



White Paper

Monitoring and Securing SCADA Networks

Published 3Q 2011

Report commissioned by McAfee, Inc.

Bob Lockhart
Senior Analyst

Bob Gohn
Research Director

Section 1

EXECUTIVE SUMMARY

1.1 Introduction

SCADA networks are just different. Compared to enterprise IT networks, they have different security objectives, most of the endpoint actors are machines rather than people, their incidents can have immediate physical consequences, and they are more likely to be targeted by hostile actors such as terrorists. Moreover, SCADA networks must operate at speeds and low latencies that enterprise networks can only covet.

Securing a SCADA network is a highly contextual activity. Simply validating that servers, storage, communications, and endpoints are operating within security policies is not enough. SCADA security must also be aware of the types of actions that are legally occurring within those policies. As a result, control system awareness must be built into the security products. Effective SCADA security needs inputs from both application and infrastructure sources. Control system event sources such as data historians can provide this enhanced visibility.

Data from control networks is more deterministic than that from enterprise networks. Better control is enabled through the ability to restrict communications to a finite set of predictable transactions. However, data volumes can become enormous when newer technologies such as synchrophasors are deployed. As such, SCADA security products must be able to quickly receive, store, and correlate very large amounts of data.

In short, monitoring and securing a SCADA network requires different actions than those for an enterprise network. The key actions for effectively monitoring SCADA networks are:

- Do nothing that negatively impacts network latency
- Restrict SCADA traffic to known and expected message types
- Isolate the SCADA network from any other networks, including the enterprise
- Collect and analyze from multiple sources beyond only IT events
- Focus on high-quality data rather than lots of voluminous reports
- Where possible, prioritize situational awareness to prevent cyber incidents
- Implement strong change management for all SCADA modifications
- Use security products that are simple to deploy and manage
- Involve SCADA operations personnel in all SCADA security decisions

1.2 **Selecting a SCADA Vendor**

Selecting a SCADA security vendor requires finding a supplier with credible experience and knowledge in SCADA operations, plus full cyber security expertise in IT and OT environments. Monitoring products should include built-in interfaces to multiple data sources such as data historians, physical security systems, and traditional IT devices. Products should be quality and stress tested in a lab environment before acceptance for production use. Look for vendors with a good reputation in the SCADA industry, formalized partnerships with key SCADA and cyber security players, and reference site installations of products that are already beyond pilot stage and performing for an entire organization.

Section 2

KEY ISSUES IN SECURING A SCADA NETWORK

2.1 SCADA Networks Are Different

Control networks are different beasts. SCADA networks manage devices that directly control the physical environment around us, often with immediate impact. If a bank posts erroneous transactions to a customer's account, it can reverse those transactions. However, an electric utility cannot reverse a blackout that has already occurred.

Control networks are deterministic; they process high volumes of mostly predictable data at mostly predictable intervals. Most of the endpoint actors in a control network are machines, not people. Control networks can include many very old devices that have little or no computing power, such as serial process monitors. Those devices are usually replaced when their expected service life ends – no sooner. These factors suggest that securing a control network is *not* identical to securing an enterprise network.

2.1.1 Security Objectives Are Different

Traditional enterprise IT networks have three fundamental security objectives: confidentiality, integrity, and availability. IT security experts appreciate having such a memorable acronym as “CIA” for their objectives. By contrast, control network security objectives can be summarized as safety, reliability, and integrity. Where enterprise security begins by keeping data private, control system security begins by making sure that no one is killed.

The greater real-world emphasis of control network security means that simply analyzing infrastructure events is not enough to achieve security objectives. Personal safety and grid reliability cannot be understood without analyzing application-level events. For example, data that are perfectly formatted under cyber security policies will appear acceptable from an infrastructure perspective. However, those same data may indicate that a grid outage is impending – something that could never be understood by an infrastructure that is simply transmitting bytes. Application intelligence must be added to the mix.

Fraud detection is a good analog in enterprise IT security. Fraudulent transactions are usually perfectly formatted and adhere to security policies – after all, fraudsters are keen to avoid notice. Enterprise IT controls such as firewalls and intrusion prevention systems do not have the business awareness necessary to detect fraud, so application layer security must also be added to the mix.

2.1.2 Critical Infrastructures Are Targets

SCADA networks can control the distribution of commodities such as electricity, water, oil, and gas. As such, they are often considered part of the critical infrastructure of a nation and therefore can become a target for actors hostile to a nation – whether those attackers might be another nation state, terrorists, activists, or organized crime.

SCADA networks present both infrastructure and control system attack surfaces. Analyzing the infrastructure attack surfaces without considering the control system attack surfaces is only half protecting the network.

2.1.3 Cyber Incidents Have Physical Consequences

Attacks against SCADA devices can have direct consequences upon the physical world around us. But intentional attacks are not the only danger to SCADA networks. As discussed in NIST Special Publication 800-82, *Guide to Industrial Control Systems (ICS) Security*, control networks are also at risk from collateral damage due to worms or control system failures, as well as unintentional consequences such as testing or configuration changes gone bad.

The same NIST document lists some well-known control system outages, including:

- Hacking the Worcester, Massachusetts public telephone system shut down phone service at its airport for the control tower, security, fire department, weather service, and carriers that use the airport.
- The Northeast U.S. blackout of 2003 had many contributing factors, including a failure of SCADA software at the transmission operator. A total of 61,800 MW load was lost.
- An unnamed natural gas utility hired a penetration tester that unknowingly attacked the production SCADA network and shut down gas supply to its customers for four hours.

