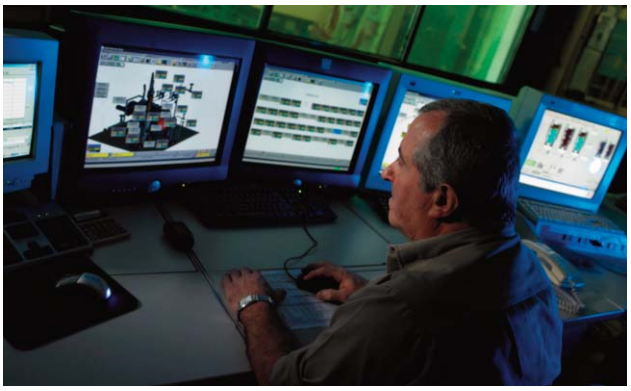
DeltaV™ Cyber Security Solutions

A Guide to Securing Your Process



A long history of cyber security

In pioneering the use of commercial off-the-shelf technology in process control, the DeltaV digital automation system's developers always understood the critical role of cyber security in this environment. From its very beginning, the DeltaV system's designers incorporated control system security as a fundamental part of their design criteria. Today, Emerson continues to improve and enhance the DeltaV system's cyber security solutions as ever more sophisticated cyber threats proliferate.

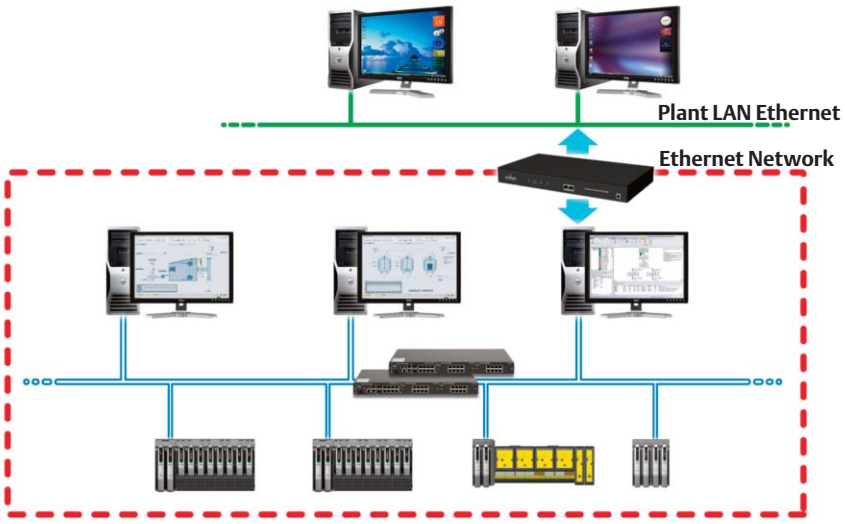
These threats have created the need for a control system able to comply with the more rigorous security policies that are being issued by process manufacturers to help protect their systems. These security policies serve as guidelines to help protect their systems while providing details that can be used to audit the systems' security level. DeltaV cyber security solutions will help you comply with the latest security policies and create a more secure control system to protect your process from cyber threats. DeltaV cyber security solutions listed in this document are presented in the context of answering the "best practice" security policies used by many companies.

Policy: The Control system must be segmented from other LANs and network devices must be authenticated to join the network.

Secure DeltaV control network

"Built for purpose" and easy to implement—the foundation of a secure network

The foundation for system security is a process control network that is segmented from other LANs in the facility. Many systems simply use network routing to create this segmentation. But this can leave the control system vulnerable.



DELTAV

EMERSON™
Process Management

The DeltaV system enforces segmentations by using a private Ethernet network so the network stays segmented from other LANs. The DeltaV system creates a "built for purpose" control network specifically designed for process control applications. All DeltaV workstations and controllers must authenticate on the network before they can participate in process control communications. This authentication prevents rogue devices from "pretending" to be DeltaV workstations.

Policy: Networks must be protected by properly configured firewalls.

