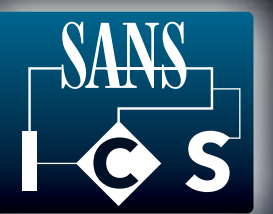


Industrial Control Systems (ICS) Security Resources



Sponsors

To get your free vendor-sponsored whitepaper, visit www.sans.org/tools.php

INDUSTRIAL DEFENDER® WHITEPAPER: **SANS 20 Critical Controls: Key Considerations for Industrial Control Systems**
www.industrialdefender.com

TREND MICRO Securing Your Journey to the Cloud WHITEPAPER: **The SCADA That Didn't Cry Wolf: Who's Really Attacking Your ICS Equipment?**
www.trendmicro.com

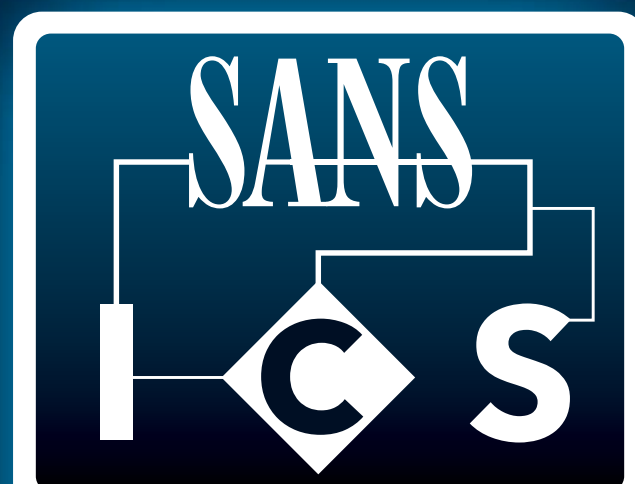
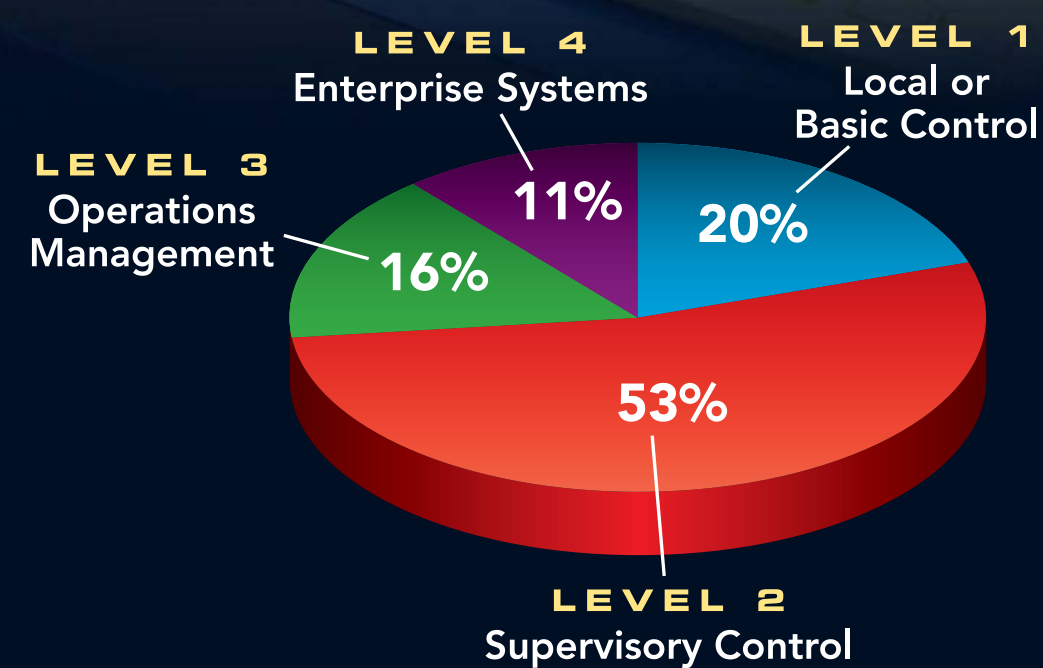
WATERFALL® Stronger Than Firewalls WHITEPAPER: **Introduction to Waterfall Unidirectional Security Gateways: True Unidirectionality, True Security**
www.waterfall-security.com

Rockwell Automation
www.rockwellautomation.com/security

CONTROL ENGINEERING
www.controleng.com

SANS, working with industry experts, is making a difference in the Industrial Control System (ICS) cyber security front. SANS has joined forces with industry leaders to, change the game, by equipping both security professionals and control system engineers with the security awareness, work specific knowledge, and hands-on technical skills they need to secure automation and control system technology. The SANS ICS team is working to provide ICS focused curriculum and certifications, as well as community resources including posters, white papers, and security practice application guidance. SANS has engaged the dedicated practitioner community that assembles during our global and regional ICS summits, and leverage leaders from enterprises, governments, and vendors from around the globe to tackle our common challenges and share working solutions.

