Trend Micro
Research Paper
2012

Toward a More Secure Posture for Industrial Control System Networks

By: Paul Ferguson

CONTENTS

INTRODUCTION

Industrial control systems (ICSs)[1] are defined as networks or collections of networks that consist of elements that control and provide telemetry data on electromechanical components such as valves, regulators, switches, and other electromechanical devices that may be found in various industries. Among these are oil and gas production, water processing, environmental control, electrical power generation and distribution, manufacturing, transportation, and many other industrial settings. Without getting into detail for each particular industry segment, each of these ICS environments shares a common fate—they are not "traditional" IT network environments and should not be treated as such. Most ICS networks share similar security challenges because of this uniqueness. These challenges are made more complex by the interaction of ICS elements with physical industrial components. Failure to properly control or maliciously controlling these elements can lead to catastrophic accidents. Many of the industrial systems managed by ICS elements are considered "critical infrastructure" and require a much more specialized security architecture than traditional IT environments.

Supervisory control and data acquisition (SCADA)[2] networks can be defined as the network layer that immediately interfaces with ICS networks as well as host systems that control and monitor elements of ICS networks.

This paper illustrates what the author believes should be considered required elements in every ICS network integration effort. It also covers best practices when integrating with SCADA and existing organizational networks as well as the rationale for and importance of each component of the suggested architecture.

DISCUSSION

First, let us discuss the concept of an "air gap,"[3] which is defined as a physical separation of systems or networks. In other words, no possible connectivity between one particular network and any other network exists (i.e., the ICS and SCADA networks, in this case).

The principle thrust of the idea is that by physically isolating a network, one removes the attackers' ability to penetrate or gain access to these assets or, at least, removes the vast majority of opportunities for attackers to do so. "Insider threat vectors," however, remain such as when an employee or another "trusted insider" either purposely or inadvertently introduces a security incident (e.g., malware introduced via a USB drive or intentional data theft). For the most part though, building an air gap between a network that needs protection and other untrusted networks goes a long way to remove the majority of security threats. Physical isolation is definitely highly valuable insofar as reducing risks with regard to ICS and SCADA network security.

In practical and operational terms, however, physically separating networks is not functionally nor operationally feasible in the real world. As Eric Byres pointed out in an article that addresses this topic,[4] businesses require certain operational functions and air gaps are not just workable solutions, as billing systems, remote metering, and other enterprise or organizational functions rely on being able to access data and systems that interface with ICS and SCADA networks.

As with virtually all other network and operational security practices, this becomes an exercise of minimizing risks, constant and consistent monitoring, as well as building a security architecture that lends itself to the highest degree of an ICS security posture.[5]

1 https://secure.wikimedia.org/wikipedia/en/wiki/Industrial_control_system
2 https://secure.wikimedia.org/wikipedia/en/wiki/SCADA
3 https://secure.wikimedia.org/wikipedia/en/wiki/Air_gap_(networking)
4 http://www.automation.com/content/scada-securitys-air-gap-fairy-tale
5 https://www.us-cert.gov/control_systems/pdf/Announcement-11-208-01.pdf

It is also worth mentioning that many ICS networks use wireless connectivity capabilities between deployed peripheral components. These capabilities greatly simplify the deployment of large electric or gas distribution networks as well as other ICS and distributed control system (DCS)[6] components. However, using this capability undermines any designed air gap elements, as security must treat any wireless component as exposed to public interference. Wireless communication networks should also use the strongest practical encryption available to prevent eavesdropping, data manipulation while in transit, or malicious data injection.

IMPORTANT INDUSTRIAL CONTROL SYSTEM SECURITY ARCHITECTURE ELEMENTS

- Rigorous patch management
- Network segmentation
- Authentication diversity
- Application control or white-listing

- Security information and event management (e.g., logs and alerts)
- Intrusion detection systems

Rigorous Patch Management

Rigorous and timely application of software patches for corrected vulnerabilities is critical, as the number of exploits for specific ICS and SCADA software platforms grows every day. The key is to not only focus on the OS but also on each and every software package installed on every device, including network management platforms, routers, switches, firewalls, intrusion detection systems (IDSs), and so on.