Secure your network perimeter with the Emerson Smart firewall

The latest technology to help you create the most secure system perimeter

Firewalls are an important element in securing the network perimeter from intrusions. Deploying firewalls typically requires configuration by "experts"; and an improperly configured firewall can leave your network vulnerable. The Emerson Smart Firewall is specifically designed for use with the DeltaV system to make firewall deployment both easy and secure.

The preconfigured DeltaV application list makes protecting your system easy as point and click. Simply select the desired DeltaV applications and the firewall will automatically create the firewall "rules" to permit only these authorized communications with the DeltaV system. (Available early 2012)

Policy: Unused switch ports must be disabled to prevent unauthorized network connections; networks should be monitored for security incidents.

Monitor and protect your network with DeltaV Smart Switches

Built for purpose with security features to protect your network and alarm on security incidents

DeltaV Smart Switches help secure your system using auto port lockdown and built-in security event alarming. Port locking provides operations personnel an easily-accessible and easy-to-use method to insure all of your unused network ports are locked down—preventing unauthorized access to the network.

Port locking provides easy access to operations personnel and easy-to-use method insuring all unused network ports are locked down.

If an unauthorized device is connected, the switch will reject the connection and provide indication that a security breach has occurred. The switch alarms if excess communications traffic is detected, indicating that a possible denial of service attack is occurring, so a threat can be quickly mitigated.

The Smart Switch provides internal network diagnostics and network event alarming so you no longer have to rely on external SNMP applications for network monitoring and alarming. This eliminates the need for external network monitoring and helps create a more secure perimeter.

"Built for purpose" to protect your networks and processes.

Policy: Only secure protocols should be used for external communications with the control system.

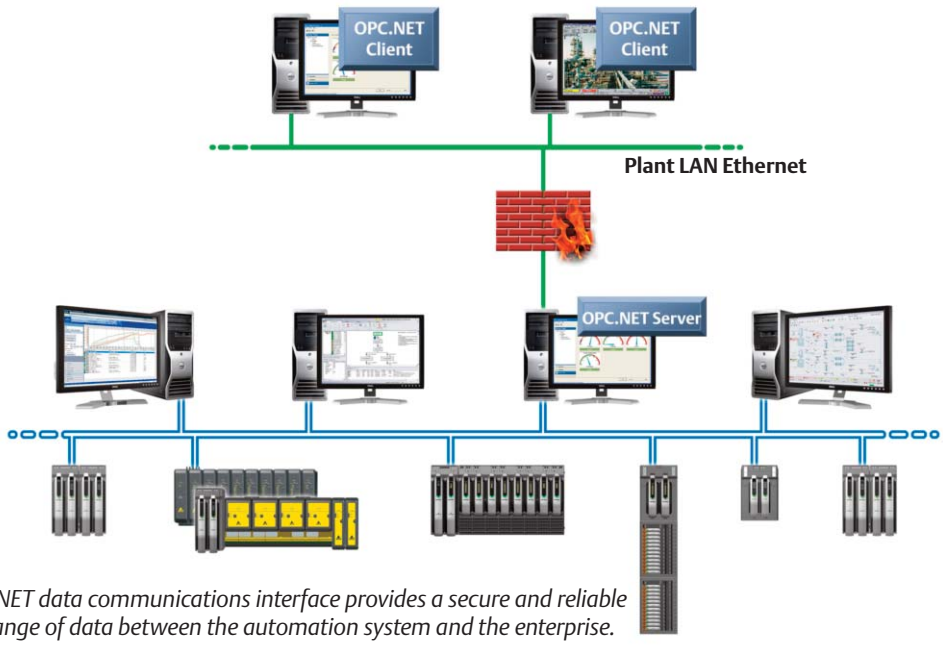
Easily create secure communications using OPC.NET

Windows .Net-based interface that addresses classic OPC security issues

OPC.NET is a new data communications interface developed by a diverse group of process industry suppliers to meet customer needs for a secure, firewall-friendly, reliable, and standardized way to exchange data between the automation system and the enterprise.

