Risk Drives Industrial Control System Cyber Security Investment

Executive Overview .................................................................3
Game Changers for Industrial Control System Cyber Security ..........4
Risk Analysis Drives ICS Security Investment .............................8
Industry Trends Mean Change for ICS Owners .............................9
Siemens Security Strategy for ICS .............................................16
Conclusions and Recommendations ..........................................19
Industrial Control Systems (ICS) Cyber Security Requires an Evolving Set of Components

Stuxnet Demonstrated that Potential Risk is High
What Level Should You Use for Investing in Security?
Executive Overview

Industrial control systems (ICS), commonly encompassing “DCS”, “PLC”, “SCADA” and others, use many of the same technologies as corporate systems and are just as vulnerable. However, the consequences of successful attacks against and infections of ICS can be much more serious and damaging. Safety, environmental impact, business sustainability and other factors are at risk.

The Stuxnet event provided evidence that all systems are vulnerable when attackers have the needed resources, skills, and sufficient time. From a risk perspective, Stuxnet provides a metric on the high end of the risk scale. This risk level is not new – we have always known it was possible – but the Stuxnet event transformed this ultimate risk from a remote possibility to something very real. Consequently, it eliminated arguments that we do not have to consider this level of risk.

ICS security strategies, components and processes have a different lifecycle than the control systems themselves. Control components are designed for a purpose, installed, and then just operated for many years. The lifecycle for ICS cyber security elements is much more dynamic and more strongly driven by industry trends such as regulations with associated penalties, changing security technologies and practices, and, of course, the dynamic nature of cyber security in general.

Industrial control systems suppliers are quite similar in their general perspective toward cyber security, although significant differences exist in organization, processes, products, and partnering details. Many of these differences are due to product type and diversity, industries served, and customer exposure and expectations.

Mid 2010, ICS security was thrust into the spotlight with the discovery of the malware labeled “Stuxnet.” The Stuxnet ICS attack appeared to be highly funded, persistent, and targeted. It targeted the operations of only a few facilities that happened to be using Siemens automation products. The surprising focus of this attack forced all automation system suppliers to re-examine their business approach to cyber security, eliminate gaps previous-
ly viewed as low risk, and improve practices in general. Across the industry, suppliers are adding and improving processes, strengthening partnerships, and adding products to help high-risk customers improve their security posture.

The participation of ICS suppliers, such as Siemens, in customer ICS security planning, design, implementation, mitigation, and maintenance continues to grow in importance. All ICS owners should build a collaborative relationship with their supplier, including becoming familiar with the supplier’s cyber security organization.

The Stuxnet attack certainly provides both a high-level metric and a good reference case for all to consider. ICS owners should perform formal risk analysis to determine the likelihood that their businesses will be the target of such a sophisticated attack and weigh that against cost of the necessary protections and consequences.

### Game Changers for Industrial Control System Cyber Security

Industrial control systems (ICS) use many of the same technologies as corporate systems and are just as vulnerable. However, the consequences of successful attacks and infections of ICS can be much more serious and damaging. Safety, environmental impact, business sustainability, and other factors are at risk. Consequently, ICS cannot be part of corporate servers, desktops, laptop, and mobile security processes. Furthermore, most agree that ICS components must be protected using processes, policies, and tools that are selected and configured specifically for ICS environments.
Public Realization that ICS are Essential to Critical Infrastructure

ICS are used in almost all forms of manufacturing, as well as many other industries, and include a diverse set of components. ICS, such as DCS and PLC-based applications, include unique devices and software such as sensors, actuators, speed control, switches and a very wide variety of automation software components.

ICS also include and connect with considerable off-the-shelf infrastructure and technology. In fact, ICS suppliers and owners use as much commercial off-the-shelf information technology as possible. This gives ICS owners the most capability for their budgets, and reduces R&D costs for ICS suppliers – no supplier could survive otherwise. The problem is that these same commercial products are common targets for hackers, cyber criminals, and malware, thereby increasing safety, environmental, business, and other risks. ICS owners and suppliers have been balancing these risks against security-focused investments for more than ten years now, but recently the game has changed because they are under considerably more scrutiny.