These examples illustrate that even with the best of intentions – such as hiring penetration testers to validate a system – things can go wrong. Control system security is necessary to mitigate the risk of such scenarios.

2.1.4 Summarizing the Differences

Error! Reference source not found., copied from NIST Special Publication 800-82, *Guide to Industrial Control Systems (ICS) Security*, presents a summary of the differences between IT (enterprise) networks and industrial control networks such as SCADA.

Table 2.1 Differing Requirements Between IT and ICS Environments

Category	Information Technology System	Industrial Control System
Performance Requirements	<ul style="list-style-type: none"> • Non-real-time • Response must be consistent • High throughput is demanded • High delay and jitter may be acceptable 	<ul style="list-style-type: none"> • Real-time • Response is time-critical • Modest throughput is acceptable • High delay and/or jitter is not acceptable
Availability Requirements	<ul style="list-style-type: none"> • Responses such as rebooting are acceptable • Availability deficiencies can often be tolerated, depending on the system's operational requirements 	<ul style="list-style-type: none"> • Responses such as rebooting may not be acceptable because of process availability requirements • Availability requirements may necessitate redundant systems • Outages must be planned and scheduled days/weeks in advance • High availability requires exhaustive pre-deployment testing
Risk Management Requirements	<ul style="list-style-type: none"> • Data confidentiality and integrity is paramount • Fault tolerance is less important – momentary downtime is not a major risk 	<ul style="list-style-type: none"> • Human safety is paramount, followed by protection of the process • Fault tolerance is essential; even momentary downtime may not be acceptable

Category	Information Technology System	Industrial Control System
	<ul style="list-style-type: none"> Major risk impact is delay of business operations 	<ul style="list-style-type: none"> Major risk impacts are regulatory non-compliance, environmental impacts, and loss of life, equipment, or production
Architecture Security Focus	<ul style="list-style-type: none"> Primary focus is protecting the IT assets and the information stored on or transmitted among these assets Central server may require more protection 	<ul style="list-style-type: none"> Primary goal is to protect edge clients (e.g., field devices such as process controllers) Protection of central server is also important
Unintended Consequences	<ul style="list-style-type: none"> Security solutions are designed around typical IT systems 	<ul style="list-style-type: none"> Security tools must be tested (e.g., offline on a comparable ICS) to ensure that they do not compromise normal ICS operation
Time-Critical Interaction	<ul style="list-style-type: none"> Less critical emergency interaction Tightly restricted access control can be implemented to the degree necessary for security 	<ul style="list-style-type: none"> Response to human and other emergency interaction is critical Access to ICS should be strictly controlled, but should not hamper or interfere with human-machine interaction
System Operation	<ul style="list-style-type: none"> Systems are designed for use with typical operating systems Upgrades are straightforward with the availability of automated deployment tools 	<ul style="list-style-type: none"> Differing and possibly proprietary operating systems, often without security capabilities built in Software changes must be carefully made, usually by software vendors, because of the specialized control algorithms and perhaps modified hardware and software involved
Resource Constraints	<ul style="list-style-type: none"> Systems are specified with enough resources to support the addition of third-party applications such as security solutions 	<ul style="list-style-type: none"> Systems are designed to support the intended industrial process and may not have enough memory and computing resources to support the addition of security capabilities
Communications	<ul style="list-style-type: none"> Standard communications protocols Primarily wired networks with some localized wireless capabilities Typical IT networking practices 	<ul style="list-style-type: none"> Many proprietary and standard communications protocols Several types of communications media used, including dedicated wire and wireless (radio and satellite) Networks are complex and sometimes require the expertise of control engineers
Change Management	<ul style="list-style-type: none"> Software changes are applied in a timely fashion in the presence of good security policy and procedures; the procedures are often automated 	<ul style="list-style-type: none"> Software changes must be thoroughly tested and deployed incrementally throughout a system to ensure that the integrity of the control system is maintained ICS outages often must be planned and scheduled days/weeks in advance

Category	Information Technology System	Industrial Control System
Managed Support	<ul style="list-style-type: none"> Allow for diversified support styles 	<ul style="list-style-type: none"> ICS may use OSs that are no longer supported Service support is usually via a single vendor
Component Lifetime	<ul style="list-style-type: none"> Lifetime on the order of 3-5 years 	<ul style="list-style-type: none"> Lifetime on the order of 15-20 years
Access to Components	<ul style="list-style-type: none"> Components are usually local and easy to access 	<ul style="list-style-type: none"> Components can be isolated and remote, and require extensive physical effort to gain access to them

(Source: NIST Special Publication 800-82)

2.2 SCADA Data Considerations

2.2.1 Data Are Deterministic

Control network endpoints are machines with specific functions that record their actions and measurements with a defined and fixed set of record types. The implementation of control devices also specifies the frequency of each of these fixed record types. Therefore, unlike with enterprise networks, it is possible to create a reasonably accurate forecast of all the traffic that a control network will generate during normal operations. Specialized situations should be addressed separately in disaster recovery plans.

This deterministic nature allows some shortcuts that are not available to enterprise network management. For example, any transaction type that has not been forecast can be discarded and not processed. However, such unexpected transactions should be passed to the event management and correlation systems for analysis. An unexpected transaction could indicate a mistake in the product installation (where it should have been anticipated). Or an unexpected transaction could indicate unauthorized or unwanted activity on the control network. Regardless, security monitoring of control networks should account for unexpected transactions and ensure that their source is understood and resolved.