Vulnerabilities in third-party software are also increasingly being targeted for exploitation. As such, these software packages must also be targeted for patching when security fixes are made available.

The goal is to apply the necessary security patches as quickly as possible without interfering with normal day-to-day operations in order to "shrink the attack window" for attackers to compromise or otherwise exploit vulnerabilities as much as possible.

Network Segmentation

One of the most important aspects of a heightened ICS security posture is proper network, operational, and element segmentation. This is the keystone of the security architecture. Anyone familiar with architecture, in general, understands the concept of the "keystone"[7]—the single, most important structural piece of the architecture. If it is removed, the entire facade collapses.

The same is true for functional segmentation in ICS environments; the success of virtually all other security elements rely on it.

While this may seem obvious, proper segmentation of the operational placement and function of each element is key to the risk reduction strategy in an advanced ICS security posture. Other elements are, of course, closely coupled with segmentation, including authentication, log management and analysis, application control, network access control, and so on, which will each be separately discussed in latter sections of this paper.

Note the distinction between the ICS network "cloud" and the SCADA functionality, as this is completely intentional since their functional roles distinctly differ.

The ICS network primarily consists of programmable logic controllers (PLCs)[8] and other DCS elements.

In essence, the SCADA network is a "bridge" between the ICS or DCS electromechanical sensors and the management systems required to monitor and control their operation.

As shown in Figure 1, the architecture should be logically separated in terms of functionality.

6 https://secure.wikimedia.org/wikipedia/en/wiki/Distributed_control_system

7 https://secure.wikimedia.org/wikipedia/en/wiki/Keystone_(architecture)

