Agenda

- Introduction to SCADA
- Importance of SCADA security
- Recommended steps
SCADA systems are usually highly complex...
...and SCADA systems are used to control complex industries
Yet....SCADA systems are actually quite basic in nature
Evolving Cyber Security threats require more aggressive and proactive Cyber Security programs strategies to stay ahead of threat actors

Global Cybersecurity Threat Landscape

Most organizations are only prepared to handle a fraction of security concerns

Known Threat Actors
- Insiders
- Criminals
- State Actors
- Hacktivists
- Affinity Groups

Vulnerabilities
- Hyper-Interconnectivity of Information Systems
- Rapid Technological Infrastructure Expansion
- Hard to Define Organizational Perimeters
- Unprepared Workforce and Culture
- Dissimilar Security Models Applied Across the Enterprise
- Misaligned Policies

Unprecedented Risk
- Intellectual Property Theft
- Government and military strategy compromised
- Monetary Losses
- Operational Disruptions
- Theft of classified information
- National security at risk
- Media Publicity
- Regulator Intervention
- Loss of Public Confidence

Representative Attacks
- Mahdi (2012)
  Trojan espionage attack designed to target Middle Eastern critical infrastructure firms, engineering students, financial services firms, and government embassies.
- Shamoorn (2012)
  Saudi Aramco, the worlds largest oil producer, was targeted by hackers for the government’s supposed support of “oppressive measures” in the Middle East.
- Gauss (2012)
  One of the most sophisticated pieces of malware yet designed to monitor bank account information and the money flow for various Middle Eastern banks.
- Use either Flame or “Cyber Skirmishes” (see subsequent slides)

Source: Booz Allen Hamilton
Translating these threats into an oil & gas environment, means there are four main areas of concern:

- **Operation Sabotages**
- **Data Security** (Database & Communication)
- **Communication Interference**
- **Grid Security**
Many new developments in SCADA have an impact on the risks of these systems which must be mitigated.

**Old**
- Highly specialized
- Closed door operations
- No remote monitoring
- Minimal/no external integration
- Serial Interfaces

**New**
- Becoming more common
- Remote monitoring and operations
- Increased integration with outside systems
- IP based communications as standard

---

**SCADA Infrastructure Security Model**

**Cyber Risk Scenarios**
- Intrusion Dynamics
- Process Disruption
- Process Control Manipulation

**Impact**
- Product Disruption
- Physical Coupling

**Economic Inoperability**
- Sector Inoperability
- Public Response

**Risk Management based on ISO 27001**
- Network Security Strategies
- Recovery Dynamics Management
- Regional Risk Management

---

"Old" developments are characterized by highly specialized, closed-door operations, no remote monitoring, minimal/no external integration, and serial interfaces.

"New" developments include becoming more common, remote monitoring and operations, increased integration with outside systems, and IP-based communications as standard.
Regular security practices are also applicable in SCADA environments (1/2)

1. Clearly define cyber security roles, responsibilities, and authorities for managers, system administrators, and users

2. Establish policies and conduct security training

3. Establish system backups and disaster recovery plans

4. Clearly identify cyber security requirements

5. Implement the security features provided

6. Establish effective configuration management processes

7. Identify and evaluate all connections to SCADA networks
The idea that SCADA systems are isolated, or air-gapped, is notoriously flawed.
Regular security practices are also applicable in SCADA environments (2/2)

8. Disconnect unnecessary connections to the SCADA network
9. Harden SCADA networks by removing or disabling unnecessary services
10. Do not rely on proprietary protocols to protect your system
11. Implement internal and external intrusion detection systems and establish 24-hour-a-day incident monitoring
12. Perform technical audits of SCADA devices and networks, and any other connected networks, to identify security concerns
13. Conduct physical security surveys and assess all remote sites connected to the SCADA network to evaluate their security
14. Establish a rigorous, ongoing risk management process
The ISA-99 Standard specifically addressed SCADA security and presents the Zoning / Conduit model
SCADA environments present their own unique challenges to implementing IT security measures

- SCADA systems usually not under control of IT
- Liaise with Engineering team in charge of SCADA systems
- SCADA systems are “always on”
- Include IT security updates in maintenance windows
- SCADA systems were never built with security in mind
- Identify work-around solutions to mitigate the risks
- SCADA systems can be in remote areas
- Physical security controls deserve full attention from IT security
- SCADA systems are not always well-documented and studied
- Build partnership with vendors to obtain relevant information
Thank you