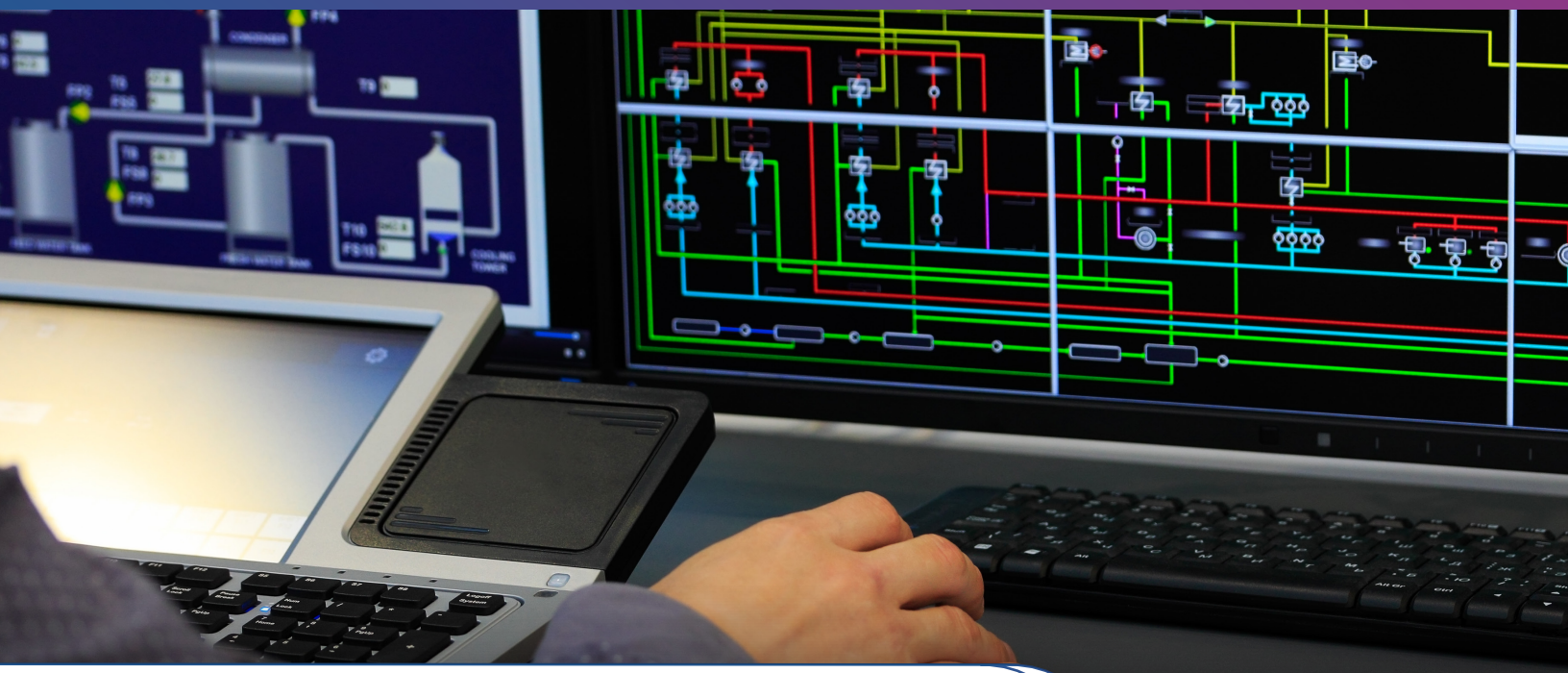


SOLUTION BRIEF

Validating SCADA Network Security

SCADA-Industrial Control Systems (ICS) Networks

Supervisory control and data acquisition (SCADA) is an industrial control system architecture for high-level process supervisory management to interface to a process plant or machinery. It provides a high level of flexibility for remote access, management, and automation of various control modules.

SCADA systems can range from just tens to thousands of interconnected devices, depending on the application. SCADA controls processes that include a myriad of industrial, infrastructure, and facility-based processes—from power generation, fabrication, refining, water treatment and distribution to heating, ventilation, and access for buildings, airports, ships, and space stations.

SCADA/ICS together form the automation backbone of such industries that leverage software intelligence to make accurate and timely decisions based on pre-fed conditions, and also provide the flexibility of remote management of such machineries.

SCADA/ICS networks are the automation backbone for remote management of industrial processes, leveraging software intelligence to make accurate and timely decisions.

KEYSIGHT TECHNOLOGIES

Why Do We Need to Test?

SCADA networks are exceptionally vulnerable

Many traditional SCADA systems now contain extensions to operate over TCP/IP to connect to and access distributed, remote systems. Using TCP/IP means these systems have the reliability and sophistication of a data transfer protocol that keeps the Internet running. However, this has also exposed SCADA networks to the vulnerabilities targeted at TCP/IP over the course of many years. On top of this, we need to consider the fact that many SCADA applications were not designed with IP network-level security in mind. Coupled with the fact that SCADA is implemented in many critical infrastructures, state and non-state actors may have special interest in such networks.

