

Operations and Security

Security is becoming a more important consideration for operations. DeltaV SIS is designed to minimize typical vulnerabilities. It supports best practices, including operational features that facilitate implementation of a comprehensive security policy.



DELTA V SIS

www.DeltaVSIS.com



EMERSON[™]
Process Management

Table of Contents

Introduction..... 3

Background on Security for the Process Industry 3

 General Framework for Security Discussion 3

 Special Issues for Automated Controls 3

 Historical Perspective on Process Control Security..... 4

 Current State on Process Control Security..... 4

Special Issues for SIS and Security 5

Critical Infrastructure Assurance Office..... 5

 History of CIAO 5

 Concerns of CIAO 5

DeltaV SIS Architecture..... 6

 How the SIS Architecture addresses security 7

Summary 8

Introduction

Security has always been a relevant concern during the design and deployment of automated control systems. But recent worldwide events, combined with technological and industry trends of the last decade, have significantly raised the visibility and public awareness of this issue. Security for automated controls systems is not a straightforward topic, and it can involve many tradeoffs between ease of use and performance versus protection. Security products and methods developed for general purpose IT applications are not always effective and can even conflict with the goals and needs of automated controls. Although security needs to be addressed as part of an overall process and products alone cannot solve the overall issue, the DeltaV system and DeltaV SIS provide an architecture that promotes and facilitates good security practices. DeltaV SIS accomplishes this without difficult or unpopular tradeoffs between operating efficiency and performance.

Background on Security for the Process Industry

There are many different and sometimes inconsistent sources of information on security. This should not be surprising, as individuals will most likely have different interpretations and viewpoints on the definition and scope of security concerns. Even with consistent definitions, individual circumstances are different. Consequently, there is no one best way to ensure security. This is especially true considering that the security needs and acceptable solutions for automated control systems will differ somewhat from those in a general Information Technology environment. The SP99 committee was officially formed by the ISA in August 2002 to address these very important issues for this industry.

General Framework for Security Discussion

Security in general is often characterized as activity directed toward protecting or preserving the confidentiality and integrity of a system or an object. Confidentiality is the prevention of unauthorized release of information, while integrity is the prevention of unauthorized modifications. The scope of security may also include preserving availability to authorized users. An example of unavailability due to unauthorized usage is a denial-of-service attack used on Internet sites. Depending on the individual situation, one aspect may be more important than the other.

Security is often viewed in terms of system vulnerabilities. For control system security there are various dimensions of vulnerabilities that need to be considered: physical security of assets, data/information security and administrative or process related vulnerabilities. Physical security is related to vulnerabilities that result from physical attack to either the process control system or the system under control. Data security would include information stored within computers and exchanged over various communication paths that can be compromised by what is generally classified as a cyber attack. Administrative security is concerned with vulnerabilities due to weaknesses in administrative policies or processes. Covering any one or even two of these dimensions will typically not provide an adequate level of security. All three must be properly addressed within a unified framework. Similarly, security measures have similar dimensions for prevention, detection, and recovery for worst-case scenarios.

Special Issues for Automated Controls

There are many similarities between the infrastructure for a typical IT environment and process controls. More important, however, there are significant differences that make IT environment security measures impractical, ineffective or perhaps even dangerous for process control. Most of the technical differences are related to the real-time response requirements and highly sophisticated and specialized software running in the process control systems, which depend on advanced distributed communication and processing features. These systems may not be compatible with standard anti-virus software and may react unpredictably to standard software patches that were not specifically tested in their set of applications. Process control systems typically run twenty-four hours a day, seven days a week. This makes timely application of security patches a problem. In addition, the potential consequences of a security vulnerability can be significantly greater in the process control environment, where the result can be destruction of physical property, environmental damage, and injury to employees and the general population.

Historical Perspective on Process Control Security

Historically, process control systems were specialized with proprietary hardware, software and communications. Data links between the control system and the IT environment were either nonexistent or limited to preprogrammed connections through another proprietary system that effectively acted as a firewall. Internet access to the control system was not even an option. Security threats were normally limited to accidental actions by employees, actions by disgruntled employees, and industrial espionage. It was inconceivable that someone would try to use automated control systems to cause catastrophic damage, even if the potential existed. The control systems included basic levels of security functionality that was sufficient for the risk profile and vulnerabilities at the time. Security was achieved to an acceptable level based on lack of knowledge (proprietary systems), lack of connectivity, and the lack of any motive to cause catastrophic harm.

