts on the power terminal block provide device monitoring capability so that loss of communications or other failures can be detected and alarmed.

However, if you wish to collect communications log data or use the extended protection features, the firewall can be assigned a unique IP address and can then be set up to allow use of these capabilities (Hirschmann HiView v3 or higher is required).

The device can be easily accessed from a workstation using its unique IP address to make configuration changes. You can also enable communications logging and collect logs on an external logging computer. Logs can then be reviewed for unauthorized access indications.

Details of this capability are available on Emerson's Guardian Support Knowledge Base where the specific instructions on how to assign an IP address and set up these firewall extended features are documented.

Reliable Hardware

The DeltaV Firewall-IPD is based on hardware produced by Hirschmann, a recognized supplier of industrial-grade networking equipment and a member of the DeltaV third-party alliance program. The firewall is a full-function Hirschmann firewall, running a custom firmware specifically configured to support ease of use within DeltaV systems.

Firewall IPD

The Firewall-IPD also provides additional configuration protection for DeltaV embedded nodes and DeltaV SIS Smart Logic Solvers. When used as an Intrusion Protection Device (IPD), the firewall will block the "SIS Unlock" message and the "DeltaV Unlock" message (available in DeltaV v13.3.1 and higher) generated by the ProfessionalPLUS Station from reaching the SIS Smart Logic Solvers or the DeltaV embedded nodes respectively. Unlocking the DeltaV embedded nodes or the SIS Smart Logic Solvers can be done from the front panel pushbutton by using a specific button sequence, by using the discrete input on the front panel of the firewall, or even by physically bypassing the firewall so the unlock message can reach the embedded nodes or the DeltaV SIS Smart Logic Solvers. The front panel button unlock is automatically reset after 30 minutes to prevent the Firewall-IPD from remaining in bypass mode. With firmware 05.3.07, the DeltaV Firewall-IPD will toggle the bypass mode on and off every time the front panel button is pressed three times, or the discrete signal transitions (positive or negative edge depending on the device's configuration). This feature protects your DeltaV embedded nodes from unauthorized access to certain functions, and DeltaV system SIS configurations from unauthorized changes coming from remote locations (Using the discrete input or physical bypass solutions must be custom engineered on a project basis).

For DeltaV v13.3.1 and higher, the DeltaV embedded nodes can be locked to prevent certain functions such as: downloads, firmware upgrades, access to the privileged menu of maintenance ports, and decommissioning. These functions are only accessible if the DeltaV embedded nodes are unlocked, and the Firewall-IPD must be in bypass mode in order to allow the DeltaV unlock command to pass.

Configuration of the Firewall

The DeltaV Firewall-IPD is a plug-and-play device that requires no configuration by the user in order to function properly. There are also a number of extended security features that may be custom configured to meet specific customer security needs. If these extended features are used, they must be configured following the specific instructions published by Emerson. It is important that only Emerson documentation is used to configure this firewall. This configuration information is published in the Emerson's Guardian Support Knowledge Base. If the firewall is custom configured, Emerson supports the use of the Hirschmann Auto Configuration Adaptor (ACA 21-USB) to save the configuration for easy device replacement – The 'ACA 21-USB' is available directly from Hirschmann. Configuration also requires a terminal access cable to interface with the Firewall-IPD through its serial port.

Supported Network Architecture in Using the Firewall

The firewall should follow the architecture described in Figure 2 (or as directed in other DeltaV documentation) when used within the DeltaV network. When installed in the field, close to the DeltaV embedded nodes and in secured cabinets or rack rooms, the firewall can also help to prevent cyber-attacks that might be caused by the unauthorized connection of computers to the network on the workstation side of the firewall.

Performance

A single Firewall-IPD can support DeltaV communications with up to eight controllers or eight redundant controller pairs as shown in Figure 2. For the best security protection, the firewall should be mounted as close to the embedded nodes as possible and should be mounted in locked enclosures or rack rooms. When used with a switch for 1:N nodes support, any unused ports on the switch located on the secure side (controller side) should be disabled to prevent access to the network on the protected side of the firewall. DeltaV Smart Switches should be used with this firewall to provide the easy lock-down of unused ports.

