Interested in learning more
about cyber security training?

# SANS Institute
# InfoSec Reading Room

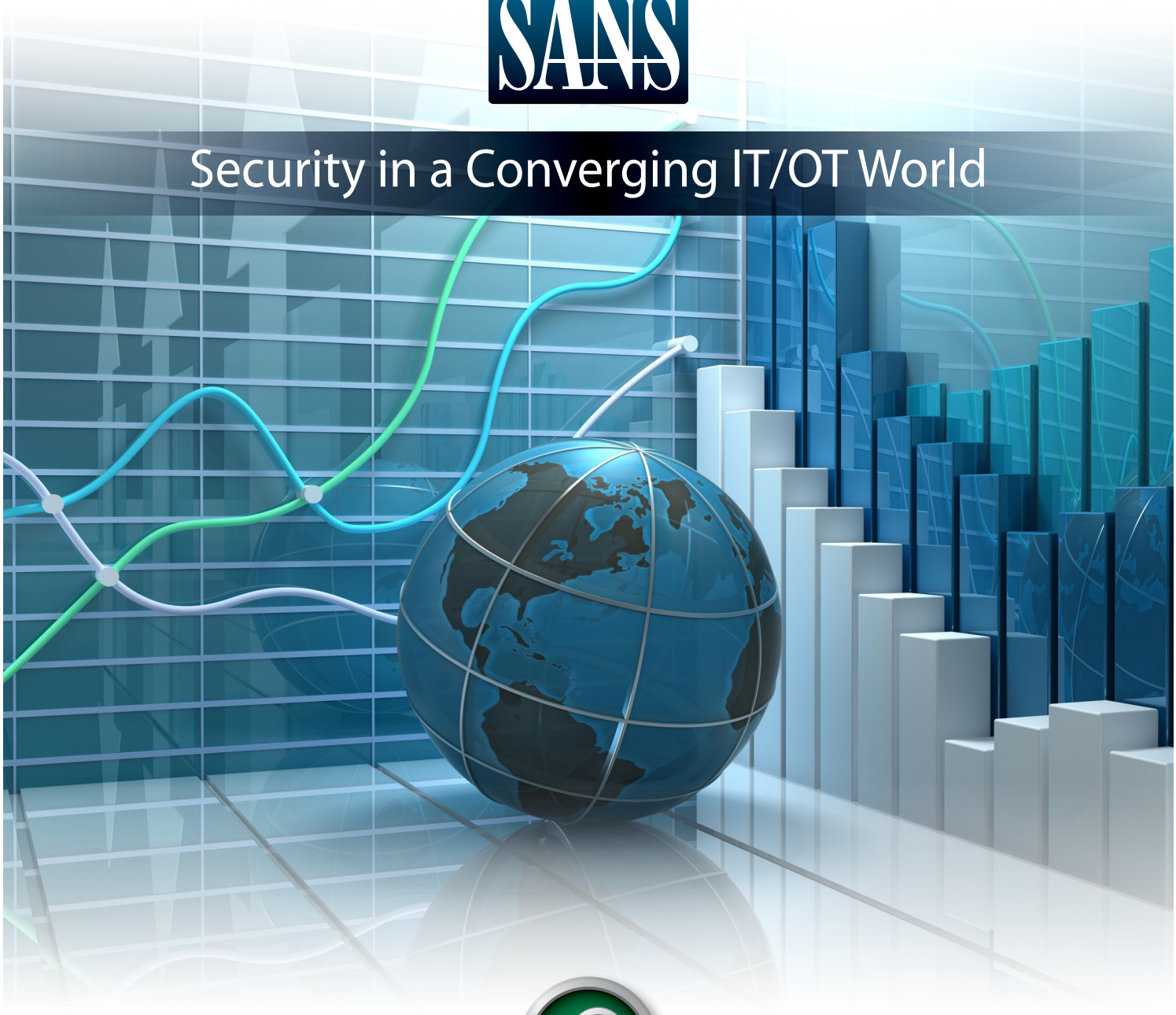
This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

## Security in a Converging IT/OT World

In this paper we look at the challenges in securing ICS environments and recommendations for effective ICS security. OT cyber security is a relatively young field with few experts, but a great deal can be judiciously drawn from IT experience. The fundamentals are the same: controlling access to devices and applications; monitoring networks to identify potential issues and direct appropriate responsive action; oversight and periodic reviews of controls and their effectiveness; securing the supply chain; and securing the...

Copyright SANS Institute
Author Retains Full Rights

# Security in a Converging IT/OT World



## A SANS Whitepaper

*Written by Bengt Gregory-Brown and Derek Harp*

November 2016

*Sponsored by*

*Sponsored by Wurldtech, a GE Company*

©2016 SANS™ Institute

# Introduction: IT-OT Convergence

A great deal has already been written about the increasing adoption of IT technologies into process control and automation systems environments,[1] but although IT and operational technology (OT)[2] networks are both digital communications systems experiencing the disappearance of a meaningful "perimeter," their differences outweigh their similarities. Notably, they use overlapping but largely different sets of networking protocols. ICS environments are engineered to execute on specific processes (A -> B -> execute C). Unlike IT environments, which are based on open query and response, OT networks are deterministic by nature and relatively predictable.