The technology situation with physical infrastructure such as electrical power generation and distribution, transportation systems, water and waste systems, building automation and others is similar to manufacturing. Some form of control system is essential to the operation of most physical infrastructure and the use of commercial components is maximized. The difference is that the consequences of a successful attack against infrastructure can be far reaching, potentially impacting a large part of a nation’s population. This makes physical infrastructure likely targets for terrorists, criminals, and hostile nations.

However, the owners of these systems are typically less technical (with small or no ICS security experts on staff) than their manufacturing counterparts and consequently less likely to have comprehensive cyber security programs in place, making them high risk.

<table>
<thead>
<tr>
<th>ICS Component Classes</th>
<th>Security Consideration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unique Devices</td>
<td>Controllers, valves, sensors, field busses, HMI, historian, Engineering stations ...</td>
</tr>
<tr>
<td>ICS Infrastructure</td>
<td>PCs, Servers, Network devices, protocols, Wireless, firewalls, security appliances, intrusion protection, identity management, monitoring, ...</td>
</tr>
<tr>
<td>Technology Platform</td>
<td>Operating System, relational database, integration software, browsers, PDF readers, portal environments ...</td>
</tr>
</tbody>
</table>

**Industrial Control Systems Contain Many Non-Control, General Purpose Components**
The growth of criminal activities and their targeted attacks raised ICS owner concerns somewhat, but banks and other commercial business were more lucrative targets with more immediate rewards.

Public Awareness Demands a Business Response

In the 1990s and early 2000s, the ICS cyber security activities of manufacturing and most physical infrastructure industries were not very visible (or interesting) to the general public, politicians, or the news media. This enabled operators and owners to set their attention to ICS cyber security at any level they wanted. Some organizations and industries took security very seriously, but others did not.

The situation now is much different. Nations now realize that poorly protected physical infrastructure could be an easy target for terrorists and hostile nations. Politicians have called for government action and made this risk visible to their constituents. This has resulted in the creation of government agencies and other groups intended to guide or force owners of ICS to implement adequate cyber security practices. Businesses in many industries can no longer decide for themselves, but must also understand external expectations.

High risk and growing general awareness has also captured the attention of the news media, further driving up visibility and interest. The media realized that the situation is emotionally charged, easily dramatized, and now interesting to the general public. Unfortunately, like other highly technical subjects, cyber security remains complex, with huge potential for misunderstanding, misrepresentation, and incorrect conclusions. ICS owners, operators, and suppliers must now consider the expectations of the public and the risk associate with adverse public opinion.

Increased public visibility to ICS cyber security issues and government involvement change the assumptions ICS owners, operators, and suppliers can use when defining strategies. They now must reexamine the state of their cyber security measures and strategies and demonstrate an increased sense of responsibility to customers, the public, and government agencies.
Stuxnet - Directed ICS Attacks Raise Potential Risk

In 2010, the most important – and certainly the most visible – ICS cyber security event was the discovery and analysis of the Stuxnet attack. The technical analysis and facts are readily available from Symantec and others, but note that a lot of incorrect and misleading information has also been published. While the Stuxnet attack demonstrated new levels of sophistication and persistence, the most lasting impact, is that it changed assumptions and risk perceptions yet again.

Historically, except for a few well-known cases, “attacks” on ICS have been insiders, independent hackers, and in general, unimpressive efforts - nothing that motivated widespread change. Additionally, ICS operators have always been concerned about, and actually sometimes experienced, downtime as a result of malicious viruses, worms, etc., that interfered with system operations.

Businesses and other ICS owners have always been concerned over the possibility of targeted attacks on ICS systems, but concerns have been dismissed quickly because of the specialized knowledge required, making the perceived risk low. Stuxnet gave us an actual case where specific ICS systems were attacked successfully (there is still some doubt about the actual damage done).