DHS Common Cybersecurity Vulnerabilities in Industrial Control Systems



Industrial Control Systems

Security Resources

POSTER

FALL 2013 | 26TH EDITION

BUSINESS ZONE

LEVEL 5 Enterprise Business Network
 Corporate level applications used to support Enterprise Business and User Goals. Items typically found in this zone include; Internet access points, Email servers, customer facing web servers, internal web servers, CRM systems, HR systems, corporate directory architectures, enterprise document management systems, and remote access VPN endpoints.

LEVEL 4 Business Unit or Plant Network
 IT shared services for a local site, business unit, or subsidiaries. Items typically found in this zone include; local file and print servers, local phone systems, site directory replicas, site specific remote access solutions, security event aggregators, and site specific Internet access points.

DEMILITARIZED ZONE

DMZ
 Provides a series of function specific zones where services and data can be shared between the zones. Items typically found in this zone include; patch management servers, Anti-Virus management systems, site specific application servers, jump host environments, business intelligence systems, backend databases for site specific applications, and development systems.

OPERATIONS ZONE

LEVEL 3 Operations Support
 Includes the functions involved in managing the operations environment. Items typically found in this zone include; operations scheduling resources, reliability tracking tools, operations simulation and modeling tools, contingency analysis tools, replicated historians, and data visualization utilities. There may also be dedicated operations specific IT services such as DHCP, LDAP, DNS, and file servers.

OPERATIONS ZONE

LEVEL 2 Supervisory Control LAN
 Includes the functions involved with operating the real-time control system. Items typically found in this zone include; control center operation workstations, Human Machine Interfaces (HMI), engineering workstations, security event collectors, operations alarm systems, communications front ends, data historians, and network / application administrator workstations.

OPERATIONS ZONE

LEVEL 1 Control Devices
 Includes the functions involved at site specific operating environments. Items typically found in this zone include; dedicated operator workstation, Programmable Logic Controllers, control processors, programmable relays, Remote Terminal Units, and process specific microcontrollers.

OPERATIONS ZONE

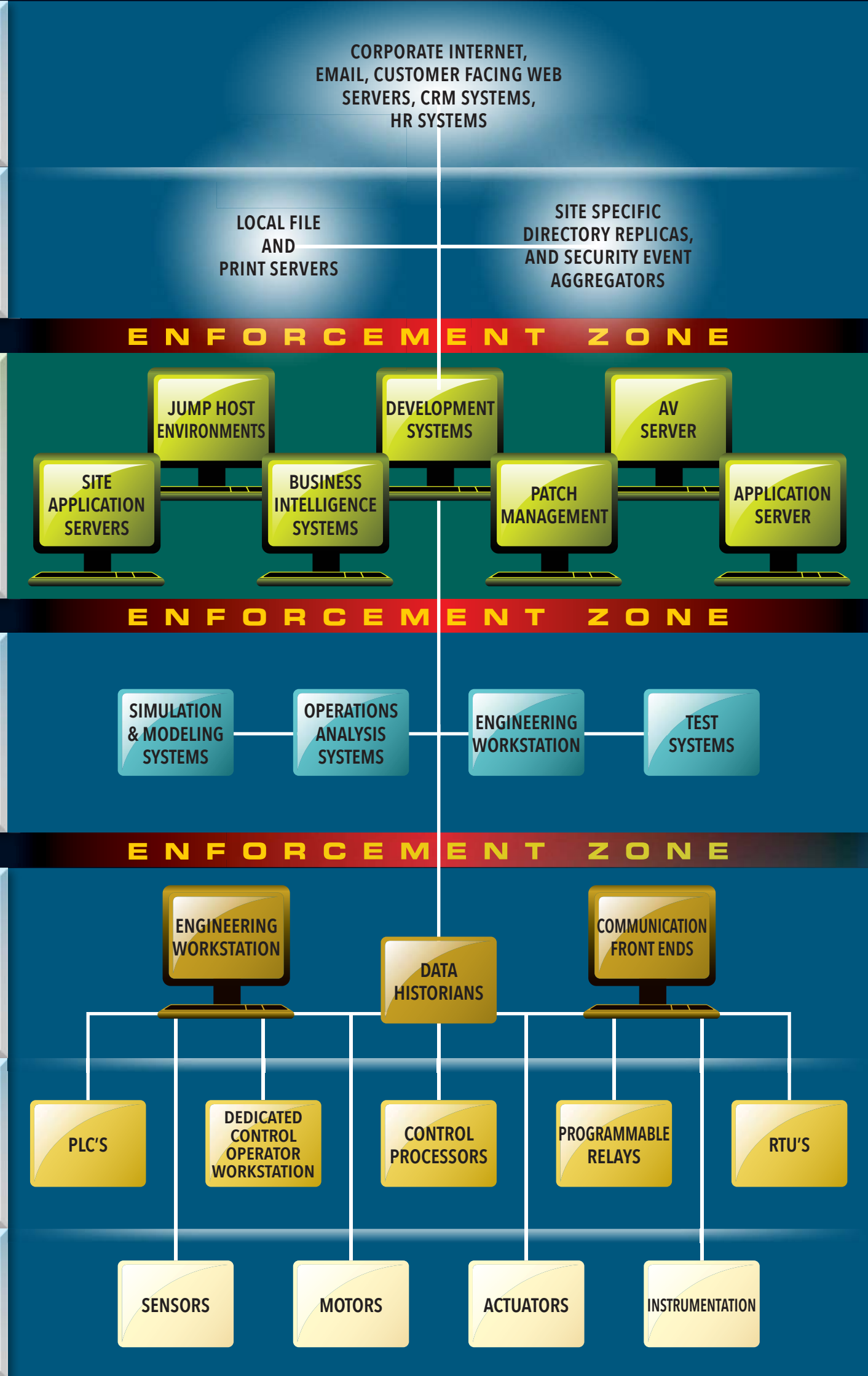
LEVEL 0 Process Control Instrumentation Bus Network
 Includes the functions involved in transitioning from cyber to physical and from physical to cyber. Items typically found in this zone include; sensors, actuators, motors, process specific automation machinery and field instrumentation devices.

