DeltaV System Cyber-Security

This paper describes the system philosophy and guidelines for keeping your DeltaV System secure from Cyber attacks.

Table of Contents

Figures

Introduction

There are many ways a plant process and a control system can be attacked, disrupting production and causing equipment damage or more severe consequences. This whitepaper will focus on reducing the probability of attacks to the control system by persons inside or outside the customer organization, who deliberately attempt to 1) improperly manipulate the system, 2) cause the system to malfunction in some manner, or 3) disrupt the proper behavior of the control system.

This whitepaper outlines the system philosophy, guidelines and rules for providing cyber-security to the DeltaV digital automation system. This document covers the DeltaV overall cyber-security policy and provides information on the handling of specific aspects of system cyber-security. For a detailed list of security best practices for a DeltaV automation system, please see the whitepaper "Best Practices for DeltaV Cyber-Security."

Control System Cyber-security is Required

Process control systems have traditionally been built on proprietary technology. This proprietary system provided a reasonable level of security from unauthorized access due to its closed nature and its lack of standardized, well-known connection methods to business networks. However, proprietary systems have become the exception, and systems are becoming open and connected.

Control system implementation continues to move toward the use of off-the-shelf technologies such as Microsoft Windows operating systems and standard, open Ethernet communications for reducing the costs of deploying the system and for facilitating ongoing maintenance. In addition, the use of open technologies has allowed the system to be more easily connected to the enterprise or plant LAN to exchange information and allow remote access to improve business performance. Being connected is no longer an option but a requirement for a successful business.

The use of open technologies exposes the control system to the same types of security issues as the plant LANs. Viruses, worms, malware and direct attacks by individuals are all possible in this new world of open control systems, just as they are with any other open LANs.

Attack Potential is Rising

Viruses, worms and other malware can infect a system and cause workstations, controllers or the entire system to perform badly. They can also corrupt a workstation or controller entirely. They can take over a computer or controller and cause it to perform unauthorized actions or to launch attacks on other computers on the network. Compromised networks, workstations or controllers can cause a loss of view to the process or disrupt control actions to the point that the process may have to be shut down to repair the control system. Disrupting the system can cause process upsets, damage equipment, create possible safety issues, and cause poor product quality. Ridding operations of infections and repairing infected computers can be time-consuming and costly.

Direct attack potential from persons outside the network is also increasing due to the ease of attack and the increasing number of participants involved. Direct attacks can affect workstations, and they can also affect process controllers through denial of service attacks and other communications disruptions.

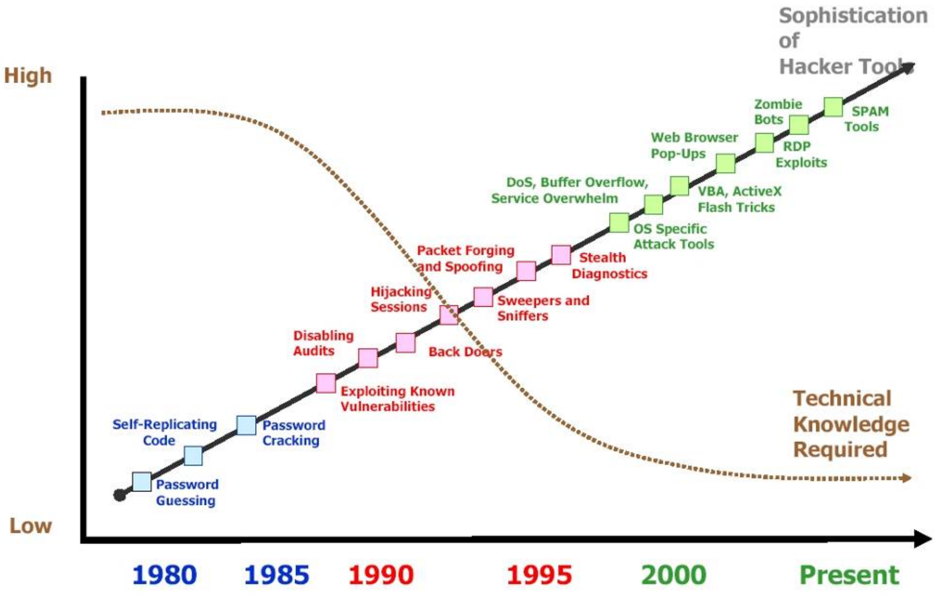

Figure 1 - Sophistication of hacker tools

Hackers and malicious individuals range from the teenage “joy-hacker” to sophisticated, sponsored, and funded professionals out to cause serious damage. Hackers have increasingly easy-to-use tools and software to aid them in their destructive efforts. Figure 1 shows how hacking has gotten easier over the years.

