PikeResearch
Cleantech Market Intelligence

Research Report

Convergence in Automation Systems Protection

Monitoring, Managing, and Securing Control Systems

Published 4Q 2011

Commissioned by Industrial Defender, Inc.

Bob Lockhart
Senior Analyst

Bob Gohn
Vice President, Research

Section 1

EXECUTIVE SUMMARY

1.1 Introduction

Automation systems seem to add new technical capabilities almost daily.

Modern automation systems use information technology (IT) capabilities to provide better control of the automation. Those IT capabilities require security, regulatory compliance, and operations management like never before. They must be managed, monitored, and protected. Since those three functions have significant overlaps in process and in data, integration among the three functions is possible.

This white paper posits an integrated solution for security, compliance, and operations management of control systems. The integrated solution can take advantage of inherent overlaps, leading to a number of benefits that include:

- Reduced expense
- Lowered risk
- Reduced labor
- Less complexity

All of these benefits can be quantified, meaning that security, compliance, and operations improvements can be justified with measurable benefits rather than emotional assertions. As automation systems pile on more and more enhancements, old control system approaches no longer suffice. The inherent complexity of those enhanced systems is greater, but as this paper will discuss, much of that complexity can be managed by systems rather than by people.

The future of automation systems for any given enterprise may hold risks, fines, and inefficiency. Or it can hold better business operations and competitive advantage. It all hinges on how the automation systems are managed, monitored, and protected.

Section 2

THREE KEY PROBLEMS IN MANAGING AUTOMATION SYSTEMS

2.1 Cyber Security

New control system technologies can manage, monitor, and optimize automation systems in real time. Visibility and control are available as never before. However, those improvements come with operating systems, applications, and hardware that can be attacked in ways that their mechanical forebears could not.

Adding automation smarts by using IT capabilities requires that sufficient cyber security be deployed at the same time. Unfortunately, many deployments of automation, such as smart grid upgrades, ignored cyber security during initial installation and may now require expensive and disruptive retrofits of security into live production environments. While such retrofits are necessary to apply appropriate protection, they are fraught with the risk of business disruption.

Unlike enterprise IT networks, securing a control network or an automation system requires real-time visibility into that network. Enterprise network security focuses on confidentiality, integrity, and availability, which can largely be obtained through visibility and control of the infrastructure-level transactions. However, automation systems place a greater premium on safety and reliability, which cannot be achieved simply through understanding the infrastructure. Control system security requires an understanding of the data being transported through the infrastructure.

Controls that rely upon modern IT capabilities require the same type of network management and security management as has been seen in enterprise IT networks for the past two decades. Control centers, such as network operations centers (NOCs) and security operation centers (SOCs) can enable better visibility and protection of a network by processing immense amounts of routine data automatically and saving only the exception cases for human intervention. Some security devices are known to produce false alarm rates as high as 99%. A well-designed operations center can automate response to those false alarms.

2.2 Governance and Regulatory Compliance (GRC)

Automation systems may have to comply with various regulatory requirements, depending on local jurisdictions and the types of systems being managed. Some entities, such as utilities, may face a wide variety of compliance requirements, such as:

- Sarbanes-Oxley, if the utility is publicly traded in the United States
- Payment Card Industry (PCI) data security standards, for credit card payments
- North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards for critical cyber assets that are part of the bulk electric system
- NERC nuclear regulations for nuclear generation assets
- Data privacy regulations in many jurisdictions, if personally identifiable information will be collected, stored, or processed

Other industries like manufacturers may have to deal with regulations such as the U.S. International Traffic in Arms Regulations (ITAR) or the Chemical Facility Anti-Terrorism

Standards (CFATS), depending on what is being manufactured.