8 https://secure.wikimedia.org/wikipedia/en/wiki/Programmable_logic_controller

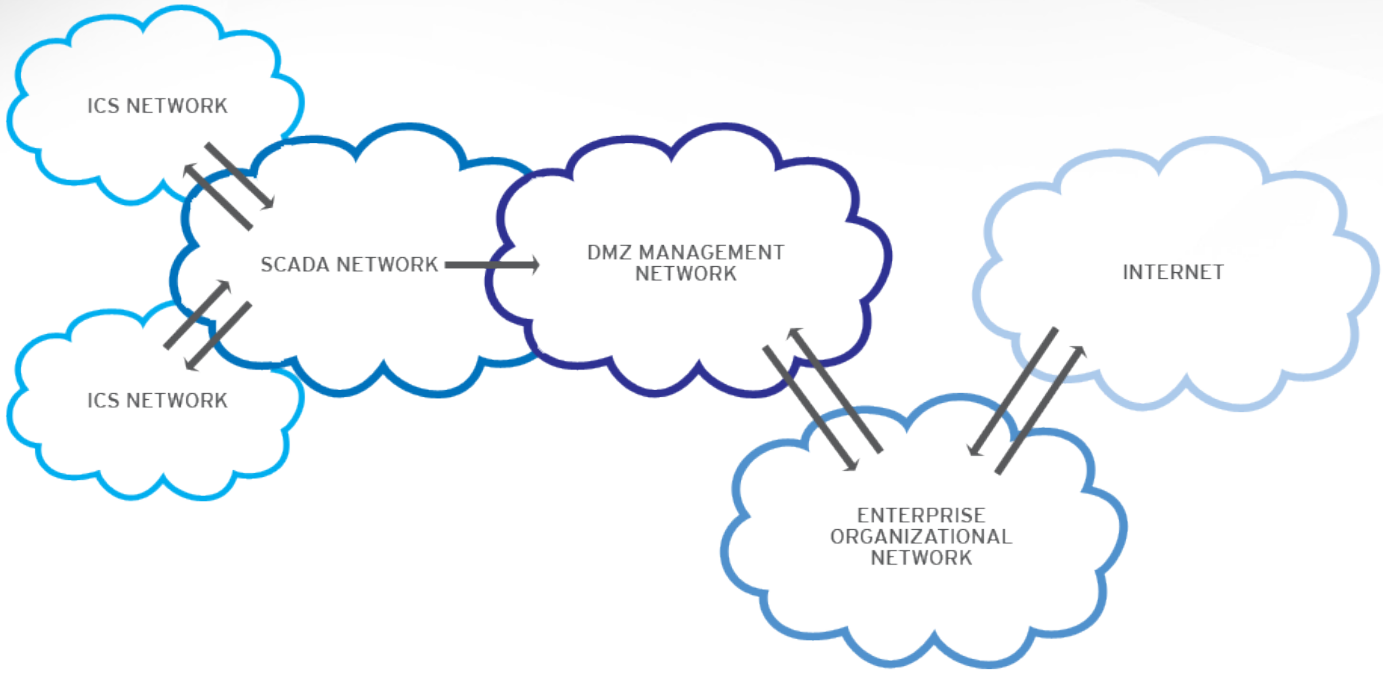

Figure 1. Segmentation: Separation of functionality

The enterprise organizational cloud in Figure 1 should ideally never directly interface with SCADA network elements. A separate boundary network such as the demilitarized zone (DMZ) management network[9] should instead provide an additional segmentation layer whose additional security functions can dramatically decrease the attack surface. As in real military conflict zones, a DMZ acts as a buffer between hostile environments and opposing forces. In it, meetings and negotiations can be held without conflict or violence. The same is true for a DMZ management network wherein certain services—neither in the enterprise organizational network nor fully exposed to the Internet yet accessible by both—can be hosted.

The objective of having a network such as that depicted in Figure 1 is to introduce layers in the network architecture that lend themselves to apply various security mechanisms. This will, in turn, allow security mechanisms to be implemented, which will thwart external attacks, incidental internal enterprise network breaches, or compromises and quickly alert administrators to other sundry attempts to subvert the security mechanisms they put in place at various locations within the architecture. This also allows the administrator to control the traffic flow wherein certain handling and processing functions can be done in a certain order with deterministic methodology.

Traffic Flow: Access Control

Notice the addition of several elements in Figure 2 although we will only focus on the device wedged between the SCADA and DMZ management networks.

9 http://en.wikipedia.org/wiki/DMZ_(computing)

