Innovative Defense Strategies for Securing SCADA & Control Systems

By: Jonathan Pollet
PlantData Technologies, Inc.

Keywords

Abstract

Over the past few years, most companies with critical infrastructure controlled by SCADA, DCS, and other process control systems have taken the approach to group all of their real-time systems in an environment called the PCN or process control network, and try to keep that environment as separate and isolated as possible from the IT and corporate networks. While this concept is a move in the right direction, treating the PCN environment like a black box and trying to manage one firewall or cyber defense solution at the border with IT is not adequate to protect from changing external and internal threats. The sensitive nature of the PLC and DCS devices controlling the critical infrastructure assets require a higher level of network segmentation and advanced defense solutions not currently recommended or available through most security firms and IT vendors.

This white paper takes a look at the fundamental issues with the current practice of securing SCADA and control systems, introduces the concept of security zones of vulnerabilities, and briefly introduces several new and unique cyber defense solutions that can be deployed at each security zone.
### Table of Contents

Defining the Problem ....................................................................................................................... 3
Figure 1 – Typical Network Diagram of SCADA and IT Networks .................................................... 4
Figure 2 – Most Only Segment SCADA and IT into Two Security Zones .................................... 4
Typical SCADA Vulnerabilities and Innovative Solutions ................................................................. 5
External Threat > ............................................................................................................................... 5
Worms, Viruses, Trojans, and Malware Corrupt SCADA Networks .................................................. 5
Figure 3 – Insufficient Network Segmentation Difficult to Defend Against External Attacks ...... 5
Figure 4 – New Data DMZ Creates a Neutral Zone 2 between IT and SCADA ............................. 6
Figure 5 – Relay Operating System and Antivirus Patches into Simulation Network for Testing .......................... 7
Figure 6 – Relay Operating System and Antivirus Patches into Live Production Systems .......... 8
External Threat > ............................................................................................................................... 8
Insecure Remote Access to SCADA Environments ........................................................................ 8
Figure 7 – Current Insecure Methods for Providing Remote Access for SCADA ......................... 9
Figure 8 – New Sample Solution for Providing Secure Remote Access for SCADA ...................... 10
Internal Threat Unintentional > ....................................................................................................... 10
Loose Access Controls Expose Entire SCADA Network ................................................................. 10
Figure 9 – Loose Access Controls Can Not Prevent Unintentional Access by Corporate Users .... 11
Internal Threat Intentional > ............................................................................................................ 12
Flat SCADA Network Design Limits Security Effectiveness .......................................................... 12
Figure 10 – Flat SCADA Architecture Design Can Not Defend Against Internal Attacks .......... 12
Internal Threat Intentional > ............................................................................................................ 13
SCADA Software and Equipment Vulnerable to Elevated Network Traffic ............................... 13
Figure 11 – Distributed Firewalls throughout SCADA Environment Can Protect End Devices 13
Conclusion........................................................................................................................................ 14
Defining the Problem

Over the past several years, with the blackouts and increased activity levels of worms and viruses like Blaster (aka MSBlast), there is a recognition that these systems that were previously proprietary and isolated systems are now connected to corporate networks, and many contain connection points from the Internet. It is also common knowledge now that the electronic equipment controlling critical infrastructure is susceptible to failure through DoS (Denial of Service), malformed packets, and malicious code caused by viruses, Trojans and worms.

Cyber security vulnerability assessments performed on SCADA and process control networks have exposed a pattern in the approach that many companies take in securing their critical assets. More than 80 percent of these electric, gas, water and energy companies mentioned that one firewall or equivalent cyber defense solution between their IT Corporate Network and process control network was sufficient for maintaining the security of their critical assets under control of SCADA and process control systems.

These companies typically considered the process control network as one large black box, and tended to approach securing these environments by attempting to isolate that environment as much as possible from any other network. While this is a good first attempt and a move in the right direction, there are additional cyber security solutions that should be taken under consideration given modern external and internal threats facing these critical assets that are connected through Ethernet and Internet-routable protocols.

On the following page, there are two diagrams shown. The first diagram shows the logical network diagram of how a typical SCADA or DCS system is networked back to the corporate network. The second diagram shows how most companies view the security of their real-time, SCADA, and process control environments. They typically only segment their network into two environments - one for corporate/IT, and the other for SCADA and process control systems.
Figure 1 – Typical Network Diagram of SCADA and IT Networks

Figure 2 – Most Only Segment SCADA and IT into Two Security Zones
Typical SCADA Vulnerabilities and Innovative Solutions

Just as with enterprise networks, the lack of access controls and network segmentation within SCADA and process control systems also creates opportunities for cyber vulnerabilities. These may be from external or internal threats. The following sections cover SCADA vulnerabilities and potential innovative solutions for solving these issues.

