Supervisory Control and Data Acquisition

Company Overview

Founded in 1944, Parsons is an engineering, construction, technical, and professional services firm with revenues of $2.7 billion in 2011.

Parsons is a leader in many diversified markets with a focus on defense/security, environmental/infrastructure, and transportation. Parsons delivers design/design-build, program/construction management, and other professional services packaged in innovative alternative delivery methods to federal, regional, and local government agencies, as well as to private industrial customers worldwide.

We conquer the toughest logistical and technical challenges and deliver landmark projects across the globe. Today, more than 11,500 employees are engaged in executing more than 2,200 projects in 25 countries around the world. For more about Parsons, please visit www.parsons.com.

The Challenge

Industrial control systems are relied on to drive critical infrastructures such as power generation and distribution, water and wastewater, transportation, and manufacturing. Control networks were originally physically isolated from business networks, with no provisions made for data transfer between the two networks.

A truly air-gapped industrial control system (ICS) is no longer the reality for most facilities. The introduction of transmission control protocol with Internet protocol (TCP/IP) to the plant floor allowed for improved operational efficiencies, cost savings, and support. Business staffs often rely on information provided by facilities’ supervisory control and data acquisition (SCADA) systems to streamline their operations. Vendors and engineering staff may require remote access to support industrial control systems from their offices. Support staff may cross the air gap whenever they patch or update their systems.

The present state of insecurity for industrial control systems continues to grab headlines, as news of vulnerabilities and exploits is released at an alarming rate. Viewed as a decade behind traditional information technology (IT) security, these systems are attractive low-hanging fruit for both external and internal enemies. Are you equipped with the expertise to adequately defend your control network from threats?
The Defense

Best practices for ICS security include a defense-in-depth approach. As a first step, this approach includes separating a company’s business and control networks. Additional measures often include installing an intrusion detection / prevention system (IDS/IPS), for monitoring and reporting.

How robust is the security posture for your ICS? A firewall is an excellent first and necessary step to cybersecurity. However, the firewall policy must be regularly reviewed to ensure that no changes to the firewall have been made to accommodate operations that also accommodate hostile activity.

Have you inadvertently provided an open door to your enemies? Are your controls engineers adequately trained to review your security appliance logs? Do they have the expertise to validate and tune IDS/IPS rules? Are they capable of maintaining situational awareness and keeping up with the landscape of evolving threats?

The Parsons Approach

With its network enterprise organization (NEO), Parsons provides cybersecurity services for asset owners and operators of ICS and SCADA systems. Our services include vulnerability assessments, security architecture design and implementation, and incident detection and response. Understanding a control network’s unique requirements of system availability, reliability, and maintainability, we work side by side with asset owners to develop robust security policies for their control networks to ensure regulatory compliance.

Parsons leverages its expertise in cybersecurity to achieve synergies with its engineering, technical, construction, and management services for critical infrastructures. We provide unique services for asset owners and operators that other solution providers may not have considered. We can assist customers with the development of new procurement language for cybersecure control network architectures. NEO can provide cybersecurity testing and accreditation services as part of field acceptance tests for construction projects. We can offer vulnerability assessments for preexisting industrial control systems, as well as for third-party “as-built” systems before they are connected to an asset owner’s control network.

Network Enterprise Organization

NEO offers security appliance configuration services, including deep packet inspection of industrial control protocols, such as Modbus TCP, to secure communications between endpoints. Our Cyber Security Operations Center (CSOC) is fully prepared for situational awareness of zero-day exploits against industrial control systems. NEO’s cleared staff of SCADA and cybersecurity experts help asset owners respond to internal and external threats and minimize downtime associated with those threats. NEO’s on-site SCADA laboratory provides opportunities to develop additional capabilities in Parsons’ SCADA security toolkit.