Nearly all of these regulations require companies to use operational procedures that comply with the regulations, to demonstrate that the processes are being monitored and to prove that the processes are operating within the parameters specified by the regulations. This can take many different flavors, but, in nearly all cases, requires that a large amount of specific data be collected from the automation systems. An automated capability to collect and measure automation system events can greatly reduce the labor expense needed to demonstrate compliance with the appropriate regulations. Also, a well-designed event collection system can indicate immediately when an automation process has ceased to comply with applicable regulations. This can trigger early correction of the noncompliance, which is generally less expensive than remedying noncompliance discovered during an audit.

Finally, nearly all compliance regimes require an authoritative database of the assets that are in-scope for that regulation.

2.3 Control System Operations

Industrial control systems enable the sophisticated management of complex functions, such as commodity distribution (e.g., electricity, water, gas), or complex manufacturing processes, such as chemicals or pharmaceuticals. These management capabilities can provide real-time feedback on the status of the process or distribution being managed and, in many cases, take action without human intervention, such as shutting down a process or modifying a set point.

Some of these management capabilities rely on modern information technology capabilities, while others are mechanically driven. The control parameters and decision matrices have often been developed over decades of experience in managing the control environment and may even be a competitive differentiator in the marketplace.

Regardless, simplicity is the key. Control networks are large and complex and so is the underlying IT that automates those networks. Control system deployments of IT should require very little on-site IT expertise by control system operators. This is possible because control networks are quite a bit more deterministic than enterprise networks, so many assumptions can be made to reduce the administrative workload. Not only does this reduce the risk of error, but it can reduce the expense of monitoring control systems.

An assembly of point solutions requires a company to know too much about the technical details of each component. A well-integrated solution can eliminate the need to understand touch-points between different technologies and can reduce the chance of error in communicating between different solutions.

A company with a large enough engineering staff can purchase all the individual components and then engineer the appropriate interfaces between those components. Or, it can purchase a suite of components that has already been integrated by the vendor. This integrated approach can be less prone to error and require a shorter deployment project, resulting in control and protection that is available much sooner than a custom solution. Purchasing an integrated solution also means that the company does not need highly qualified engineers on staff to integrate the point solutions.

Section 3

WE HAVE MOST OF THE SOLUTION PIECES BUT NONE OF THE GLUE

3.1 No Architecture

Many automation systems, such as supervisory control and data acquisition (SCADA) networks, have evolved over several decades, meaning that a master plan never existed for their final state. New automation capabilities might have been added as a result of entering new business areas, the availability of new technology, or to reduce the cost of an existing process. However, it is rare that the entire automation system was developed based on a single architecture or framework that identifies the applicable policies to protect, monitor, and manage the system. More likely, its development has been opportunistic over the years.

3.2 Managing Control Networks Is Challenging

The lack of architecture makes control network management challenging. First, network topology often does not exist to define exactly what communications are in place. Second, the lack of an architecture may mean that many non-compatible solutions have been deployed. So, it may incorrect to assume that all the automation capabilities interface with each other and form a working whole, unless quite a bit of customization has occurred.

3.3 Change Must Be Managed

Automation systems are rightly famous for the rigorous change management by which new processes are added to a control system or existing ones are modified. This is due to the great risk of physical consequences from unexpected impacts of a change. However, the same change control disciplines have not been implemented into the IT capabilities that enable modern automation systems. For example, operating system patches may require 1-2 days for deployment into an enterprise IT system, but the same patches may require more than a year for deployment into an automation system. Some control system vendors pre-package operating system patches to reduce IT support needed onsite. This can reduce this patch window, in turn, reducing the exposure to current threats. Strong change management and configuration management can also reduce effects from the law of unintended consequences.

3.4 Attackers Take the Path of Least Resistance

Meanwhile, cyber-attacks are often based upon a systematic probing of the control network until the attackers can find a weak spot. An assembly of strong cyber security capabilities may not prevent an attack if inconsistent interfaces exist between the various protections. Again, this requires a well-integrated security solution that is overseen by engineers whose only job is to ensure that integration. Those engineers might be in-house for a specific company or employed by the cyber security vendor.