SAFETY ZONE

Safety Zone
 Safety specific systems that are engineered for a specific protective function. Items typically found in this zone include all items identified in Level 0 and 1 with a dedicated purpose for a safety control function like; acoustic monitoring, liquid chemistry monitoring, vibration monitoring, emission monitoring and in most safety systems there exists a control function that serves to protect the operation and personnel.

ENFORCEMENT ZONE

Enforcement Zone
 Includes the functions necessary to segment and protect the various zones within an ICS environment. Items typically found in this zone include; Firewalls, Routers (with ACL's), Application Firewalls, Data Guard technology, and unidirectional data diode technology. Technologies implemented may differ at the various enforcement zones within an ICS environment depending on the business needs and the level of risk determined at a specific enforcement zone.



SANS ICS410: ICS/SCADA Security Essentials

Five-Day Program | Laptop Required | 30 CPEs

The SANS Industrial Control Systems Team is working to develop a curriculum of focused ICS courseware to equip both security professionals and control system engineers with the knowledge and skills they need to safeguard our critical infrastructures. The entry-level course in the SANS ICS Curriculum is ICS410: ICS/SCADA Security Essentials.

This course provides students with the essentials for conducting security work in Industrial Control System (ICS) environments. Students will learn the language, the underlying theory and the basic tools for ICS security in industrial settings across a diverse set of industry sectors and applications. This course will introduce students to ICS and provide the necessary information and learning to secure control systems while keeping the operational environment safe, reliable, and resilient.

Global ICS Professional Certification

GIAC, working with industry experts, has developed a vendor neutral, practitioner-focused Industrial Control System certification.

The Global Industrial Cyber Security Professional Certification (GICSP) assesses a base level of knowledge and understanding across a diverse set of professionals who engineer or support control systems and share responsibility for the security of these environments. This certification will be leveraged across industries to ensure a minimum set of knowledge and capabilities that an IT, engineer, and security professional should know if they are in a role that could impact the cybersecurity of an ICS environment.

Securing the Human

SANS has expanded the focus of the popular Securing the Human product into two ICS focused areas. First, **Securing the Human for Utilities** is a computer-based training program with specific focus on the NERC CIP Standards. This training consists of seven core modules that provide an overview of NERC and FERC, an Introduction to the NERC CIP Standards, and a series of topics on physical and electronic access controls, as well as information protection and incident response.

In addition, SANS has developed **Securing the Human for Engineers**, which focuses on security behaviors for individuals who interact with, operate, or support Industrial Control Systems. This training consists of 10 core modules and provides an ICS overview, an understanding of ICS attacks, and covers basic system and network defense approaches in an ICS environment, as well as governance and policy resources.

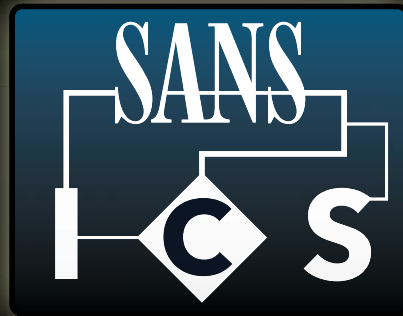
These programs were developed to not only assist your organization in meeting compliance requirements through continued training and standard reporting, but also change human behavior and reduce risk.