OPC.NET provides a standard .Net interface for real-time and historical process data and alarms and events data access. OPC.NET is interoperable with new .Net-based applications and existing OPC COM-based clients and servers to deliver a secure data communication path—even on legacy systems.

OPC.NET is based on Windows Communication Foundation (WCF), the latest communications technology from Microsoft. It enables fast and efficient data communications between Windows-based clients and servers, and delivers secure and reliable data communications through firewalls and to non-Windows systems. OPC.NET solves the security issues associated with using classic OPC communications through a firewall.



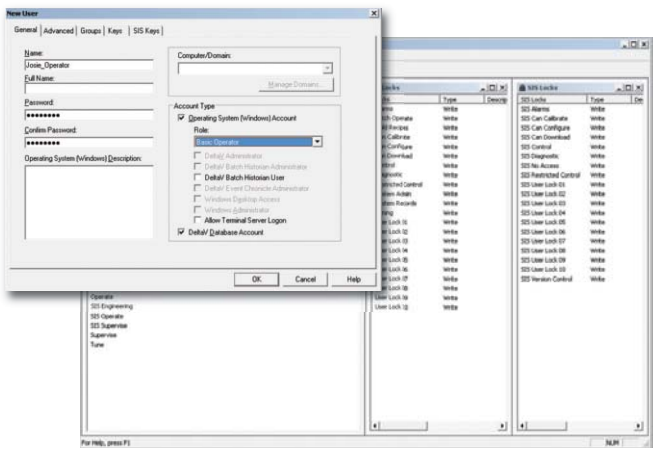
OPC.NET data communications interface provides a secure and reliable exchange of data between the automation system and the enterprise.

Policy: Each user must have a user name and password; role-based user access should be used to assign user privileges based on the user's job function, and separation of duties must be maintained for critical functions.

Easy and flexible User Management

Role-based user access makes it easy to create users with exactly the right privileges

The DeltaV User Manager makes it easy to implement DeltaV user access security built on the proven Microsoft password management capabilities and Active Directory. Coupled with the DeltaV role-based user access, the DeltaV User Manager provides the tools to make sophisticated role-based user administration easy to implement and manage. Pre-defined user access groups make it easy to assign users the right privileges for their jobs. Group privileges can be modified or new groups can easily be created to meet specific needs. Users can be given privileges site-wide or segmented by plant area. Making it easy to create users with operating privileges in one area and view-only privileges in other areas to maintain a secure span of control for plant operations. DeltaV roles support "separation of duties" so that a critical task cannot be performed by just one person. For example a person making configuration changes may not be allowed to implement the changes without a second person authorizing the implementation.



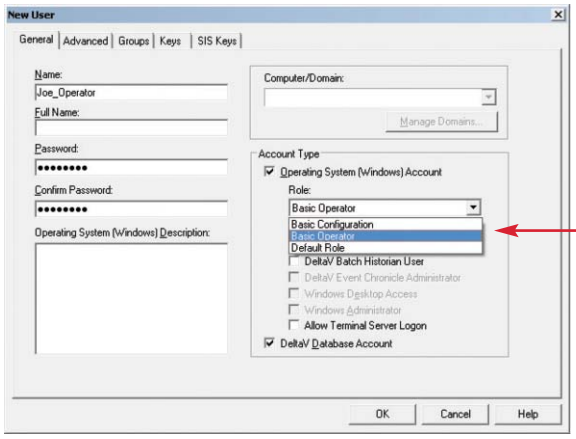
Policy: Users should access the system based on "least privilege" user access.

Easily assign users the most secure Windows privileges

The pre-built Windows security groups makes it easy to create restricted users to protect your workstations

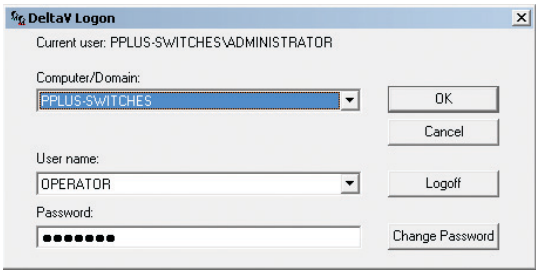
Fundamental to creating secure user access is to insure that users run under Windows with "least privilege" —having only those privileges required to do their jobs.