Stuxnet did not raise the bar for all ICS owners. It is an extreme case, infecting thousands of systems, but impacting only a few because of the specific damage it intended and the techniques it used. However, we can make several significant observations from the Stuxnet event:

- It showed that high-impact operations (factories, utilities ...) that depend on ICS are vulnerable to directed attacks when motivations are high enough. Even proprietary systems are not roadblocks when the necessary motivation and resources come together.

- It verified that the required attack team size and skill required is significant – more than a few people – but even this is not much of an inhibitor when the stakes are high. Development of Stuxnet may have actually lowered the barrier somewhat - especially for similar situations.
• It showed that isolating ICS from general-purpose networks does not guarantee safety. Complementary protections and controls are necessary.

• Subsequent to the Stuxnet discovery, product demonstrations showed that application whitelisting technologies would have blocked some attack paths.

• Antivirus, while helpful for other issues, would not have helped because the vulnerabilities were either unknown or had not been corrected.

• It showed that attacks can go undetected for considerable time, causing ongoing disruption, impact performance, quality, and costs. Better monitoring is badly needed.

• It reminded us that people and practices are a very large part of the overall ICS vulnerability.

Even though there are many lessons to be learned from Stuxnet, the actual impact on the industry has not been as large as one would expect based on the amount of press it received, because the situation is relatively unique.

Risk Analysis Drives ICS Security Investment

The Stuxnet event provided evidence that all systems are vulnerable when attackers have the key resources and sufficient time. From a risk perspective, Stuxnet provides a metric on the high end of the risk scale. This risk level is not new – we have always known it was possible – but the Stuxnet event transformed this ultimate risk from a remote possibility to something very real. Consequently, it eliminated arguments that we do not have to consider this level of risk.

Many businesses and organizations will consider it very unlikely that that they will be attacked with the same effort as Stuxnet, and they are right. This means that they may not need to go to the same extremes to protect their systems. They may not need to make the same investment in security
technology, may not need to implement the same policies and processes, and may not need to invest heavily in a cyber security staff.

Balancing risk against investment is a very complex decision. It requires considering likely threat levels, the cost of implementing and maintaining various security measures and processes, the impact of successful security events, and other factors. Businesses and organizations vary widely in their ability to perform a thorough and comprehensive risk analysis, but where ICS is involved, they must find ways to make risk analysis and mitigation a routine and critical process.

Currently, businesses spend over 2 percent of their ICS budgets on cyber security, not counting internal staffing costs. In the future, cyber security will almost certainly get a larger portion of ICS budgets. (Corporate IT spends about 3.5 percent of its IT budgets on cyber security.) Increased spending is linked primarily to more extensive regulation with associated penalties, the dynamic nature of cyber security, and the evolution of security technologies. This means that businesses should make certain that their risk analysis and associated budgeting processes are adequate.

**Industry Trends Mean Change for ICS Owners**

ICS security strategies, components, and processes have a different lifecycle than the control systems themselves. Control components are designed for a purpose, installed, and then just operated for many years. Widespread changes to the control components are usually only triggered when the suppliers update or obsolete their system components, which is not very frequent.

The lifecycle for ICS cyber security elements is much more dynamic and more strongly driven by industry trends. For example, regulations typically have compliance timetables that pace changes to ICS security components and processes, independent of ICS owner business plans. Furthermore, changing threats and new
vulnerabilities mean that security processes and components must change to continue to perform their function. Other influences include changing ICS owner-supplier relationships and the evolution of device security compliance testing.

It is critical that ICS operators stay on top of industry trends related to cyber security and make sure their own strategies, investments, and processes keep pace.

**Detailed Guidance Drives Critical Infrastructure Industries**

The critical national infrastructure industries, such as energy, chemicals, and water, have experienced the most external scrutiny due to risk of impacting large portions of the public. In the US at least, this high risk has stimulated creation of regulations and guidelines that could result in financial penalties to ICS owners.
In the case of the North American power industry, NERC (North American Electric Reliability Corporation) has already developed detailed standards for critical infrastructure protection (CIP) that must be followed by ICS owners (see figure).