2.2.2 Data Are Device-Specific

SCADA devices collect large amounts of data that have specific knowledge about specific operations of the control network. Thus, any analysis of control system events must include an awareness of the content of those events in terms of control system reliability and integrity. This awareness enables better correlation of control system events with security events and helps the event management and correlation systems to operate more efficiently, as discussed below.

2.2.3 Data Volumes Can Become Gargantuan

The electric utility industry is bracing itself for a deluge of information from AMI networks in the form of interval data taken every 15 minutes from each meter. An AMI system of 5 million smart meters would create about 175 billion readings in a year. While that number is indeed large, there are already enterprise networks that process trillions of events per month at larger record sizes than interval readings.

Control systems may generate significantly more data. For example, synchrophasors, while far fewer in number than smart meters, can take readings as frequently as 60 times per second. That equates to 54,000 readings in the same 15 minutes that a smart meter takes one interval reading. At that extreme sampling rate, 74 synchrophasors would

generate as many readings as 4 million smart meters. And synchrophasors represent only one type of control network device.

Control networks can produce extremely large amounts of data, not all of which has cyber security relevance. Managing the security of a control network requires the ability to identify and store the needed control network events without flooding the security system with unnecessary data. Efficient data selection reduces storage volumes and accelerates event correlation.

2.2.3.1 *Correlation Should Merge IT and SCADA Events*

Stuxnet presents perhaps the most compelling example of an attack that combined infrastructure and application attack vectors. On the infrastructure side, there were zero-day attacks involving removable storage devices. On the application side, there were default logon passwords that could not be changed and manipulation of control commands for centrifuges. Stuxnet was a combined attack that had to operate at several layers (including cultural) in order to be effective. Even if a good enterprise SIEM had been in place, it would mostly likely have only observed correctly formatted commands to the centrifuges. Analysis of control codes to physical devices is beyond the scope of an enterprise-only product.

2.3 Other Considerations

2.3.1 SCADA Networks Must Be Isolated from Enterprise Networks

SCADA networks should receive as little data as possible from enterprise networks, and communications from enterprise to control networks should be tightly controlled. In nuclear installations, the control network is often isolated from enterprise networks through communications channels that are one-way at the physical layer, such as data diode deployments. This prevents the relatively unstructured data flows of enterprise networks from entering the deterministic world of control networks.

However, data flows from control networks to enterprise networks can be allowed as long as the enterprise network adequately protects control network data. Correlating enterprise and control network data in a single environment must occur on the enterprise network. Control network event correlation requires the ability to send the required data to the enterprise network while retaining the tight controls on traffic in the opposite direction. These controls are familiar to utilities that have already deployed data historian products.

2.3.2 Monitoring Legacy Devices Can Be Challenging

Many older legacy devices do not have the ability to format and send events to an event manager or a correlation engine. In those cases, the data historian can be conscripted as an event source for devices that cannot themselves generate the events. This requires the event manager and correlation engines to be able to extract relevant information from the data historian in order to have full visibility of control network events. The ideal system for this correlation would be equally competent at identifying, normalizing, and correlating both IT and OT security events.

Section 3

KEY ACTIONS TO SECURE A SCADA NETWORK

3.1 Preserve SCADA Integrity

Control networks share many attributes with enterprise networks, but other aspects are not the same at all. For example, the concept of “real-time” in control and enterprise networks is quite different. An operating system patch that might be applied to an enterprise network several days after it is received. By contrast, some simple patches on a control network may take up to two years to apply due to the need to wait for operations approvals and outage windows.

3.1.1 Monitoring Must Not Disrupt Low Latency

A good credo for control system security comes from medical practice: First, do no harm. Any security that is deployed into a control network must not hinder the network’s ability to function. A key consideration is the low network latency required for successful control network management. For example, a common practice in enterprise network security is to scan the entire network for vulnerabilities every day. Some network administrators validate network stability by pinging every device – as often as once per second – to ensure that it is still online. These same activities can prove extremely disruptive to control network functions such as monitoring and managing an energy transmission grid.

Therefore, passive approaches that do not contribute additional network traffic such as out-of-band network monitors should be employed where possible. Event collection should use existing mechanisms like data historians, rather than adding new collectors and additional traffic to the control network.

3.1.2 Restrict SCADA Traffic to Expected Message Types

SCADA devices produce predictable sets of messages. A temperature monitor produces temperature readings, a flow meter produces flow readings, and so on. Thus, in a well-managed SCADA network where all the devices are known, it is possible to know nearly all the message types that would be encountered in the network. Control consoles and HMIs may contribute a slight amount of unpredictability to the message types.

Any traffic that does not belong on the control network – i.e., it cannot be associated to a device on the network – should be logged for further investigation but otherwise ignored. In some cases, it may be legitimate traffic that was not recognized during the network design. In other cases, it may be illegitimate traffic from rogue devices or users connected to the network. Security event management tools can be set to identify and report such unexpected transactions and correlate them with other events at the same time or location.

Event management tools that can track baselines on this activity (by IP, user, application, or other category) can be configured to alert and notify when legitimate traffic is occurring in higher-than-expected volumes.

