

ICS WHITEPAPERS

NEXDEFENSE
Seeing Through the Fog of Complexity — How a foundational tool like NexDefense's SOPHIA can ensure ICS/SCADA systems stay reliable, predictable, and secure
nexdefense.com

paloalto
Next-generation Security for SCADA and ICS
paloaltonetworks.com

Rockwell Automation
Design Considerations for Securing Industrial Automation and Control System Networks
rockwellautomation.com

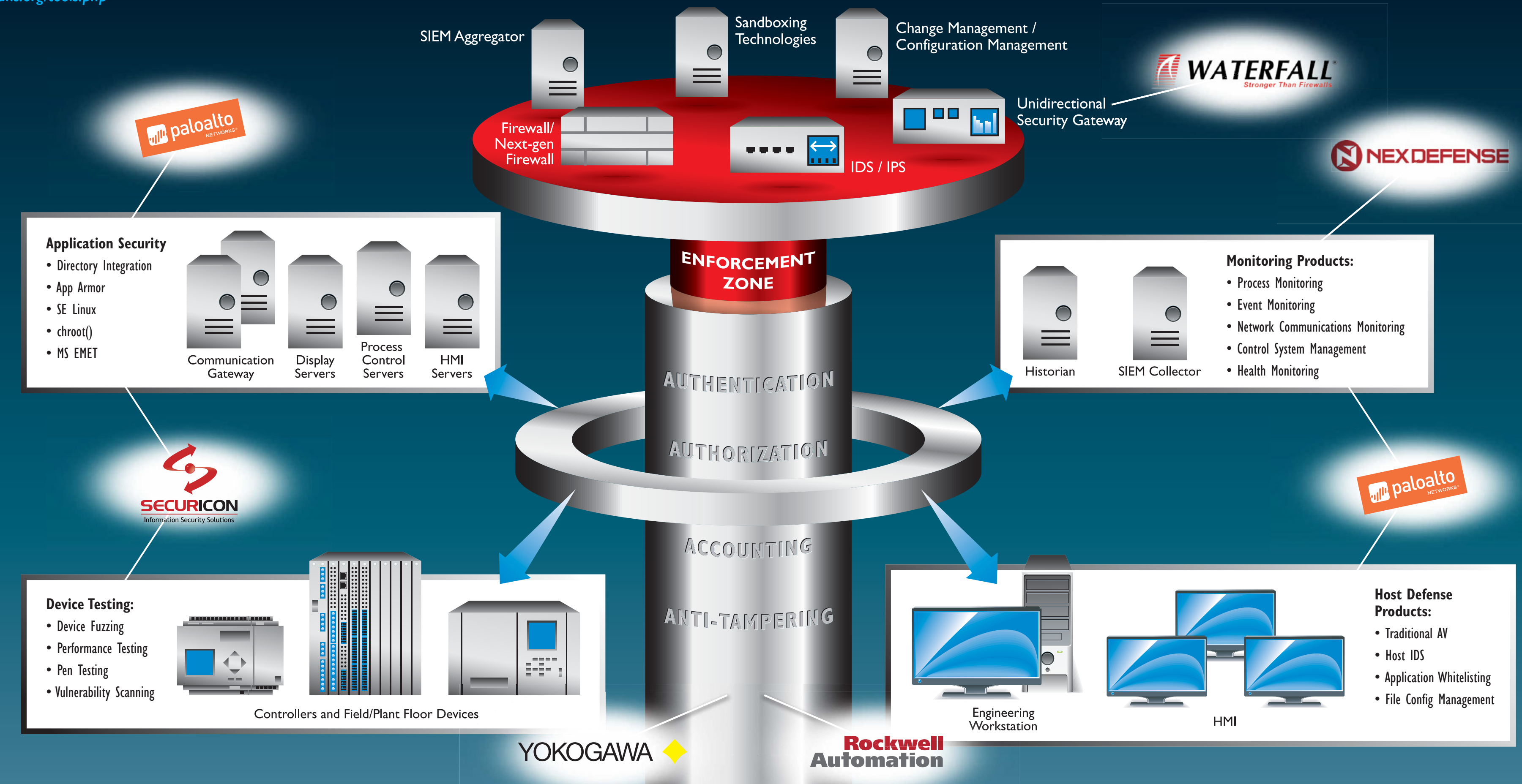
SECURICON
Information Security Solutions
Strategies for Industrial Device Testing
securicon.com

WATERFALL
Stronger Than Firewalls
Expendible ICS Networks
waterfallsecurity.com

YOKOGAWA
Yokogawa's Comprehensive Lifecycle Approach to Process Control System Cyber-Security
yokogawa.com

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

ICS SECURITY SOLUTIONS MAP



TRENDS
SOLUTIONS
TRAINING

SANS ICS
Industrial Control Systems
A term used to describe the personnel, hardware, and software components that read inputs and control outputs in a manner that bridges the Cyber and Physical worlds.