- SANS ICS Homepage**
<http://www.sans.org/ics>
- DHS ICS-CERT**
<http://ics-cert.us-cert.gov>
- DHS Cybersecurity Evaluation Tool**
<http://ics-cert.us-cert.gov/Assessments>
- NERC ES-ISAC**
<http://www.esisac.com/SitePages/Home.aspx>

- ICS-ISAC**
<http://ics-isac.org>
- Cybersecurity Vulnerability NISTB Program**
<http://energy.gov/oe/downloads/common-cyber-security-vulnerabilities-observed-control-system-assessments-inl-nstb>
- Vulnerability Analysis of Energy Delivery Control Systems**
<http://energy.gov/oe/downloads/vulnerability-analysis-energy-delivery-control-systems>

- NIST SP 800-82 Guide to ICS Security**
<http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf>
- ISA-99 Control System Security Committee**
<http://isa99.isa.org/ISA99%20Wiki/Home.aspx>
- NERC CIP Standards**
<http://www.nerc.com/pal/Stand/ReliabilityStandards.aspx>



Control Systems Are a Target



www.sans.org/ics

www.securingthehuman.org

Network Access

- Internet accessible systems are being mapped by ERIPP or SHODAN, or are easily locatable through search engine queries
- Malware can spread vertically through the network by trusted system to system connections or VPN
- It is very easy to maneuver undetected throughout a control environment
- There is potential to leverage non-routable trusted communication paths

Interconnects

- ICS systems can be attacked by exploiting applications that communicate through network segmentation
- Connections to other organizations, plants or systems
- Many ICS environments are susceptible to network-based Man in the Middle Attacks

Dial-Up

- ICS assets can be remotely accessible through traditional dial-up modems that have little access control protections
- Numerous ICS assets at a location can be accessed through a single dial-up access point with a multiplex device that enables connections to many ICS assets
- Old attack vectors can still be successful in ICS environments

System Management

- Attackers can take advantage of long delays in patching and operating system upgrades
- Attackers can take advantage of systems with no anti-virus, or out-of-date signatures
- Attackers will leverage default usernames and passwords or weak authentication mechanisms
- Attacks will be difficult to detect due to minimal asset security logging capability
- Attackers will leverage file access techniques to move data in and out of the ICS environment through physical removable media or trusted communication paths utilized for system maintenance

Supply Chain

- Third party vendors, contractors or integrators can be attacked in an attempt to ultimately attack an ICS asset owner or multiple asset owners
- ICS hardware and software can be directly breached or impacted prior to arriving in the production ICS environment

You may not realize it, but your organization's Industrial Control System (ICS) environments are a target for cyber attackers. The ICS automation, process control, access control devices, system accounts and asset information all have tremendous value to attackers. This poster demonstrates the many different ways attackers can gain access to an ICS environment and demonstrates the need for active security efforts and ICS engineer training that will enable informed engineering decisions and reinforce secure behaviors when interacting with an Industrial Control System.

In many cases these are not one-off attacks, but are planned for with reconnaissance, multiple attacks and adjustments. These are campaigns that happen over the course of months, and they require system owners and operators to be vigilant and recognize when something is not right.



ICS Security goal: Ensure the safe, reliable and secure operation of ICS environments from procurement to retirement

Abnormal activity or unexplained errors deserve a closer security look

Governance

- Attackers can leverage the lack of corporate security policies, procurement language, asset inventory and standardization that exist in many ICS environments
- Attackers can have greater impacts on ICS environments, as ICS assets are often not considered in the preparation phase of security incident response planning and containment approaches
- ICS risk and hazard assessment are not always evaluated with the loss of cyber integrity which, can lead to a loss of availability, impacts due to interdependencies and misuse of critical components or functions
- In some sectors ICS assets are often architected or assessed from a compliance perspective and not always assessed from a security perspective

Social Engineering

- Request for Proposals often contain a wealth of information regarding an ICS environment
- Vendors frequently post information about a project they are working on for an ICS customer
- Employee social media sites often contain technology architecture information and, possibly, images of ICS work environments
- Engineer professional bios can provide a helpful map of your ICS
- Publicly available information regarding an ICS asset owners' vendor relationships, conference attendance, committee participation and domain registrations can all be leveraged against the organization

Physical Security

- Attackers can leverage the physical locations of numerous ICS assets that could be located in remote geographies or are unmonitored, even when little to no physical access controls ICS assets can be physically stolen or obtained
- ICS assets can be physically stolen or obtained secondhand with access to sensitive information that could be used in planning an attack
- Physical changes or alterations to ICS devices are often difficult to detect

Cyber Actors

- Nation States
- Insiders and other trusted parties (such as contractors / vendors / integrators)
- Criminal Hacker
- Politically motivated attackers (hacktivists)
- Script Kiddies