3.1.3 Avoid Traffic from Enterprise to SCADA Network

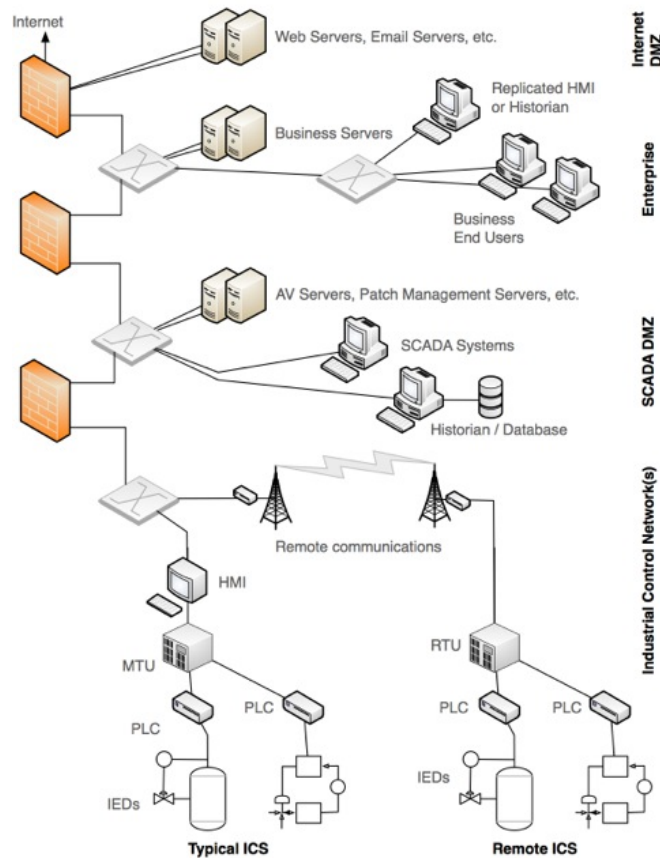
SCADA networks should be isolated from enterprise networks. First, enterprise networks are normally connected to the public Internet – the source of many cyber-attacks – and isolation can mitigate the risk that attacks travel from the Internet to the enterprise to the

control network. Historically, many SCADA networks have been implemented with minimal security and may not be able to withstand many cyber-attacks against which enterprise networks are protected. Additionally, restricting traffic flows helps preserve the low latency required in control networks.

The most common approaches to isolating a SCADA network are demilitarized zones (DMZs) and one-way connections. In either case, the enterprise and control networks consider each other to be mutually untrusted networks.

Figure 3.1 shows a good DMZ deployment that isolates a SCADA network from an enterprise network. In this deployment, each network has its own firewall guarding entrance to the DMZ. All traffic between networks must pass through the DMZ, enabling the respective firewalls to enforce their rule sets. As shown here, it is also possible to place some resources used by both networks, such as the data historian, inside the DMZ. This approach can further reduce traffic between the two networks, with data historians and data servers acting as a proxy for enterprise requests for control network data.

Figure 3.1 DMZ Isolation of Control Networks



(Source: Syngress)

A critical point to remember in Figure 3.1 is that a significant portion of a typical SCADA network may still be using serial protocols. Although nearly impossible to quantify, Pike Research has heard anecdotally that as much as 60% of control systems are still connected using serial protocols. Regardless of the exact percentage, there are still quite

a few products for sale that bridge serial protocols with Ethernet, most with specific SCADA market messages, which indicates demand for this capability. Data historians that can collect data from serial devices can form a substitute event generator for those devices, but only if the data historian is integrated with the security event manager. And it remains true that the security of any network is only as strong as its weakest link, so even just a few serial devices can place a very large network at risk.

A second and stronger approach uses a one-way connection such as a data diode between the control and enterprise networks. This guarantees one-way communications at the physical layer. However, some utilities may require limited two-way communications in certain scenarios. Data diode solutions were originally deployed in nuclear power generation plants, but are now increasingly seen in conventional energy generation environments, plus related industries such as oil and gas.

3.1.4 Strong Change Management for All SCADA Changes

SCADA operations managers have a history and a culture of being extremely conservative with change approvals due to the potential of non-reversible physical consequences if a change were to have unexpected impacts upon the SCADA network. This effect has intensified as IT-capable devices have replaced purpose-built hardware in control networks. There is no logical reason for SCADA managers to relax their conservative approach. Rather, stronger change management is required to better ensure that SCADA network changes or new devices and software can be safely and reliably deployed.

The Information Technology Information Library (ITIL) is focused on IT networks, but many of its approaches such as change management and configuration management can be applied to a control network. Regardless of the approach selected, it is necessary to thoroughly understand and test changes before implementing them in a control network. The preparation should include a back-out plan and back-out triggers.

3.2 Collect All the Relevant Data

3.2.1 Do Not Restrict Monitoring to IT Data

As previously noted, control networks such as SCADA are more contextual than general-purpose enterprise networks. Cyber incidents on SCADA networks usually have physical consequences and, unlike with enterprise networks, it is nearly impossible to separate infrastructure events from application events. Therefore, effective security monitoring of SCADA networks requires access to more than just infrastructure events.

Effective monitoring and security of control networks requires visibility not just to infrastructure components, but also to the control components that are being managed. Consequently, the best-suited tools for securing a control network will have built-in awareness of control network events. This suggests that general-purpose security products from the enterprise world will need some added intelligence to function effectively in control networks.

