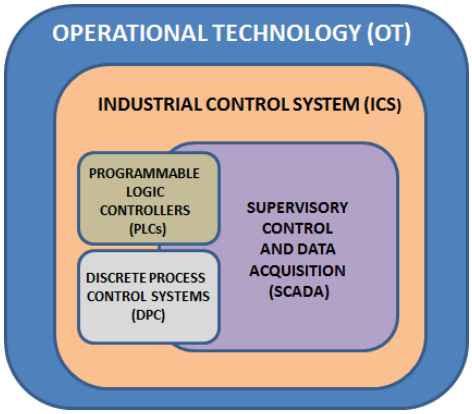
Supervisory Control and Data Acquisition



This paper will focus on securing Supervisory Control and Data Acquisition (SCADA) networks and information technology components. To understand SCADA we first need to understand the ecosystem in which SCADA exists. Computing systems that manage industrial operations are broadly referred to as "Operational Technology" (OT). Within this sector high-availability and mission-critical elements are commonly focused on. To address this need "Industrial Control Systems" (ICSs) are leveraged. Two technologies are most often used for ICS to continuously control processes includes "Programmable Logic Controllers" (PLCs) and "Discrete Process Control Systems" (DPCs). The overall management of Industrial Control Systems is usually performed with SCADA technology. SCADA works with PLCs and DPCs. SCADA collects operational data to control and optimize the system. While SCADA is not a single specific technology, common features of SCADA include the ability for technicians to observe system status, manage processes being controlled, out-of-band alerts and alarms, and a graphic interface. A SCADA application consists of two key elements: the machine, plant or process to be monitored and the network of intelligent devices interfacing with them. Sensors and controllers can be placed at any critical point in a managed process, more sensors and controllers allow a more detailed view in real time, correct errors, increase productivity and efficiency.

SCADA systems are used in

Electric power generation, transmission and distribution.
Electric utilities use SCADA systems to detect current flow and line voltage, to monitor the operation of circuit breakers, and to take sections of the power grid on or offline.

Water distribution and wastewater collection systems.
Provincial and municipal water use SCADA to monitor and regulate water flow, reservoir levels, pipe pressure and other factors.

Buildings, facilities and environments.
Facility managers use SCADA to control HVAC, refrigeration units, lighting and entry systems.

Manufacturing.
SCADA systems manage parts lists for just-in-time manufacturing, regulate industrial automation and robots, and monitor process and quality control.

Mass transit.
Transit authorities use SCADA to regulate electricity to light rapid transit systems, and buses; to automate traffic signals for rail systems; to track and locate trains; and to control railroad crossing gates.

Traffic controls.
SCADA regulates traffic lights, controls traffic flow and detects out-of-order signals.

Security Considerations for SCADA applications

Process control and SCADA systems have traditionally been designed for the purpose of control, efficiency and safety. These systems were usually isolated without connection to public networks, today there is an increasing need for interconnected systems and controls. Once isolated systems connect to larger open networks that expose them to threats they never expected, such as worms, viruses, hackers, other nation states, and terrorists. SCADA applications differ significantly from the enterprise computing environment, but increasingly rely on standard computing technologies. The personnel who work with these systems usually do not have the knowledge to protect the computer systems in the network. SCADA applications can be better protected by using techniques, controls, and tools developed for information security technology. For example, changing default passwords, using password complexity, encrypting data at rest and in-transit, and system patching are all important factors to keep SCADA systems safe.

Applying a risk management approach

The risk management approach is used to identify and avoid the potential cost, schedule, and performance/technical risks to a system, take a proactive and structured approach to manage negative outcomes, respond to them if they occur, and identify potential opportunities that may be hidden in the situation.

Asset Management
A thorough understanding of all assets and their interdependencies ensures that nothing is overlooked. The scope should be clearly defined and an appropriate level of protection for the security of these systems should be sought. This is a very important perpetual task.

Assessing the business risk
There are a number of methods for estimating business risk. One method is to express the risk on the basis of the likelihood of a risk occurring and the effects that would result. The likelihood of a risk occurring corresponds to the threat, the attractiveness of the target and the vulnerability of an asset.

