DeltaV™ Controller Firewall

- 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.
- Purpose-built, fully supported DeltaV security solution.

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

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 cybersecurity 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 originating from the workstation side of the firewall.

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. It is highly recommended to be installed in Electronic Marshalling based systems.

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. (On DeltaV v12 and newer systems the DeltaV Controller Firewall is no longer required for Achilles certifications).

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 set up 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 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, by using the discrete input on the front panel of the firewall or by physically bypassing 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. (Using the discrete input or physical by-pass solutions must be custom engineered on a project basis).

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 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 Process Management. It is important that only Emerson Process Management documentation be used to configure this firewall. This configuration information is published in KBA AK-1400-0078 (or AP-0600-0127 for the VE6201) on the DeltaV Support site (**http://www.emersonprocess.com/systems/support/home/index.aspx** (requires password access)) If the firewall or SIS-IPD is custom configured DeltaV supports the use of the Hirschmann Auto Configuration Adaptor (ACA 21-USB) to save the configuration for easy device replacement (available directly from Hirschmann). Configuration also requires a terminal access cable to interface to the serial port on the firewall/SIS-IPD.

Supported Network Architecture in Using the Firewall

The firewall should be implemented only in the architecture described in the graphic on page 4 (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: The DeltaV Controller Firewall and SIS-IPD are designed and supported to be installed only as described in this and other DeltaV documentation. They are 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. These devices are specifically set up and tested to be used to protect controllers from specific types of cyber-threats. The SIS-IPD provides added protection for DeltaV SIS. Please see the appropriate DeltaV knowledge-based articles for more detailed information on the use of these solutions.

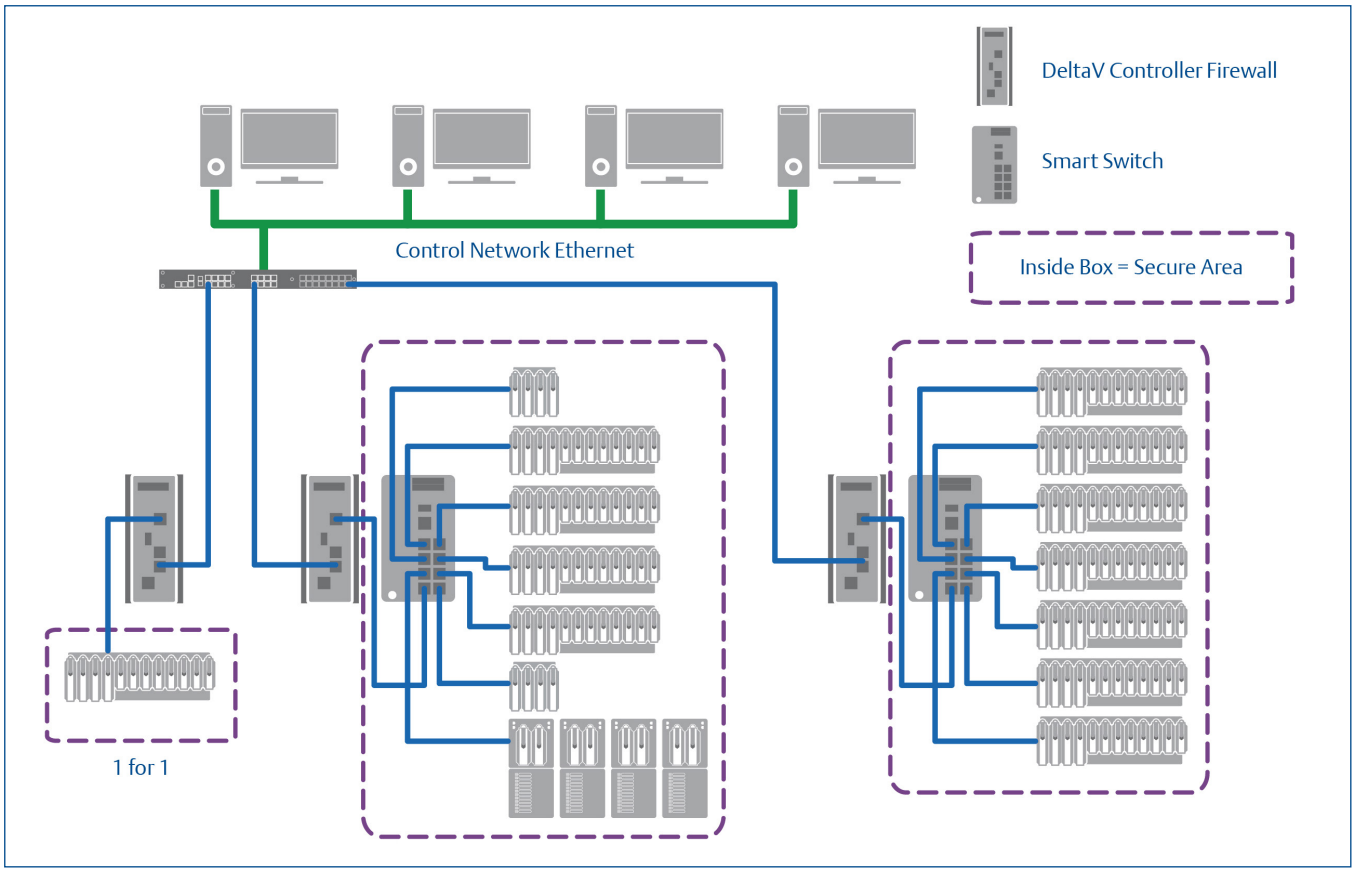
Note: From time to time it may be necessary to update the operating system software in these firewalls. These updates will be distributed through our installed-base-management organization and will be available only to users on DeltaV Foundation Support. Updates from sources other than Emerson Process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