3.2.2 Large Data Volumes Must Not Delay Correlation Activities

In control networks, speed is of essence. Control networks truly execute in real-time, and seconds lost in collecting and correlating data can be the difference between a near miss and a disaster. Data collection must keep up with the speed at which new events are generated. In many control networks, data historians are already doing this, in the process extracting the relevant data to the historian's server in the DMZ or on the enterprise network. Therefore, if the data historian is adequately coping with event volumes,

interfacing security event correlation to the data historian can collect the required events without any further load on the control network.

Obviously, data must be quickly collected and normalized into a database. One of the most common causes of poor event management performance is a bottleneck in the normalization process. Often, this is due to selecting inappropriate data structures for the amount of data that must be processed. In worst cases, the wait time to normalize events can be multiple days. This would, of course, not be acceptable for a control network that must correlate events and identify incidents in near real-time.

3.2.3 Correlation Tools Must Use Their Understanding of SCADA

Event correlation tools must have not only SCADA awareness, but also the ability to use that awareness in detecting incidents that an IT-only event cannot detect. Below are two sample situations that are caught by casting a wider net that includes non-IT events.

- Many spear phishing or malware attacks in an enterprise network can be easily detected by existing preventive tools or recognized by event correlation tools after the fact. However, a similar attack against a control network might then use an HMI to begin making changes to the control environment. Within the context of infrastructure information, a traditional event correlation tool will see this as application functions following established security policies. Yet, a SIEM that is integrated with a data historian will also see the related set point changes and recognize them as anomalous, triggering an incident that can be investigated. Greater awareness of the control system enables recognition of events that would otherwise be missed.
- Greater visibility into other systems can also provide improved situational awareness. For example, a number of unsuccessful logons to a control console followed by a successful logon could be a forgetful user, one with many passwords to remember, or a remote attacker who has brute-forced the password. It is difficult to know. Add in correlated information from the physical access system and the situation becomes clearer. If the same user has not badged into the control room then either (a) the credentials are being used by someone who is not physically in the control room – which is very bad; or (b) the credentials are being used by someone who entered the control room without badging in, most likely by tailgating. This is not as bad, but still warrants immediate attention. Without the extra visibility into the physical access system, there would be little basis on which to make a decision.

3.2.4 Correlation Tools Must Be Fast

Correlation engines must be able to deal with very large volumes of data – e.g., the synchrophasor taking 60 readings per second for several years – and produce results in a hurry. Every event correlation product will boast something like “unparalleled processing speed with unique correlation” for maximum visibility into a system. In a control network, promises are not enough. Potential performance, as Bear Bryant once said, “means you ain’t done it yet.”

Selecting an event correlation tool for control networks requires performance validation in a lab setting using real-world events and real-world volumes. If possible, the testing should simulate several months or a year of operations. This approach will identify any performance issues before the product is deployed, perhaps before the product is licensed. Additionally, stress testing can expose any problems in data normalization, a frequent but rarely understood cause of poor event correlation performance.

3.3 SCADA Monitoring Must Be Simple

3.3.1 Avoid Products That Are Complicated to Install or Operate

Cyber security product costs can be like icebergs. The parts you can see, license and maintenance prices, are similar to the 10% of an iceberg that is above the ocean surface. The vast bulk of the operating costs, like the vast bulk of an iceberg, are hidden below the surface. The major cost component of most security products is staffing – often five to ten times as expensive as licenses and maintenance. Greater complexity in a security product can mean even larger staffing expenditures. Moreover, increased complexity – especially during deployment – often has a direct causal relationship with increased system outages or errors.

Selecting any security product requires a total cost of ownership (TCO) analysis for the intended service life of the product. A great deal on a product that requires a full-time staff of expensive cyber security experts to operate may not be such a great deal at all.

3.3.2 Do Not Hinder Emergency Response Actions

Control networks present alarms in real-time that require response in real-time. Security products must not do anything to prevent or delay real-time responses to potential problems. As a simple example, transmission grid control consoles may be better off without a password authentication. Fumbling to find a password during a high stress emergency situation could prevent timely actions needed to resolve a problem. Alternate measures such as improved physical security for the control room may be considered.

On a deeper level, incident response may require quick access to control network event data to understand what has happened that requires a response. Systems with simpler human-machine interfaces and more built-in control system intelligence can speed the investigation needed to determine the proper response actions. Likewise, later root cause analysis, after the storm has passed, can proceed more quickly with easier-to-use systems.

3.3.3 Highly Skilled Workers Will Also Be Highly Recruited

A little discussed disadvantage of managing a complex IT system is that very few people are truly qualified to operate them. This creates a strong demand for those few qualified people, so the likelihood of a single utility holding on to such a performer is low. Most technicians with high-demand skills understand and employ the career strategy of changing employers every 18 to 24 months to maximize salary and benefits. Losing a key performer at a key time can leave the SCADA correlation system essentially unmanaged, requiring expensive third-party professional services to fill in the gap until a new candidate is hired. By contrast, a system that arrives fully configured and ready to run with minimal human intervention removes the risk of hiring and then losing highly skilled staff.

3.4 Produce Actionable Data

3.4.1 Quality Not Quantity Matters

Many detective security technologies suffer from a surfeit of false positives. For example, host-based intrusion detection is notorious for producing false positives. Nearly all event correlation products can help mitigate the impact of false positives by understanding when not to worry. A high rate of false positives can be a drain on response time and unnecessarily consume enormous amounts of bandwidth and event storage space. Obviously, it is preferable that a monitoring tool should identify only the few events that require further action or investigation, rather than a large volume of events with the real

problems hidden somewhere in the list. Product testing should include scenarios to ensure that event correlation identifies the needles without reporting the entire haystack.

