Feature

SCADA Cybersecurity Framework

Samir Malaviya, CISA, CGEIT, CSSA, works with the Global Consulting Practice-GRC practice of Tata Consultancy Services and has more than 17 years of experience in telecommunications, IT, and operation and information risk management. Malaviya is currently leading an engagement for a large investment bank in New York, USA. Malaviya can be reached at *samir.malaviya@tcs.com* or *samir.malaviya@gmail.com.*

Supervisory control and data acquisition (SCADA) systems are rapidly changing from traditional proprietary protocols to Internet Protocol (IP)-based systems. Modern IP-based SCADA systems are now inheriting all the vulnerabilities associated with IP. Attempts are being made to fight new threats to SCADA systems by players in the industrial world; however, the current approach is frequently reactive or compliance-based. This article proposes a comprehensive model for establishing a framework for securing SCADA systems. The proposed framework's components are aligned to existing IT security best practices—keeping in mind the challenges and requirements unique to SCADA systems.

The current trend in SCADA is Transmission Control Protocol/Internet Protocol (TCP/IP)-based systems. This is a huge transformation from traditional proprietary protocols. The advantage of TCP/IP in terms of cost-efficiency, effectiveness and interoperability will accelerate the inevitable trend of adoption of TCP/IP for SCADA. Since vulnerabilities in TCP/IP are widely known, governments and the general public are becoming more and more concerned about various doomsday scenarios of large-scale cyberattacks. Federal governments and industry bodies are reacting to these threats by prescribing various regulations and standards. Cyberthreats are evolving while some of the compliance programs in place provide only point-in-time snapshots of security postures of organizations.

SCADA SYSTEMS

Most critical infrastructure, including major utilities infrastructure, industrial networks and transport systems, are controlled by SCADA systems. SCADA systems are smart, intelligent control systems that acquire inputs from a variety of sensors and, in many instances, respond to the system in real time through actuators under the program's control. The SCADA system can function as a monitoring/supervisory system, control system or a combination thereof.

SCADA VS. IT SECURITY REQUIREMENTS

Moving to IP-based systems provides tremendous economic advantages in a time of intense competition. Consequently, more and more systems are expected to move toward IP-based systems. For example, the advantages of migrating from a proprietary radio-based network to an IP-based network include shared network resources across multiple applications, network improvements such as added redundancy and capacity across all applications, shared network management systems, and having to maintain only one skill set for onsite support staff. However, all known vulnerabilities and threats associated with traditional TCP/IP are available for exploitation, making it a challenge for the SCADA security community. Although all risk factors associated with IT systems apply to SCADA systems, it is not possible to completely superimpose an IT security framework on SCADA systems. **Figure 1** describes the potential differences between IT security and SCADA security.

GOVERNING SCADA SECURITY

Industry organizations are developing standards for their vertical industries. These include, for example:

- **Electric:** North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)
- **Chemicals:** Chemical Industry Data Exchange/American Chemistry Council (CIDX/ACC)
- **Natural gas:** American Gas Association 12 (AGA 12)
- **Oil and liquids:** American Petroleum Institute (API)
- **Manufacturing:** International Society for Automation/International Electrotechnical Commission (ISA/IEC 62443) (formerly ISA 99)

Figure 1—SCADA Vs. IT Security		
Category	**Information Systems**	**Control Systems**
Risk impact	• Loss of data	• Loss of life, production
Risk management	• Recover by reboot • Safety a nonissue	• Fault tolerance essential • Explicit hazard analysis expected
Reliability	• Occasional failures tolerated • Beta test in field acceptable	• Outages unacceptable • Quality assurance testing expected
Performance	• High throughput demanded • High delay and jitter accepted	• Modest throughput acceptable • High delay a serious concern
Security	• Most sites being insecure • Little separation among intranets on same site • Focus on central server security	• Priority to functionality and reliability • Tight physical security • Information systems network integrated with plant network • Focus on central server as well as edge control device stability
System operation and change management	• Generic, typical operating systems • Straightforward upgrades • Changes using automated deployment tools	• Proprietary operating systems • Software changes in consultation with vendors only
Communications	• Standard communications protocols • IT networking practices	• Mix of proprietary and standard communication protocols • Networks requiring the expertise of control engineers
Component lifetime	• Lifetime on the order of three to five years	• Lifetime on the order of 15-20 years

Some governments have come up with their own regulations and standards, e.g., the US National Institute of Standards and Technology (NIST), the UK Center for Protection of National Infrastructure (CPNI) and The Netherlands Center for Protection of National Infrastructure (CPNI).

However, compliance to standards/regulations does not guarantee continuous security, but it does provide a snapshot of required controls at a point in time.

As new threats are identified almost daily, SCADA systems require a dynamic risk-based approach to keep pace with evolving threat scenarios.

IT security and risk professionals who have worked in traditional areas such as banking, finance or telecommunications are facing the same challenges of continuously evolving threats and risk. Most traditional IT security frameworks are modeled on standards/guidelines from ISACA, NIST or the International Organization for Standardization (ISO).