The pre-built DeltaV user role of "Basic Operator" makes it easy to create restricted users—just assign the user(s) to this role and they automatically become a restricted user. This user role has pre-defined privileges and is tested to ensure that users will be able to perform all of the operator or maintenance functions. They're locked out of workstation functions they do not need to access as part of their normal job functions. There are also other user roles available that allow users to create customized Windows security groups to meet a variety of user access requirements. In a properly secured system most users will be designated as "restricted users"—those who have access only to specific applications and operating system functions. Preventing accidental or deliberate damage to critical workstation files. Restricted users do not have privileges to install programs, thus preventing malware from being installed on the workstation, preventing the risk of infection. Restricted users do not have access to portable media devices such as floppy drives, DVD or CD drives or USB ports where malware could be introduced into the workstation.



"Basic Operator" makes it easy to create restricted users.

Policy: Users must log in to the system using a unique user name and password. Two factor authentication should be used to secure access on critical workstations. Operator workstations should auto-start to the operator interface application to limit access to the operating system functions.



Help users stay secured

Provide secure access to DeltaV workstations

DeltaV technology makes it easy to comply with security policies that require individual user log-in for system access—without impacting user response to critical control functions. DeltaV operators can easily "switch users" during shift changes without shutting down critical control applications as they log out and in to the system. The DeltaV system provides the option to auto-start the operator interface for streamlined, secure user log-in process. The DeltaV system provides enhanced user security by supporting two-factor authentication using Smart Cards.

Solutions to protecting your process from cyber threats.

Policy: Workstations shall implement operating system hardening strategies to reduce the attack points in the system.

Cyber harden your DeltaV Workstations

Use government-approved operating system parameters to secure your workstations

Best practices for cyber security dictate that Windows-based workstations have operating system parameters configured to the most secure settings. The Center for Internet Security (CIS) is one well respected provider of these secure settings used to harden the Microsoft operating system against cyber attack.

DeltaV technologists have tested a set of CIS-approved secure settings on system workstations for Windows 7 and for Server 2003 and Server 2008. These hardening settings are applied to DeltaV workstations to help you meet site security policies. In DeltaV v11 the hardened settings are applied as part of the standard Windows 7 and Server 2008 operating system configuration—a further step in creating a "secure, out-of-the-box" user experience with the DeltaV system.

Policy: Microsoft security updates must be applied to all workstation in a timely manner—within days of release by Microsoft.

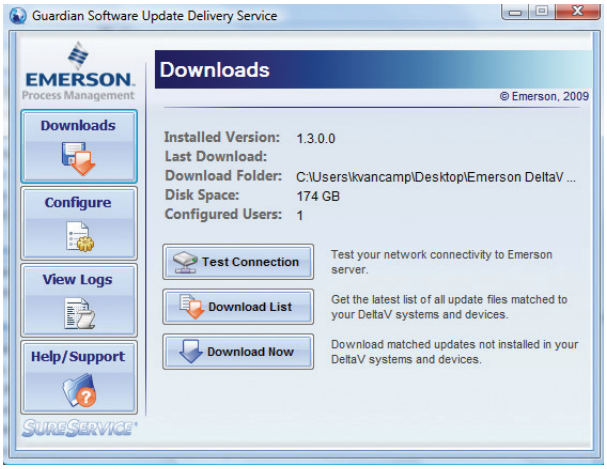
Confidently and easily apply Microsoft security updates every month

DeltaV technologists test and certify Microsoft security updates every month

Keeping operating system security updates current is an important part of maintaining a secure system. Emerson's expert DeltaV technology team tests and certifies the applicable Microsoft security patches each month and within 72 hours of release. The DeltaV system reduces the effort to maintain a secure systems by supporting the use of Microsoft Windows Server Update Service (WSUS) to automatically distribute updates to all workstations in the system.