3.4.2 Prevention Is Better Than Detection – Situational Awareness

As the second example in Section 3.2.3 shows, the right event correlations can detect the *possibility* of an incident before it occurs. Knowing that credentials for a control console have been used when that person does not appear to be in the control room can trigger immediate response. In some scenarios, those responses can prevent disruptive or destructive actions from being taken. Greater visibility into non-infrastructure systems provides a greater ability to recognize irregular situations that should be addressed by identifying illogical situations. Where possible, situational awareness should be preferred over identification of past problems.

That is not to say that detective countermeasures are a bad thing. There will always be attack scenarios that cannot be anticipated, and so there must be enough information available to determine what exactly happened. During first response to an event, sufficient information must be available to determine what actions must be taken immediately to stop or limit the damage. Later on, during root cause analysis, that extra information can inform better decisions to prevent recurrence of the incident.

3.4.3 Focus Is to Preserve Reliability

Control networks exist to preserve the safety and reliability of the distribution or manufacturing processes that they manage. Reliability, in turn, has a heavy dependence upon data integrity. Confidentiality is somewhat less of a concern in control networks, though some data such as user passwords should obviously be kept secret. Again, this points to a greater need for control system awareness in security tools. Whereas an enterprise event correlation system might never have any rules parsing actions taken within the application, event correlation for control networks must include rules to correlate security events with control actions (equal to application actions in an enterprise network). These rules are necessary to find higher-level attacks against the control network.

3.5 Incident Response Must Be Specific to SCADA Incidents

3.5.1 IT Personnel Can Rarely Resolve SCADA Incidents

A SCADA security incident response team must include staff that operate the control network, in addition to IT security experts. Relying solely on IT security experts to respond to control network incidents could result in a far greater follow-on incident than the incident that triggered the response. The operations team members should have last approval for any mitigating actions taken on the control network. Security incident response team members must be immediately available when an incident is declared. This type of availability often requires a commitment from executive-level management to enforce it.

3.5.2 Incidents Can Have Consumer and Public Relations Impacts

Control system cyber events often have physical consequences that are observed – some are extremely obvious – by persons outside the utility. Beyond preventing or detecting incidents, a utility can enhance or destroy its reputation during recovery from an incident. Control networks, such as power grids and AMLs, are an emotional topic among the media and consumers.

Cyber security incident response teams should include a person responsible for media relations. All public statements about the incident and its response should be issued by the assigned media relations expert or by executive team members who have been briefed by media relations.

Section 4

WHAT TO LOOK FOR IN A VENDOR

4.1 Quality of Staff

When considering potential vendors, it is critical to convince yourself that their staff is adequately qualified to produce and manage the products they are proposing to you. In the area of SCADA security, there are two distinct areas where vendor staff should be qualified: SCADA industry background and cyber security background. It is not necessary that a single person have all these qualifications, but the organization must be able to present enough qualified personnel to satisfy you.

4.1.1 SCADA Industry Qualifications

Successful vendors of SCADA security products will employ SCADA industry veterans. Given the newness of this technology, those veterans are often much better versed in control system operations than in cyber security. That is normally acceptable, as they can rely upon the vendor's existing cyber security expertise. A vendor that cannot present staff members with control system experience should be viewed with suspicion. Your own control systems staff will be able to quickly judge the validity of the vendor's claims.

4.1.2 Cyber Security Qualifications

Naturally, any vendor offering cyber security products of any type should have a staff with strong cyber security qualifications. The most widely trusted cyber security certifications are:

- Certified Information Systems Security Professional (CISSP) from (ISC)²
- Certified Information Systems Auditor (CISA) from the Information Systems Audit and Control Association (ISACA)
- Global Information Assurance Certification (GIAC) from GIAC

There are other certifications held by talented and well-qualified cyber security practitioners. Some are specialized for areas such as assessments, architecture, management, or specific hardware platforms. None of these certifications guarantees excellence, but since most require several years' experience and passing a challenging exam, they at least demonstrate commitment to cyber security as a discipline. As with SCADA qualifications, your own cyber security staff will be able to quickly judge whether a vendor's security personnel are sufficiently skilled and experienced to support your requirements.

4.2 Products

4.2.1 Technology

There are multiple effective technical approaches to create a suitable event management and correlation product. Most of those effective approaches are considered trade secrets by their inventors and are not available for review. While some approaches may not be appropriate at all, it is very difficult to determine from marketing literature what technology will work for you.

To identify appropriate products for your situation – and to eliminate those that are not – requires an understanding of the environment in which the product will function. Variables such as transaction rates and times, network topography, and even corporate culture can have a bearing on which product is right for you. Lab demonstrations among selected products can resolve much of the uncertainty. Define the scenarios you must address, including the data volumes and response processes, and then test each product against your requirements. No amount of vendor literature can substitute for actual demonstration. And since event monitoring is often expensive and disruptive to install, many companies only get one chance to get it right before executive leadership cancels the program. So do the right testing to avoid nasty surprises.