System Compatibility

Language Support: The firewall can be installed on any language system. Instructions and setup information is in English only.

Other Information: The DeltaV Firewall-IPD should be a component of your overall security program. When properly installed, the firewall provides an additional layer of protection for your control system to further protect the DeltaV embedded nodes from the effects of communication floods and denial-of-service attacks. The firewall does not protect the DeltaV workstations from becoming infected nor will it protect workstations from being affected by these types of attacks. It will keep a denial-of-service attack from an infected workstation from impacting the embedded nodes performance or visibility.

Note 1: The DeltaV Firewall-IPD is designed and supported to be installed only as described in this and other DeltaV system documentation. It is not suitable for use as a general-purpose firewall and should not be installed in other locations within the DeltaV system unless our documentation specifically states otherwise. These devices are specifically set up and tested to be used to protect DeltaV embedded nodes from specific types of cyber-threats, and it also provides added protection for DeltaV SIS safety systems. Please refer to Emerson's Guardian Support Knowledge Base for more detailed information on the use of these solutions.

Note 2: Whenever necessary, Emerson will release updates to the operating system software of the Firewall-IPDs. These updates will be distributed through the Guardian Support portal. Updates from sources other than Emerson must not be installed.

Note 3: The DeltaV Firewall-IPD is the drop-in replacement for the DeltaV Controller Firewall as well as the DeltaV SIS-IPD and compatible with all supported DeltaV versions offered by Emerson.

Achilles Certification

Although highly recommended to protect the DeltaV embedded nodes against cyber-attacks, for DeltaV v12.3

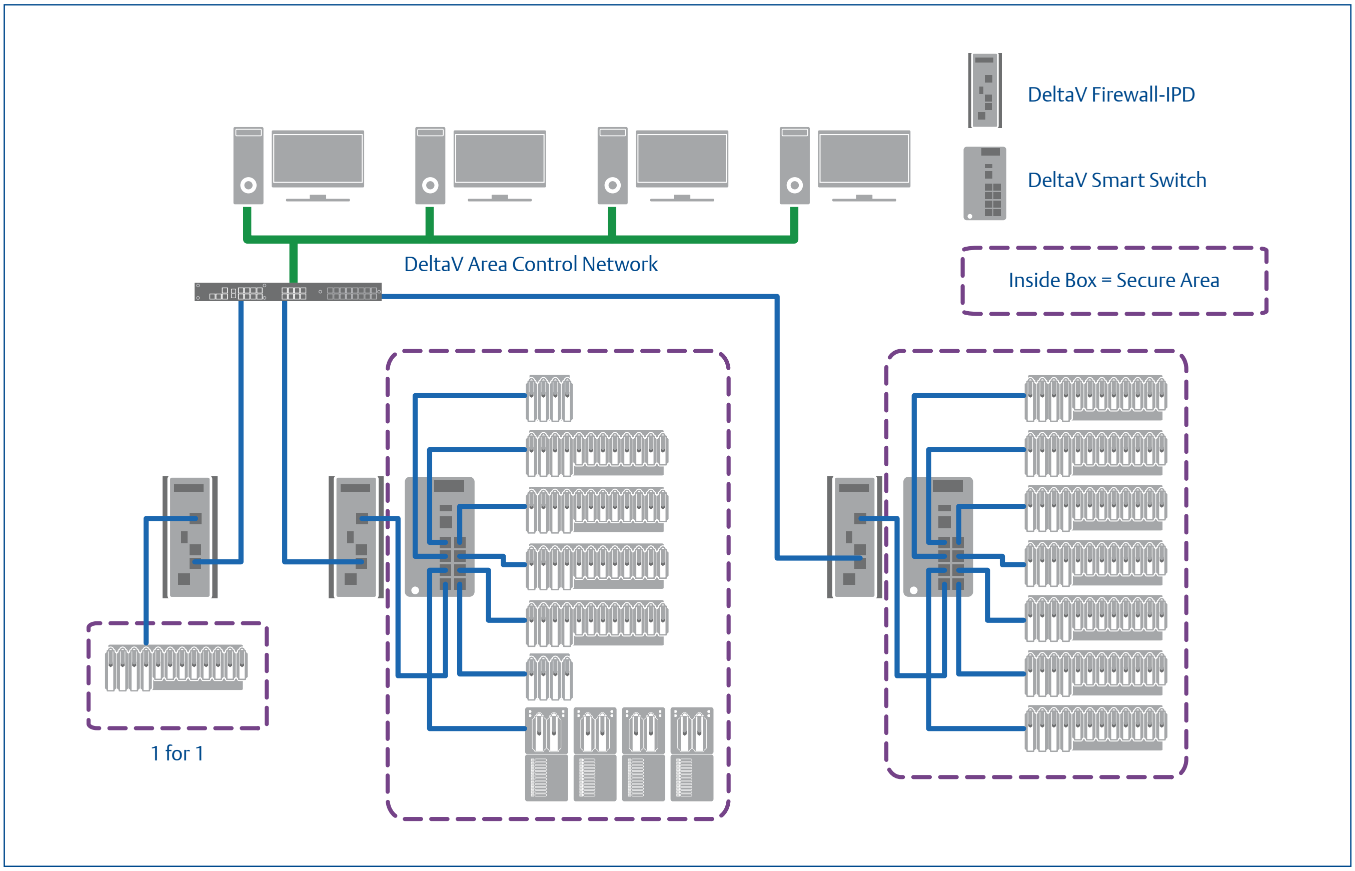
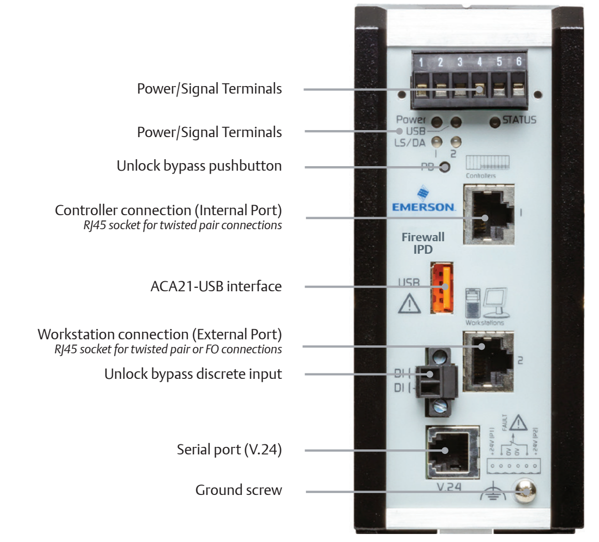