POSTER

ics.sans.org

Intro to the ICS Curriculum

ICS CURRICULUM

TRADITIONAL COURSE TREND

- SEC301** Intro to Information Security GIAC: GISF
- ICS410** ICS/SCADA Security Essentials GIAC: GICSP

ADVANCED ICS COURSES

- HOSTED** Assessing and Exploiting Control Systems (Hosted by UtiliSec)
- HOSTED** Critical Infrastructure and Control System Cybersecurity (Hosted by CYBATI)
- ICS515** ICS Active Defense and Response
- SANS' Advanced Cybersecurity Courses:** Cyber Defense: SEC501 • SEC502 • SEC503 • SEC511; Forensics: FOR408 • FOR508 • FOR610; Hands-on Exercise: SEC562 (CyberCity)

AUTOMATION EVENTS

- 1700: EARLY 1700s: René-Antoine Ferchault de Réaumur proposed ideas for automatic devices to provide feedback for the purposes of control.
- 1788: James Watt's steam governor provided proportional control of the throttle.
- 1900s: Use of relays, and control cabinets in remote rooms to turn things on/off by use of switches and monitor recorders.
- 1950s: Machine tools were automated with Numerical Control (NC) using punched paper tape.
- 1959: First use of distributed control throughout a large industrial plant.
- 1969: Modicon 084 the first programmable controller implemented. (Modicon stood for Modular Digital CONTroller.)
- 1971: Allen-Bradley designed and named the Bulletin 1774 PLC and coined the term "Programmable Logic Controller".
- 1973: Modbus introduced to allow PLCs to talk with one another.
- 1976: Remote I/O introduced.
- 1986: PLCs are linked to PCs.
- 1990s: Fieldbus protocols to include ControlNet, DeviceNet, Profibus, and Fieldbus Foundation. Quickly followed by Ethernet and TCP/IP connectivity for PLCs.
- 2000 & BEYOND: Open Technology Movement. ICS vendors begin migration from proprietary networks, software, and hardware platforms to open architectures.
- 2001: First PAC is introduced.
- 2003: First controllers with embedded web server.

- 2005: SCADA workstations shipped to utility with infections.
- AUG 2005: Zotob worm infects 13 U.S. auto plants causing shutdowns and delays.
- NOV 2006: Breach into Pennsylvania water plant installation of spyware on plant's computer systems.
- AUG 2007: Los Angeles traffic system cyber intrusion by insiders (labor strike).
- JAN 2008: Commuter tram collision by glancing blow and derailment due to unauthorized switching in the city of Lodz, Poland.
- JUL 2008: Revelation by U.S. government official that cyber attacks have resulted in power outages in multiple regions outside the United States.
- FEB 2009: Conficker Worm gets into ICS along with 12 million general computers. It infected power generation plants in the U.S.
- 2009: Off-shore oil platform hacks impact leak detection systems. Unauthorized access and control of off shore platform leak detection and monitoring system.
- SEP 2009: Utility smart meters are compromised in scale resulting in lost revenue.
- DEC 2009: Virus infection of OPC servers at Petro-chemical plant in South Africa.
- 2010: Stuxnet worm discovered. Stuxnet is a computer worm that was discovered in June 2010 but evidence suggests variations may have dated back to 2005 and was designed to target ICS and impact a specific process.
- SEP 2011: Duqu malware discovered.
- DEC 2011: APT attacks on gas pipeline sector.
- 2012: Houston water system compromise.
- MAY 2012: Flame malware discovered.
- SEP 2012: Telvent intrusion, company warns ICS customers (ICS supplier).
- JUN 2014: Havex Trojan is discovered in ICS-focused water-holding attacks — observed capability to locate OPC servers and attempts to exfiltrate collected data.

