CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION

SCADA and Industrial Controls Systems Protection

POWER'S CYBERSECURITY SERVICES

> Network Designs
> Enterprise and Infrastructure Planning
> SCADA System Development and Migration
> Server Configuration
> Server Client Environment Design
> Virtualization and Emulation
  > Pre-Installation Proof of Concept
  > Low Impact Failure Mode Analysis
  > Pre-Deployment Testing
> Process Simulation
> Cloud Migration
> Windows XP Migration to Windows 7/8
> Windows Server 2003 to 2008/2012 Migrations
> Patching / Updating / Upgrading / Recapitalization
> Vulnerability Assessments
> Penetration Tests (via subcontractor in support of Vulnerability Assessments)
> Security Weakness Mitigation Reports
> Firewall Configuration
> Traffic Routing Configurations
> Security Policy and Specifications for Developers and Suppliers
> Ethernet Switch and Gateway Configuration

CONTACT

Auston Miller
Federal Services Program Manager
571-346-7624

PROTECT YOUR ENTERPRISE INDUSTRIAL CONTROL SYSTEMS AND CRITICAL INFRASTRUCTURE

SCADA & Industrial Control Networks Vulnerable to Cyber Attack

The SCADA and industrial control system (ICS) networks supporting your critical utilities infrastructure contain numerous cyber vulnerabilities that can easily be reconfigured by external entities. Reliability and availability have been the key objectives of control system component manufacturers, not security. Even the most modern control systems are typically 10 to 15 years behind the security curve, leaving mission-critical infrastructure vulnerable to attack. This means the network-enabled devices that control heating, cooling, and electrical power can be compromised, leading to a devastating loss of mission.

The Great Northeast Blackout of 2003 demonstrated the vulnerability of the North American infrastructure and the impact of a widespread power outage.

System Maintenance & Upgrade Risks

Most SCADA networks are maintained by plant staff with limited IT knowledge and even less IT administrative accesses. Alternatively, most IT and networking personnel are not tasked with assessing the vulnerabilities of their facility's industrial control system. Consequently, these SCADA and control systems are neglected over time and present significant vulnerabilities.

Vulnerabilities can be compounded because upgrades—even routine security patches—are often avoided to mitigate downtime risk. As a consequence, entire controls system infrastructures require hardware upgrades and network overhauls to protect against the effects of longtime neglect and from potential cyber attacks.

POWER's Team Designs Reliable, Available, *and* Secure Systems for Critical Infrastructure Protection (CIP)

POWER's SCADA and controls team has more than 20 years' experience across industries developing high-availability solutions that work best for our clients. We help our secure clients avoid mission downtime by providing:

- **Vulnerability Analysis and Assessment.** Our cleared team of experts can work with the entire spectrum of secure clients to provide vulnerability analysis. We identify system devices and map network topology to identify vulnerabilities in both ICS process and design.
- ***Monitoring and Maintenance Plans***. We "fingerprint" systems to identify unneeded services and systems; develop management plans; practice defense in depth design (DiD); and use virtualization to simulate patches, installs, and upgrades.
- ***ICS Design and Implementation***. We develop plans for system replacement and modernization and provide N+x redundant ICS designs.

Virtualization Reduces Upgrade Risks

POWER's team virtualizes and imitates your upgraded controls systems before they're installed. This approach provides a low-impact deployment solution for systems requiring high levels of security and availability without jeopardizing mission continuity.

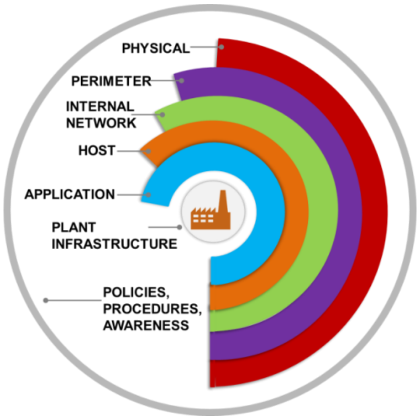
CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION

SCADA and Industrial Controls Systems Protection

POWER'S CYBERSECURITY SOLUTIONS ENHANCE YOUR NETWORK SECURITY AND CRITICAL INFRASTRUCTURE PROTECTION

- Full service cyber analysis and vulnerability assessments
- Implementation and Engineering Support for Cyber Solutions
- Use ISA95 tiered network model as a baseline
- Implement VLAN segmentation Implement site-wide Layer 2 port security, ACLs
- Identify and isolate PLC network
- Implement an authorized device policy for all ICS systems
- Evaluate, identify and implement Wireless security, radius, encryption
- Manage remote access security

Defense in Depth: Protecting Your PLC
Protecting your critical assets depends on a defense in depth (DiD) approach with "layers" of security as pictured at right. POWER's engineers use DiD design concepts to protect against attacks.



PROJECTS

U.S. Government, SCADA and Control System Vulnerability Compliance Assessment, Multiple Locations
POWER deployed an enterprise sustainability team to address operations' continuity and availability across several government facilities. POWER's team evaluated SCADA systems and associated control and communication infrastructure at six facilities. Analyses included failure-mode analysis, single-point-of-failure analysis, and recommendations for corrective actions and ICD 503 compliance.

U.S. Government, SCADA Infrastructure Implementation, Undisclosed Location
Upgraded site with no SCADA infrastructure and multiple buildings to provide real-time monitoring and operation of a 24/7 facility for all critical and non-critical infrastructure. Systems included chilled water operations, power generation and distribution, RUPS, and classified document destruction systems. POWER's cyber-security solutions defined a multi-tiered and segregated network to identify the appropriate data path depending on security and criticality of data. Minimized attack surface and vector vulnerabilities and provided simulation to test solution prior to deployment. Implemented ICD 503-compliant cyber solutions and plan for post implementation testing and patching.

ARGO, U.S. Government, Bloom Energy Fuel Cell, Undisclosed Location
ARGO/POWER supported design for a fuel-cell power plant with a grid of nine 200 kW fuel cells that produce 1.8 MW of power at 480 V. POWER designed the SCADA system to integrate the fuel cells into the standard utility power supply for the base, monitor the performance characteristics of the fuel cells, and collect data for evaluation. The SCADA system design utilized the Open Systems International, Inc. (OSI) Monarch™ platform to fully integrate all monitoring and control requirements into the client's existing SCADA system.

U.S. Government, SCADA Support, Undisclosed Location, CONUS
ARGO/POWER designed and implemented a communication infrastructure for remote, secure SCADA interface for all critical infrastructure, including power and HVAC. POWER designed a multi-tiered network utilizing routed and un-routed protocols to protect data visibility from external facilities. All data was amalgamated to one port and one access point over a secure network.

U.S. Government, SCADA Support, Undisclosed Location, OCONUS
Identical to CONUS effort above providing one terminal but with visibility to multiple facilities.

POWER ENGINEERS