4.2.2 Interfaces

SCADA event correlation requires the ability to gather events from many different types of platforms. The most effective products will be those with the widest breadth of platform coverage. In this sense, breadth means branching out beyond traditional IT devices such as firewalls and intrusion prevention systems. An earlier example in this white paper required an interface from the physical access badge reader controller. Other interfaces might be programmable logic controllers (PLCs) or remote terminal units (RTUs). Many of these interfaces can be accomplished via a single interface to a data historian, which already has those interfaces built-in. However, the event manager must still support a taxonomy that understands events from those devices.

4.2.3 Standards

SCADA security still has few applicable standards or regulations, and almost none are globally applicable. Still, a serious vendor will support your compliance with standards that apply to you. In the United States, for example, electricity transmission grids fall under the NERC CIP reliability standards. Compliance with any set of standards can be expensive if it is not built-in to the systems to deploy. Therefore, identify the standards with which you must comply and consider vendors whose products comply with those standards and include pre-built compliance reporting.

Any standards compliance activities that will not be supported by your licensed products should be included in the TCO analysis. Compliance tasks are extremely labor-intensive and can quickly generate large incremental staff expenses.

4.3 SCADA Industry Reputation

Event management and correlation is not a great place to be a pioneer. Leave the early adopting for those with less to lose. When considering vendors, speak with peer companies in your industry and your other technology providers. How well is each company known within SCADA circles?

4.4 Industry Partnerships

4.4.1 SCADA Partners

SCADA security vendors can build better products when they are well connected to the SCADA industry itself. Therefore, consider first those vendors that can demonstrate working, formalized partnerships with SCADA technology providers. Ask to have staff from the SCADA partners in the meetings with your prospective vendors. This will enable you to assess the degree of integration and cultural fit between your vendors and their SCADA partners. Ask probing questions about how the SCADA partners make your vendors' products better.

4.4.2 Security Partners

Since you will be dealing with a cyber security vendor to begin with, partnerships with other security vendors are less important than partnerships with SCADA companies. However, partnerships with other security vendors can add depth to the vendor's offerings by integrating well-trusted technologies into the product set. Again, look for working, formalized partnerships and ask to have some of the partner staff attend your meetings with your prospective vendors.

4.5 Successful Implementations

Continuing the theme that this is not the best place to be an early adopter, insist upon visiting or at least speaking with several reference clients that are up and running with the same technology that you intend to license. Even if it requires a non-disclosure agreement, do it. Do not accept reference visits for pilot programs, nor for programs that are still in implementation phase. Include members of your control systems operations team in the reference visits or contacts so that the relevant operational issues will be discussed.

Visit clients that are running a large-scale deployment of the same technology. Speak with key performers in several areas – the chief information officer, chief security officer, chief operating officer, and as many operations executives as the client will let you contact. Speak with the chief purchasing officer (or equivalent) to find out how negotiations with the vendor are conducted. Ask the chief security officer if you may speak with the manager of the incident response team.

In summary, restrict your search to vendors that can demonstrate satisfied clients running their products on a large scale.

Section 5

ACRONYM AND ABBREVIATION LIST

Advanced Metering Infrastructure	AMI
Antivirus.....	AV
Certified Information Systems Auditor	CISA
Certified Information Systems Security Professional.....	CISSP
Confidentiality, Integrity, and Availability.....	CIA
Control System Security Program.....	CSSP
Critical Infrastructure Protection.....	CIP
De-Militarized Zone (between two untrusted networks).....	DMZ
Global Information Assurance Certification.....	GIAC
Human-Machine Interface.....	HMI
Identity and Access Management.....	IAM
Industrial Control System.....	ICS
Information Systems Audit and Control Association.....	ISACA
Information Technology Infrastructure Library	ITIL
Information Technology.....	IT
Intelligent Electronic Device	IED
International Standards Organization	ISO
Internet Protocol.....	IP
Master Terminal Unit.....	MTU
Megawatt.....	MW
National American Electric Reliability Corporation	NERC
National Institute for Standards and Technology (U.S.)	NIST
Operating System	OS
Operations Technology	OT
Programmable Logic Controller	PLC

Remote Terminal Unit	RTU
Security Information and Event Management.....	SIEM
Supervisory Control and Data Acquisition	SCADA
Total Cost of Ownership.....	TCO
United States.....	U.S.