Furthermore, ICS is cyber-physical, often directly affecting the real world. This means that risk calculations include potential impacts in scope and at scales greater than in information-only environments, including but not limited to loss of lives, ecological damage, intellectual property theft, brand damage and revenue losses. The traditional IT priorities of confidentiality, integrity and availability are shifted in ICS; safety and availability reign as the key drivers in ICS. Whereas some industries will be beholden to regulatory or compliance drivers as well, the fact is that production environments are central to revenue and profits. To the extent that cyber events can disrupt safety or availability, ICS cyber security is quickly emerging as a top priority.

In this paper, we will look at the challenges in securing ICS environments and recommendations for effective ICS security. We hope readers will use the concrete and specific steps offered for immediate security benefits to their organizations. OT cyber security is a relatively young field with few experts, but a great deal can be judiciously drawn from IT experience. The fundamentals are the same: controlling access to devices and applications; monitoring networks to identify potential issues and direct appropriate responsive action; oversight and periodic reviews of controls and their effectiveness; securing the supply chain; and securing the human factor through awareness training. It is in the design and application of these basics to the particular considerations and technical nature of control systems and process control networks (PCNs) that things diverge the most, and it is here that we will focus.

[1] "IT/OT Convergence: Bridging the Divide," http://ics.sans.org/media/IT-OT-Convergence-NexDefense-Whitepaper.pdf

[2] See Appendix A: Glossary.

# ICS Security Programs

Operational technology environments were historically isolated from other networks both physically and by their use of proprietary protocols, so their security was focused on physical controls. For most of their history, "air gaps" prevented remote access. The usual set of locks, guards, background checks, etc., limited exposure to direct threats. Because of this isolated and often proprietary environment, OT cyber security is roughly a decade behind the maturity level of IT security in many ways, including organizational development, funding, available tools and skilled resources.

Looking at funding in particular (tools and resources are addressed below) as a driver of other areas, IT has historically allocated 5 to 10 percent of its total spend on cyber security,[3] but OT has had no corresponding budget because there was no perceived cyber threat. As demand for OT cyber security funding has increased, the questions of budget sources and governance has complicated matters. Should IT departments expand their purview (and funds), or should OT business units, which arguably understand the risk factors of service interruptions best and on whose shoulders security incidents fall most directly, pay for and control the allocations on resources for this new security mission?

Justification for funds continues to be challenging in many companies regardless of where responsibility for ICS cyber security lies. Statistical data on ICS security breaches is limited, and prior to experiencing an incident, the case for new spend can be hard to make to organizational leaders. Reporting of ICS security incidents is infrequent and generally light on details, and this lack of data compounds the challenge of developing security management plans. Unlike in IT information security, there are very few companies or situations where reporting a cyber incident is required. Where are the greatest risks, and where should money and efforts be focused for greatest effectiveness? Figure 1 shows how risk awareness is increasing.

**How serious does your organization perceive current threats are to the cyber security of its control systems?**

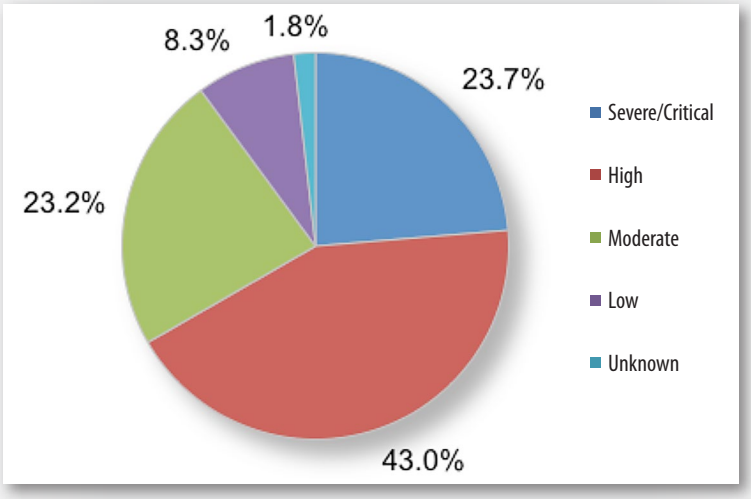



*Figure 1. Current Perceived Threat Level to ICS[4]*

[3] "IT Security Spending Trends," www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697

[4] "SANS 2016 State of ICS Security Survey," www.sans.org/reading-room/whitepapers/analyst/2016-state-ics-security-survey-37067, p. 5.

# Unique Challenges to Securing ICS Environments

ICS environments differ significantly from the traditional enterprise. For example, ICS equipment suppliers often include remote access to devices as a contractual requirement for service level agreements. This communications channel enables ongoing performance data gathering as well as tuning and optimization, which reduces downtimes and maintenance costs but also creates potential conduits for threat actors to gain entry into the control system network. Additionally, while techniques may exist to reduce device vulnerability to remote attacks, many vendor contracts prevent modification of assets on grounds of warranty violation.