External Threats >
Worms, Viruses, Trojans, and Malware Corrupt SCADA Networks

![Diagram of insufficient SCADA network segmentation](image)

Figure 3 - Insufficient Network Segmentation Difficult to Defend Against External Attacks

Having only one cyber defense solution in place at the perimeter of the SCADA or PCN environment often leaves the SCADA workstations and servers, telecom networks, and PLC and RTU controllers vulnerable to self-propagating, polymorphic worms that change faster than antivirus vendors can react. With additional security zones, and with port-level security and firewalls between each security zone, worms and viruses can be stopped regardless of whether the antivirus solution has the latest signature file. In addition to segmenting the SCADA environment through the use of firewalls, an antivirus solution can be set up that never needs to be directly connected to the internet, yet still automatically gets signature updates and distributes them to computers in the SCADA environment.
Since directly connecting the SCADA environment to either the corporate IT network or the internet can expose the SCADA environment to additional vulnerabilities and threats, a better solution is to create a new neutral security zone (Zone 2) that is in its own DMZ (De-Militarized Zone). This neutral data historian DMZ will create a buffer between the corporate IT network and the SCADA environment, and there are many benefits to this design.

The main benefit for this new buffer zone is that data can be staged here from the SCADA environment and then moved onto other IT environments. Instead of having multiple IT connections directly into the SCADA environment, all data collection and archiving can be moved out to this Data Historian DMZ, thus further limiting access into the SCADA environment and allowing a tighter set of firewall rules to be written between this zone and the SCADA environment. The concept of "least privilege" can be applied here so that only those with required access to the SCADA systems and components are allowed into the SCADA environment. All other users, which only really require access to the data collected from the SCADA Systems, can be given access to those systems in the data historian DMZ.
Another benefit of having this new data historian DMZ or Zone 2 is to set up relay servers that can relay or forward on operating systems and antivirus update patches from the IT side of the network into the SCADA or control systems environment. If there is access to a simulation or development network with SCADA hardware and software setup, then it is highly recommended that these new operating system and antivirus patches be tried on these test environments first before moving forward. The diagram below in Figure 5 shows how a secondary operating system or antivirus patching systems can up placed in this new Zone 2, or data DMA zone, so that we can relay the updates and patches down into the test environment, to try them in the test environment before applying the patches or updates to the live production systems.

![Diagram](image.png)

Figure 5 - Relay Operating System and Antivirus Patches into Simulation Network for Testing

Once the patches are tested to work in the simulation network, without adversely affecting any of the SCADA functions, then the same systems in Zone 2 can be used to relay those patches into the live production environment.
Even though the patches have been tested on the simulation network, there still may be a risk to automatically pushing patches out to those systems running in production mode. One option is to patch the systems one at a time. Another option is to manually patch the systems by walking up to the workstation or server and updating the operating system or antivirus patches by referring back to the systems in the Zone 2 area for the source of the patches.

**External Threat > Insecure Remote Access to SCADA Environments**

In addition to other external threats coming in through the internet and corporate IT firewalls, there still exists the threat of direct access behind the firewall through dialup modem access. These dialup modem connection points only require knowledge of a short password or simplistic 4-digit PIN code to gain direct access into the heart of the SCADA environment. The combination of a simplistic authentication method, and the ability to directly access and manipulate SCADA hardware and software - with little or no audit trail - makes these modem connections viable points of entry for external threats.
The diagram below in Figure 7 depicts several points of entry into the SCADA environment through the use of modem or insecure VPN access. Both allow the external system to gain a direct connection into the SCADA environment, and any malicious code on the external system or external networks can easily crawl into the SCADA environment through the bridged connection made with this type of external access.

Figure 7 – Current Insecure Methods for Providing Remote Access for SCADA

In addition to the vulnerabilities pointed out in current modem access into SCADA environments, modem access only provides a low-bandwidth connection for troubleshooting, repairing, or maintaining SCADA system components. A new solution should require stronger authentication, while restricting direct access into the SCADA environment. It should also provide an audit trail with all access to the system time stamped and logged by username.

By combining a 2-factor OTP (One Time Password) solution with thin-client computing (Citrix or Terminal Services), remote access could be provided that not only does multiple checks for access authentication, but also limits access into the SCADA environment by holding the remote user in a DMZ zone and only providing thin-client session access into the SCADA environment.

The remote user, after providing the changing 6-digit code from the token, is then prompted again for a secret 4-digit PIN code, and the combination of both the 6-digit code and the 4-digit PIN code creates a OTP (one time password) into the system. Once authenticated into the DMZ zone, the remote user must then enter another username and password to access the thin-client server. Once authenticated into the thin-client environment, the remote user is presented with a desktop session based the user's access profile. Those remote users with system administrator profiles can have access to PLC Programming or SCADA/HMI development software so that changes can be made and downloaded into the SCADA environment.
The diagram below in Figure 8 shows how this new type of secure remote access authenticates the remote user, then contains the user inside the data historian DMZ, while allowing the thin-client session to have access into the SCADA environment through the SCADA firewall.