Over the last 15 years, lower-cost open computing platforms, both hardware and software, progressed to where they became attractive for use in process automation. The reasons for this transition were faster product development, lower costs and increased flexibility. These systems increasingly make use of commercial operating systems and communication networks. At the same time, automated control systems have become more connected to provide enterprise-level applications and ease of use. These applications drive convergence of automation and enterprise network information that are now based on compatible infrastructure, which allows direct and transparent communication pathways and collapses of the number of layers in the communication networks.

The open platforms also have security vulnerabilities that are well published and available to anyone including persons who would like to exploit them. Worldwide connectivity through the Internet has demonstrated the ability to spread malicious agents, which exploit security vulnerabilities across the globe in a time period measured in hours rather than weeks or months.

In addition, there are now groups and individuals who would like to spread fear and disrupt any feeling of normalcy with little or no regard for the value of national infrastructure or human life.

In summary, today's environment is increasingly hostile with higher levels of threat. At the same time, much of the process automation infrastructure is based on standard components with known vulnerabilities, fewer layers of protection from diverse protocols and more accessibility from outside a plant's boundary. These changes all emphasize the need for additional security for countering this trend.

Current State on Process Control Security

Most sources agree that the best security efforts systematically assess vulnerabilities and threats and develop security measures, practices and procedures. A fundamental reason for this is that security is only as strong as its weakest link. For example, the best security to cyber attack will not guarantee safety if weak or ineffective personnel procedures make an operation vulnerable to physical access.

Protection techniques against physical and administrative vulnerabilities have been developed by government and industry. Currently, however, the only guarantee of protection from exploitation of vulnerabilities in computer software and communications is full isolation of the computer.

There is an abundance of other methods to reduce risk without total isolation, but any one single level is definitely not sufficient. Multiple levels of diverse protection, where diversity ideally extends to the operating systems and other software, are the best scenario. It is also best to have multiple levels of networks separated by the previously discussed layers of protection. Other mechanisms include contingency plans based on levels of fault tolerance and redundancy, such as the ability to disconnect from higher-level communication networks and remain in operation in isolation with localized operator terminals if higher levels of the communication networks are compromised. Standard IT products should be carefully evaluated for compatibility and lack of negative side effects in this specialized environment.

Special Issues for SIS and Security

All of the issues previously discussed also apply to safety instrumented systems (SIS), but the consequences are often higher for an SIS.

The following are potential differentiators for SIS applications:

- By definition safety systems are typically associated with potential dangerous applications necessitating protection for personnel and infrastructure or the prevention of a toxic substances release.
- SIS can help mitigate a physical act of terrorism, but if its selected safety functions were covertly disabled, it could be used to enable or leverage physical acts of terrorism.
- An SIS can mitigate cyber attacks on the BPCS that could potentially result in dangerous situations unless the SIS is also able to be compromised.
- Since SIS applications are typically associated with the processes that have the highest potential for negative consequences, some experts advise securing any safety systems first, as the highest priority. This is a simplified approach and does not necessarily provide complete and sufficient coverage but is a logical starting point especially until entities such as the ISA SP99 release more comprehensive information.

Critical Infrastructure Assurance Office

History of CIAO

The US Critical Infrastructure Assurance Office (CIAO) was created in May 1998 to coordinate the federal government's initiatives on critical infrastructure assurance. The CIAO's primary areas of focus are to raise issues that cut across industry sectors and ensure a cohesive approach to achieving continuity in delivering critical infrastructure services. CIAO's major initiatives are to coordinate and implement the national strategy, assess the U.S. government's own risk exposure and dependencies on critical infrastructure and raise awareness and educate public understanding and participation in critical infrastructure protection efforts.

In October 2001, the President's Critical Infrastructure Protection Board was created to coordinate federal efforts and programs relating to the protection of information systems and networks essential to the operation of the nation's critical infrastructures.

In November 2002, the CIAO was incorporated into the Department of Homeland Security.