Further complicating the goal of securing ICS assets are safety regulations, which may also prevent modifications to equipment. Such regulations can be governed at multiple levels of government and industrial sector bodies, making the determination of possible asset security steps a challenging one. Similar regulations may require operators to provide data to third parties, and whether this is accomplished through a standing communications conduit or by exporting that data to removable media, either method establishes a target for malicious actors seeking that proprietary information.

Given that ICS defenders have to successfully navigate the maze of requirements and restrictions and identify steps to improve security of the systems and networks under their charge, implementing these changes has even greater challenges in an OT environment. With equipment (and often, software) life cycles running into decades, control system environments maintain a more diverse collection of legacy equipment (much incapable of running modern security software), creating a larger and more complex list of variables to check potential impacts against.

Limited device virtualization options and the high cost of industrial equipment further affect the ICS environment, making it nearly impossible to test changes except on the actual operational devices during scheduled downtimes. This state of affairs means change testing and implementation must fit into downtime allowances often only hours or minutes per year, and rescheduling means delays of months at best. This schedule inflexibility also makes segmenting flat process control networks a challenging task, as network traffic interruptions or delays resulting from the introduction of new networking equipment or re-addressing a network can themselves disrupt operations.

Whereas information systems were developed around historic objectives of fault tolerance, interoperability and ubiquitous connectivity, therefore incorporating dynamic addressing, routing and recovery into system protocols, control systems originated very differently. Scores of industrial protocols,[5] generally designed to serve highly specific functions and with little or no ability to incorporate other aspects (e.g., security), are a given in the IT world. Traditional packet inspection tools developed for IT networks will not work in these environments.

Given the above challenges, it is important to keep in mind that ICS networks can be secured without disrupting production by planning and implementing a coordinated, step-by-step program of gaining visibility into control network traffic and establishing security policy mechanisms to protect that traffic. All aspects of the program laid out herein are intended to accomplish those two objectives: seeing what is going on in a PCN and limiting that activity to approved transactions.

[5] List of automation protocols: https://en.wikipedia.org/wiki/List_of_automation_protocols

# ICS Security Recommendations

As difficult as it may be to protect control systems, our shared goal remains developing and implementing a plan to overcome the challenges. Regardless of the objective, the success of any plan relies on clear communications of goals and the means to reach them. Security can be a difficult subject to communicate, particularly to non-practitioners, but risk management provides a methodology commonly understood among organizational leaders, and it begins with evaluation of risks and tolerances.

Most, if not all, OT-dependent entities have plans in place to manage physical and environmental risks to safety and operational performance. These plans, which should already define acceptable levels of risk, should be expanded to include network-based threats to control and automation systems.

**Recommendations**

Security programs are not one-size-fits-all, but this list includes capabilities that are key to preventing, identifying, prioritizing and resolving threats to any networked environment:

- Network segmentation
- Access control and credentials management
- Deep protocol inspection and intrusion detection
- Incident response
- Vulnerability and patch management
- Cyber security assessment and audit plan
- Procurement security policies
- Security awareness program

Organizations lacking resources skilled in this subject area will need to develop them or make use of consultancies with relevant expertise. With risks and tolerances defined, leaders can choose appropriate management strategies (e.g., accept, transfer, avoid, mitigate) and budgetary allowances for each, including ICS security. This approach presents the case for funding in a structured and defensible manner.

Ownership of and responsibility for ICS assets have always fallen to operational business units. The trend of converging technologies has led to developing multiple models of securing their networks, with organizations choosing between bringing IT into ICS environments, adding or training cyber security-skilled resources inside the ICS business units, or some blended or collaborative approach between the two groups. Governance is more than workforce ownership, of course, and models must address questions of budgetary control, priority setting and leadership, all of which affect how security controls will be planned and implemented.

To keep this paper of reasonable length, we have painted a security plan in broad strokes, leaving it to readers to adapt these recommendations to their unique conditions. Many available sources[6] go into greater detail on individual recommendations.

[6] SANS Reading Room, www.sans.org/reading-room

## Segment Networks

Segmentation is fundamental to securing any network. The risks and operational specifications of ICS networks make it vital to protecting them. Yet, many ICS/OT networked environments remain flat, inhibiting defenders from implementing zone-based controls, or attempt to use IT security techniques to segment, which are expensive and time-consuming.

The particular model and controls will depend on the specifics of an organization's business and network structures, but at a minimum will require the following:

1. Document physical, logical and application network maps. If no such maps exist, this can be a time-intensive effort, particularly without the use of ICS network visibility tools, but it is essential to both ensure full information is available to security teams and reduce the potential of service interruptions during later implementation steps.
2. After network maps are complete and validated, continually maintain their accuracy as software and hardware assets change becomes a high-level responsibility.

After the current state of networks is documented, network security experts can work with other stakeholders to define the future, desired design. Conceptual design work can be carried out in parallel with the actual mapping process, but architects must engage with many areas of the organization to ensure all required communication conduits are preserved and not negatively affected during the implementation phase.

The segmentation of physical and logical networks will involve implementing security controls on all access points, restricting traffic to a single segment wherever feasible and allowing inter-segment traffic only as required for operations. This process should include controlling traffic not only by protocol but also by source and destination. Figure 2 offers an example of network segmentation. Actual maps are likely to be much more complex and have many more segments/security zones.

