Using Defense in Depth to Safely Present SCADA Data for Read-Only and Corporate Reporting

Rick Bryson

Introduction

SCADA systems provide for wide-area collection and control in a utility, industrial, or process control system, generally in an isolated and secure network. System events, alarms, and metered data are presented to users in an operations control center HMI and to applications such as Outage Management Systems (OMS), Distribution Management Systems (DMS), Energy Management Systems (EMS), and historical archiving systems. To protect sensitive data, prevent unwanted operations, and provide reliable operation of monitored systems, the SCADA network must be protected from outside invasion by both nefarious and unintentional damaging influences. Complete separation from the SCADA network and other networks, such as corporate IT or the Internet, is a common practice to facilitate the necessary protection.

Data Sharing vs. Data Protection

Although securing information is relatively simple, sharing secure data introduces many challenges. Corporate and IT entities need or desire information from the SCADA system but should not directly access it. Operator training and reporting stations need up-to-date information on the SCADA system, but should not have direct access or control capabilities to devices on the SCADA network. This white paper explains a method of providing a read-only copy of SCADA data to corporate executives, IT, and operator training and reporting centers while providing layers of security to protect the SCADA network from upstream-based attacks. The data sharing plan includes the following features:

- Specific (user-defined) data are sent one way from SCADA to a read-only demilitarized zone (DMZ) network.
- Syslog messages are sent one way to the DMZ Syslog server to provide information needed for operations.
- Specific (user-defined) data are sent one way from the DMZ network to the Corporate network.
- Specific (user-defined) Syslog messages are sent one way from the DMZ network Syslog server to the Corporate network Syslog dashboard.
- A read-only HMI resides on the DMZ network as an exact duplicate of the actual SCADA HMI.
- The DMZ network HMI detects intrusions and acts as a honeypot to hold the attention of would-be intruders while it sends appropriate alarms, thus providing some time to further protect the SCADA and Corporate networks.

Figure 1 shows the conceptual segregation of the Corporate, DMZ, and SCADA networks.

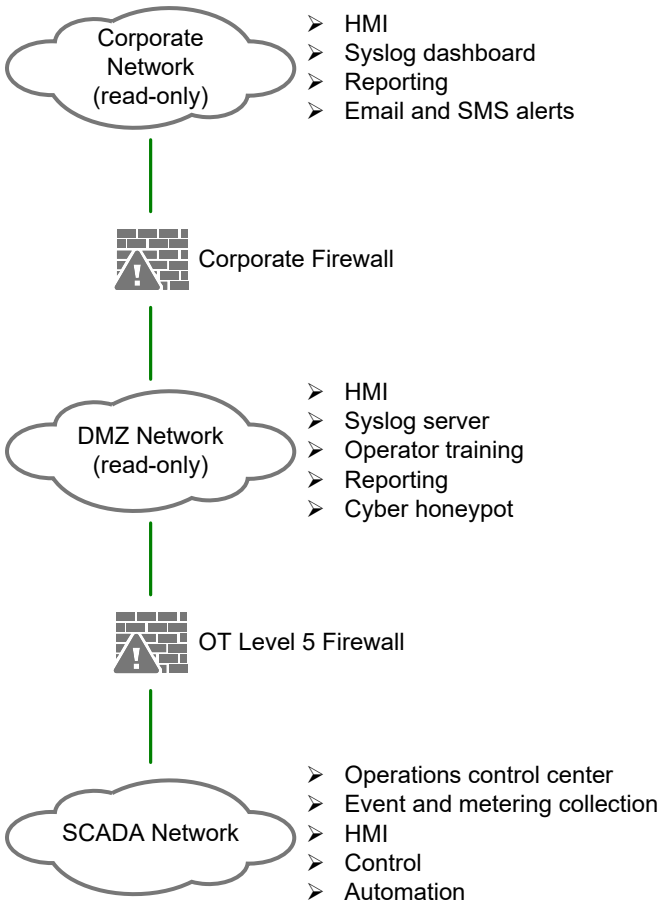

Figure 1 Network Firewalls

SCADA Network

The SCADA Network in Figure 1 includes the main operations center, SCADA server machines, OMS, DMS, EMS, and historical archive. Also included are all downstream IEDs. There are no open connections into the SCADA network from outside the OT Level 5 Firewall. A data aggregation device residing on the SCADA network gathers SCADA data from the SCADA system and populates a user-configurable data list. In systems of less than 100,000 points, this data aggregation device could be an SEL-3555 Real-Time Automation Controller (RTAC) that gathers SCADA data via an industry-standard protocol, such as DNP3, IEC 61850 MMS, etc. The RTAC then pushes the data via a connectionless UDP message through the OT Level5 Firewall to another RTAC residing on the DMZ Network. Devices in the SCADA network send pertinent Syslog message through the OT Level 5 Firewall via connectionless UDP messaging to a Syslog server residing on the DMZ Network. An SEL-3620 Ethernet Security Gateway provides the user configuration and system protection needed for this type of firewall protection. You can further protect the system by defining network flow rules in a software-defined networking (SDN) switch, such as the SEL-2740S SDN Switch. An SDN switch provides the user with configuration tools to engineer exact flows, network reconfiguration, and traffic restriction in a deny-by-default architecture. Use of the SDN controller provides tools to define path-level control, but also supports matching rules in Layer 1 through Layer 4 of the packet. Advantages include greatly enhanced security in the network, very precise control on network reconfiguration, and, in this example, precise definition of network traffic. Configure the SDN switch to eliminate all traffic

passing from one network to the other, except for the specific one-way UDP message streams for the SCADA data and Syslog messages being pushed through the OT Level 5 Firewall to the read-only DMZ network.