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

For v12.3 and newer the firewall is not required for Achilles certification. For DeltaV versions prior to v12.3 the Controller Firewall is also part of the solution required to deliver an Achilles Communications 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. (Redundant networks not show for simplicity)

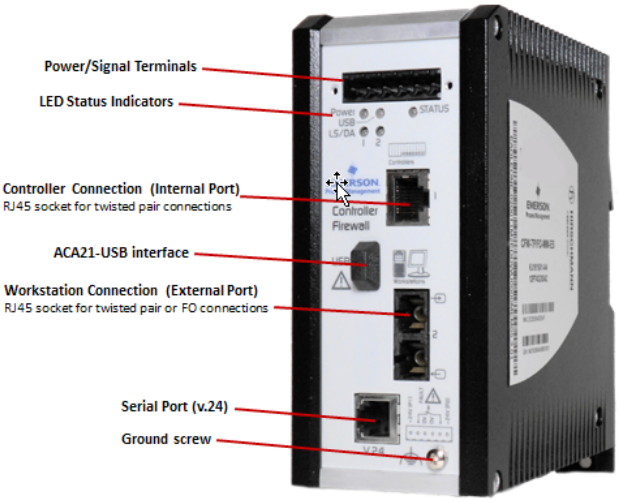
Installation Information

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 Front Panel Elements

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. *Note: Except for being 0.5 inches wider these devices are functionally drop in replacements for the VE6201 Controller Firewall and the VS6202 SIS-IPD.*
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 Mbits/s Twisted Pair port (TP)- RJ45-socket, auto-crossing, autonegotiation, auto-polarity.
Workstation Port	10/100 Mbits/s Twisted Pair port RJ45-socket, auto-crossing, auto-negotiation, auto-polarity or 100 Mbits/s MultiMode Fiber Optic (FO-MM).
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	50/125um	0-8 dB	0-5 km	1.0 dB/km	800 MHz*km
MM	1300nm	62.5/125um	0-11 dB	0-4 km	1.0 dB/km	500 MHz*km
SM	1300nm	9/125um	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 (SIS-IPD only)	Used for remotely by-passing the SIS protection function to allow unlocking the SIS Logic solver. This function is disabled by default in the SIS-IPD. 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 Controller Firewall will drop and log all packets with identical source and destination IP addresses and ports.
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.

Power requirements		
Operating Voltage	24 V DC (-25% to +30%)	
Model Number	**Maximum Power Consumption**	**Power Output**
VE6203-1	5W	17 Btu(IT)/h
VE6203-2	6W	20 Btu(IT)/h
VE6203-3	5W	17 Btu(IT)/h
VE6203-4	6W	20 Btu(IT)/h
VE6203-5	5W	17 Btu(IT)/h
VE6203-6	6W	20 Btu(IT)/h
VS6203-1	5W	17 Btu(IT)/h
VS6203-2	6W	20 Btu(IT)/h
VS6203-3	5W	17 Btu(IT)/h
VS6203-4	6W	20 Btu(IT)/h
VS6203-5	5W	17 Btu(IT)/h
VS6203-6	6W	20 Btu(IT)/h