To avoid unnecessary repetition, the term “attack” will include viruses, worms, malware, trojans and other automated intrusion-enabling software, as well as manually directed attacks by persons outside the control network.

Threats are Coming from External Agents

In the last few years, the location of threat agents has changed. In the past, much of the problem was attributed to people internal to the plant, such as disgruntled employees or just accidental or inadvertent actions that caused system disruptions. Recent security incident analysis is showing that the current threats are coming more from people outside the plant than inside. This trend is also indicative of the increasing number of people trying to break into systems, the ease of use of their tools, and the increasing sophistication of the “hackers” themselves.

Figure 2 shows the shift in agent location of the people trying to disrupt systems.

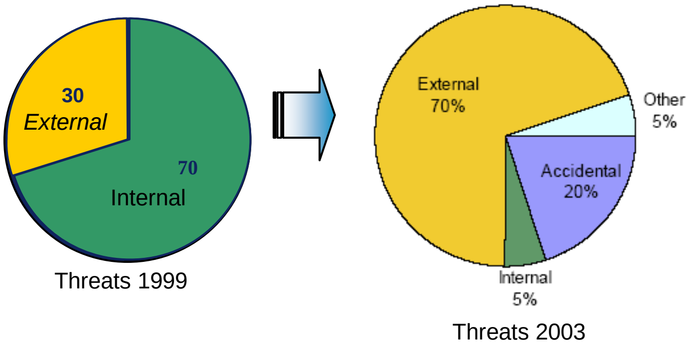

Figure 2 - Threat agents are becoming more external

Security Basics—Rings of Protection

A recognized, common security technique that is employed in the protection of assets is called "rings of protection" (this may also be called "defense rings", "layered security" or "security zones"). Figure 3 is an illustration of this protection. This model works for both physical protection and cyber-protection. An intruder must get past successive layers of protective devices and hurdles to get to the important parts of a system, the purpose being that, as intruders find it more and more difficult to successfully attack a system, they will abandon their efforts and look for easier prey. Much of the security protection is provided by good security practices used in the facility or site—including site physical security and plant LAN network access security.

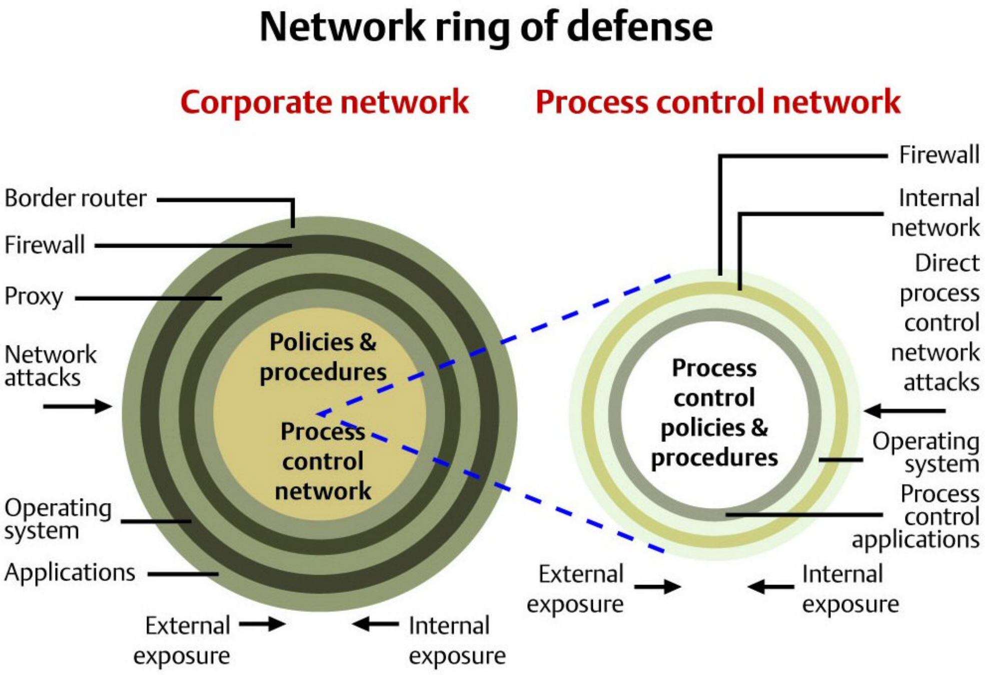

Figure 3 - Rings of protection make it difficult for intruders to penetrate the system