3.5 Control Systems SOCs or NOCs Are Not Often Deployed

The underlying computing, networking, and storage capabilities that enable automation system protection, monitoring, and management may not be well-understood in a given company. While it is common to see large and sophisticated control rooms for power grids or manufacturing plants, the NOC approach that is commonly seen in enterprise networks is rarely found in control networks.

Section 4
THE SOLUTION

4.1 Security/Compliance/Operations

4.1.1 Integrate Three Management Functions into a Single Solution

Security, compliance, and operations management have many overlapping functions and data requirements that can be reduced to a single set of data and functions. For years, security practitioners have warned that security is not the same thing as compliance, although compliance functions are often a subset of security functions, with some regulation-specific reporting appended. The concept of a subset clearly implies that these overlapping functions only need to be done once.

Operations systems management is a more recent discipline, as more and more IT technologies are overlaid on control systems to produce smart grids, intelligent manufacturing, and similar optimized operational environments. Operations management also uses many of the same functions as security and compliance to meet challenges, such as improved visibility into a control network and better ability to prevent outages or disruptions. Other processes like incident and problem management can have significant overlap among security, compliance, and operations.

No matter what the process, the functions common to all three areas – security, compliance, and operations – only need be done once.

4.1.2 Use the Same Information to Solve Multiple Challenges

An obvious benefit of combining security, compliance, and operations into a single solution is that the same information can be used for all the purposes. For example, all three areas require an accurate asset register: it is difficult to secure assets unless you know what assets you have; it is impossible to demonstrate compliance for assets of which you are unaware; and you can only manage those assets that you know exist.

Many control systems have old or incomplete asset registers, as changes have been made over the years or decades. The process of creating an asset register of record is difficult enough to do once – to create and then keep three separate registers synchronized with the same information makes no sense at all.

4.1.3 Bring Both Operations and IT into the Solution

Perhaps the most critical error that companies make when managing and protecting their control systems is building a solution without input from all the stakeholders. Critically, IT and operations teams should have input into each solution that will be applied. Very few people understand both IT and operations concepts at a deep enough level to fully define both sets of requirements for control network protection. And both teams must have a seat at the table and a voice in the deliberations on what solutions will be adopted.

Implementing a solution to manage, monitor, or protect a control network that does not include input from both IT experts and operations experts is only half a solution. In many cases, significant cultural hurdles may need to be overcome, but it is essential to bridge any chasm between the two teams so that an open dialogue can produce the best possible security, compliance, and management solution.

4.2 Process Improvements Available

Bringing security, compliance, and operations management under a single umbrella can bring significant benefits to several aspects of the business. Those activities can be achieved at a lower cost, while reducing complexity and error rates – all of which are measurable ROIs.

4.2.1 Reduce Cost

Combining management of security, compliance, and operations can be an immediate cost reduction from the decreased amount of technology necessary to perform these functions, such as reduced processing, reduced storage due to data used in all three functions, and reduced communications required when the same system performs all three functions.

Possibly more significant, the largest cost driver in these systems is most often the staff required to manage and operate them. Having a system that performs all three functions in one and focuses on simplicity, the operation of the system becomes more straightforward and requires fewer staff, with less rigorous training requirements.

4.2.2 Reduce Errors

Combining multiple management functions into a single system can reduce error rates in several ways. First, it simply requires less work, so processes with an expected human or process error rate result in fewer errors. The definition of "an error" can be vague – a single error may require reprinting a compliance report or it may require recovering from a citywide blackout. Reducing staff and cost needed for day-to-day operations enables more time to focus on improvements to reduce the number of high-impact errors.

Merging three functions into a single control management system can also reduce errors by reducing the amount of data capture or processing operations that must be performed. Additionally, changes that affect all three systems – security, compliance, and operations – need only be made once.

4.2.3 Reduce Financial Consequences

Reducing errors directly feeds reduced financial consequences. Unlike IT cyber incidents, a control system cyber incident can have immediate physical consequences. These consequences, such as power outages or manufacturing disruptions, can have both immediate and long-term financial consequences. The immediate consequences can be lost revenue from the inability to sell a product or a commodity.