Similar work is under way in other critical infrastructure industries, demanding the attention of ICS owners and suppliers alike. Furthermore, these regulations are not static. Industry roadmaps call for periodic review and updates to keep standards relevant. As a result, critical infrastructure industries must invest more heavily in people and processes than other industries.

The NERC-CIP requirements are just one example. Government activities and regulations drive cyber security spending in many areas. Business systems have been struggling to protect various forms of business and personal information, and these concerns are finding their way into ICS networks as well.

In some cases, businesses can be fined and penalized. For example, the US Chemical Industry Anti-Terrorism Standards (CFATS) allows for a penalty of $25,000 per day. NERC-CIP identifies penalties ranging from $1,000 to $1,000,000 per day, depending on violation severity level.

### ICS Cyber Security Dynamics Drive Continued Investment

Even in industries with no regulations, ICS cyber security is still very dynamic, requiring constant attention from ICS owners from the time of system conception to the time the systems are retired. Cyber security cannot be an afterthought, but instead, must be part of system design and installed even before the applications are built – systems can be compromised during initial integration and staging.

New attacks and vulnerabilities are discovered almost daily, requiring someone within each business to assess risk and develop mitigation strategies. Complex systems receive weekly patches to operating systems, PDF readers, database management systems, network devices, and others.
These require risk assessment, testing, and grouping into batches because ICS cannot be shut down as frequently as patches are issued.

Even the security components themselves add workload and issues. Some tools, such as antivirus, must be updated frequently or they become ineffective quickly. The sophistication of some attacks demands that ICS owners monitor systems closely for anomalies to detect attacks and “stealth” activities. Better ICS monitoring tools are needed.

Almost all businesses with ICS struggle with the additional workload, along with how to develop and maintain sufficient cyber security skills and how to cope with the changing nature of cyber security. With few exceptions, ICS owners are forced to accept high risk under increasing scrutiny.

**Organizational Trends Force Changes in Practices**

With staffing and skill development a major problem, it should not be a surprise that ICS owners are searching for the best organization to manage cyber security in environments such as distributed factories, plants, and electrical utilities. Traditionally, ICS have been designed and installed by engineering, often using outside systems integrators, and run by the operations organizations. In large businesses, corporate IT was seldom involved, and had little knowledge of ICS. However, corporate IT is now often needed because of their strong cyber security and system management skills, and businesses are searching for effective ways to include them.
It is unlikely that all ICS suppliers will adopt the same cyber security business model, but instead, will evolve toward two to three business models.

Businesses are now either creating an operations IT support section within corporate IT, creating an IT organization within operations, or possibly even creating a separate operation IT organization. Other ways to provide more extensive support for operations IT systems are also being discussed, such as using third-party security services. The complexity and time now required to implement, monitor, and maintain adequate ICS cyber security and the associated risk, provides ample motivation for trying new approaches.

**The ICS Supplier Role Gets More Collaborative**

One of the biggest changes over the last few years has been solidifying the role of ICS suppliers in their customers’ cyber security activities. This, in turn, fuels the development of effective ICS supplier security-related business models. The importance and value of supplier involvement is now broadly appreciated, stimulating change in how suppliers develop products, what suppliers offer, and depth of supplier partnerships with security specialists.

Cyber security for industrial control systems has been evolving and “best practices” for ICS suppliers are starting to emerge. For example, by now, all ICS suppliers should have security-related product development methods baked into their processes and should offer comprehensive security guidance to their customers. They should also make sure their products are compatible with third-party party security products, and should educate their support staffs about all aspects of ICS cyber security.

Almost all ICS owners have products from multiple ICS suppliers and ICS owners would like their suppliers to take a stronger role in developing and maintaining ICS security. But ICS security requires an evolving set of third-party security components, some third-party services, and includes end user practices and policies. This makes it difficult for ICS suppliers to know exactly what business strategy to follow, and has led to differing ICS supplier approaches.

Suppliers differ most relative to the offering of security-specific products and services. Some ICS suppliers manufacture and sell security products, others offer third-party products on their price list, and others offer none, but test with leading general-purpose security products. Similarly, some ICS suppliers offer formal services for sale and others simply help custom-
ers as part of their normal support. It is unlikely that all ICS suppliers will adopt the same cyber security business model, but instead, will evolve toward two to three models according to customer industry needs and business preferences.