Service	
Diagnostics	LED's (power, link status, device status, USB device status), signaling contact (24 V DC / 1 A), log file.
Configuration	Command Line Interface (CLI), web interface, auto configuration adapter (ACA11). Configuration is not required to install and use the firewall and SIS-IPD out of the box. Configuration is only required for custom configurations required by users.
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		
	Controller Firewall and SIS-IPD Standard Temperature	**Controller firewall and SIS-IPD Extended Temperature/Conformal Coating**
Operating Temperature	0°C to + 60°C (+32°F to +140°F)	-40°C to +70°C (-40°F to +158°F)
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 (≈ +6561 ft (+2000 m)) maximum 1060 hPa (≈ −1312 ft (−400 m))	
Air Pressure Storage	minimum 700 hPa (≈ +9842 ft (+3000 m)) maximum 1060 hPa (≈ −1312 ft (−400 m))	
Laser Protection	Class 1 in compliance with IEC 60825-1.	
Degree of Protection	IP20	

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 0.14 in. (3.5 mm) amplitude. Marine: 2 Hz... 13.2 Hz with 0.04 in.(1 mm) amplitude. Standard: 8.4 Hz ... 150 Hz with 0.04 oz (1 g). Marine: 13.2 Hz ... 100 Hz with 0.03 oz (0.7 g).

Approvals (all Models)
CE - 2004/108/EC (EMC) - 2011/65/EU (RoHS)
CSA C22.2 No. 213 Canadian National Standard(s) for Non-incendive Electrical Equipment for Use in Class I, Division 2 Hazardous Locations.
C-Tick
EAC (F/K/A GOST)
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.
IEC 60825-1 Safety of Laser Products.
ISA 12.12.01, United States Standard for Safety for Non-incendive Electrical Equipment for Use in Class I and II, Division 2 and Class III, Divisions 1 and 2 Hazardous (Classified) Locations.
cUL 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: Germanischer Lloyd (GL).

DeltaV Controller and Workstation Usage	
Controllers Supported	DeltaV v8.4 or higher. Up to 8 controllers or 8 redundant controller pairs and up to 16 CHARM I/O Cards per controller (128 CIOCs) 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 controller firewalls. For more than 8 controllers or 8 redundant controller pairs, more firewalls must be installed in parallel.
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 Controller Firewall	
DeltaV Controller Firewall- standard temperature range (0°C to +60°C) – Controller Port Twisted Pair RJ45/Workstation Port Twisted Pair RJ45.	VE6203-1
DeltaV Controller Firewall- extended temperature range (-40°C to +70°C), ATEX, conformal coating – Controller Port Twisted Pair RJ45/ Workstation Port Twisted Pair RJ45.	VE6203-2
DeltaV Controller Firewall- standard temperature range (0°C to +60°C) – Controller Port Twisted Pair RJ45/Workstation Port Fiber Optic Multimode SC.	VE6203-3
DeltaV Controller Firewall- extended temperature range (-40°C to +70°C), ATEX, conformal coating – Controller Port Twisted Pair RJ45/ Workstation Port Fiber Optic Multimode SC.	VE6203-4
DeltaV Controller Firewall- standard temperature range (0°C to +60°C) – Controller Port Twisted Pair RJ45/Workstation Port Fiber Optic Singlemode SC	VE6203-5
DeltaV Controller Firewall- extended temperature range (-40°C to +70°C), ATEX, conformal coating – Controller Port Twisted Pair RJ45/ Workstation Port Fiber Optic Singlemode SC	VE6203-6
DeltaV SIS-IPD	
DeltaV SIS IPD - standard temperature range (0°C to +60°C) – Controller Port Twisted Pair RJ45/Workstation Port Twisted Pair RJ45.	VS6203-1
DeltaV SIS IPD - extended temperature range (-40°C to +70°C), ATEX, conformal coating – Controller Port Twisted Pair RJ45/ Workstation Port Twisted Pair RJ45.	VS6203-2
DeltaV SIS IPD - standard temperature range(0°C to +60°C) – Controller Port Twisted Pair RJ45/Workstation Port Fiber Optic Multimode SC.	VS6203-3
DeltaV SIS IPD - extended temperature range (-40°C to +70°C), ATEX, conformal coating – Controller Port Twisted Pair RJ45/ Workstation Port Fiber Optic Multimode SC.	VS6203-4
DeltaV SIS IPD - standard temperature range (0°C to +60°C) – Controller Port Twisted Pair RJ45/Workstation Port Fiber Optic Singlemode SC	VS6203-5
DeltaV SIS IPD - extended temperature range (-40°C to +70°C), ATEX, conformal coating – Controller Port Twisted Pair RJ45/ Workstation Port Fiber Optic Singlemode SC	VS6203-6
Note: Except for being 0.5 inches wider these products are functionally drop in replacements for the VE6201 Controller Firewall and VS6201 SIS-IPD products.	

Emerson Process Management
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
www.emersonprocess.com/deltav

DELTAV™

EMERSON™
Process Management