Longer-term financial consequences may emerge from legally mandated non-performance penalties, performance credits based on service level agreements, equity devaluation of publicly traded securities, or even legal action brought by those affected by the outage. Control systems that can be proven more reliable may also result in lower corporate risk premiums when risk transfer strategies are used.

4.2.4 Reduce Process Duplication

Security, compliance, and operations management sometimes require identical processes. Consider the processes necessary to collect and analyze control network events. Those events must be captured from control system devices, mapped to the appropriate taxonomy for specific processing, normalized, stored, correlated, and reported – to name but a few functions. Security must do all of these functions so that countermeasures can be activated when necessary and to provide visibility to operations staff for exceptional

circumstances. Compliance requires the same processes, so that the appropriate evidence can be identified, extracted, and reported, depending on what audits are being prepared. And operations management needs the same processes so that timely decisions about control settings can be made. Would it make more sense to perform the same functions three times – once for each system – or to perform them once and make the results available to all three systems?

4.2.5 Reduce Labor Requirement

Compliance can be a huge labor sink. The amount of staff required to assemble evidentiary documentation can be truly frightening in the absence of an automated compliance solution. If activities like security and operations management are not done in the same manner as compliance, then it is likely that the information needed for compliance will not be available in compliance formats, but only in formats that serve the needs of security or of operations management. This adds yet more labor requirements to create and validate compliance-specific reports.

Some of the activities required for collecting and correlating control system events can require highly skilled individuals to define and operate those systems. Such high skill levels often demand higher pay grades and the needed resources may be in short supply.

4.2.6 Reduce Complexity

As noted earlier, simplicity is key. A single manufacturing plant may have over one million process measurements being taken at one-second intervals. It is critical that such complex environments operate with as little process variance and human intervention as possible, so that control can be automated. As an additional benefit, reduced complexity can enable stronger security by creating fewer exception situations, which is usually when vulnerabilities are found, and by making compliance easier to measure and demonstrate.

4.3 Replace Fear, Uncertainty, and Doubt with ROI in Security Programs

One of the biggest failings of traditional cyber security programs is their inability to demonstrate a measurable ROI. Many cyber security projects are, therefore, justified with the threadbare triad of fear, uncertainty, and doubt (FUD). As the past three decades have shown in the enterprise IT world, this is seldom a winning strategy, especially when being sold to executives who have made their careers by successfully taking on risk. For some, minimal security is just another risk to be managed.

As the sections above have indicated, improved and collaborative management of security, compliance, and operations can produce measurable financial returns. Scare tactics can be replaced by a business case. And the often asked question, “What am I getting for my money?” can finally be answered.

4.4 Focus on the Business Instead of the Administration

The reduction of cost, labor, errors, and duplication means that the company that uses this approach has more money and staff to apply to its core business, rather than to the administrative activities needed to manage a control network. Fewer outages also mean fewer times that a staff member is disrupted from their normal day-to-day work in order to respond to a crisis. Even the public face of a corporation can be improved with fewer outages, resulting in fewer bad news scenarios to manage.

Section 5
WHAT IF WE DO NOT SOLVE THIS?

5.1 Risks

Operational risks, such as outages and disasters, have been well understood by control systems managers for decades. While risks, by definition, can be managed but never eliminated, stronger management of security, compliance, and operations can be effective in reducing both probability and potential impact of known risks.

Cyber asset risks are relatively new to control systems and only became popular with the 2010 identification of Stuxnet, which had been operating with impunity for nearly a year before it was discovered. Most cyber-attacks against control systems have been sweeping in nature, looking for or exploiting a fault that may exist in many installations. However, like Stuxnet, some well-targeted attacks have occurred, such as Night Dragon, which appears to specifically target competitive intelligence gathering from oil & gas systems. How the collected information will be used has not yet been observed.