In addition, Emerson's Guardian Support can totally automate the security update distribution and reduce the time from certification to deployment in your system to a matter of days. Using your DeltaV system information, Guardian will automatically select the correct updates for your system and ensure they are distributed to your workstations based on your patch distribution preferences.

Emerson also offers Extended Software Support to help enable your installed DeltaV system to deploy security updates and extend its lifecycle.



Guardian automatically selects the correct updates for your system and ensures they are distributed to your workstations based on your patch distribution preferences.

Policy: Anti-Virus software must be installed on all workstations and kept up-to-date with the latest threat signatures.

Confidently and easily manage anti-virus software and updates

DeltaV software supports Symantec Anti-Virus with automatic updates to all workstations

The DeltaV system supports industry standard Symantec Endpoint Protection Software, so it's easy to protect your network from malware. Every workstation can be equipped and easily managed with the Symantec scanning software and standard tools. Emerson tests to insure the Symantec software does not interfere with the proper functioning of the control system so you can be confident that protecting your system will not impact robustness. Using our instructions, you can easily automate the distribution of new signatures to all workstations based on your security policy requirements. Guardian Support can also deliver anti-virus signature updates so you only have to setup a single connection to obtain anti-virus updates, security patches, and DeltaV hotfixes. Giving you a single source to keep your DeltaV protected and up-to-date.

Policy: Process controllers must be protected from network denial of service attacks such that operator workstations never lose the ability to communicate with controllers.

Maintain operator visibility to DeltaV controllers at all times

Add an extra layer of protection to DeltaV controllers

The DeltaV Controller Firewall is a purpose-built security appliance that is installed in the DeltaV Control LAN. The firewall provides an additional layer of protection from denial of service attacks and network discovery intrusions against a DeltaV controller. The firewall will filter network communications to prevent denial of service attacks from impacting control visibility and access to essential control functions. The firewall can inhibit device discovery attempts by blocking the typical methods that hackers use to find devices to attack. If a device can't be found or open ports cannot be discovered then a security attack cannot be launched. The firewall is pre-configured for plug-and-play implementation in the network so it can be easily installed without impacting control network performance.

Policy: Process controllers should demonstrate communications robustness based on compliance to device security certification standards.

DeltaV controllers meet level one Achilles certification

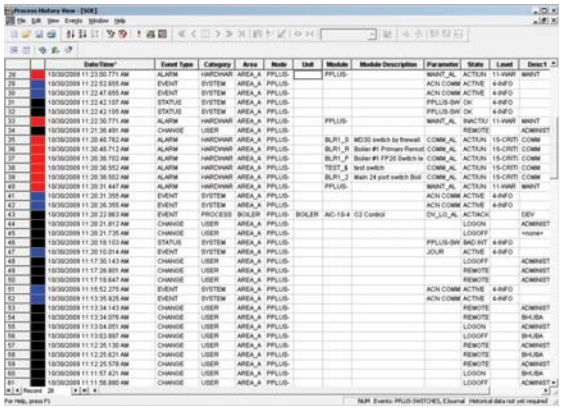
Certified protection from loss of essential control services due to cyber attacks

Achilles certification provides assurance that the DeltaV controller, when used in conjunction with the controller firewall, will maintain essential services such as control functions, process view, process alarms, and operator command functions during periods of unusual or intentionally malicious network traffic.

One of the latest cyber security advances is the ability to use automated testing to validate the security level of a device. Wurldtech Achilles certification provides assurance that the DeltaV controller, when used in con-junction with the controller

Cyber security—an essential part of your control system implementation.

firewall, will maintain essential services such as control functions, process view, process alarms, and operator command functions during periods of unusual or intentionally malicious network traffic.



All event information is easily available for consolidated analysis of security events and communications logs.