Section 6

TABLE OF CONTENTS

Section 1	1
Executive Summary	1
1.1 Introduction.....	1
1.2 Selecting a SCADA Vendor	2
Section 2	3
Key Issues in Securing a SCADA Network	3
2.1 SCADA Networks Are Different.....	3
2.1.1 Security Objectives Are Different	3
2.1.2 Critical Infrastructures Are Targets.....	3
2.1.3 Cyber Incidents Have Physical Consequences	4
2.1.4 Summarizing the Differences	4
2.2 SCADA Data Considerations	6
2.2.1 Data is Deterministic	6
2.2.2 Data is Device-Specific	6
2.2.3 Data Volumes Can Become Gargantuan.....	6
2.2.3.1 Correlation Should Merge IT and SCADA Events.....	7
2.3 Other Considerations	7
2.3.1 SCADA Networks Must Be Isolated from Enterprise Networks	7
2.3.2 Monitoring Legacy Devices Can Be Challenging	7
Section 3	8
Key Actions to Secure a SCADA Network	8
3.1 Preserve SCADA Integrity.....	8
3.1.1 Monitoring Must Not Disrupt Low Latency	8
3.1.2 Restrict SCADA Traffic to Expected Message Types	8
3.1.3 Avoid Traffic from Enterprise to SCADA Network.....	8
3.1.4 Strong Change Management for All SCADA Changes.....	10
3.2 Collect All the Relevant Data	10
3.2.1 Do Not Restrict Monitoring to IT Data	10
3.2.2 Large Data Volumes Must Not Delay Correlation Activities.....	10
3.2.3 Correlation Tools Must Use Their Understanding of SCADA	11
3.2.4 Correlation Tools Must Be Fast.....	11
3.3 SCADA Monitoring Must Be Simple.....	12
3.3.1 Avoid Products That Are Complicated to Install or Operate	12
3.3.2 Do Not Hinder Emergency Response Actions	12
3.3.3 Highly Skilled Workers Will Also Be Highly Recruited.....	12
3.4 Produce Actionable Data	12
3.4.1 Quality Not Quantity Matters	12
3.4.2 Prevention Is Better Than Detection – Situational Awareness	13
3.4.3 Focus Is to Preserve Reliability.....	13
3.5 Incident Response Must Be Specific to SCADA Incidents	14
3.5.1 IT Personnel Can Rarely Resolve SCADA Incidents.....	14
3.5.2 Incidents Can Have Consumer and Public Relations Impacts.....	14
Section 4	15
What to Look for in a Vendor	15
4.1 Quality of Staff.....	15
4.1.1 SCADA Industry Qualifications.....	15
4.1.2 Cyber Security Qualifications	15

4.2	Products	15
4.2.1	Technology	15
4.2.2	Interfaces	16
4.2.3	Standards	16
4.3	SCADA Industry Reputation.....	16
4.4	Industry Partnerships	16
4.4.1	SCADA Partners	16
4.4.2	Security Partners	17
4.5	Successful Implementations	17
Section 5	18
Acronym and Abbreviation List	18
Section 6	20
Table of Contents	20
Section 7	22
Table of Charts and Figures	22
Section 8	23
Scope of Study	23
Sources and Methodology	23

Section 7

TABLE OF CHARTS AND FIGURES

Figure 3.1	DMZ Isolation of Control Networks.....	9
Table 2.1	Differing Requirements Between IT and ICS Environments	4

Section 8

SCOPE OF STUDY

This white paper examines cyber security issues for industrial control systems with a specific focus on security event monitoring as it applies to industrial control networks such as SCADA. Pike Research aims to present an objective analysis of the issues faced in monitoring security events for SCADA networks, as well as various approaches to resolving those issues. This white paper does not recommend any specific vendor products or forecast any market sizes.

Analysis in this white paper includes earlier research conducted for Pike Research reports on smart grid cyber security and industrial control security. For those reports, we interviewed a wide variety of stakeholders, including utilities, security vendors, systems integrators, component manufacturers, and well-known subject matter experts. Note that Pike Research analyzes the state of cyber security in a given marketplace by comparing it to widely accepted baselines such as ISO 27002:2005, NIST 800-82, U.S. Department of Homeland Security CSSP Defense-in-Depth, and NERC CIP standards. Additionally, we perform a significant amount of secondary research by tracking the deployment of smart grid technologies and following trends in the smart grid marketplace.

Cyber security is an extremely broad market with hundreds of established providers and countless startups. To examine every possible security provider in the smart meter market would have produced a report of incredible length. Therefore, Pike Research surveyed a representative population of stakeholders to obtain a comprehensive picture of smart meter security while limiting the report to a practical size. To do this, we selected only a few stakeholders from each area of the control network environment.

SOURCES AND METHODOLOGY

Pike Research's industry analysts utilize a variety of research sources in preparing Research Reports. The key component of Pike Research's analysis is primary research gained from phone and in-person interviews with industry leaders including executives, engineers, and marketing professionals. Analysts are diligent in ensuring that they speak with representatives from every part of the value chain, including but not limited to technology companies, utilities and other service providers, industry associations, government agencies, and the investment community.

Additional analysis includes secondary research conducted by Pike Research's analysts and the firm's staff of research assistants. Where applicable, all secondary research sources are appropriately cited within this report.

These primary and secondary research sources, combined with the analyst's industry expertise, are synthesized into the qualitative and quantitative analysis presented in Pike Research's reports. Great care is taken in making sure that all analysis is well-supported by facts, but where the facts are unknown and assumptions must be made, analysts document their assumptions and are prepared to explain their methodology, both within the body of a report and in direct conversations with clients.

Pike Research is an independent market research firm whose goal is to present an objective, unbiased view of market opportunities within its coverage areas. The firm is not beholden to any special interests and is thus able to offer clear, actionable advice to help clients succeed in the industry, unfettered by technology hype, political agendas, or emotional factors that are inherent in cleantech markets.

Published 3Q 2011

© 2011 Pike Research LLC
1320 Pearl Street, Suite 300
Boulder, CO 80302 USA
Tel: +1 303.997.7609
<http://www.pikeresearch.com>

This publication is provided by Pike Research LLC (“Pike”). This publication may be used only as expressly permitted by license from Pike and may not otherwise be reproduced, recorded, photocopied, distributed, displayed, modified, extracted, accessed or used without the express written permission of Pike. Notwithstanding the foregoing, Pike makes no claim to any Government data and other data obtained from public sources found in this publication (whether or not the owners of such data are noted in this publication). If you do not have a license from Pike covering this publication, please refrain from accessing or using this publication. Please contact Pike to obtain a license to this publication.