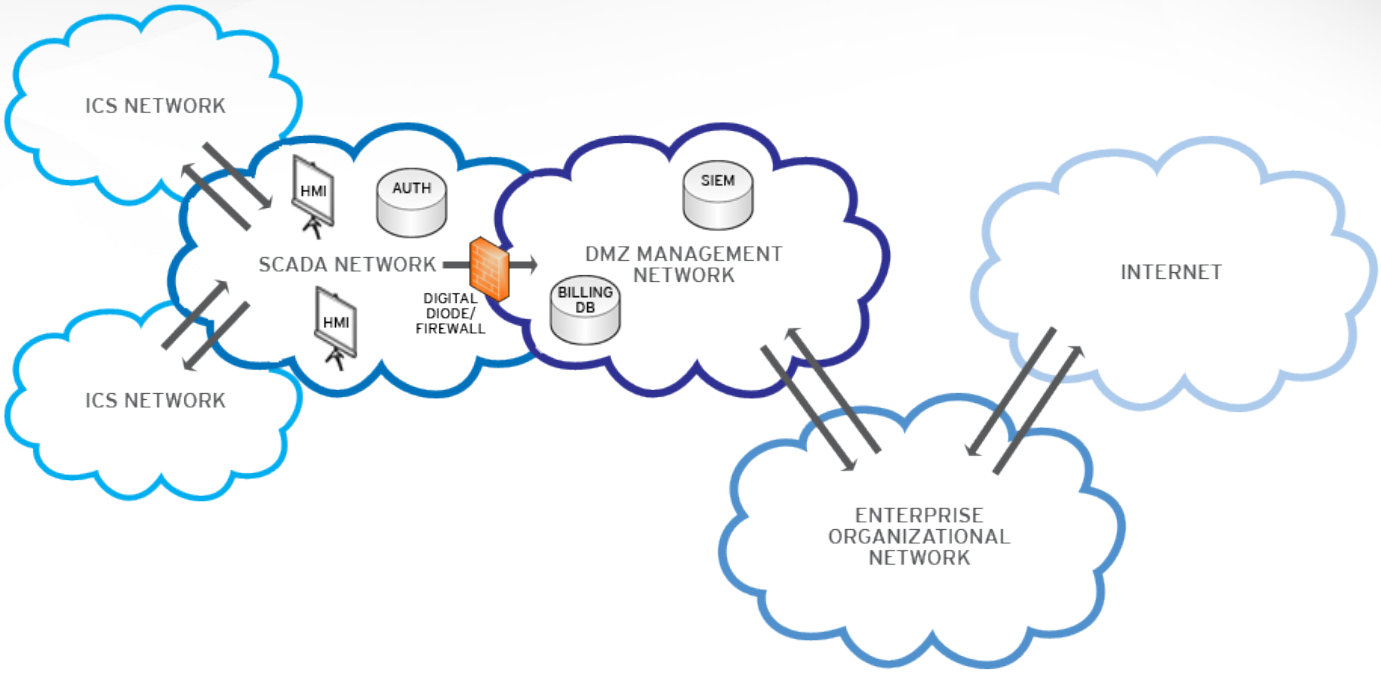

Figure 2. Placement of network elements

The device that has been added is a specialized firewall, one that only lets traffic flow in one direction, also known as a "digital diode" or a "unidirectional firewall." A digital diode is a specialized device that only allows optical light to propagate in one direction, thus truly only allowing unidirectional traffic flow.

As Dale Peterson noted in a blog post[10] in July 2011, digital diodes enjoy a certain popularity within the ICS network community for their specialized functionality.

Discussing specific elements within an ICS architecture that refers to the traffic control properties of a digital diode is important because there need not be any other traffic control device in it. Firewalls may exist elsewhere in the corporate network but there should not be any other device that impedes the flow of information in the ICS network. A firewall may also be substituted for a digital diode should bidirectional traffic be desired or required.

The reason behind this is simple—impeding the immediate flow of traffic in an ICS environment can be worse than an externally induced security incident. ICS elements require immediate traffic connectivity so any effort to impede ICS network traffic is self-defeating insofar as it is a security threat.

Going back to the specifics of traffic flow control, only allowing traffic to flow between devices that actually need to communicate with one another should be made a requirement. In other words, the unidirectional firewall should only be configured to permit traffic to flow from devices that have been authorized; all others should be denied.

Although not shown in Figure 2, there should be a firewall between the DMZ management and enterprise organizational networks in order to control access of authorized traffic to the ICS components of the architecture.

Authentication Diversity

Authentication is another critical key system that must be considered. It is highly recommended that isolation of authentication infrastructure be established between the authentication systems in the enterprise organizational network and those that interface with the SCADA or ICS network.

10 http://www.digitalbond.com/2011/07/19/air-gaps-dead-network-isolation-making-a-comeback/#more-10382

The reason behind the isolation is simple—if an account in the enterprise organizational network is somehow compromised, compromised credentials can be used to gain unauthorized access to resources in the SCADA or ICS network (e.g., network management platforms). By diversifying the credential databases, an account compromised from one database should not have any impact on accounts in other databases. This, however, assumes that appropriate password reuse and complexity policies have also been put in place.

To establish a more robust security posture for an ICS network, consider a completely separate and diverse authentication system. This ideally includes the use of multifactor authentication. Critical operations may also benefit from establishing multiuser authentication requirements.