CONSTRUCTS OF A SCADA SECURITY FRAMEWORK

An ideal SCADA security framework should have the following characteristics:

- Comprehensive and evolving to meet a changing threat profile
- Meets the availability requirements of SCADA systems
- Meets the risk management and performance requirements typical of SCADA systems
- Scalable to meet different standards and regulations as applicable

The proposed SCADA security framework can be subdivided into the following areas:

1. **Governance, risk and compliance administrative controls**—Utilized for setting up the rules of engagement; includes policies, standards, exception management, and risk and compliance frameworks. Because these controls are not technical in nature, they are often described as administrative controls.

2. **SCADA controls**—This area is designed to cater to specific SCADA requirements. Some of the SCADA security requirements are specific to the SCADA world.
3. **Data and application security**—SCADA data, proprietary applications development and maintenance are covered in this area. One of most important areas covered here is change management.
4. **System assurance**—This area covers unique SCADA security requirements such as system resilience and secure configurations.
5. **Monitoring controls**—As SCADA protocol and applications are weak by design, monitoring becomes one of the important areas of the SCADA security framework.
6. **Third-party controls**—Most SCADA systems are supplied by third parties, including vendors and partners, necessitating a separate area for third-party security in the SCADA security framework.

These areas of the SCADA security framework further expand into 22 subsections. The six areas and underlying 22 subsections are presented in **figure 2**.

ADMINISTRATIVE CONTROLS

Controls that are not implemented using tools and technology are defined as administrative controls. The GRC framework is covered here. The following subsections are included in this area:

1. **Organizational leadership and security organization**—Organizational leadership takes complete ownership of SCADA security and sets the direction at the top to provide the necessary funding, structure and buy-in for the SCADA security program. Without involvement of organizational leadership, important programs such as the SCADA security program cannot succeed. Security organization refers to setting up the SCADA security organization with clearly defined roles and responsibilities.
2. **Policy, standards and exceptions**—The "rules of the game" are set by the policies and standards. Policies and standards provide direction to the organization and to the organization's constituents and their expectations. These rules are to be followed by all with the goal to protect the organization. The expectation is to have separate SCADA security policies and standards to complement the organization's policies and its IT security policies. Deviations from policies and standards are recorded as exceptions. In the SCADA world, availability and stability are the most important criteria to be considered. Deviations, such as security controls not being implemented on time, need to be recorded as an exception, and necessary compensatory controls need to be implemented.
3. **Risk assessments**—The risk profile of an organization is gauged using this important tool, available to management. Risk assessments also help an organization to dynamically respond to emerging threats and risk at periodic intervals.
4. **Compliance framework**—Most of the industries where SCADA systems are in use are heavily regulated. A well-designed compliance framework allows an organization to meet its compliance requirements seamlessly.

Figure 2—SCADA Security Framework

Administrative Controls	SCADA Controls	Data and Application Security	System Assurance	Monitoring Controls	External Controls
Organizational leadership and security organization	Asset management	Data security	System resilience	Incident management	Vendor security management
Policy, standards and exceptions	Identity and access management	Application security (development and maintenance)	Secure configuration	Threat monitoring	Partner security management
Risk assessments	Vulnerability management	Change management	Business continuity and disaster recovery planning	Forensics	
Education and training	SCADA network security controls	Malicious code detection/prevention			
Compliance framework	Physical security				

SCADA CONTROLS

As described in **figure 1**, IT risk and SCADA security have different priorities and requirements. Some of the unique requirements for SCADA cybersecurity are:

1. **Asset management**—Identification and classification of SCADA assets and specifically SCADA cyberassets are covered by this area.
2. **Identity and access management**—Account administration, authentication and authorization, password management, and role/attribute-based access to SCADA systems are covered by this area.
3. **Vulnerability management**—The majority of SCADA systems are supplied by vendors. SCADA systems are built on popular operating systems (OSs), such as Windows, and use TCP/IPs, which are inherently insecure. However, there are unique challenges faced by SCADA, including availability requirements, performance requirements and low bandwidth associated with SCADA systems. Vulnerability management in SCADA needs to be treated as a separate discipline, distinct from vulnerability management associated with IT in general.
4. **SCADA network security controls**—The SCADA network needs to be protected from other networks including the corporate network. The controls that help in achieving the goal of securing a SCADA network are covered by this subsection.
5. **Physical security**—SCADA systems are often connected and spread across wide areas. Remote technical unit (RTU) devices are often placed at a long distance from programming logic controller (PLC)/SCADA control centers. This is a unique challenge for physical security in the SCADA security framework.