Figure 2 - Typical installation example of the Firewall-IPD in a DeltaV network (Redundant networks not shown for simplicity).

and newer the Firewall-IPD is not required for Achilles Communications certification of DeltaV embedded nodes. For DeltaV versions prior to v12.3 the Firewall-IPD is part of the solution required to deliver an Achilles Communications Certified controller for customers who require this level of certification in their control systems.


Power/Signal Terminals
Power/Signal Terminals
Unlock bypass pushbutton
Controller connection (Internal Port)
RJ45 socket for twisted pair connections
ACA21-USB interface
Workstation connection (External Port)
RJ45 socket for twisted pair or FO connections
Unlock bypass discrete input
Serial port (V.24)
Ground screw
1 2 3 4 5 6
Power
USB
LS/DA
STATUS
PB
EMERSON
Firewall IPD
USB
DI
V.24

DeltaV Firewall-IPD Front Panel Element

ISASecure System Security Assurance (SSA) Certification

The DeltaV Firewall-IPD is required if the DeltaV architecture is expected to be certifiable to the ISASecure SSA certification in version 14.3 (i.e. ISA/IEC 62443 series of standards compliance). For DeltaV v14.3.1 Feature Pack 1, this requirement is no longer applicable as the firewall is not required to block SNMP version 1 communications to DeltaV embedded nodes in newer releases of DeltaV software. Emerson still recommends the use of DeltaV Firewall-IPDs in your system for added security ptotections.