In February 2003, Department of Homeland Security Secretary Tom Ridge released two strategies:

- The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets that identifies a clear set of national goals and objectives and outlines the guiding principles to secure the infrastructures and assets vital to national security, governance, public health and safety, economy and public confidence.
- The National Strategy to Secure Cyberspace to engage and empower Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact.

Concerns of CIAO

The CIAO is concerned with the number of critical infrastructure components with low levels of protection, both physical and cyber. These facilities are potential terror targets, which are chosen typically by a combination of impact and level of protection. Various public concerns have been identified in the following areas related to the process controls industry:

- Electrical generation and transmission
- Control of dams and waterways

- Transportation systems
- Public drinking water
- Petrochemical facilities

The original focus for automated controls was originally on SCADA systems but has since broadened to include all aspects of automated control for the industries at risk.

At this point voluntary cooperation is being requested but there is pressure from some groups for stronger requirements.

DeltaV SIS Architecture

The DeltaV SIS physically plugs directly to a DeltaV system as a doublewide I/O module as shown in Figure 1. The DeltaV SIS represents a completely separate controller and I/O subsystem that is not in any way dependent on the standard DeltaV controller to perform its safety function. The proper operation of this subsystem is independent of the railbus communications and has its power supplied by an independent source. Railbus is used only for maintenance activities and to provide visibility of the SIS variables to Operator Stations. In addition the SIS has an internal firewall on the railbus interface to insure that it cannot interfere with safety functionality.

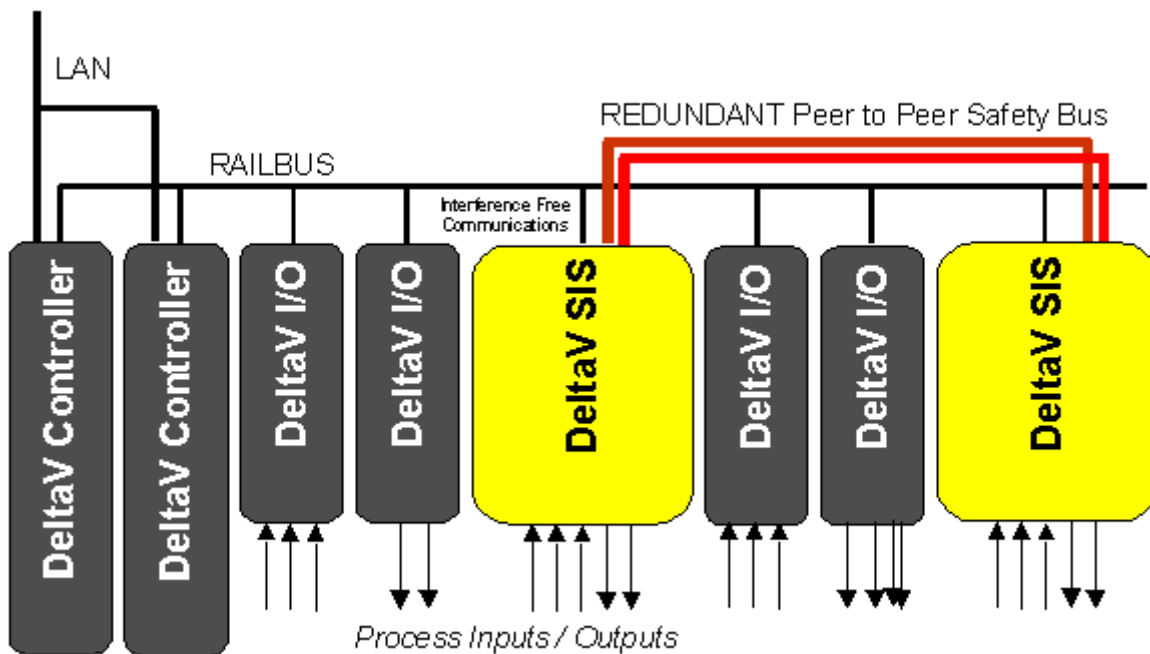


Figure 1 DeltaV System with SIS

In addition to the independent safety controller, the DeltaV SIS has its own dedicated and safety rated I/O points, 16 for each SIS module. Although rare, a safety integrity function that requires more than 16 I/O points can use I/O points and other information from other SIS modules under the same DeltaV controller accessed through the dedicated Peer to Peer safety critical communications channel. The Peer to Peer Safety Bus physical layer is fully contained and limited to the scope of one DeltaV controller and its DeltaV I/O backplane. It uses a proprietary time slot and fully deterministic protocol.

