DeltaV™ Controller Firewall

The DeltaV Controller Firewall provides additional security protection from for your DeltaV controllers

- Provides an additional level of economical cyber-protection to your DeltaV™ controllers

- Easy, out-of-the-box protection, in a plug-and-play solution

- Layered implementation that can be added to your system at any time

- Meet Cyber Security Achilles Level 1 Certifcation

- Purpose-built, fully supported DeltaV security solution

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 Controller Firewall is a hardware device that is installed within a DeltaV network between the controllers and workstations. The DeltaV Controller Firewall provides an additional layer of cyber-security protection that can be installed within the DeltaV Control network. It functions to provide additional protection for controllers installed on the secure side of the firewall against message flooding and denial-of-service attacks**.**

EMERSON
Process Management

Benefits

Even more protection. If your security risk assessment determines that additional protection is required to prevent automated cyber-attacks on your system, the controller firewall can be economically installed on your system to mitigate these threats.

Easy to deploy. The firewall 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 controller firewall can be installed during your initial system implementation or at any later time when you decide you need additional protection for your controllers.

Meet customer cyber security requirements for Achilles™ Certifications. The controller firewall is part of the solution to provide Achilles Certified DeltaV controllers for customers who require this optional security certification for their controllers.

The DeltaV controller firewall is a fully supported solution. The firewall is "purpose-built" and is specifically configured and tested to function in a DeltaV network. It is setup to serve the very specific purpose of protecting a DeltaV controller from cyber-attacks and to provide an Achilles Certified implementation of the DeltaV controller. As a fully supported DeltaV product the Controller Firewall is available only from Emerson Process Management.

Product Description

The DeltaV Controller Firewall is a 24-volt DIN rail-mounted hardware firewall specifically configured to be installed in a DeltaV system and support DeltaV communications 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 controllers to communicate bi-directionally with DeltaV workstations.

The firewall can be installed in a one-to-one configuration in front of each controller, or it can 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 controller firewall is easy to install in your DeltaV network. Since it comes preconfigured 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 controller firewall is preconfigured 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 the web interface disabled. Default DeltaV firewall rules are included so that no configuration is required. Alarm contacts on the power strip provide device monitoring capability so that loss of communications or other failures can be detected and alarmed.

However, if you wish to collect communication 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.

The device can easily be 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 by accessing DeltaV knowledge-based articles where the specific instructions on how to assign an IP address and set up these firewall extended features are documented.

Reliable Hardware

The DeltaV Controller Firewall 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 specifically configured to support ease of use within a DeltaV system.

DeltaV Controller Firewall

DeltaV SIS Intrusion Protection Device (IPD)

The controller firewall is also available in a special version that provides additional configuration protection for DeltaV SIS Logic Solvers. This version of the firewall will block the "SIS Unlock" message generated by the ProfessionalPLUS Station from reaching the Logic Solver. Unlocking the Logic Solver can be done by from the front panel pushbutton by using a specific button sequence or optionally the user can physically bypass the firewall so the unlock message can reach the Logic Solver. The front panel button unlock is automatically reset after 30 minutes to prevent the IPD from remaining unlocked. This feature protects your SIS configurations from unauthorized changes coming from remote locations. (Physical by-pass solutions must be custom engineered on a project basis)

Optional Solution

The controller firewall is an *optional solution* and would be installed only when your risk assessment determines that this extra layer of protection is warranted. The firewall should be deployed only if the risk assessment of the control system determines that the controllers cannot be adequately protected from denial-of-service attacks by deploying other protection methods, such as disabling media ports on a workstation and installing anti-virus software. The firewall should be used only to provide supplemental protection to a system that is already following our best practices for DeltaV system security.