Security Basics—Defense in Depth

Defense in depth (DiD) is a variation on the rings of protection scheme. As the different security rings are in place there is also protections enabled within the rings. A physical security example might be guard dogs loose between two sets of perimeter fences. In a cyber-security configuration, installing an intrusion detection or prevention system within the LAN after a firewall allows the system to detect and/or stop breaches of the perimeter firewall.

DeltaV Security—Protection Rings and Defense in Depth

As in the example in the previous section, the foundation of DeltaV protection is based on placing the DeltaV network at the center of a “protection ring” or protection layers and providing as much system isolation as possible. Figure 4 (page 7) shows how this isolation can be achieved using our best-practices guidelines.

Placing the DeltaV automation system at the “center of the ring” or 2 or 3 zones within the plant LAN is to protect the control LAN from attacks originating in the plant LAN network space. This is very different from a typical IT security strategy where the protection direction is to protect the plant LAN from “edge devices” such as client workstations where attacks tend to originate from email and web-introduced viruses, worms and other malware. A properly configured DeltaV system is not an edge device and, if properly secured, will not be an avenue of attack to the plant LAN. The security strategy for a DeltaV automation system is to protect the system from attack from both the plant LAN and by direct access to the control system itself by properly managing user and network access to the system.

In a typical business network a client/user workstation has direct access to email and mostly unrestricted access to the World Wide Web. This direct access, even if properly filtered and monitored, can allow attacks to the plant LAN nodes using the client workstations. An attacker using the Internet access can make intrusions to the plant LAN from the client workstations. A typical intrusion path is from the plant LAN Internet connection into a client workstation to attack the plant LAN from this client station. Automated attacks can also come from a malware program running on a client station.

In a DeltaV system, the workstations do not have email or Internet access and do not provide an attack path to the plant LAN. The CD-ROM, diskette drives, and USB ports can be disabled to prevent the introduction of malware resulting from unauthorized use of these devices.

The Role of DeltaV System Architecture in Cyber-Security

To aid in understanding DeltaV security, it is necessary to understand that the DeltaV system is supplied as an automation system made up of specific tested and supported hardware components, software components and specific configurations of the equipment. It is not a loose collection of the off-the-shelf hardware and software components built into a system by the end user or integrator. The DeltaV digital automation system is a specific set of hardware and software (some of which is off the shelf), assembled and configured into a self-managed, private control network and automation system.

The DeltaV system is always configured as a dedicated, private control network. DeltaV does not support direct network connections between a plant LAN and the control LAN; it does not permit an outside, non-DeltaV LAN connection direct to a hub or switch on the DeltaV network. All external network connections must be made through a DeltaV workstation with a firewall-capable router or router and separate firewall device between the workstation and the plant LAN. DeltaV system security philosophy and implementation depends on this network isolation. No network segmentation using switches or routers to segment the DeltaV system from the plant LAN or other process LANs is allowed.

Figure 4 (page 8) showing the layer-protection architecture also depicts a typical DeltaV system showing connections to plant field devices and interfaces to the plant LAN. Note that the only connection to the plant LAN (or other non-DeltaV LAN) is through a DeltaV workstation using a router/firewall device to isolate the system from the plant LAN workstations. There are no plant LAN connections made at the network device level within the control system network.

In a DeltaV network, complete isolation from a non-DeltaV LAN, except by making a connection through a workstation, is necessary for proper deployment of a DeltaV system. It is much more than a best practice: it is required for the installation of a DeltaV system.

