SECURING INDUSTRIAL CONTROL SYSTEMS: A MATTER OF LIFE AND DEATH

Modern life depends on automation. Almost every time we turn on a faucet, switch on a light or jump on a train we are relying on Industrial Control Systems (ICS) to manage processes like water purification, electricity generation and mass transit signalling. But relying on computers for such essential tasks requires absolute trust in their security, since attacks which disrupt these basic necessities could trigger catastrophic economic and public health and safety collapse.

Unlike in the past, most ICS vendors now use standard IT technologies within their solutions, allowing companies to connect ICS components like SCADA with corporate networks and other operational technologies such as Enterprise Resource Planning (ERP) and Manufacturing Execution Systems (MES). While this convergence of technologies can improve productivity and profitability, it also dramatically increases the risk of ICS cyber-attack by creating new vectors for less skilled hackers to launch attacks.

ICS ON THE FRONTLINE

Stuxnet, Shamoon and Havex are widely known examples of this type of threat which continues to grow as global initiatives like Smart Grid lead to systems that are increasingly connected to public and private networks.

Positive Technologies understands the risks and challenges associated with securing industrial systems. Our research organization includes a dedicated team of ICS experts that has already uncovered more than 200 ICS 0-day vulnerabilities. Our specialists have carried out dozens of ICS audits and security assessments on systems from vendors including ABB, Honeywell, Schneider Electric, Siemens and Yokogawa.

Conducting these practical security audits, on a regular basis, gives Positive Technologies a comprehensive understanding of how to detect and eliminate ICS vulnerabilities.

CRITICAL SYSTEMS REQUIRE A DIFFERENT APPROACH

Securing industrial control systems is essential, but also uniquely challenging. Unlike traditional IT systems, a control system going offline for even minutes can be catastrophic. For this reason, it can take organizations months or sometimes years to roll-out even the smallest ICS patches or updates. You can't treat your ICS like just another desktop or business application, but still you must proactively identify vulnerabilities and potential attack vectors, assess and prioritize threats, and remediate weaknesses where possible. You also need to demonstrate compliance with a growing array of regulatory security standards.

Positive Technologies' track record of protecting leading industrial brands, conducting extensive practical research and working with ICS vendors gives us unique insight into the ICS threatscape, where the greatest risks are often created by operators, contractors and vendors. Whether intentional or accidental, misuse of ICS components like PLCs can introduce critical vulnerabilities and configuration changes to your systems. Our experience suggests hackers are far more likely to exploit these weaknesses than use targeted malware or system-specific vulnerabilities.

HIGHLIGHTS

- Increase Visibility with expert audits and analysis of all ICS components: ERP, MES, SCADA, HMI, PLC and RTU
- Automate Assessments and track ICS vulnerabilities, configurations and compliance levels in Siemens SIMATIC, Schneider Electric Wonderware and more
- Get Smarter by leveraging the knowledge of our expert research team that has uncovered 200+ ICS 0-day vulnerabilities

HOW SMART IS YOUR SMART GRID?

8,000,000 W

The instant power generated by European solar and wind power stations that our researchers found were vulnerable to attacks via the Internet due to weak security in Smart Grid management and cloud platforms

SIEMENS

"We value the IT security expertise of Positive Technologies. Their research and experience has helped us to improve the security of our automation products and better protect our customers' facilities."

David Heinze, Manager for Industrial Security, Siemens

Enel

"The research provided by Positive Technologies changed our view of cyber security and helped us redefine our strategic direction for securing our SCADA infrastructure."

Francesco Ceccarelli,
Head of Security Governance and Business Intelligence, Enel, Italy's largest power company

MOSENERGO

"The results from several security assessments completed by Positive Technologies will allow us to improve the security of our power generation company…and to focus on our key areas of risk."

Network Security Team,
Mosenergo, a Gazprom subsidiary

KNOW WHERE YOU'RE VULNERABLE

Our defense-in-depth approach to ICS security already helps many large manufacturing, petrochemical, utility and transportation companies meet their ICS security challenges head-on with:

+ **Automated Security Assessments of all ICS elements with MaxPatrol**—secure PLC/RTU, SMI, SCADA, MES and ERP systems with automated audit, compliance, vulnerability and configuration management. ICS-specific features include:
  + Support for industrial protocols such as Modbus, S7, DNP3 and IEC104
  + Safe Scanning Mode to minimize performance impact on systems under assessment
  + Audit and configuration analysis for ICS specific settings

  But MaxPatrol isn't just a solution for operational technologies. It also supports your full range of traditional IT systems from workstations and operating systems to servers and network equipment, allowing you to combine IT and OT security management in a single solution. More than 1,000 businesses already trust MaxPatrol.
+ **ICS Security Audits and Compliance Checks**—get the complete picture of your current security levels with deep technical audits and compliance assessments of all the technologies, systems and devices in your network, including your existing perimeter controls. Positive Technologies' ICS experts will construct a confidential, customized threat model that identifies your highest priority risks. They can also determine your level of compliance with relevant standards including NERC CIP and ISA99.
+ **ICS Threat Intelligence Monitoring**—stay ahead of the hackers with regular security updates direct from our research team including 0-day vulnerability alerts, anomaly detection and remediation tactics.
+ **ICS Security Configuration Hardening Guides**—be confident your systems are in peak condition with checklists created by Positive Technologies based on our extensive industry knowledge, hands-on research and vendor partnerships. Compare the current configurations of your ICS components including SCADA, PLC and RTU with our recommended settings for optimum security.

To ensure the reliable availability of industrial systems and critical services, you must be able to see where you are vulnerable, automate security to minimize human error, govern systems on public and private networks, monitor risk and adapt to advancing cyber security threats.

With unrivalled expertise in critical infrastructure protection backed by one of the world's top research teams, Positive Technologies is the ideal partner to help you secure your ICS networks and keep the lights on.

About Positive Technologies

Positive Technologies is a leading global provider of enterprise security solutions for vulnerability and compliance management, incident and threat analysis, and application protection. Commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on Industrial Control System, Banking, Telecom, Web Application, and ERP security, supported by recognition from the analyst community. Learn more about Positive Technologies at ptsecurity.com.

POSITIVE TECHNOLOGIES

info@ptsecurity.com ptsecurity.com