THE HISTORY OF ICS

Detailed History of ICS whitepaper available at ics.sans.org/resources

ICS SECURITY EVENTS

- 1982: Unincorporated report of a Trojan program inserted into SCADA system software that caused an explosion along the Trans-Siberian pipeline.
- MAR 2000: A former consultant accessed the control system of the plant and released up to one million litres of sewage into the surrounding waterways.
- APR 2000: Media reports about GAZPROM cyber incident impacting operational systems.
- JAN 2003: Plant computers infected by Slammer worm. The worm entered the plant network via a contractor's infected computer connected via telephone dial-up directly to the plant network, thus bypassing the firewall.
- AUG 2003: The Blaster worm infected the communication system of a U.S. railway company — the dispatching and signaling systems were affected and passenger and freight traffic systems were disrupted.
- DEC 2003: DCS system found infected with Nachi (AKA Welchia) virus on 8 APCs.
- 2005: SCADA workstations shipped to utility with infections.
- AUG 2005: Zotob worm infects 13 U.S. auto plants causing shutdowns and delays.
- NOV 2006: Breach into Pennsylvania water plant installation of spyware on plant's computer systems.
- AUG 2007: Los Angeles traffic system cyber intrusion by insiders (labor strike).
- JAN 2008: Commuter tram collision by glancing blow and derailment due to unauthorized switching in the city of Lodz, Poland.
- JUL 2008: Revelation by U.S. government official that cyber attacks have resulted in power outages in multiple regions outside the United States.
- FEB 2009: Conficker Worm gets into ICS along with 12 million general computers. It infected power generation plants in the U.S.
- 2009: Off-shore oil platform hacks impact leak detection systems. Unauthorized access and control of off shore platform leak detection and monitoring system.
- SEP 2009: Utility smart meters are compromised in scale resulting in lost revenue.
- DEC 2009: Virus infection of OPC servers at Petro-chemical plant in South Africa.
- 2010: Stuxnet worm discovered. Stuxnet is a computer worm that was discovered in June 2010 but evidence suggests variations may have dated back to 2005 and was designed to target ICS and impact a specific process.
- SEP 2011: Duqu malware discovered.
- DEC 2011: APT attacks on gas pipeline sector.
- 2012: Houston water system compromise.
- MAY 2012: Flame malware discovered.
- SEP 2012: Telvent intrusion, company warns ICS customers (ICS supplier).
- JUN 2014: Havex Trojan is discovered in ICS-focused water-holding attacks — observed capability to locate OPC servers and attempts to exfiltrate collected data.

TRANSPORTATION

- Rail**
 - Switching
 - Sensor monitoring
 - Signal monitoring
 - Traction systems
 - Safety systems
- Shipping**
 - Terminal operations
 - Crane control
 - Cargo management systems
 - Aviation
 - Air traffic control systems
- Warehouse Distribution**
 - Inventory tracking
 - Conveyor systems
 - Automated product delivery
 - Automated storage and retrieval systems
 - Automated guided-vehicle systems
- Highway/Road**
 - Traffic control systems
 - Bridge monitoring systems
 - Traffic monitoring systems



NATURAL GAS

- Gas flow metering
- Flow control and pressure management
- Alert and alarm systems
- Monitor temperature levels
- Pipeline pressure monitor
- Odorant management systems
- Condensate tank levels
- Liquefaction control systems
- Vaporization control systems
- Boiloff control systems
- Well head control
- Field compression



- Upstream systems:**
 - Ballast control systems
 - Drilling control systems
 - Gas compressor control
 - Water treatment systems
 - Concrete batch control systems
 - Helicopter fueling systems
 - Safety-instrumented systems
- Midstream systems:**
 - Process control systems monitoring and controlling temperature, flow, pressure, weight, and viscosity
 - Safety-instrumented systems
- Downstream systems:**
 - Storage, pretreatment, distillation, and dispatch control systems
 - Safety-instrumented systems

ELECTRIC

- Transmission**
 - Switching
 - Circuit breaker control
 - Protective relaying
 - Distribution automation logic components
- Generation**
 - Turbine control systems
 - Boiler control systems
 - Acoustic monitoring systems
 - Heat rate systems
 - Coal handling systems
 - Emission monitoring systems
 - Water chemistry systems
 - Vibration control systems
 - AGC systems



HEALTHCARE

- Patient vital sign monitoring systems
- MRI monitoring systems
- Infusion systems
- Implanted medical devices
- Nurse monitoring stations
- Operating room environmental control systems