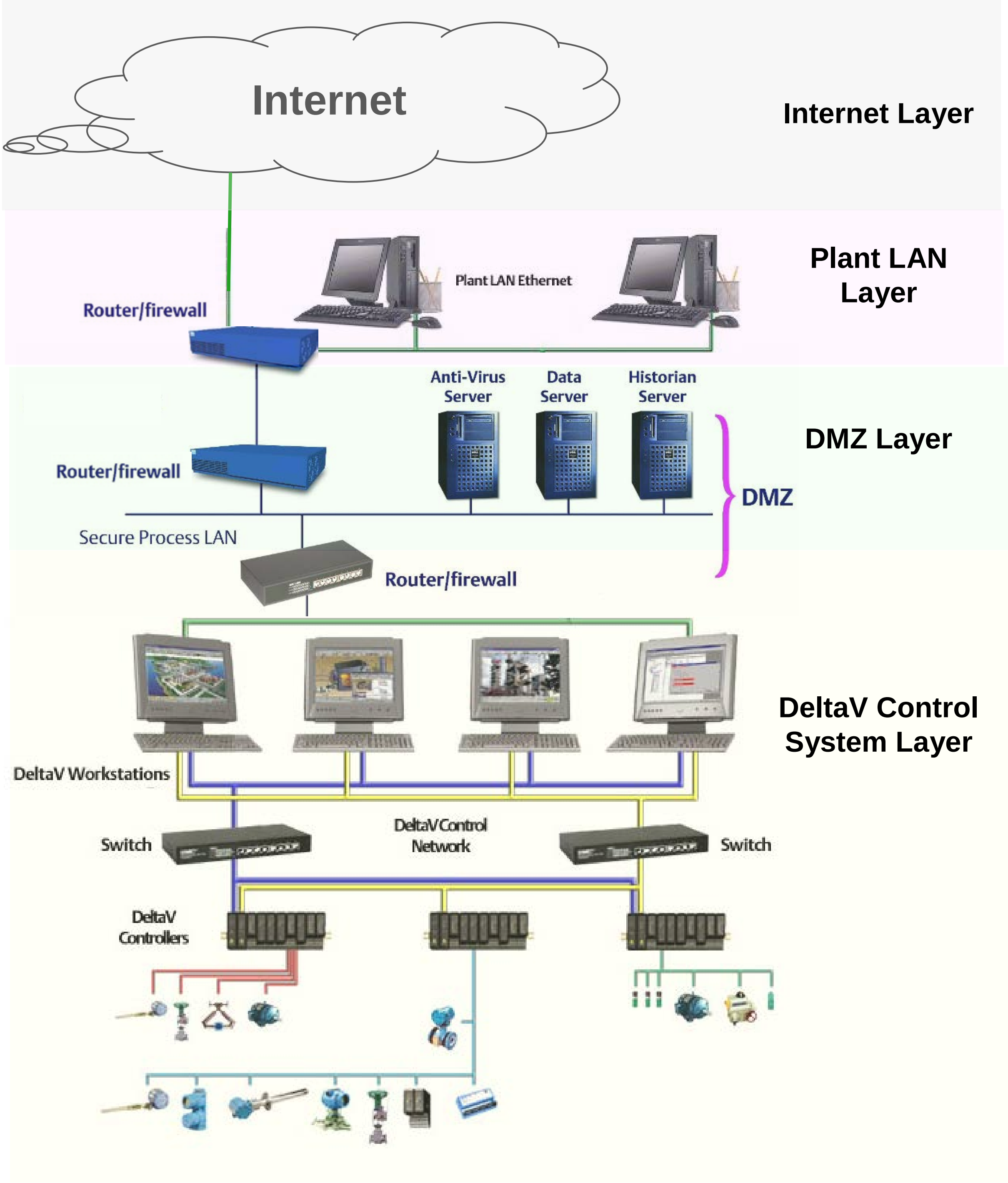

Figure 4 - A layered network configuration provides the basis for a sound security plan

Control System Availability—a High Priority for Security Implementation

Another requirement of control system security is that it must not negatively impact system robustness and up-time. Included in this is ease of maintenance where easy and rapid replacement of system equipment is critical. Implementing system security using network equipment that requires a complex setup of the configuration to maintain both security and system communications should not be deployed because improper configuration can cause the control system to fail.

The following three factors—confidentiality, integrity, and availability—are generally accepted in terms of system security in the following order of importance :

- Confidentiality refers to limiting information access and disclosure to a set of authorized users and preventing access by or disclosure to unauthorized users.

- Integrity refers to the trustworthiness of information resources. It includes the concept of "data integrity" – i.e., that data has not been changed inappropriately.

- Availability refers to the availability of information resources including the uptime of the system.

In a control system environment, this order is exactly the opposite.

In a control system:

- Maintaining the system availability is paramount.

- Data integrity on the communications network is a close second in priority.