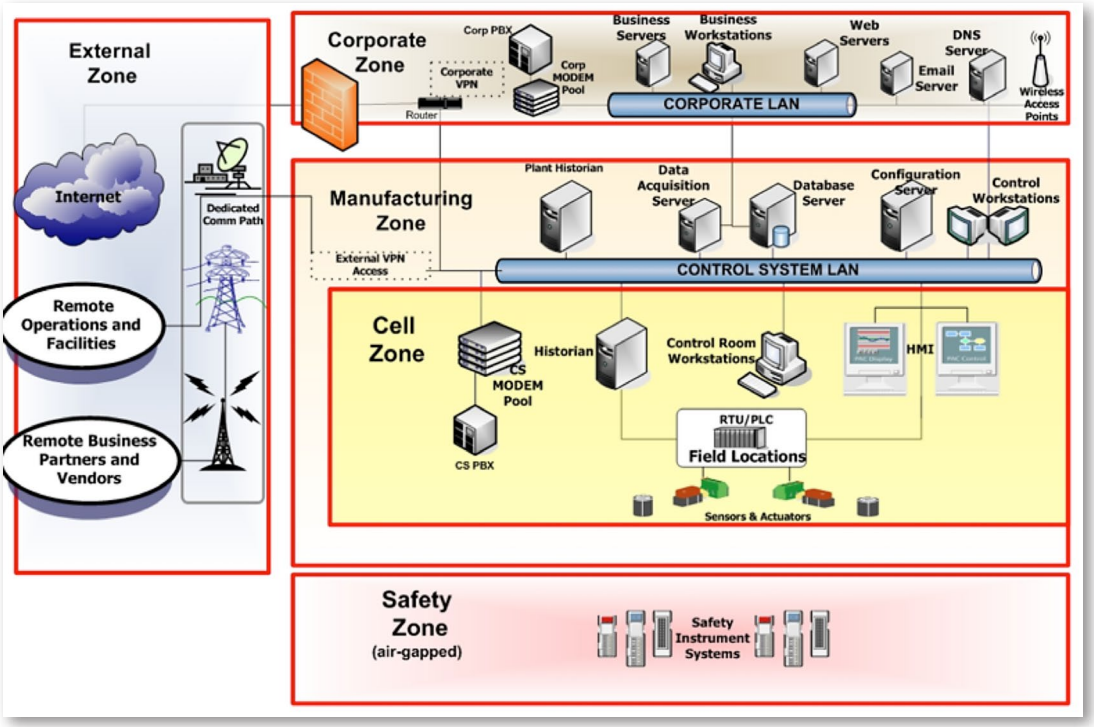



*Figure 2. A Simple Conceptual Example of Network Segmentation*

The key value of ICS-OT network segmentation is to have a means by which policies can be applied to specific zones, and where potential cyber IOC (indications of compromise) can be identified and contained, rather than having an open, flat network where malware can move laterally (across the PCN network) or vertically (up into the DMZ or enterprise network).

## Access Control: Establish a Credential Security Program

As network segments are defined to control communications, security practitioners must also capture details of existing user roles and align credentials with the new controls. The inventory of devices and applications carried out in the first phase of creating network maps should include documenting access controls (policies, passwords, biometrics, etc.) on individual devices and applications, both as currently and potentially configured. For example, can applications be configured with password strength and renewal requirements, and if so, with what parameters? The strength of these controls should match the security level of the zones in which the assets reside and allow only the minimum access and privileges necessary to achieve operational missions.

User credentials must be unique to individuals and managed by roles. The former ensures not only accountability of human resources but also traceability data for auditing and forensic purposes. Managing user credentials by roles greatly simplifies what can otherwise be a Sisyphean task[7] of establishing and maintaining the alignment of users and assets.

It is likely that some assets (likely legacy hardware) will lack the capacity for access restrictions or installation of compensating security applications. Securing these "unsecurable" items will require compartmentalization, effectively constructing segments around them and their communication partners.

## Deep Protocol Inspection and Intrusion Detection

ICS network security is predicated on visibility—the ability of defenders to see, understand and act on traffic within that network, just as in the IT world. Even though process control networks tend to have less traffic, for multiple reasons visibility into that activity has long been very limited by the distinct differences between IT and ICS protocols. The latter, generally proprietary and often developed to operate within very specific and limited parameters of timing and network media, require device command- and parameter-aware inspection for validation. Historical IPS/IDS solutions are based on firewall technology and compare packets against known signatures. But they do not evaluate the impact of the packet contents on the destination devices(s), nor can they evaluate an entire data flow in state (i.e., multiple packets that comprise a process command flow). The assumption, often acceptable in an IT environment, that endpoints are secured against discrete malicious packets (e.g., antivirus software) cannot be relied upon in an OT network, where devices may have no capacity to protect themselves.

It is only within recent years that tools have become available to safely monitor, gather and analyze ICS network traffic without negatively affecting operations, assets and personnel, potentially catastrophically.