Securing an Automated World

Learn why ICS security should be on your career map

ics.sans.org

CHEMICAL



- Batch process control and continuous process control systems
- Monitoring and control of process temperature, pressure, flow rate, liquid level, gas level, and chemical makeup
- Chemical reactor control
- Mixing systems
- Distillation column control
- Environmental monitoring of gas, liquid, and solid discharge
- Safety-instrumented systems

WATER

- Monitoring source water
- Treatment process control
- Pressure control
- Flow control
- Wastewater collection system monitoring
- Pump station monitor and control
- Valve pump and mixing monitor and control

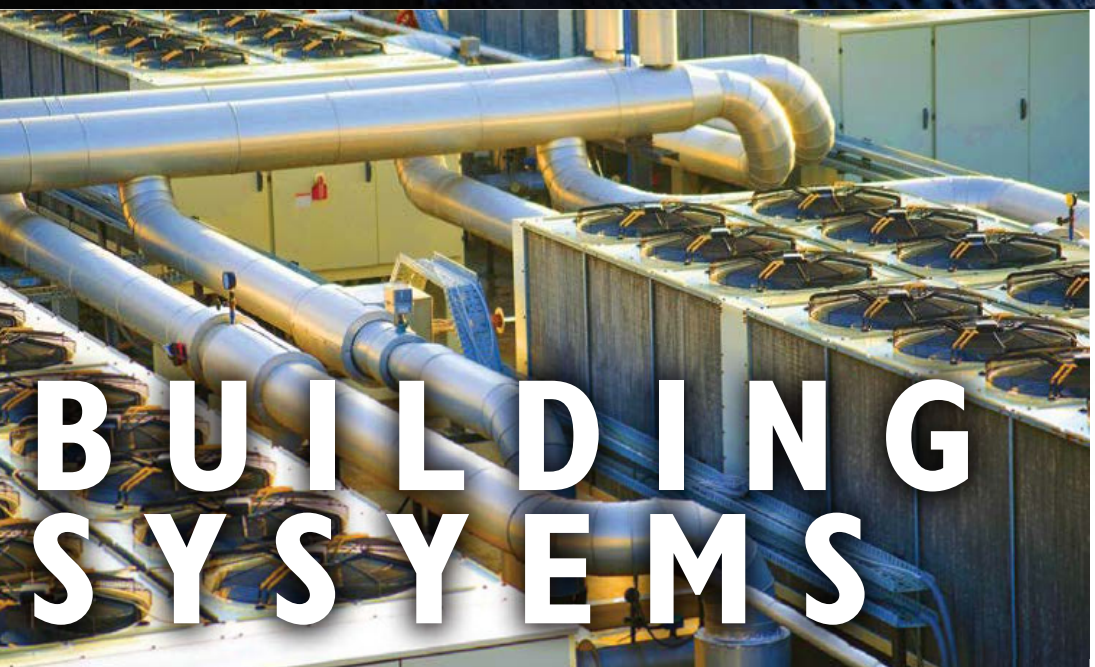


- Light manufacturing**
 - Etching control – Chemical Mechanical Planarization (CMP)
 - Lithography control
 - Processing temperature
 - Process pressure
 - Cooling and heating rates
- Heavy manufacturing**
 - Robotic arm assembly
 - Weld controllers
 - Sealing and dispensing systems
 - Quality test systems
 - Production line control systems
 - Press control systems
 - Hydraulic press controls
 - Flat metal line feeder control
 - CNC systems

MANUFACTURING

BUILDING SYSTEMS MGT

- Switch gear management
- Lighting control
- HVAC control systems
- Fire suppression systems
- Physical access control and monitoring systems
- Facility management systems
- Air quality systems
- Water treatment systems
- Boiler control systems



CONTROL CENTER OPERATIONS



- Control Centers**
 - Energy management systems
 - Communications front end
 - Inter-control center communication systems
 - Operator alarm systems
 - Contingency analysis
 - State estimation
 - Automatic generation

OTHER SECTORS

- Amusement Parks**
 - Amusement park ride control
 - Theme element activation
 - Safety systems
- Mining**
 - Dust management systems
 - Ventilation performance systems
 - Machine long travel monitoring systems
 - Conveyor alignment detection
 - Ground water level monitor
- Food and Beverage**
 - Packaging systems
 - Food safety systems
 - Batch mixing process systems
 - Clean and sterilizing in-place systems
 - Ingredient, work in progress, and finished goods tracking systems



Visit SANS' CyberCity: sans.org/netwars/cybercity