Application Control or White-Listing

Application white-listing is another control mechanism that should be considered for "special-purpose" platforms such as human management interface (HMI) stations. Application white-listing software programs are designed to only allow the execution of preauthorized software programs. In the event of a compromise, application white-listing should not allow the execution of malicious software or malware and Trojans designed to subvert the security of a system or allow access to software that have not been authorized to execute on an affected system.

The use of application white-listing also prevents both malicious and inattentive user behaviors from expanding the target surface by adding unauthorized programs or other software that may introduce malware or software that makes the system more vulnerable to exploitation. It should, however, be noted that application white-listing may complicate and/or exacerbate the patch management and patch application process, so this should also be taken into consideration.

Security Information and Event Management

SIEM solutions refer to "a combination of the formerly disparate product categories of security information management (SIM) and security event management (SEM). SIEM technology provides real-time analysis of security alerts generated by network hardware and applications. SIEM solutions come as software programs, appliances, or managed services and are used to log security data and generate reports for compliance purposes."[11]

In other words, logs and alerts from virtually all platforms and/or devices are exported to a single platform where they can be analyzed in real time in order to better understand and detect any anomalous behavior in the network. This includes authentication errors, firewall rule set violations, access logs, IDS logs, and virtually any other type of information desired to provide a comprehensive analysis of network events, traffic flow control, access violations, and so on.

In fact, SIEM analysis within the boundaries of the ICS or SCADA network should be very straightforward, if not simpler, than in traditional enterprise networks because the traffic patterns are known and not chaotic as in traditional IT networks. These "known" patterns should be mapped out in advance since normal traffic in the ICS network will rarely deviate from these. Any deviation from these patterns will quickly reveal abnormal, anomalous, or unauthorized traffic behaviors or events.

Intrusion Detection Systems

An IDS[12] is an integral and, as some security experts would argue, mandatory part of a good network security posture, as it allows the network security administrator to use preconfigured patterns to detect malicious traffic patterns as well as to create alerts that flag configuration policy violations.

The policy violations, detected malicious or attack traffic, and other alerts can also be exported to the SIEM platform for additional processing and logging.

11 https://en.wikipedia.org/wiki/Security_information_and_event_management

12 https://en.wikipedia.org/wiki/Intrusion_Detection_System

The number and placement of IDS networks very much depend on the level of security posture desired. At least one should be used at the boundary between the enterprise organizational network and the DMZ management network. However, additional IDS networks can be used—each with more customized rule sets and specific ICS signatures—at other boundaries in the architecture.

CONCLUSION

It should be noted that no mention has been made of deploying antivirus software. This is a decision that must be made by each individual organization and, in most cases, may be mandated by other regulatory regimes. Also, be aware that antivirus software may interfere with application white-listing and that, in practice, the proper implementation of application white-listing should negate the need for antivirus software.

As noted earlier, perhaps the ideal situation for any ICS network is complete isolation—no connectivity to external networks whatsoever. However, realistic day-to-day business operations most often do not allow that luxury.

The architecture of how ICS networks interface with the other components of an enterprise network is critical to providing a more heightened security posture. To protect sensitive ICS networks, proper segmentation of traffic flow must be provided, restricted access control and authentication must be required, traffic and alert logs must be analyzed, and alert notifications must be appropriately addressed.

None of these components alone are magic bullets. Taken together, however, these steps can go a long way in helping increase the security posture of any ICS network deployment and should be endorsed by network security administrators.

TREND MICRO™

Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years' experience, we deliver top-ranked client, server and cloud-based security that fits our customers' and partners' needs, stops new threats faster, and protects data in physical, virtualized and cloud environments. Powered by the industry-leading Trend Micro™ Smart Protection Network™ cloud computing security infrastructure, our products and services stop threats where they emerge—from the Internet. They are supported by 1,000+ threat intelligence experts around the globe.

TREND MICRO INC.

10101 N. De Anza Blvd.
Cupertino, CA 95014

U.S. toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003
www.trendmicro.com

TREND MICRO™

Securing Your Journey to the Cloud

©2012 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.