**Standards and ICS Compliance Programs Will Help**

While all ICS suppliers are committed to making their systems secure, the facts are that ICS comprise many components, new and old, and many of those components are not made by ICS suppliers. Consequently, many ICS components can be made by teams that are insufficiently security conscious. Increasing sophistication of attacks and likelihood of directed attacks exacerbates this problem.

Many ICS owners feel that industry compliance processes improved industrial safety significantly and work is under way to apply that experience to ICS cyber security. The most recent security compliance activity has been organized within ISA. The ISA Security Compliance Institute (ISCI) was formed a few years ago and, in 2010, released its first test specifications. ISCI is now qualifying test laboratories.

Prior to that, Wurldtech offered Achilles-based security testing services and tools that suppliers could use during product development. Wurldtech and ISCI recently aligned their test specifications and are working to align their activities. Other forms of testing also preceded the ISA work, such as that at Idaho National Laboratories, and this continues.

Many large ICS owner businesses believe in the value of security compliance testing and some include specific tests in their purchase specifications. ICS owners also participated in the formation of related standards and groups. This guarantees that compliance testing will become a standard process for ICS component suppliers.

**ICS Security Technologies and Practices Evolve Methodically**

Security technologies by themselves cannot guarantee that systems are safe from attack. However, technologies are an essential element for protecting both legacy and new ICS systems. Overall, ICS owner and suppliers have
lagged in the use of specific security technologies relative to their corporate IT counterparts, and for good reason. Most security technologies require some adaption to be suitable for ICS. Furthermore, ICS owners must be very cautious about disrupting control systems because of the high cost and high business impact.

<table>
<thead>
<tr>
<th>Component</th>
<th>Technology</th>
<th>Utilization in ICS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewalls</td>
<td>Evolving to cover more of the communications stack, several types</td>
<td>Always deployed at perimeter, also used to create zones, a few ICS specific firewalls are offered</td>
</tr>
<tr>
<td>Antivirus</td>
<td>Security suppliers building comprehensive protection packages, beyond basic AV.</td>
<td>Commonly deployed on all stations in ICS. Must be up to date – a challenge for ICS</td>
</tr>
<tr>
<td>Identity Management</td>
<td>Traditionally done in applications, but easier to manage in common directories</td>
<td>User info tending toward common directories, rights still in applications</td>
</tr>
<tr>
<td>Application Whitelisting</td>
<td>Run only apps and components approved, maintain as update apps</td>
<td>Infrequently used now but high value and likely to become common</td>
</tr>
<tr>
<td>IDS/IPS</td>
<td>Many variations that look for anomalies, alert, automated actions</td>
<td>Infrequently used in ICS, more monitoring is needed</td>
</tr>
<tr>
<td>Network Access Control</td>
<td>Protect ICS components from plug in devices - laptops</td>
<td>Infrequently used, likely to increase</td>
</tr>
<tr>
<td>Remote Access</td>
<td>Variety of solutions from simplistic to sophisticated</td>
<td>Many differing strategies, need standardized solutions</td>
</tr>
<tr>
<td>Security System Monitoring &amp; Management</td>
<td>Few that are built for ICS components and practices, remote monitoring important</td>
<td>Infrequently used, likely to be a centralized function, needed for quick response to issues</td>
</tr>
<tr>
<td>Security Patch Management</td>
<td>There are many patch management systems for corporate IT and home users but there are none designed for ICS</td>
<td>Few ICS owners have automated patch management, but most have documented processes</td>
</tr>
</tbody>
</table>

**General-Purpose Security Components Must Be Adapted for ICS Use**

Each ICS environment requires a security architecture that ensures comprehensive coverage and many security technologies (see table above). It is not feasible for ICS suppliers to develop a comprehensive set of security components just for ICS. In addition, general-purpose security component suppliers (McAfee, Symantec, Cisco...) cannot justify creating a product
just for the ICS industry. Accordingly, the ICS industry must first determine how a general-purpose solution can be adapted for ICS environments. Then, ICS owners must accept the solution. Most ICS owners want to avoid being the first to deploy a new technology and prefer “field-proven” solutions. Consequently, this process typically takes time and explains the current situation.