Installation Information

To provide the greatest protection, the DeltaV Firewall-IPD is mounted on a DIN-rail in close proximity to the DeltaV embedded nodes. Depending on the geographical distribution of the DeltaV embedded nodes, the firewall can be deployed in a 1:1 configuration to protect a single node or in conjunction with a DIN-rail mounted network switch to provide a 1:N configuration (a maximum of eight controllers can be connected to the Firewall-IPD). Note that the installation shown in Figure 2 is an example architecture supported for this firewall.

The firewall can support up to eight redundant pairs of controllers using a pair of VE6041 8-port DIN-rail mounted DeltaV Smart Switches (a single VE6041 will only provide connections for up to 7 controllers) or a single VE6042 or VE6043 modular DeltaV Smart Switch.

Workstations should never be installed on the secure (controller) side of the firewall to maintain the security level provided by installing the firewall.

The controller firewall can support up to eight controllers and 16 CHARM I/O Cards (CIOC) per controller (128 CIOCs in total) on the secure side of the firewall. CIOCs and controllers should be connected to the same secure side of the same firewall if there is any need to communicate.

Product Hardware Details

Product Description (applies to both Firewall and the SIS IPD)	
Description	DeltaV Firewall-IPD. Stealth, Multiple Client Transparent Mode
Power Supply/ Signaling Contact	1 plug-in terminal block, 6-pin
V.24 Serial Interface [user setup access]	1 x RJ11 socket
Port Types and Quantity	
Controller Port	10/100 Mbps RJ45 copper port, auto-crossing, auto-negotiation, auto-polarity.
Workstation Port	10/100 Mbps RJ45 copper port, auto-crossing, auto-negotiation, auto-polarity or 100 Mbps Fiber Optic (single-mode or multi-mode).
Twisted Pair	
Length of a twisted pair segment max. 100 m (for Cat5e cable)	

Fiber Optic 100BASE-FX						
Ports	**Wave Length**	**Fiber**	**System Attenuation**	**Example for FO line length****	**Fiber Attenuation**	**BLP/ dispersion**
MM	1300nm	50/125µm	0-8 dB	0-5 km	1.0 dB/km	800 MHz·km
MM	1300nm	62.5/125µm	0-11 dB	0-4 km	1.0 dB/km	500 MHz·km
SM	1300nm	9/125µm	0-16 dB	0-30 km	0.4 dB/km	3.5 ps/(nm·km)

*** Including 3 dB system reserve when compliance with the fiber data is observed.*

Digital Input and Relay Output	
Relay Output Signal Contact	Switching current max. 1 A, SELV Switching voltage max. 60 V DC, SELV Relevant for North America: max. 30 V DC, Class 2, resistive load.
Digital Input	Used for remotely bypassing the DeltaV and the DeltaV SIS protection functions to allow unlocking the DeltaV embedded nodes and the DeltaV SIS Smart Logic Solvers. This function is disabled by default in the Firewall-IPD (can be configured through the serial port). Maximum permitted input voltage range −32 V DC ... +32 V DC Nominal input voltage +24 V DC Input voltage, low level, status "0" -0.3 V DC ... +5.0 V DC Input voltage, high level, status "1" +11 V DC ... +30 V DC Maximum input current at 24 V input voltage 15 mA Input characteristic according to IEC 61131-2 (current consuming) Type 3
Security	
Stateful Inspection Firewall	Firewall rules (incoming/outgoing, modem access, management)
Storm Protection	The firewall will filter TCP Connections and ARP/Ping Frames per second to preset values.
LAND Attack Protection	The firewall will drop and log all packets with identical source and destination IP addresses and ports.
Intrusion Protection	The IPD feature blocks the DeltaV and the DeltaV SIS "unlock" commands to prevent unauthorized access to the DeltaV embedded nodes and changes to the SIS Smart Logic Solver configuration. The IPD function can be temporarily bypassed (resets in 30 minutes) to allow DeltaV embedded nodes and the DeltaV SIS Smart Logic Solvers to be unlocked. The bypass can be implemented from the front panel button on the Firewall-IPD using a specific button sequence. Optionally a user specified physical bypass switch can be installed on a per project basis.