DMZ Network

The DMZ network in this example includes facilities to present SCADA information in a read-only format, while providing a layer of defense between the SCADA and Corporate networks. An exact duplicate copy of the SCADA HMI resides in the DMZ network and is populated with live read-only data as delivered through the one-way UDP message stream from the SCADA data aggregator, as described in the previous section. This provides visualization of the SCADA data sent by the RTAC, as well as the following benefits:

- Operators can train on the read-only system with live SCADA operational data without the risk of causing any issues on the live system.
- Visualization provides all necessary live SCADA information to engineering and planning groups that are not involved with primary SCADA operations without risking accidental or malicious control operations.
- If intruders do breach the DMZ network and find the read-only HMI, they will assume they are on the active SCADA system and will be delayed from further attempts to compromise the system as system administers are notified of the attack.

The first two listed benefits address an important concept in security, which is providing least privilege needed in the system. New operators who are training on the system, energy management and planning engineer groups, or non-primary operations personnel in the SCADA control center are not given direct access to the live system. They can view a specifically defined set of live SCADA data on the read-only HMI, but cannot operate remote IEDs or directly affect SCADA operations.

In application, the read-only HMI is an exact duplicate of the SCADA HMI, with all data objects mapped using internal virtual tags. On the SCADA HMI, those virtual tags are mapped to actual SCADA metering, indication, and control points. On the read-only HMI, the virtual tags are mapped to the read-only data supplied through the UDP read-only stream from the RTAC located on the SCADA network. Control type virtual tags on the read-only HMI are not mapped to actual control points, but instead are configured to log actions in the system SOE log, which in turn send Syslog messages. This provides a honeypot (i.e., delay mechanism) as intruders attempt to compromise what they believe is the live system by operating control objects on the HMI. Each control operation they attempt generates an alert via Syslog or other alert mechanism. Administration immediately takes action to isolate the intrusion and disable any further access to the system before further breaches can be attempted.

Corporate Access to SCADA Data

A second aggregator device, which could be the read-only RTAC, is located in the DMZ network and contains a secondary list of read-only data that it pushes to another RTAC in the Corporate network. Additionally, the DMZ network Syslog server is configured to forward necessary Syslog messages to a Syslog dashboard on the Corporate network. For example, suppose a SCADA RTAC detects a potential security attack in a remote site by a user who was recently separated from the company. In conjunction with the alarm sent to SCADA operations, the RTAC also sends a Syslog message to the server residing on the DMZ network, which then forwards the message to the Corporate network Syslog dashboard. Conversely, although a Syslog message indicating

that one of the SCADA printers is out of paper may be of interest at the SCADA operations center, it does not contain information needed by users on the Corporate network.

As with the SCADA-to-DMZ network connection, the connection between the DMZ network and the Corporate network is not only protected by the corporate firewall, an SEL-3620, with a one-way data flow configuration, but it is also protected by a one-way SDN data flow mapping provided by the SEL-2740S. The DMZ RTAC populates network global variable lists (NGVLs) from its list of read-only data, and then it transmits the NGVLs as UDP data objects through the SDN path and corporate firewall to the RTAC residing on the Corporate network. The DMZ Syslog server mines and forwards needed Syslog messages through the SDN switch and corporate firewall to a corporate Syslog dashboard. A customized HMI, such as can be provided by another RTAC, on the Corporate network presents a web-based view of real-time SCADA values to corporate consumers. Corporate consumers of the information can view the HMI from remote web browser sessions or through ODBC connections using Microsoft Excel or custom ODBC applications. The corporate Syslog dashboard can mine Syslog messages to determine what alerts are needed and perform actions such as sending emails, SMS messaging, or simple logging. For example, alerts generated in the previous example scenario (i.e., a breached read-only HMI in the DMZ network) are received as Syslog messages and then sent to appropriate authorities through SMS text and email messages. Because email and SMS alert messaging are not sent via the DMZ Syslog server, the DMZ network has no need of any external (e.g., Internet, etc.) connections through the corporate firewall.

Conclusion

By using a defense-in-depth approach, you can provide read-only SCADA data and Syslog messages to corporate or other networks. The layered defense includes adding a DMZ network, read-only HMI and Syslog server, and a one-way data sending mechanism through SDN and unidirectional firewall rules. The read-only DMZ network provides not only least-privilege access to live SCADA data for training and non-primary operations use, but adds the benefit of a buffer zone to slow down would-be intruders while alarming that an intrusion is in progress. Email, SMS, and other alerts that access outside networks are only generated outside of the DMZ to further reduce the risk of infiltration. By designing the data flow as unidirectional from SCADA to upstream sources, we reduce the risk of nefarious or other unwanted traffic entering the secure SCADA network, while providing needed information at a corporate level.

Biography

Rick Bryson received his B.S. in computer science from Texas A&M University. He has worked 26 years developing firmware, software, and integration solutions for RTUs, controllers, and SCADA systems in the oil, gas, water, wastewater, and electrical utility markets. He has served on the DNP Technical Committee. Rick joined Schweitzer Engineering Laboratories, Inc. in 2008 and divides his time between system integration and validation, training development, and working with customers on automation, integration, and application engineering solutions.