[7] https://en.wikipedia.org/wiki/Sisyphus

Prior to the availability of products that enable deep protocol inspection, ICS network security had to focus heavily on isolation tactics—attempts to maintain the historical "air gap." OT owners and operators were wary of the demonstrated potential for IT scanning and monitoring tools to interfere with ICS network traffic (introducing lag and corrupting or dropping packets) and equipment (scanning packets being mistakenly interpreted as commands by devices designed for limited communications scenarios). As a result, they were generally unwilling to allow their use in control and automation environments.

Many of the newer tools use passive data gathering and out-of-band analysis[9] methods to avoid interfering with command communications. These tools may include deep protocol inspection engines (PIE) to see the specific content of state-aware data flows, in which commands and parameter can be validated within the operational context. Security practitioners can now see what one asset is messaging to another, identify which traffic is normal and what is anomalous, and develop controls accordingly.

### Network Communication Whitelisting (and Blacklisting)

ICS networks tend to have much lower volumes of traffic than IT environments. Much of this traffic consists of communications between devices and controllers and is driven by operational activity, making it highly deterministic. That is, when assets have been inventoried and routine traffic baselined, a "fingerprint" of expected communications can be established and whitelisted. Communications whitelisting is particularly crucial within the PCN (e.g., connecting controllers and PLCs) to ensure that operational processes are protected from unauthorized changes. In the broader ICS network, monitoring and analysis tools can use this listing to alert on anomalous network activity. Accomplishing a similar task is impractical in IT environments due to the high levels of variability in their network traffic.

Going beyond whitelisting of expected communications, the predictability of ICS networks makes it possible to blacklist certain traffic. With a sufficiently advanced protocol inspection engine designed specifically for OT networks, it is even possible to block this blacklisted activity. Doing so requires protocol inspection and analysis engines capable of capturing and tracking complex protocol states and validating the legitimacy of the data flow in full context with sufficient speed to determine which packets and flows to block and which to pass without negatively impacting operational network traffic.

[8] Industrial control and automation systems often have lower bandwidth networks than business or enterprise IT and may be negatively affected by additional communications traffic. In addition, most are real- or near-real-time systems with little to no tolerance for latency.

[9] OOB analysis, used by network anomaly detection tools prioritizing non-interference over the ability to block traffic, analyzes data gathered passively from communications traffic but avoids introducing latency by suspending packets during analysis.

For maximum effectiveness, the listing (whether white-, grey- or blacklisting) of communications optimally takes multiple factors into account, including:

- **Devices**. ICS equipment, unlike computing devices in IT environments, is not general-purpose. Each device is designed and configured to do (and communicate) a very limited number of things and talk to a very specific list of devices. Any other activity would be considered anomalous and trigger an alert or other action by ICS network monitoring tools.
- **Applications.** Although software running in an OT environment is often broader in scope than the equipment, it is nonetheless very limited relative to general IT applications, and its normal activity can be documented sufficiently to identify what communications it should (and should not) be originating.
- **Commands.** All communications listings require a level of context awareness, none more so than commands and parameter (such as set points). Context awareness in the form of policy engines is needed to evaluate whether those commands fit normal operational parameters. ICS network monitoring tools must ask whether a particular command should be sent from a particular source and to a particular device, and take appropriate action.
- **Communication protocols.** Just as command-bearing packets must be evaluated for their acceptability, network anomaly detection tools must determine whether a particular source should be communicating with a particular protocol (e.g., Modbus, Profinet or OPC) to a particular destination and take appropriate action.

Figure 3 shows this breakdown in graphical form.

| | | Evaluation Factors | | | |
|---|---|---|---|---|---|
| | | Device | Application | Command | Protocol |
| Traffic Categories | Whitelist | ***Potential Actions:*** • None (Log only*) | | | |
| | Greylist** | ***Potential Actions:*** • Log • Flag for analysis and rules development*** | | | |
| | Blacklist | ***Potential Actions:*** • Log • Flag for analysis and rules development • Block | | | |

* Logging is recommended on all traffic for potential forensic value.

** Greylist may exist only as default; i.e, all traffic not on white- or blacklists.

*** Refers to development of additional rules/signatures to define traffic as either white- or blacklist.

*Figure 3. Determining Whether to Black-, Grey- or Whitelist Communications*

### Alerting and Responding

With traffic monitoring and virtual segmentation in place and network communication whitelists established, ICS defenders must define appropriate responses to anomalous network activity. If a PIE tool is implemented, blacklisted communications are to be blocked and defenders alerted. Another category, which we will call the "greylist," consists of traffic not defined as black or white, and network anomaly detection tools must also alert security personnel of these. Over time, some grey items will be added to whitelists or blacklists; others will remain as acceptable but indicative of conditions calling for human intervention, such as asset deterioration, network equipment performance issues, new equipment coming online, etc.

Alerts and responses to them are prioritized by the level of associated risk. Traffic negatively affecting safety and operational performance, for example, has highest priority and calls for immediate intervention; organizations with IPS in place may block these. Traffic indicative of a non-destructive security breach (such as communications leaving the control network zone routed to the Internet) might be allowed temporarily while security practitioners investigate the extent of the breach, depending on organizational conditions and guidelines.