Power Requirements		
Operating Voltage	24 V DC (-25% to +30%)	
Model Number	**Maximum Power Consumption**	**Power Output**
VE6205T1	5W	17 Btu(IT)/h
VE6205T2	6W	20 Btu(IT)/h
VE6205T3	5W	17 Btu(IT)/h
VE6205T4	6W	20 Btu(IT)/h
VE6205T5	5W	17 Btu(IT)/h
VE6205T6	6W	20 Btu(IT)/h

Service	
Diagnostics	LEDs (power, link status, device status, USB device status), signaling contact (24V DC / 1 A), log file.
Configuration	Command Line Interface (CLI), web interface, auto configuration adapter (ACA 21-USB). Configuration is not required to install and use the Firewall-IPD out of the box. Configuration is only required for custom configurations.
Other Services	Services supported - NTP, console connection, HTTPS, SSH, SNMP V3
Redundancy	
Redundancy Functions	DeltaV network redundancy only (support for Hirschmann ring configuration or Hirschmann firewall redundancy features are not supported in a DeltaV system). Redundant 24 V DC power supply.

Ambient Conditions		
	Firewall-IPD Standard Temperature	**Firewall-IPD Extended Temperature Conformal Coating**
Operating Temperature	0°C to + 60°C (+32°F to +140°F)[1]	-40°C to +70°C (-40°F to +158°F)[1]
Storage/Transport Temperature	-40°C to +85°C (-40°F to 176°F)	
Relative Humidity (non-condensing)	10% to 95% both storage and operating	
Air Pressure Operation	minimum 795 hPa – approx. +2,000 m (+6,561 ft) maximum 1060 hPa – approx. -400 m (−1,312 ft)	
Air Pressure Storage	minimum 700 hPa – approx. +3,000 m (+9,842 ft) maximum 1060 hPa – approx. -400 m (−1312 ft)	
Laser Protection	Class 1 in compliance with IEC 60825-1	
Degree of Protection	IP20	

[1] *Please refer to this white paper to learn more about the effects of heat and airflow inside an enclosure.*
http://www.emerson.com/documents/automation/effects-of-heat-airflow-inside-an-enclosure-en-us-170664.pdf

Mechanical Construction	
Dimensions (W x H x D)	60.6 x 145.3 x 128.2 [mm] (2.39 x 5.72 x 5.04 [in])
Mounting	DIN Rail 35 mm
Weight	660 g (1.46 lb)
Mechanical Stability	
IEC 60068-2-27 Shock	15 g, 11 ms duration
IEC 60068-2-6 Vibration	Standard: 5 Hz ... 8.4 Hz with 3.5 mm (0.14 in) amplitude Marine: 2 Hz... 13.2 Hz with 1 mm (0.04 in) amplitude Standard: 8.4 Hz ... 150 Hz with 1 g (0.04 oz) Marine: 13.2 Hz ... 100 Hz with 0.7 g (0.03 oz)

Approvals (all Models)
CE 2014/30/EU (EMC) - 2011/65/EU (RoHS) – 2104/34/EU (ATEX)
CAN/CSA No. 213 Non-incendive Electrical Equipment for Use in Class I, Division 2 Hazardous Locations
RCM
EAC Russia
EN 55022 Information Technology Equipment – Radio disturbance characteristics – Limits and methods of measurement
EN 60950-1, Information Technology Equipment – Safety – Part 1: General requirements
EN 61000-6-2, Electromagnetic Compatibility (EMC) – Part 6-2: Generic standards – Immunity for industrial environments
EN 61000-6-4, Electromagnetic Compatibility (EMC) – Part 6-4: Generic standards – Emission standard for industrial environments
FCC 47 CFR Part 15 Code of Federal Regulations
IEC 60825-1 Safety of Laser Products
ISA 12.12.01 Non-incendive Electrical Equipment for Use in Class I and II, Division 2 and Class III, Divisions 1 and 2 Hazardous (Classified) Locations 1 and 2 Hazardous (Classified) Locations
UL 508 Safety for Industrial Control Equipment
Approvals (Extended Temperature Models only)
EN 60079-0 (ATEX Zone 2) Explosive Atmospheres – Part 0: Equipment – General requirements
EN 60079-11 (ATEX Zone 2) Explosive Atmospheres – Part 11: Equipment protection by intrinsic safety
EN 60079-15 (ATEX Zone 2) Explosive Atmospheres – Part 15: Equipment protection by type of protection
Marine: DNV-GL
EAC Ex (Russia)