DATA AND APPLICATION SECURITY

Well-known incidents such as Stuxnet and Flame have created widespread interest in SCADA data and application security. This area's subsections include the following controls for data, application, change management and malicious code detection/prevention controls:

1. **Data security**—SCADA data are often communicated in open text without encryption. Although confidentiality is not a top priority for SCADA, integrity and availability are of concern for SCADA security professionals. Data security covers availability, integrity and confidentiality controls associated with the protection of data.
2. **Application security**—SCADA applications present a unique challenge for security professionals. SCADA applications are often developed by third-party vendors that have provided SCADA hardware devices. These applications are often built without following standard system development life cycle (SDLC) processes. Security is not a priority for SCADA application developers, whose only priority often is making the system work. The scope for SCADA security developers is to provide secure guidelines to vendors and to teams evaluating the purchase of new SCADA devices, and to complete static/dynamic analysis and penetration testing. SCADA security professionals are expected to provide guidelines to application security professionals as the approach for SCADA vulnerability testing/pen testing needs a different approach than traditional IT testing.
3. **Change management**—The challenge in change management for SCADA is to ensure that change does not disrupt the functioning of devices, as often the impact can be the threat of loss of life. Due to this, change management is another uniquely challenging field for SCADA security professionals.
4. **Malicious code detection/prevention**—Malicious code including a virus/malware/trojan can be extremely harmful to SCADA systems and underlying infrastructure. It is important to protect applications from malicious codes.

SYSTEM ASSURANCE

The foremost priority for SCADA systems is to ensure availability of systems. With this goal in mind, the following subsections are covered in this area:

1. **System resilience**—Ensuring that SCADA systems are always available requires the system to be designed with a resilience goal in mind. System resilience includes designing resilient architecture for SCADA systems, ensuring goals are met during normal operations, incidents and changes to systems.
2. **Secure configuration**—SCADA systems and the communication protocols are inherently insecure. Ensuring underlying systems are built securely is of paramount importance. System hardening/patches are covered by this subsection.
3. **Business continuity/disaster recovery planning (BCP/DRP)**—Systematic and orderly recovery from disasters and business continuity processes is covered by this subsection.

MONITORING CONTROLS

As described earlier, SCADA applications and protocols are inherently insecure. Other known issues with SCADA systems are the following challenges associated with applying patches—a result of which is monitoring compensatory controls:

1. **Incident management**—Established and documented incident management processes are the keys to ensuring orderly handling of incidents. Most regulations also stress efficient processes for incident management and incident reporting.
2. **Threat monitoring**—SCADA applications and protocols are inherently insecure; lack of awareness and dependency on vendors for applying patches, wide area networks and the need for segregation for SCADA networks make threat monitoring one of the most important sections in SCADA security controls. Often, monitoring is used not only for detection and prevention, but in many cases, it is also applied as a compensatory control.
3. **Forensics**—Often SCADA system breaches have serious impact on an entire geographic area. Forensics helps in unearthing and establishing incidents.

THIRD-PARTY CONTROLS

Third-party vendors often supply SCADA systems. For SCADA security professionals, controls related to third parties, including vendors and partners, are critical:

1. **Vendor security management**—Vendors play important roles in SCADA. SCADA devices and applications are often supplied by vendors. Many times vendors manage the infrastructure, including IT maintenance, SCADA systems, IT and SCADA networks, and/or managed security service providers. Vendor security is an important area to establish necessary controls over vendors and SCADA security for an enterprise. One control for vendor management is contract management, ensuring security is part of standard contracts and specifications for vendors and reviewing and evaluating vendors for security.
2. **Partner security management**—In today's interconnected world, organizations that rely on SCADA networks are often interdependent. Partner security management, in which rules of engagement between partners are established, caters to this area.

SCADA SECURITY FRAMEWORK USE CASES

The SCADA security framework can be used by organizations to set up their SCADA organization, SCADA security policies/standards and risk control framework, which can be further used for risk assessments and benchmarking the organization's SCADA security.

Organizations can build upon the SCADA security framework to frame short-, medium- and long-term security plans, selecting appropriate tools and technology to secure SCADA networks and devices.

CONCLUSION

SCADA/industrial control systems come with their own unique challenges and require a thoughtful approach for the security community to provide a comprehensive solution to meet security needs in this area. A cybersecurity framework is an important area; however, its implementation is a first step in the journey to establish a reliable and comprehensive cybersecurity solution for SCADA systems. The next steps in this framework include:

1. Creation of controls mapping to each subsection with clearly measurable goals
2. A maturity model for benchmarking organizations' SCADA security posture
3. A technical implementation blueprint

An ideal implementation of the SCADA security framework would include a GRC tool, an identity access management (IAM) tool set, network segmentation and security monitoring—a sound recipe for continuous control monitoring.

REFERENCES

North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP), *www.nerc.com/page.php?cid=2%7C20*

PCSF Congress of Chairs, *Cyber Security Combined Glossary Project*, "AGA 12 Series," *http://ics-cert.us-cert.gov/practices/pcsf/groups/d/1176393761-combined_glossary_2007_03_28.pdf*

Phinney, Tom; "ISA/IEC 62443: Industrial Network and System Security," International Society for Automation/International Electrotechnical Commission, *www.isa.org/autowest/pdf/Industrial-Networking-and-Security/Phinneydone.pdf*

UK Center for Protection of National Infrastructure (CPNI), *www.cpni.gov.uk/advice/cyber/Critical-controls/*

National Institute of Standards and Technology (NIST), *Guide to Industrial Control Systems (ICS) Security*, NIST SP 800-82, *http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf*

Panetta, Leon; US Defense Secretary speech reference on Industrial Control Security, 2012