Besides the additional security features of this new type of remote access solution, additional benefits include a full auditing trail of whom, how, and when access is made into the SCADA environment. Also, since the remote access solution is media independent, remote access can be made with higher broadband connections so that the quality of the connection is enhanced.

**Internal Threat Unintentional >**
**Loose Access Controls Expose Entire SCADA Network**

Another fundamental security weakness with having one defense solution at the perimeter of the SCADA network, is the potential for loose access controls. Since there is only one layer of defense between the corporate LAN and the SCADA or process control LAN, that one defense solution must be implemented in a very sound manner and tested. In recent vulnerability and risk assessments performed on energy, utility and manufacturing companies, a common problem was weak ACLs (Access Control Lists) implemented in the router or firewall between the corporate IT and SCADA environments.
Most router implementations that we have analyzed use ranges of IP addresses to limit access into the SCADA environment. Today’s automated hacker tools and scanning utilities can be set up to automatically try several ranges of IP addresses for brute force entry. Even without these automated tools, an insider with physical access to the corporate network could place a sniffer on the network and log all packets, thus having the ability of seeing which address space is allowed to go past the perimeter security device.

On one occasion, a summer intern overheard us use the word SCADA, and he stated that he had “found some computer called SCADA01 and EMS05” on the network. He did not know what they were for, but he showed us that he had access to all of the files on these servers. Tighter access controls at the perimeter defense device (router or firewall), and additional network segmentation, will go a long way to preventing unintentional access into the SCADA environment. Please reference Figure 9 below to see how loose access controls and weak ALCs in the perimeter defense solution between IT and SCADA networks can expose the entire SCADA environment to unintentional access by inside employees and contractors.
Flat SCADA Network Design Limits Security Effectiveness

The typical defense solution at the perimeter only succeeds at providing a limited defense solution for attacks coming from outside the SCADA environment. Most likely, the entire SCADA environment is a flat network. Anyone with access to any system within the SCADA environment has access to the entire SCADA environment. For example, without additional security solutions and defense layers implemented down in the SCADA network, how can a company prevent a historical database consultant from downloading code to their ethernet PLCs, or accessing files on the other SCADA servers? Figure 10 below shows that this type of SCADA network architecture does not provide sufficient containment within the various SCADA components.

There should be a method for limiting access to the low-level SCADA end devices that control the physical process. Access to the SCADA and process control computer workstations and control room computer equipment should not automatically mean access to the controllers that operate physical equipment.

Additionally, if the SCADA computers are impacted by a virus, most likely the process under control of the PLC, RTU, or IED can continue operation in automatic mode with the last setpoint while computer administrators restore the SCADA workstations or servers that were impacted. If there is not another division of access between the SCADA computer equipment and the SCADA end devices that control real physical plant equipment, then these potential threats from self-propagating viruses, worms and Trojans can have a much larger impact on the end devices, and have proven several of them to fail under lab conditions.
**Internal Threat Intentional >**  
**SCADA Software and Equipment Vulnerable to Elevated Network Traffic**

Devices like PLCs, RTUs and IEDs that control physical equipment, should be in a different security zone, with additional access controls for limiting access to them. The SCADA Servers and operator consoles should be in another security zone. It has been proven in several research studies, and in our own testing of SCADA equipment, that these controllers are susceptible to crash when the network is at elevated bandwidth level, or if malformed network packets are sent to the SCADA software or equipment.

Currently, with only one large flat SCADA network, these end devices are not protected in the case that the SCADA computers and workstations are impacted. One of the best ways to protect these end devices is to segment the SCADA environment into additional operational zones and deploy distributed firewalls throughout the SCADA environment to provide additional access controls between each zone.

![Distributed Firewalls throughout SCADA Environment](image)

*Figure 11 – Distributed Firewalls throughout SCADA Environment Can Protect End Devices*
Conclusion

With the changing and emerging threats to SCADA and process control systems, owners and operators of these systems should take a closer look at the cyber access controls currently used to defend these systems against external and internal threats. The industry embrace of Ethernet TCP/IP communications in the late 1990’s has introduced into the SCADA and process control systems marketplace components with Ethernet communications capabilities. Now it is very common to find IP communications throughout the SCADA and process control systems environment.

The trend continues within owners and operators of SCADA systems to provide only one perimeter cyber defense solution at the connection between the SCADA and IT networks. This one defense solution, such as a firewall, is a good start, but leaves the inside of the SCADA environment insecure and vulnerable.

This flat network design within the SCADA environment allows both external and internal threats to propagate and affect the end devices that control physical equipment. Several new and innovative techniques are available to use in securing the inside of the SCADA environment, as well as providing secure remote access to it.

Knowing what vulnerabilities lie within the SCADA and Process Control Systems, how external and internal threats can take advantage of these vulnerabilities, and knowing how to implement new defense solutions to deter, defend and detect cyber threats is key to protecting these critical systems.

# # #