DeltaV Controller and Workstation Usage	
Controllers Supported	DeltaV v8.4 or higher. Up to eight controllers or eight redundant controller pairs and up to 16 CHARM I/O Cards per controller (128 CIOCs in total) can be installed on the secure side of the firewall. We recommend using the VE6043 DeltaV Smart Switch for more than seven controller/CIOC connections. Please consult the CHARM Installation instructions for more information on installing devices using firewalls. For more than eight controllers or eight redundant controller pairs, more firewalls must be installed in parallel. All DeltaV embedded nodes are supported and can be further protected when the Firewall-IPD is included in the system design. DeltaV embedded nodes include DeltaV Controllers, Wireless I/O Card (WIOC), Ethernet I/O Card (EIOC), Virtual I/O Module (VIM), CHARM I/O Card (CIOC), etc.
Workstations Supported	DeltaV v8.4 or higher. Any number of workstations can be connected through the workstation port of the firewall.

Ordering Information

Description	Model Number
DeltaV Firewall-IPD	
DeltaV Firewall-IPD - standard temperature range (0°C to +60°C) – Controller Port copper RJ45 / Workstation Port copper RJ45	VE6205T1
DeltaV Firewall-IPD - extended temperature range (-40°C to +70°C), ATEX, conformal coating – Controller Port copper RJ45 / Workstation Port copper RJ45	VE6205T2
DeltaV Firewall-IPD - standard temperature range (0°C to +60°C) – Controller Port copper RJ45 / Workstation Port Fiber Optic Multi-Mode SC connector	VE6205T3
DeltaV Firewall-IPD - extended temperature range (-40°C to +70°C), ATEX, conformal coating – Controller Port copper RJ45 / Workstation Port Fiber Optic Multi-Mode SC connector	VE6205T4
DeltaV Firewall-IPD - standard temperature range (0°C to +60°C) – Controller Port copper RJ45 / Workstation Port Fiber Optic Single-Mode SC connector	VE6205T5
DeltaV Firewall-IPD - extended temperature range (-40°C to +70°C), ATEX, conformal coating – Controller Port copper RJ45 / Workstation Port Fiber Optic Single-Mode SC connector	VE6205T6
Note 1: Except for being 0.5 inches wider the VE6205 Firewall-IPD is functionally the drop-in replacement for the VE6201 Controller Firewall and the VS6202 SIS-IPD products.	
Note 2: The VE6205 Firewall-IPD is the drop-in replacement for the VE6203 Controller Firewall and the VS6203 SIS-IPD products.	

The VE6205 DeltaV Firewall-IPD product is expected to provide an additional layer of protection to your DeltaV system to help avoid certain types of undesired actions.The VE6205 Firewall-IPD product represents only one portion of an overall DeltaV system security solution. The use of the VE6205 Firewall-IPD product does not guarantee that your DeltaV system is secure from cyber-attacks, intrusion attempts, or other undesired actions. Users are solely and completely responsible for their control system security, practices and processes, and for the proper configuration and use of the VE6205 Firewall-IPD product.

Related Products

- DeltaV Smart Switches – the DeltaV Smart Switches and the DeltaV Network Device Command Center are also part of the DeltaV family of built-for-purpose security related products.

Prerequisites

- To customize the Firewall-IPD configuration it is helpful to have basic knowledge of Ethernet networking including network addressing and routing.

Emerson
North America, Latin America:
☎ +1 800 833 8314 or
☎ +1 512 832 3774

Asia Pacific:
☎ +65 6777 8211

Europe, Middle East:
☎ +41 41 768 6111

🌐 **www.emerson.com/deltav**

The contents of this publication are presented for informational purposes only, and while diligent efforts were made to ensure their accuracy, they are not to be construed as warranties or guarantees, express or implied, regarding the products or services described herein or their use or applicability. All sales are governed by our terms and conditions, which are available on request. We reserve the right to modify or improve the designs or specifications of our products at any time without notice.