Attractiveness refers to the attractiveness of a target for a potential attacker. An attacker might find an electric substation to be a more attractive target than a potato chip factory. The attractiveness term contributes to the likelihood of a risk occurring and can often be incorporated within the threat term. Combining these terms gives an expression for business risk in terms of threat, impact, attractiveness, and vulnerabilities.

Business risk = F (Threat x Impact x Attractiveness x Vulnerability)

Understanding threats
Depending on the industry (e.g. power plants, oil refineries), the understanding of the particular risks to the business cannot be exaggerated. In addition to widespread computer threats, there are specific threats to different types of industries or applications. For example, power plants have a different threat profile than an oil refinery.

Once a threat profile has been created, threat scenarios should be developed for all potential threats that could disrupt business continuity. An organization's threat profile includes various use cases for threat scenarios tailored to the organization. When creating threat scenarios, the business selects critical assets, threat actors and possible attack vectors. This process is repeated for each scenario.

Understanding Impacts
Threat scenarios help with estimating what impacts certain threats may have on the business and what actions should to be taken for business continuity if vulnerabilities are exploited.

Threat scenarios will prepare the organization to deal with:

- Events that results in harm to individuals, the environment or damage to the site.
- Events that results in the site being non-compliant with regulatory requirements.
- Events that results in the emergency shutdown system being automatically invoked with no human intervention.
- Events that results in the site electing to shut down its operations.
- Events that would result in the site continuing to operate less efficiently or cost-effectively or in production being reduced.

Understanding vulnerabilities
Vulnerabilities of software, firmware, and hardware are discovered on a daily basis. Vulnerability management is the means to identify, eliminate or control the inherent risk of vulnerabilities. Scaling the vulnerability management program is important to meet business requirements, complexity, the IT environment and physical security.

Benefits of understanding the business risk
By applying a risk management approach, the organization maintains an understanding of risks, asset management, priority of systems, threats based on impact assessments, and prioritized vulnerabilities.

Securing SCADA Networks

There are several important steps that should be taken in order to secure SCADA networks:

- Patching operating systems, applications and components
- Control application communications between SCADA networks and other networks
- Control application communications within SCADA networks
- Control who and what is permitted to interact with SCADA networks and systems
- Monitor all networks closely and react quickly to viruses and attacks

Due to their potential criticality, patching of SCADA systems is not always possible in the timescales needed to prevent an exploit. Using an in-depth defense strategy by applying application layer security both at the RTU host level and at the network level.

Defense-in-depth consists of a security system with integrated multiple detection mechanisms including:

- Application aware firewalls
- Hardened Border Perimeter (IPS, Firewalls, VPNs, Stateful Packet Inspection)
- Automated updating of antivirus and Intrusion Prevention Systems
- Network Anomaly and DoS prevention
- Web filtering
- Anti-virus detection
- Application control
- Database protection
- Web application protection

Recommendation

Adoption of basic security hygiene practices with SCADA systems have generally not kept pace with the rest of the IT industry. SCADA systems are often used for critical infrastructure, and as a result this combination raises the risk level significantly. Public sector organizations have a responsibility to implement reasonable security. All public sector organizations should harden existing SCADA systems and ensure practices are in place for the secure deployment of any new SCADA systems. Change management practices should also address SCADA security. Careful configuration of security controls on SCADA systems is crucial to mitigate risk.

As with any interconnected system, SCADA systems must be protected from threats both internal and external. Layered defenses must be utilized in order to achieve the best defense. It also cannot be overstated that the personnel working with these systems have education in IT Security and security technologies / methodologies to enable them to identify and deal with issues in a timely manner.

Public sector organizations should begin addressing SCADA security with a strong sense of urgency.

Resources:

ISA99, Industrial Automation and Control Systems Security

http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821

National Cybersecurity and Communications Integration Center (NCCIC) Industrial Control Systems

http://www.us-cert.gov/control_systems/

A Collection of Resources for Getting Started in ICS/SCADA Cybersecurity

http://www.robertmlee.org/a-collection-of-resources-for-getting-started-in-icsscada-cybersecurity/

An excellent video from Editor Walt Boyes on Supervisory Control and Data Acquisition systems, history and Security.

https://www.youtube.com/watch?v=bfxr5DikdP0

OT, ICS, SCADA – What's the difference?

https://www.kuppingercole.com/blog/williamson/ot-ics-scada-whats-the-difference