Achilles Level One Certification

The Controller Firewall is also part of the solution required to deliver an Achilles Certified controller for customers who require this level of certification in their control system. For more information on Achilles Certification please see www.wurldtech.com.
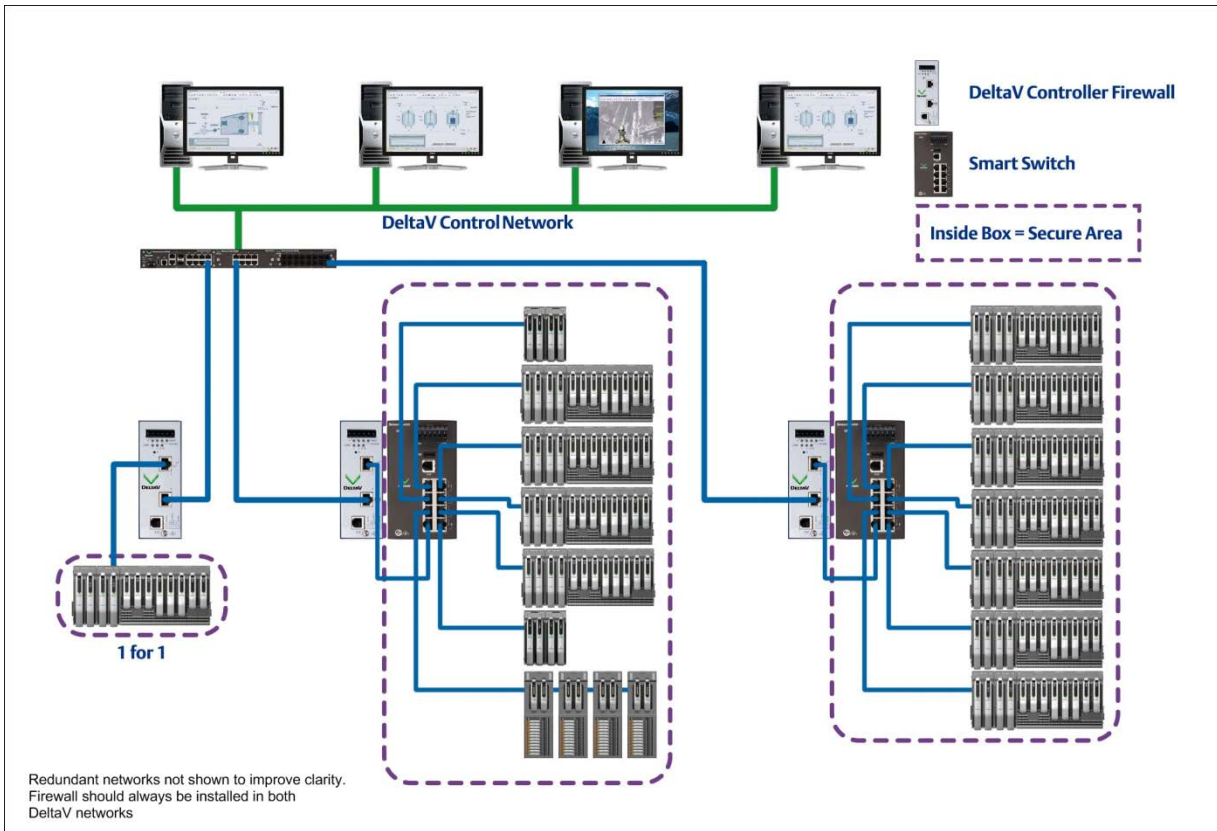
One typical installation example of the controller firewall in a DeltaV network.
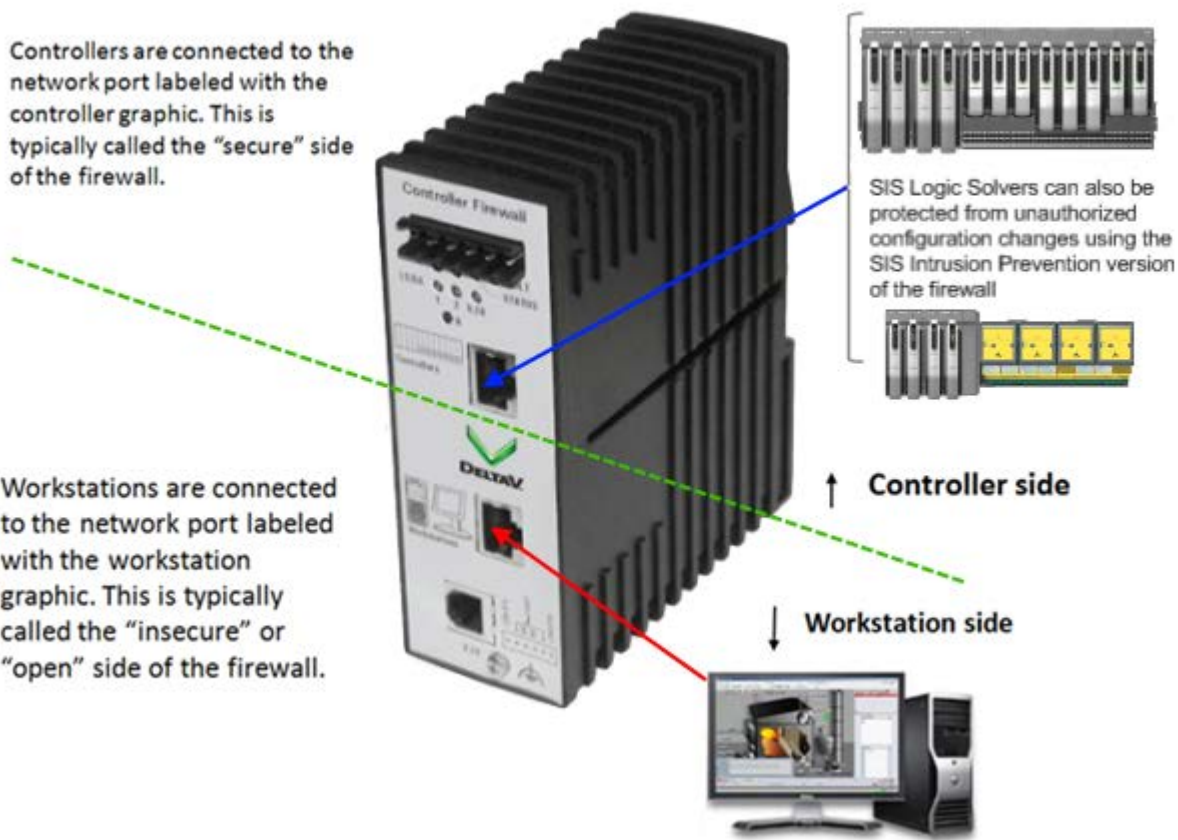
Installation Information