Figure 2 shows the higher level architecture that extends beyond the scope of a single DeltaV controller. The Peer to Peer network can optionally be expanded to transfer Boolean type variables between DeltaV SIS modules under different DeltaV controllers in diverse locations. This is accomplished by use of Message Propagation Gateways, (MPG) with an extension of the proprietary deterministic protocol over fiber optic cables. The Advanced Control Network uses standard Ethernet communications and provides connections between the DeltaV controllers, operator terminals, and engineering tools, but it does not provide any direct connection to the DeltaV SIS modules.

All external non-safety communications with the DeltaV SIS must pass through filtering and verification functions in the DeltaV controller and the firewall within the DeltaV SIS. In addition to the Operator Station, other engineering tools contain extensive configurable levels of access control. This is based on the already familiar and easy to use DeltaV security with extensions to support differentiated access control appropriate for SIS applications.

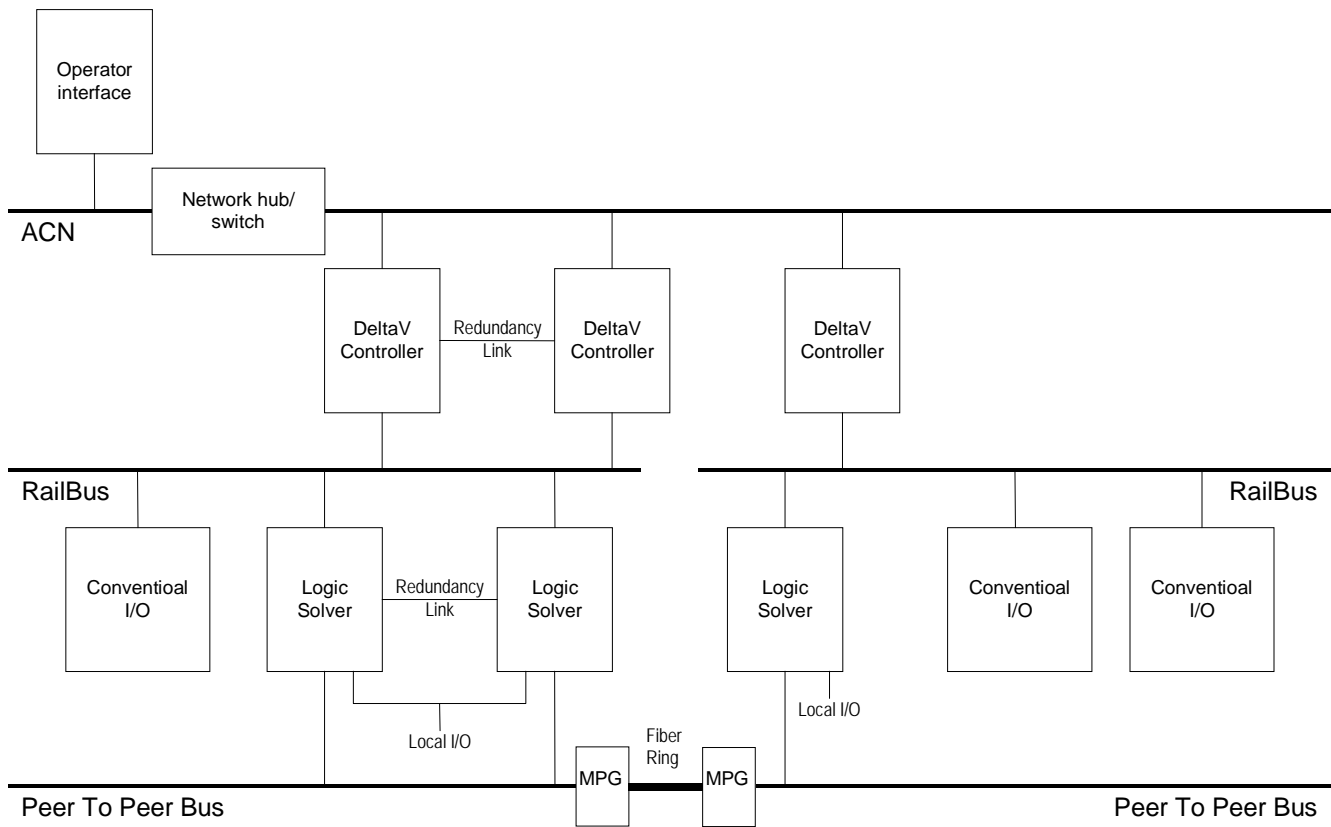


Figure 2 DeltaV / DeltaV SIS High Level Architecture

How the SIS Architecture addresses security

The design of the DeltaV SIS addresses each of the three dimensions of vulnerability.

The fully integrated DeltaV SIS module is designed to be located in the vicinity of the equipment being monitored and controlled and eliminates the need to run I/O or communication wiring outside the immediate area and the Peer to Peer Safety bus has no easy access point which facilitates physical security measures. The DeltaV controller and its railbus communications also only exist within a limited distance with no easy access point and can easily be fully contained with simple physical security barriers such as secured cabinets.

The full featured selection of security controls with differentiated levels of security for basic and SIS control in the operator terminal and engineering tools should be compatible with whatever administrative policies are adopted as part of a security program implemented for the site.

The data integrity of the DeltaV SIS over communication networks is protected by various measures at the exposed interfaces.

The Advanced Control bus has no direct access to the DeltaV SIS module. All communications from the Advanced Control bus to the DeltaV SIS must pass through the DeltaV controller where they are screened and verified to be valid prior to being passed to the DeltaV SIS over railbus, where they are then subject to a special firewall specifically designed to prevent interference with safety operations from the railbus interface. This firewall even includes features to prevent denial-of-service attacks from a large number of valid messages being used to disrupt its operation.

The data integrity of safety critical communications is protected by the following measures:

- The Peer to Peer physical layer is physically protected from easy access and is confined to small distance, which is easily secured by additional physical means of protection.