5.2 Penalties

Poor management of security, compliance, or operations can result in large fines. The most familiar penalties are fines for non-compliance, such as NERC's ability to levy fines up to $1 million per day per violation. One large U.S. utility paid NERC a fine of $25 million for noncompliance. The reported fine for a U.S. gas pipeline explosion during 2008 was $38 million, exacerbated by the utility's perceived inadequacies within control system management.

In the private sector, large distribution or manufacturing agreements can include heavy performance credits if mutually agreed service levels are not achieved. Outages due to insufficient cyber security may result in settlements under civil law if the company cannot demonstrate that it has applied due care to the protection of its cyber assets.

5.3 Inefficiencies Continue

Using three separate solutions when one would suffice can result in increased operating costs for hardware, software, communications, and staffing, as well as increased capital expenditures. And the non-overlap of systems that process lots of identical data and processes may preserve operational inefficiencies that could otherwise be eliminated.

5.4 Some Enterprise IT Techniques Can Be Applied

Many of the techniques suggested in this white paper can be borrowed from enterprise IT networks. Security and compliance have long been intertwined, with compliance often the driving factor for the purchase of enterprise IT security products. Capabilities like security event management can be used to produce reports for compliance activities, such as Sarbanes-Oxley. Those approaches can be carried over to control environments and take advantage of the deterministic nature of control networks to prepackage IT capabilities that require little maintenance. Similarly, enterprise IT networks use processes like the Information Technology Infrastructure Library (ITIL) to define a configuration management database (CMDB), which can be a system of record for the operational management of devices, such as servers, storage, and telecommunications. The CMDB can equally be an input into cyber security and compliance functions, which are also asset-based.

Section 6

SUMMARY

6.1 In Brief

As noted several times in this white paper, monitoring, management, and protection of automation systems continue to advance through the application of IT capabilities and can be made more efficient by integrating these three functions into a single solution that takes advantage of overlapping processes, data, and technology needed by each. An integrated solution to security, compliance, and operations can reduce workload and expense by processing more of the complexity inside the system itself and freeing the company to focus on running its business more effectively. And unlike traditional enterprise networks, the IT that is integrated into a control network must be well-packaged to avoid the need for high levels of IT skills on the control network.

Reduced complexity also implies lower staffing requirements and staff positions that do not require highly trained individuals that might be expensive and in short supply. Companies that continue to use traditional approaches to control system management, including a near-firewall between IT and operations teams, run the risk of being left behind as their competitors discover more efficient approaches to these problems.

The changes are only just beginning.

Section 7

ACRONYM AND ABBREVIATION LIST

Chemical Facility Anti-Terrorism Standards ..... CFATS

Configuration Management Database ..... CMDB

Critical Infrastructure Protection ..... CIP

Fear, Uncertainty, and Doubt ..... FUD

Governance and Regulatory Compliance ..... GRC

Information Technology ..... IT

Information Technology Infrastructure Library ..... ITIL

International Traffic in Arms Regulations ..... ITAR

North American Electric Reliability Corporation ..... NERC

Network Operations Center ..... NOC

Payment Card Industry ..... PCI

Return on Investment ..... ROI

Security Operations Center ..... SOC

Supervisory Control and Data Acquisition ..... SCADA

United States ..... U.S.

Section 8

TABLE OF CONTENTS

Section 9

SCOPE OF STUDY

This white paper examines security, compliance, and operations management issues for automation systems, such as SCADA and distributed control networks. The goal of this white paper is to suggest an approach for securing, monitoring, and managing automation systems that can take advantage of the latest technical advances, while at the same time enable companies to reduce the burden of managing those environments. This white paper does not recommend any specific vendor products or forecast any market sizes.

Research for this white paper also includes earlier research 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. 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. Pike Research also performs a significant amount of secondary research by tracking 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 as complete a picture as possible of smart meter security, while limiting the report to a usable 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 4Q 2011

1320 Pearl Street, Suite 300
Boulder, CO 80302 USA
Tel: +1 303.997.7609
http://www.pikeresearch.com