To provide the greatest protection, the DeltaV Controller Firewall is mounted on a DIN rail in close proximity to the controllers. Depending on the geographical distribution of the controllers, the firewall can be deployed in a 1:1 configuration to protect a single controller or in conjunction with a DIN mounted network switch to provide a 1:N configuration (N<=8). Note that the installation shown above is the only architecture supported for this firewall.

For redundant controllers, the firewall can support up to 8 redundant pairs of controllers using a pair of VE6041 8 port 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 8 controllers and 16 Charm I/O Cards (CIOC) per controller (128 CIOCs) on the secure side of the firewall. Charm I/O cards located on the workstation side of the firewall can also communicate with a controller on the secure side of the firewall. However it is a recommend practice to keep CIOC and controllers on the secure side of the firewall.

DeltaV Controller Firewall connection details

Controllers are connected to the network port labeled with the controller graphic. This is typically called the "secure" side of the firewall.

SIS Logic Solvers can also be protected from unauthorized configuration changes using the SIS Intrusion Prevention version of the firewall

Workstations are connected to the network port labeled with the workstation graphic. This is typically called the "insecure" or "open" side of the firewall.

↑ Controller side

↓ Workstation side

The Controller firewall can protect the controller and the SIS Logic Solver from security threats

Product Hardware Details

Product description (applies to both Firewall and the SIS IPD)	
Description	DeltaV Controller Firewall or SIS IPD Stealth, Multiple Client Transparent Mode
Port type and quantity	Trusted Port: 1 x 10/100BASE-TX, TP-cable, RJ45-socket, auto-crossing, auto-negotiation, auto-polarity Untrusted Port: 1 x 10/100BASE-TX, TP-cable, RJ45-socket, auto-crossing, auto-negotiation, auto-polarity For Fiber optic support a separate Fiber Optic media converter is required. The firewall is only available with an RJ-45 copper port.
Firmware version supported	Firewall IOS version v.3.1 (DeltaV supported firmware version)
Power supply/signaling contact	1 plug-in terminal block, 6-pin
V.24 interface [user setup access]	1 x RJ11 socket

Network size - length of cable	
Twisted Pair	0 - 100 m
Security	
Stateful inspection firewall	Firewall rules (incoming/outgoing, modem access, management), (Note – additional functions not supported on DeltaV firewall)
Intrusion Protection (SIS IPD only)	The IPD function blocks the DeltaV Safety Logic Solver "unlock" command to prevent changes to Logic Solver configuration. The IPD function can be temporarily disabled (resets in 30 minutes) to allow Logic Solve changes from the front panel button on the IPD using specific button sequence. Optionally a user specified physical bypass switch can be installed on a per project basis.
Antivirus protection	The built-in anti-virus function of the firewall is not supported in the DeltaV implementation
Power requirements	
Operating voltage	24 V DC (-25% to +30%)
Current consumption at 24 V DC	max. 335 mA
Service	

Diagnostics	LED's (power, link status, data, error, ACA) signaling contact (24 V DC / 1 A), log file
Configuration	Command Line Interface (CLI), web interface, auto configuration adapter (ACA11), (SolSoft policy server (ISCM) is not supported)
Other services	Services supported - NTP, serial, HTTPS, SSH, SNMP V1/V2/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 power supply
Ambient conditions	
Operating temperature	0 ºC to +55 ºC (32 0F to 131 0F)
Storage/transport temperature	-40 ºC to +80 ºC (-40 0F to 176 0F)
Relative humidity (non-condensing)	10% to 95%
MTBF	27.4 years; MIL-HDBK 217F: Gb 25 ºC
Mechanical construction	
Dimensions (W x H x D)	47 mm x 131 mm x 111 mm (1.85 in x 5.16 in x 4.37in)
Mounting	DIN Rail 35 mm
Weight	340 g (.75 lbs)
Protection class	IP 20
Mechanical stability	
IEC 60068-2-27 shock	15 g, 11 ms duration, 18 shocks
IEC 60068-2-6 vibration	1 mm, 2 Hz - 13,2 Hz, 90 min.; 0,7g, 13,2 Hz - 100 Hz, 90 min.; 3,5 mm, 3 Hz - 9 Hz, 10 cycles, 1 octave/min.; 1g, 9 Hz - 150 Hz, 10 cycles, 1 octave/min

EMC interference immunity	
EN 61000-4-2 electrostatic discharge (ESD)	6 kV contact discharge, 8 kV air discharge

EN 61000-4-3 electromagnetic field	10 V/m (80 - 2000 MHz)
EN 61000-4-4 fast transients (burst)	2 kV power line, 1 kV data line
EN 61000-4-5 surge voltage	power line: 2 kV (linie/earth), 1 kV (linie/line), 1 kV data line
EN 61000-4-6 conducted immunity	3 V (10 kHz - 150 kHz), 10 V (150 kHz - 80 MHz)
EMC emitted immunity	
FCC CFR47 Part 15	FCC CFR47 Part 15 Class A
EN 55022	EN 55022 Class A
Approvals	
Safety of industrial control equipment	cUL 508
Germanischer Lloyd	Germanischer Lloyd