- The Peer to Peer protocol ensures deterministic communications that can not be disrupted without detection.
- The Message Propagation Gateways extend the physical layer over fiber optics, which is difficult to tap.
- The Message Propagation Gateway protocol continues the deterministic communications which identify any loss of integrity whether caused by random hardware failures or intentional attempts to compromise the system.

Multiple layers of integrity checking protect the stored configuration. Downloads are subject to a secure authorization and verification mechanism and the integrity of the stored configuration is checked periodically and would detect any modifications that were made by some unknown means, including hardware failures.

Summary

Although security has always been a relevant concern for design and deployment of automated control systems, recent worldwide events combined with technological and industry trends of the last decade have significantly raised the visibility and public awareness of this issue. The concerns are not unfounded as multiple industry trends contribute to increased vulnerability at the same time as potentially increasing threats. The issues involved with electronic computing vulnerabilities are especially difficult and dynamic at this point in time. The SP99 Committee was officially formed by the ISA in August 2002 to address the lack of reliable information and standards for security issues in this industry.

Security products and methods developed for general purpose IT applications are not always effective and at times in conflict with the goals and needs of automated controls. Security needs to be addressed as part of an overall process. While products alone cannot solve the overall issue, the DeltaV and DeltaV SIS design and architecture promotes and facilitates good security practices. DeltaV SIS accomplishes this without the need for difficult or unpopular tradeoffs of operating efficiency or performance. In many ways the DeltaV SIS architecture reverses many of the recent trends that have increased security vulnerabilities plus includes sophisticated and configurable authentication and authorization capabilities.

In a limited resources environment many recommend first securing the highest risk areas, which are typically the ones with an SIS, while waiting for better guidance from SP99 and other groups.

This page intentionally left blank.

To locate a sales office near you, visit our website at:

www.DeltaVSIS.com

Or call us at:

Asia Pacific: 65.777.8211

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: 65.777.8211

Europe, Middle East, Africa: 48.22.630.2443

North America, Latin America: +1 412.963.4000

© Emerson Process Management 2009. All rights reserved. For Emerson Process Management trademarks and service marks, go to:
<http://www.emersonprocess.com/home/news/resources/marks.pdf>.

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 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 design or specification of such products at any time without notice.



DELTA VSIS

www.DeltaVSIS.com



EMERSON[™]
Process Management