Some security components such as firewalls and antivirus are common in ICS and being used as-is. Even then, they are problematic for ICS environments. To be effective, antivirus databases require weekly, if not daily, updating. Firewalls are complex to configure and must be monitored, handling events and issues as they occur. Actually, some ICS suppliers have resorted to developing firewalls specifically for classes of ICS environments to alleviate customer problems. It is still difficult for the small groups that manage most ICS environments to find time to perform these and other security tasks a frequently as needed.

Application whitelisting is one of the most promising technologies for improving protection of ICS, especially unknown threats. Several ICS suppliers offer or plan to offer their customers third-party-based solutions. Other technologies will likely lag the acceptance of whitelisting. One of the most obvious needs is for a common security component and device monitoring software in ICS environments.

It is unlikely that general-purpose security component suppliers will ever offer ICS-specific solutions. This leaves the work to the ICS suppliers and other ICS security specialists. End users and systems integrators then must fill the gaps.

**Siemens Security Strategy for ICS**

Industrial control systems suppliers are quite similar in their general perspective toward cyber security, although they differ significantly in organization, processes, products, and partnering details. Many of these differences are due to product type and diversity, industries served, and customer exposure and expectations.

In 2010, ICS was thrust into the security spotlight
when the highly funded, persistent, and targeted Stuxnet attack was discovered. According to security companies such as Symantec, while the attack infected thousands of desktop systems, it needed PCs with certain Siemens industrial software installed. By the end of 2010, only 24 Siemens customers had reported being infected by Stuxnet, and none was the actual target. These customers removed the malware with no adverse impact on their automation systems. The actual targets are still not known with certainty.

This level of this attack forced Siemens and in fact all other automation system suppliers to re-examine their business approach to cyber security, eliminate gaps previously viewed as low risk, and improve practices in general. Across the industry, suppliers are adding and improving processes, strengthening partnerships, and adding products to help high-risk customers improve their security posture.

**Siemens Organizational Approach to Security**

Siemens has security expertise distributed throughout the company’s Industry Sector organization, including the Industrial Automation and Industry Services divisions. This includes Simatic S7, Simatic PCS 7, and Simatic NET product categories. Within the Industry Sector, the Siemens Security Lab drives considerable security activity for PCS 7 and WinCC, and by departments for professional services. The Siemens Security Lab was created in 2004 and operates separately from traditional product testing facilities. In addition to testing, the Security Lab is responsible for developing Siemens security architecture and concepts by designing, implementing, testing, documenting, and improving new security techniques, procedures, and products.

The company manages its security architecture with a dynamic process in which the architecture is challenged on a regular basis by Siemens Corporate Technology’s Computer Emergency Response Team (CERT) using penetration tests.
Siemens CERT has been protecting Siemens internal IT infrastructure and supporting secure product development since 1998. It is established as an independent auditor and trustworthy partner to respond to security incidents, develop preventive measures, and assess information security.

In early 2011, Siemens created the company’s Security Network, intended to facilitate the fastest possible response to customer and industry security events and issues. This is not a rigid set of processes but recognizes that different situations require different processes. However, support of each unique situation starts with best practices such as consistent internal and external communications and collecting lessons, feeding them to product and other organizations for implementation of improvements.

**Siemens Security Offerings Reflect a Growing Need**

Siemens manufactures and offers a firewall of its own, “Scalance S,” intended for use in ICS environments. Siemens also offers the PCS 7 AddOn automation firewall, based on Microsoft Forefront Threat Management Gateway (TMG). Additionally, the company tests its products for compatibility with three antivirus products: Symantec, Trend Micro, and McAfee.