DeltaV Controller and Workstation Usage	
Controllers supported	DeltaV v8.4 or later. Up to 8 controllers or 8 redundant controller pairs and up to 16 Charm I/O Cards per controller (128CIOCs) can be installed on the secure side of the firewall. We recommend using the VE6043/VE6045 DeltaV Smart Switch for more than 7 controller/CIOC connections. Please consult the Charm Installation instructions for more information on installing devices using a controller firewall. For more than 8 controllers or 8 redundant controller pairs, more firewalls must be installed in parallel.
Workstations supported	DeltaV v8.4 or later. Any number of workstations can be connected through the workstation port of the firewall.

Configuration of the Firewall

The DeltaV Controller Firewall 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 configured to meet specific customer security needs. If these extended features are used, they must be configured following the specific instructions published by Emerson Process Management. There are some standard features and capabilities of the firewall software that must not be configured or enabled/disabled if the device is to function properly within the DeltaV digital automation system. It is important that only Emerson Process Management documentation be used to configure this firewall. This configuration information is published in KBA AP-0600-0127 on the DeltaV Support site (http://www.emersonprocess.com/systems/support/home/index.aspx (requires password access))

Supported Network Architecture in Using the Firewall

The firewall should be implemented only in the architecture described in the graphic on page 7 (or as directed in other DeltaV documentation) when used within the DeltaV network. When installed in the field close to the controllers and in secured cabinets or rack rooms, the firewall can also help prevent cyber-attacks on the controllers that might be caused by the unauthorized connection of computers to the network on the workstation side of the firewall.

Performance

A single firewall can support DeltaV communications with up to eight controllers or eight redundant controller pairs as shown in the graphic on page 3. For the best security protection, the firewall should be mounted as close to the controllers as possible and should be mounted in locked enclosures or rack rooms. When used with a switch for 1:N controller 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.

DeltaV Operate for PROVOX and DeltaV Operate for RS3 Support: The firewall can be used on a DeltaV system using these operator workstations.

Other Information: The DeltaV Controller Firewall 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 controllers from the effects of communications 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 controller performance or visibility.

Note: This firewall is designed and supported to be installed only as described in this and other DeltaV documentation. It is not suitable for use as a general-purpose firewall and should never be installed in other locations within the DeltaV system unless our documentation specifically states otherwise. It is specifically set up and tested to be used to protect only controllers from specific types of cyber-threats. Please see the appropriate DeltaV knowledge-based articles for more detailed information on the use of this solution.

Note: From time to time it may be necessary to update the operating system software in these firewalls. These updates will be distributed through our installed-base-management organization and will be available only to users on DeltaV Foundation Support. Updates from sources other than Emerson Process Management must not be installed.

Ordering Information

Description	Model Number
DeltaV Controller Firewall- 24v DIN mounted hardware firewall specifically configured for use in the DeltaV control system LAN	VE6201
DeltaV SIS IPD - 24v DIN mounted hardware firewall specifically configured for use in the DeltaV control system LAN.	VS6202

Prerequisites

■ The DeltaV Controller Firewall and SIS IPD is
supported for use in DeltaV v8.4 (or later) networks.

To locate a sales office near you, visit our website at:
www.EmersonProcess.com/DeltaV
Or call us at:
Asia Pacific: 65.6777.8211
Europe, Middle East: 41.41.768.6111
North America, Latin America: +1 800.833.8314 or
                                                        +1 512.832.3774

For large power, water, and wastewater applications
contact Power and Water Solutions at:
www.EmersonProcess-powerwater.com
Or call us at:
Asia Pacific: 65.6777.8211
Europe, Middle East, Africa: 48.22.630.2443
North America, Latin America: +1 412.963.4000

www.DeltaV.com

EMERSON
Process Management