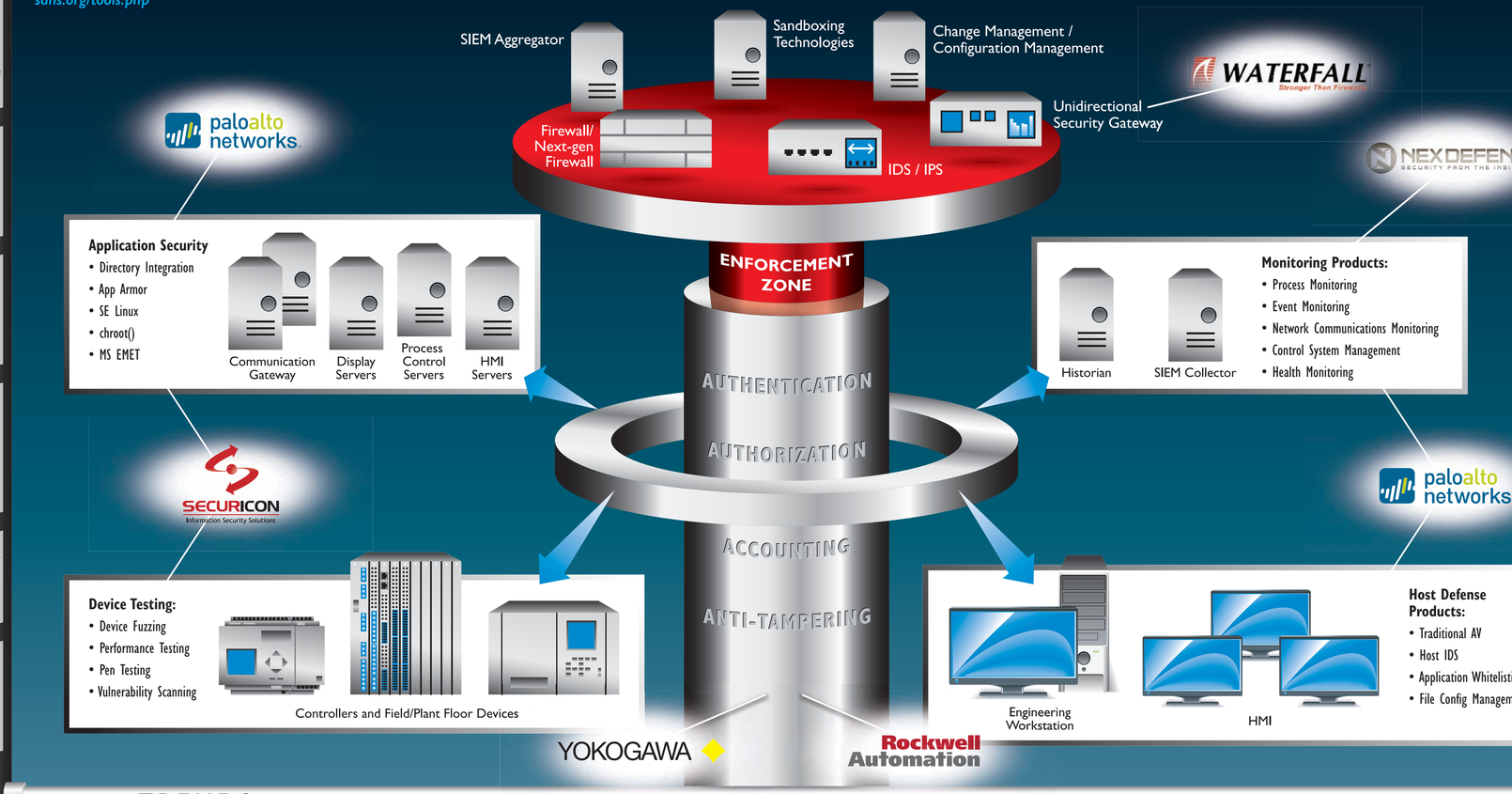
To get your free vendor-sponsored whitepaper, visit sans.org/tools.php