- Confidentially is the third priority concern.

These goals are important, but in the control system world our security efforts must be directed with a different priority than in the typical information world. When trade-offs on control system security must be made, decisions generally must be made for what is best in keeping the control system available versus what protects the confidentially of data.

This translates into control system security practices such as user-password-lockout parameters, implementing operating system patches correctly, and not setting up network security features (such as MAC address filtering or VLANS) within the control system network itself. If not done properly, this will impact the ability of the control system devices to communicate with each other.

Also, corporate information technology policies and procedures must either be amended or revised for use in the control system or a new, specific set of security policies and procedures specifically for the control LAN must be implemented.

For DeltaV users, it is critical that the network be set up using current DeltaV installation instructions and using only those network device features supported on the DeltaV LAN to maintain system availability and maintainability.

DeltaV Security Features

- Basic system security for a DeltaV system is relatively easy to implement and monitor. A list of best practices for securing a system is listed in the whitepaper “Best Practices for DeltaV Cyber-security*”.*

- The DeltaV system has been developed with system security features as a main design criterion. The system has many features that provide a level of built-in security.

- The system has inherent system isolation—it is designed to run on an isolated network separate from other LANs.

- The DeltaV system uses a proprietary protocol for control system communications.

- Connections to other LANs are not required for the proper functioning of the control system.

- The DeltaV system supports physical configurations with equipment located in locked down enclosures, with system diagnostics and administration done over the network. Local equipment access is not required for routine maintenance procedures or system troubleshooting.

- Authentication and authorization:
    - User authentication is based on a separate DeltaV user manager and passwords.
    - Users have role-based authorization to perform only specific tasks within the DeltaV system.
    - DeltaV devices are authenticated as part of system configuration and must be specifically installed to act as a DeltaV workstation or controller. Unauthorized workstations cannot participate in DeltaV communications.

- DeltaV tests and supports anti-virus software on the workstations as an added level of security.

- DeltaV tests and certifies Microsoft security patches each month to maintain system integrity.

- DeltaV controllers have been hardened to mitigate specific, well-documented hacker attacks.

- DeltaV workstations are hardened as part of the DeltaV install procedures to disable specific operating system services that are not used by the system. In addition, DeltaV runtime does not require access to floppy or CD-ROM drives or USB ports. Therefore, these devices can be disabled to further harden the workstation computer.

Getting Started with DeltaV System Cyber-Security

There are a few basic activities that need to be done as part of implementing system security.

- Start with a risk analysis of the control system. Establish a “system boundary” for the DeltaV system and determine what you are doing or what can be done to protect against unauthorized intrusions across this boundary.

- Decide how secure you need to be. One method is to look at cost-to-implement versus security requirements. Another is to review the probability of attack versus consequences of a successful intrusion. An isolated system has a much lower chance of being attacked.

- Organizations also must implement good policies and procedures and carefully select technologies. Ultimately, security is a process, not just a technology solution, and most, if not all, unauthorized access events can be prevented through enforcing good discipline and practices in a process control environment. Enforcing desirable, consistent, and effective behavior is key to improving and maintaining security

- Searching the web for "SCADA security" or "control system security" will yield many citations with details on these and other system security issues. Note that SCADA is a generic term used by the government and other institutions for any process control-related system. Some suggested sites are:
    - http://www.sandia.gov/scada/home.htm Sandia National Labs site
    - http://www.dhs.gov/dhspublic/display?content=4359 Dept. of Homeland Security
    - http://www.isd.mel.nist.gov/projects/processcontrol/ NIST process control security
    - http://www.niscc.gov.uk/niscc/scada-en.html UK cyber security site
    - www.inl.gov Idaho National Labs
    - www.isa.org ISA Site – search for security
    - http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821 ISA SP99 system security committee – report 1 and 2 have information on system security.

Summary

There is no silver-bullet procedure or technology that can be done once in creating a secure control system. System security is a lifestyle change, not a diet. Maintaining a secure DeltaV system requires planning, ongoing assessment, and some amount of effort to ensure that security policies are observed and that all users are trained and educated on the security policies and procedures. The DeltaV system with its dedicated, isolated, private control LAN provides an excellent foundation for maintaining a secure system. From this foundation we can implement layers of security technology and develop the appropriate plant/site/process level security procedures to help maintain a cyber-protected system.

This page intentionally left blank.

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

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.