Whatever decisions are made about alerting on and responses to various anomalous traffic activity, those changes not only must be configured in the security management tool but also documented and communicated to personnel in order for them to fulfill their role in the security process.

## Establish an ICS Security Incident Response Program

Organizations dependent on control and automation systems are of many sizes, but all should have at least rudimentary business continuity and/or disaster recovery (BC/DR) plans that address partial-to-full operational outages. ICS security incidents have historically risen to these levels only seldom,[10] but factors both technological (IT-OT convergence, increasingly networked ICS devices) and political (increasing use of cyberspace by hacktivists, rogue states, non-state actors and foreign nations) support the belief that such events may occur more frequently in the future. Evidence of increasing numbers of cyber attacks on industrial control and automation system networks,[11] in particular advanced persistent threat (APT)[12] incursions, is widely available.[13]

Whether a specific event rises to the level of "incident" in an organization or not, the ICS security team's alerting and response plan must integrate with the larger BC/DR plan to ensure timely and smooth engagement of appropriate resources to address events with minimal impact to the organization.

## Establish a Vulnerability and Patch Management Program

It is well established that the connection to IT networks and the integration of IT components into ICS environments subject those environments to the vulnerabilities of those networks and components. ICS security therefore requires the engagement of IT security practices. Control systems, however, do have vulnerabilities of their own and are, in most cases, less free to apply patches and updates. Long cycles between patching and updating windows mean many systems run unpatched despite awareness of vulnerabilities.

Patching and updating optimally work hand in hand with vulnerability tracking and resolution, something with which IT security practitioners are generally familiar. As challenging as these tasks are in an OT environment, they are an essential component of a complete security program. The ICS security team must track relevant software changes and coordinate with device owners and operators to implement them (where implementation is possible) promptly without causing service interruptions. The team must also configure compensatory controls to protect assets and operations wherever patches and updates cannot be applied (or cannot be applied for an extended period of time). Patching and updates need to be managed not only for control and automation systems but for networking infrastructure as well.[14]

[10] SICS-Cert, Cyber-Attack Against Ukrainian Critical Infrastructure, https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

[11] "Manufacturers Suffer Increase in Cyberattacks," www.darkreading.com/vulnerabilities---threats/manufacturers-suffer-increase-in-cyberattacks/d/d-id/1325209

[12] "Critical Infrastructure Incidents Increased in 2015: ICS-Cert," www.securityweek.com/critical-infrastructure-incidents-increased-2015-ics-cert

[13] "Industrial Control System Security: Top Ten Threats and Countermeasures 2016," www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_005E.pdf?__blob=publicationFile&v=2

[14] "The Secret Behind the NSA Breach: Network Infrastructure Is the Next Target," www.darkreading.com/endpoint/the-secret-behind-the-nsa-breach-network-infrastructure-is-the-next-target/a/d-id/1326729

## Establish an ICS Security Assessment and Audit Plan

The finest security program cannot guarantee zero breaches. Even a vigilant and skilled security team armed with the best adaptive intrusion detection technologies (which uses expert guidance and long learning cycles to improve accuracy of detection) can be fooled by "slow attacks," and APTs dwelling in a network are often discovered only during security audits.[15] Furthermore, periodic assessments are a necessity to gain insight into the effectiveness of current security practices and inform decision-making regarding potential improvements.

Security audits vary as to how deeply they dig into the details of networked environments, and the greater the amount of information gathered, the more labor-intensive they are. Organizations must determine the frequency of assessments at different levels of thoroughness based on their risk profiles and capabilities. But with the dwell time of many network breaches exceeding several months,[16] it is clear that security monitoring activities are often insufficient to detect these infiltrations. The cost of performing in-depth audits must be weighed against the potential impact of threat actors maintaining access to proprietary systems and data. Best practices recommend at least minimal security assessments (including confirming and updating inventories of devices, applications and network connections) quarterly and full ones at least annually.

The design and performance of security audits require specialized knowledge and skills, particularly in ICS environments. Few organizations have personnel with these competencies on staff, and the costs of acquiring them can be prohibitive in this time of high demand for qualified cyber security resources. The quality of an assessment depends on the quality of the auditors, who must be knowledgeable and experienced in the specific areas needed to ensure the thoroughness of their findings. Companies lacking these resources internally are advised to enlist the services of third-party experts as needed.

[15] "Industrial Cybersecurity Threat Briefing," http://www.slideshare.net/BoozAllen/booz-allen-industrial-cybersecurity-threat-briefing (slide 20).

[16] "Global Security Report Shows Majority of Companies Do Not Detect Breaches on Their Own," https://securityintelligence.com/news/global-security-report-shows-majority-of-companies-do-not-detect-breaches-on-their-own/

## Establish Procurement Security Policies

The overall trend of integration and increased connectivity is perhaps nowhere more prevalent than in ICS suppliers, and this state of affairs opens new opportunities for compromise. The subject is a lengthy one,[17] and the problem has many parts.[18] Organizations need to enact security controls on conduits between their vendors and their ICS devices and networks, but they must also work with those suppliers to improve the security design of existing and future products and processes, and to validate the security of supplier organizations themselves.[19] More than one ICS owner has downloaded malware from a trusted vendor site, later discovering that the software was placed on that site and disguised by malefactors as legitimate updates.[20] A posture of trusting only with verification is highly recommended.