ICS Security Solutions Map



Automation Events

René-Antoine Ferchault de Réamur proposed **ideas for automatic devices** to provide feedback for the purposes of control	EARLY 1700s
James Watt's **steam governor** provided proportional control of the throttle	1788
Use of relays and control cabinets in remote rooms to turn things on/off by use of **switches and monitor recorders**	1900s
Machine tools were automated with Numerical Control (NC) using **punched paper tape**	1950s
First use of **distributed control** throughout a large industrial plant	1959
Modicon 084 the first **programmable controller** implemented. (Modicon stood for MOdular DIgital COntroller.)	1969
Allen-Bradley designed and named the Bulletin 1774 PLC and coined the term **"Programmable Logic Controller"**	1971
Modbus introduced to allow PLCs to talk with one another	1973
Remote I/O introduced	1976
PLCs are linked to PCs	1986
Fieldbus protocols to include **ControlNet, DeviceNet, Profibus,** and **Fieldbus Foundation.** Quickly followed by **Ethernet** and **TCP/IP** connectivity for PLCs	1990s
Open Technology Movement ICS Vendors begin migration from proprietary networks, software, and hardware platforms to open architectures	2000 & BEYOND
First PAC is introduced	2001
First controllers with **embedded web server**	2003
NERC CIP Standards become enforceable	JUL 2008
DHS ICS-CERT is created	NOV 2009
First ePAC is introduced	2013

The History of ICS

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

1700 – 1900 — 1st Industrial Revolution — **Mechanical Production Powered by Steam**

1900 – 1970 — 2nd Industrial Revolution — **Mass Production Powered by Electricity**

1970 – 2000 — 3rd Industrial Revolution — **Automation of Production by Electronics**

2001 – 2004

2005 – 2010

2011 – PRESENT — **Automation of Cyber-physical Systems and the Internet of Things**

ICS Security Events

1982	Uncorroborated 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
	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-holing attacks – observed capability to locate OPC servers and attempts to exfiltrate collected data

TRENDS

SOLUTIONS

TRAINING

Industrial Control Systems (ICS) 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.

SANS ICS Industrial Control Systems

POSTER

FALL 2014 | 32ND EDITION

ics.sans.org

Intro to the ICS Curriculum

Securing the Human (STH) Security Awareness Products

STH End User These modules cover the broadest set of users and a wide range of cybersecurity awareness topics.

STH Utility These modules focus on cybersecurity awareness and NERC CIP training program needs for utilities.

STH Engineer These modules focus on individuals who support, engineer, or interact with control system cyber assets.

ICS Curriculum

Traditional Course Trend

SEC301 Intro to Information Security — GIAC: GISF

This course is for individuals new to information technology that need to understand the basics of information assurance, computer networking, cryptography, and risk evaluation.

ICS410 ICS/SCADA Security Essentials — GIAC: GICSP

This course is for individuals who interact with or who could impact Industrial Controls System environments. The roles performed by personnel specific to this field can roughly be divided into four domains:

- IT (includes OT support)
- IT Security (includes OT security)
- Engineering
- Corporate, industry, and professional standards

GICSP — Global Industrial Cyber Security Professional

This GIAC certification is being leveraged across industries to ensure a minimum set of knowledge and capabilities that IT, engineers, and security professionals should know if they are in a role that could impact the cybersecurity of an ICS environment.

Advanced ICS Courses

HOSTED Assessing and Exploiting Control Systems — Hosted by: UtiliSec

This course is for individuals with responsibility for performing pentesting and vulnerability discovery within ICS environments.

HOSTED Critical Infrastructure and Control System Cybersecurity — Hosted by: CYBATI

This hands-on course is for individuals with the responsibility of securing control systems and control system components.

HOSTED *Coming Soon!* Advanced ICS Defense Course — Hosted by: RED TIGER SECURITY

ICS515 ICS Active Defense and Response

This course is for individuals with responsibility for generating and using ICS threat indicators in an effort to actively modify defense systems against new threats, respond to intrusions and perform triage to prevent future intrusions.

SANS' Advanced Cybersecurity Courses:
Cyber Defense: SEC501 • SEC502 • SEC503 • SEC511
Forensics: FOR408 • FOR508 • FOR610
Hands-on Exercise: SEC562 (CyberCity)

Securing an Automated World

Learn why ICS security should be on your career map

ics.sans.org

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

OIL

Upstream systems:
- Ballast control systems
- Drilling control systems
- Gas compressor control
- Power generation 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

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
- Evironmental monitoring of gas, liquid, and solid discharge
- Safety-instrumented systems

HEALTHCARE

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

MANUFACTURING

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

BUILDING SYSYEMS 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