The Siemens security staff, which has been supporting customers for some time, recently began to offer billable services for industrial IT security. These services may be used in any phase of system lifecycle. For example, Siemens consulting may be used for vulnerability assessments or engineering studies before system integration. Siemens can also design and implement overall security solutions and can support ongoing assessments and other activities such as cyber forensics and penetration testing.

Siemens’ security roadmap reflects emerging needs that relate to recent industry activities. Siemens recently released additional offerings for IP protection (know-how protections solutions are already available for Series 300 & 400). In the next phase, Siemens will add Secure-IO, Secure-PLC, and
Secure-PC/HMI offerings. In addition to new solutions, Siemens is working on many security features such as improved user administration, role-based access, increased use of encryption, intrusion detection, applications whitelisting technology, and further exploitation of familiar technologies such as firewalls.

Conclusions and Recommendations

The Stuxnet attack and industry trends aimed at improving and more effectively managing security, has provide us with a new set of assumptions to be used during security strategy development. One of the key outcomes was to highlight the importance of risk assessment.

- The potential impact of compromised critical infrastructure is interesting to the general public and successful attacks can be very damaging to brands as well as creating safety and cost issues. Both ICS owners and their suppliers can be impacted, no matter who is at fault.

- The participation of ICS suppliers, such as Siemens, in customer ICS security planning, design, implementation, mitigation, and maintenance continues to grow in importance. All ICS owners should build a collaborative relationship with their supplier, including becoming familiar with the supplier’s cyber security organization.

- The Stuxnet attack certainly provides both a high-level metric and a good reference case for all to consider. ICS owners can determine the likelihood that their businesses will be the target of such a sophisticated attack, and weigh that against cost of the necessary protections and consequences. ICS suppliers must use the Stuxnet experience to re-examine their practices and make adjustments based on lessons learned.

- With enough resources and time (secrecy is important), targeted and persistent attacks such as Stuxnet are likely to achieve some degree of success, no matter how much we invest in protections. Technologies, such as whitelisting, that need no knowledge of the attack to be effective, have the most promise for increasing protections. Furthermore, additional monitoring and systems
management is needed in most situations to detect anomalies as soon as possible, hopefully before damage is done. ICS suppliers will more frequently play a crucial role in interpreting anomalies.
Analyst: Robert Mick
Editor: Paul Miller

Acronym Reference: For a complete list of industry acronyms, refer to our web page at www.arcweb.com/Research/IndustryTerms/

- APCT: Advanced Process Control
- CERT: Computer Emergency Response Team
- CFATS: Chemical Industry Anti-Terrorism Standards
- CIP: Critical Infrastructure Protection
- DCS: Distributed Control System
- DMZ: Network Buffer/Isolation Zone
- HMI: Human Machine Interface
- ICS: Industrial Control System
- IDS: Intrusion Detection System
- IPS: Intrusion Protection System
- ISA: International Society of Automation
- ISCI: ISA Security Compliance Institute
- IT: Information Technology
- NAC: Network Access Control
- NERC: North American Electric Reliability Corporation
- PC: Personal Computer
- PDF: Adobe document format
- PDF: Programmable Logic Controller
- SCADA: Supervisory Control and Data Acquisition

Founded in 1986, ARC Advisory Group is the leading research and advisory firm for industry. Our coverage of technology from business systems to product and asset lifecycle management, supply chain management, operations management, and automation systems makes us the go-to firm for business and IT executives around the world. For the complex business issues facing organizations today, our analysts have the industry knowledge and first-hand experience to help our clients find the best answers.

All information in this report is proprietary to and copyrighted by ARC. No part of it may be reproduced without prior permission from ARC. This research has been sponsored in part by Siemens. However, the opinions expressed by ARC in this paper are based on ARC’s independent analysis.

You can take advantage of ARC’s extensive ongoing research plus experience of our staff members through our Advisory Services. ARC’s Advisory Services are specifically designed for executives responsible for developing strategies and directions for their organizations. For membership information, please call, fax, or write to:

ARC Advisory Group, Three Allied Drive, Dedham, MA 02026 USA
Tel: 781-471-1000, Fax: 781-471-1100, Email: info@arcweb.com
Visit our web pages at www.arcweb.com