## Establish a Security Awareness Training Program

The considerations of designing and implementing a security awareness training program are beyond the scope of this paper and written about extensively[21] elsewhere.[22] The importance of such a program should not be underestimated, particularly with the growing record of breaches begun with phishing[23] and social engineering.[24] The effectiveness of training, fortunately, is relatively easy to measure and of great value in optimizing efforts.[25]

[17] "Combatting Cyber Risks in the Supply Chain," www.sans.org/reading-room/whitepapers/analyst/combatting-cyber-risks-supply-chain-36252

[18] "Best Practices in Cyber Supply Chain Risk Management," www.nist.gov/itl/csd/upload/NIST_USRP-Cisco-Cyber-SCRM-Case-Study.pdf

[19] "Validating Supply Chain Cybersecurity," www.darkreading.com/partner-perspectives/intel/validating-supply-chain-cybersecurity/a/d-id/1323597

[20] "Russian Hackers Target Industrial Control Systems: US Intel Chief," www.securityweek.com/russian-hackers-target-industrial-control-systems-us-intel-chief

[21] "How to Craft a Security Awareness Program That Works," www.cio.com/article/3076228/security/how-to-craft-a-security-awareness-program-that-works.html

[22] "Does Security Awareness Training Even Work?" www.csoonline.com/article/2987822/data-protection/does-security-awareness-training-even-work.html

[23] "Everything We Know About Ukraine's Power Plant Hack," www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/

[24] "Social Engineering Confirmed as Top Information Security Threat," www.computerweekly.com/news/4500273577/Social-engineering-confirmed-as-top-information-security-threat

[25] "Is Your Security Awareness Training Program Working?" www.csoonline.com/article/3118401/security/is-your-security-awareness-training-program-working.html - tk.rss_socialengineering

# Conclusion

Securing connected control and automation system networks is a great responsibility requiring the coordinated efforts of many organizational resources and often even changes to corporate culture. It is also an ongoing activity with no end state; continuing and accelerating technological developments will not cease to create or uncover new vulnerabilities exposing the infrastructure to intentional or accidental dangers. Organizations must recognize up front that establishing a successful, sustainable security program is a huge, complex and very long-term effort, but it can and must be done. The importance of protecting these systems goes beyond any one organization, and this will only become more evident as the web of interconnected systems continues to expand. As daunting as it may seem, it is accomplishable. The experiences of many experts in this field have shown that, by following the steps outlined in this document, ICS network defenders can greatly reduce both the number of security incidents affecting their organizations and the impact of such incidents.

# Appendix A: Glossary

- **ICS**—Industrial control system. Used interchangeably with OT and CAS. DCS and SCADA are examples of ICS. Refers to a network of sensors, actuators, controllers, operator terminals, etc., their connected devices, equipment and software. Includes the network layer providing connectivity and communication.
- **OT**—Operational technology. Used interchangeably with ICS and CAS.
- **CAS**—Control and automation system. Used interchangeably with OT and ICS.
- **PCN**—Process control network. Used interchangeably with ICS/OT/CAS network.
- **DPI**—Deep packet inspection. Network routing equipment may only read the first header of communications packets to determine where to direct it. Stateful packet inspection (SPI) reads the second or protocol header as well to ensure packets are part of a known active session. DPI reads packet contents to gather additional data and analysis to, for example, monitor for spam, viruses, intrusion detection or protocol non-compliance.
- **Dwell time**—Period of time between infiltration of malicious actor(s) into a network and the discovery of that incursion.
- **Network monitoring tool**—Used within this document as an umbrella term to cover applications and appliances that monitor network traffic, including those with additional capabilities such as intrusion detection and intrusion prevention. Used interchangeably with network anomaly detection tools.
- **Network anomaly detection tool**—See *network monitoring tool*.
- **PIE**—Protocol inspection engine. Technology designed to inspect and protect against malicious data flows that utilize industrial protocols found in an ICS/OT environment.

# Appendix B: Further Reading

NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security
http://dx.doi.org/10.6028/nist.sp.800-82

Australian government's Trusted Information Sharing Network (TISN) for Critical Infrastructure Resilience—SCADA Good Practice Guides (available to TISN members)

NERC (North American Electricity Reliability Corporation) Critical Infrastructure Protection (CIP) Manuals

ANSI/ISA-99: Security for Industrial Automation and Control Systems
https://www.isa.org/isa99/

# About the Authors

**Bengt Gregory-Brown** is a consultant to the SANS ICS program and the principal analyst at Sable Lion Ventures LLC, a virtual accelerator focused on emerging cyber security solutions. He brings 20 years of experience to bear in his writing about the management of IT and infrastructure projects, enterprise security governance, information security risk analysis, regulatory compliance and policy conformance for high-profile companies. Bengt has managed multiple patents from ideation through the development and issuing phases.