Policy: Employ tools and techniques to monitor events, detect attacks, and provide identification of unauthorized use of the system.

The DeltaV event journal logs alarms, user activities and other system events

The event journal provides easy access to control system events

The DeltaV event journal provides details of user activities on the control applications and is a great addition to the Microsoft event logs to provide significant information on security-related events happening on the DeltaV system. Windows event logs provide details on operating system events—such as failed login attempts, file access attempts and successes. The DeltaV User Manager also logs events to the Windows event log. The DeltaV event journal provides details on events specifically around the control system applications including user switching, and security alarms from unauthorized network connection attempts on locked DeltaV Smart Switches.

The DeltaV Smart Switch and controller firewall can also be configured to provide communication logs to a centralized SysLog Server so a complete picture of network communications can be monitored. All of the event information is easily available to user-selected software for consolidated analysis of security events and communications logs.

Policy: DeltaV Security services are here to help meet your unique needs meeting your security policies

DeltaV Security Services

SureServices will help you create the most cost-effective system security solution

Emerson's Security Assessment Service includes an examination of the physical and electronic security of your DeltaV process control system. The assessment is based on product security installation guidelines, best practices and site security policies and procedures.

The security assessment will establish a baseline of the process control system perimeter and internal security conditions. This baseline will include a review of the installation and security procedures used to protect the process control system from internal and external threats.

Emerson's Security Assessment Services will give you an assessment of security gaps and latent threats to the Emerson process control system, and provide prioritized improvement recommendations that can help assure your process control system's availability and operational integrity.

Additional security-related services include:

- Network security design consulting for the DeltaV process control system and associated communication interfaces
- Implementation support for security assessment recommendations
- Consultation on updating your security policy and associated documents to address the findings of the security assessment
- Periodic assessment of the system security conditions after the initial security assessment findings have been addressed.

Depend on DeltaV secure process control solutions

DeltaV cyber security solutions help you meet the most stringent security requirements while maintaining ease of use and system robustness

Creating a secure control system without sacrificing ease of use and system robustness is a major challenge and is especially important in mission-critical process control environments. DeltaV system security solutions provide an excellent balance between ease of use and security, so you can be assured of enhanced system security while maintaining the ease of use and robustness you expect from your process control system.

DeltaV security solutions follow "defense in depth" layered security practices and are designed to be compliant with emerging cyber security standards such as the "ISA SP99 Security for Industrial Automation and Control Systems". And though the standards are not fully in place, by being involved in the standards development process, Emerson is able to design security solutions that will allow customers to easily meet or exceed these standards as they are issued in the future.

Cyber security has become a necessary and essential part of control system implementation. Emerson Process Management is dedicated to helping you implement the most cost-effective security solutions possible so you can concentrate on the core business of producing high quality products at the lowest cost and remain competitive in your marketplace.

For more information on DeltaV security solutions go to *www.emersonprocess.com/DeltaV* and search on "security" or contact your local Emerson/DeltaV sales office.

To obtain information about Microsoft Security patch certifications with the DeltaV system, please contact your local Emerson/DeltaV sales office. This information is only published on the DeltaV System Support Website which requires password access.

DeltaV™ Cyber Security Solutions

Emerson Process Management
12301 Research Blvd.
Research Park Plaza, Building III
Austin, Texas 78759 USA
T +1 512.835.2190
F +1 512.832.3443
www.EmersonProcess.com/DeltaV

The information provided in this document is intended to educate the reader about some of the DeltaV security solutions available. This information represents only a portion of the activities and solutions required to implement an overall DeltaV system security solution. Emerson Process Management does not represent or warrant, and specifically disclaims any express or implied representation or warranty that the use of this information will prevent system disruption due to 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 implementation of these practices in protecting their control system.

The contents of this publication are presented for informational purposes only, and while every effort has been made to ensure their accuracy, they are not to be construed as warrantees 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 design or specification of such products at any time without notice.

Form F-00054 /Printed in USA/200 AQ/ 07-11

DELTAV

EMERSON™
Process Management