**Derek Harp** is currently the director for ICS Global Programs at SANS and chair of the GICSP Steering Committee. He is responsible for organizing events, resources and initiatives that educate and enable increased collaboration within the entire ICS security community. Derek has served as a founder, CEO or advisor of early-stage companies for the past 18 years with a focus on cyber security. He is a former U.S. Navy officer with experience in combat information management, communications security and intelligence.

# Sponsor

*SANS would like to thank this paper's sponsor:*

wurldtech
A GE Company

Last Updated: January 4th, 2019

# Upcoming SANS Training

**Click here to view a list of all SANS Courses**

| | | | |
|---|---|---|---|
| SANS Sonoma 2019 | Santa Rosa, CAUS | Jan 14, 2019 - Jan 19, 2019 | Live Event |
| SANS Threat Hunting London 2019 | London, GB | Jan 14, 2019 - Jan 19, 2019 | Live Event |
| SANS Amsterdam January 2019 | Amsterdam, NL | Jan 14, 2019 - Jan 19, 2019 | Live Event |
| SANS Miami 2019 | Miami, FLUS | Jan 21, 2019 - Jan 26, 2019 | Live Event |
| Cyber Threat Intelligence Summit & Training 2019 | Arlington, VAUS | Jan 21, 2019 - Jan 28, 2019 | Live Event |
| SANS Dubai January 2019 | Dubai, AE | Jan 26, 2019 - Jan 31, 2019 | Live Event |
| SANS Las Vegas 2019 | Las Vegas, NVUS | Jan 28, 2019 - Feb 02, 2019 | Live Event |
| SANS Security East 2019 | New Orleans, LAUS | Feb 02, 2019 - Feb 09, 2019 | Live Event |
| SANS SEC504 Stuttgart February 2019 | Stuttgart, DE | Feb 04, 2019 - Feb 09, 2019 | Live Event |
| SANS FOR610 Madrid February 2019 (in Spanish) | Madrid, ES | Feb 11, 2019 - Feb 16, 2019 | Live Event |
| SANS London February 2019 | London, GB | Feb 11, 2019 - Feb 16, 2019 | Live Event |
| SANS Anaheim 2019 | Anaheim, CAUS | Feb 11, 2019 - Feb 16, 2019 | Live Event |
| SANS Northern VA Spring- Tysons 2019 | Vienna, VAUS | Feb 11, 2019 - Feb 16, 2019 | Live Event |
| SANS Scottsdale 2019 | Scottsdale, AZUS | Feb 18, 2019 - Feb 23, 2019 | Live Event |
| SANS Zurich February 2019 | Zurich, CH | Feb 18, 2019 - Feb 23, 2019 | Live Event |
| SANS Dallas 2019 | Dallas, TXUS | Feb 18, 2019 - Feb 23, 2019 | Live Event |
| SANS New York Metro Winter 2019 | Jersey City, NJUS | Feb 18, 2019 - Feb 23, 2019 | Live Event |
| SANS Secure Japan 2019 | Tokyo, JP | Feb 18, 2019 - Mar 02, 2019 | Live Event |
| SANS Riyadh February 2019 | Riyadh, SA | Feb 23, 2019 - Feb 28, 2019 | Live Event |
| SANS Reno Tahoe 2019 | Reno, NVUS | Feb 25, 2019 - Mar 02, 2019 | Live Event |
| Open-Source Intelligence Summit & Training 2019 | Alexandria, VAUS | Feb 25, 2019 - Mar 03, 2019 | Live Event |
| SANS Brussels February 2019 | Brussels, BE | Feb 25, 2019 - Mar 02, 2019 | Live Event |
| SANS Baltimore Spring 2019 | Baltimore, MDUS | Mar 02, 2019 - Mar 09, 2019 | Live Event |
| SANS Training at RSA Conference 2019 | San Francisco, CAUS | Mar 03, 2019 - Mar 04, 2019 | Live Event |
| SANS Secure India 2019 | Bangalore, IN | Mar 04, 2019 - Mar 09, 2019 | Live Event |
| SANS St. Louis 2019 | St. Louis, MOUS | Mar 11, 2019 - Mar 16, 2019 | Live Event |
| SANS Secure Singapore 2019 | Singapore, SG | Mar 11, 2019 - Mar 23, 2019 | Live Event |
| SANS San Francisco Spring 2019 | San Francisco, CAUS | Mar 11, 2019 - Mar 16, 2019 | Live Event |
| SANS London March 2019 | London, GB | Mar 11, 2019 - Mar 16, 2019 | Live Event |
| SANS Secure Canberra 2019 | Canberra, AU | Mar 18, 2019 - Mar 23, 2019 | Live Event |
| ICS Security Summit & Training 2019 | Orlando, FLUS | Mar 18, 2019 - Mar 25, 2019 | Live Event |
| SANS Norfolk 2019 | Norfolk, VAUS | Mar 18, 2019 - Mar 23, 2019 | Live Event |
| SANS Bangalore January 2019 | OnlineIN | Jan 07, 2019 - Jan 19, 2019 | Live Event |
| SANS OnDemand | Books & MP3s OnlyUS | Anytime | Self Paced |