With SCADA operating over IP networks, the line between IT and OT has blurred...however, many OT teams are not prepared to handle threats in ICS networks.

Prepared criminals and unprepared defenders

Operation Technology (OT) workforces aren't as well versed in dealing with such adversaries as Information Technology (IT) teams. IT teams have been dealing with the world of IP for a long time and are more capable of finding exploits, eliminating threats, and engaging in strong forensics. With SCADA operating over IP networks, the line between IT and OT has blurred considerably. However, many OT teams are not prepared to handle threats in ICS networks.

Key Issues	
Highest Risk	SCADA systems are often employed for controls of key infrastructure elements, facilities, and Industrial processes. Any cyber-security events to such entities can lead to national or international catastrophes.
Expensive	SCADA systems are extremely expensive, so building a test environment closely replicating production environments can have prohibitive costs.
Unique and Proprietary	SCADA networks and applications are almost always customized for the purpose and secretive, creating challenges in creating realistic test scenarios.
Lack of Training	The teams managing SCADA networks are not well-versed in cyber-threat landscapes. They need proper training in realistic lab environment.
Increased Risk	SCADA networks are exceptionally vulnerable and the attacks on SCADA has increased exponentially year over year. In addition, these SCADA systems rarely go through regular patch updates, making these networks even more vulnerable.

When the possibilities can be catastrophic, can't leave anything to chance

A common assumption is that since SCADA networks are generally isolated from the traditional IP networks, they are secured by virtue the being obscure. However, obscurity doesn't necessarily mean security—especially if we are talking about packet data.

Nation states or motivated individuals have found different ways to attack such networks. From the much talked about Stuxnet (causing damage to Iran's nuclear program), to the first SCADA-caused power outage in Ukraine, there are several documented instances of high-profile and lesser-known SCADA attacks.

These attacks expose the need to increase the resiliency of SCADA networks with regular testing, validation, and remediation. SCADA OT/IT teams need test labs that allow them to emulate real-world application and security traffic to test what-if scenarios, updates/upgrades, and new systems before going live.

Nation states or motivated individuals have found different ways to attack such networks— from the much talked about Stuxnet, to the first SCADA-caused power outage in Ukraine.

Overcoming Challenges and Validating SCADA Networks

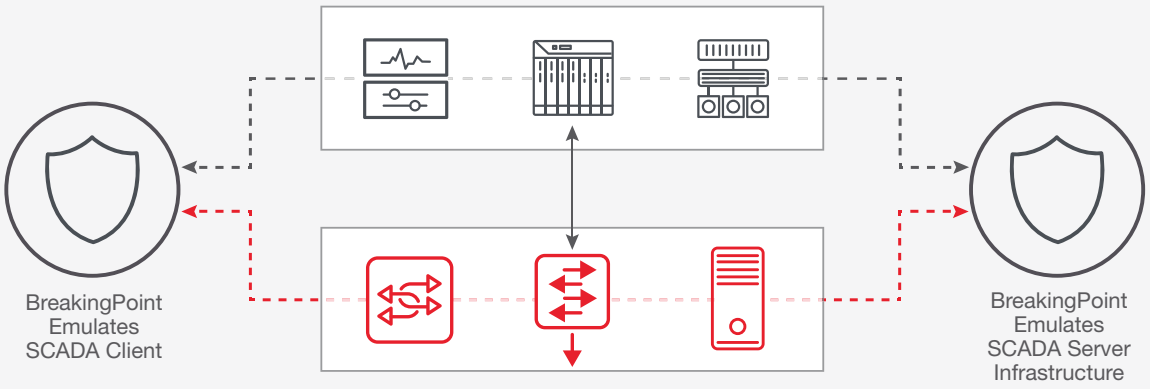
Building a cost-effective SCADA/ICS lab

Problem: The biggest issue with the implementation of a realistic SCADA lab is the prohibitive cost of some of the real equipment and the infrastructure. The SCADA security equipment, like firewalls, intrusion prevention systems, and security analytics, is much cheaper as compared.

Solution: BreakingPoint can create a simulation of complex, distributed SCADA networks including tens to thousands of endpoints; applications like Modbus, IEC, and Bacnet; and also exploits and malware. Such simulations help organizations measure the resiliency of systems, make purchase decisions, train OT teams on SCADA security incidences, and make new technology deployments decisions.

BreakingPoint solves the biggest issue with creating a realistic SCADA lab — the prohibitive cost of replicating the real equipment and infrastructure.

SCADA Network Test



BreakingPoint emulates SCADA end points and infrastructure, along with realistic application and attack traffic so you can test the network.

Creating traffic relevant to a particular environment

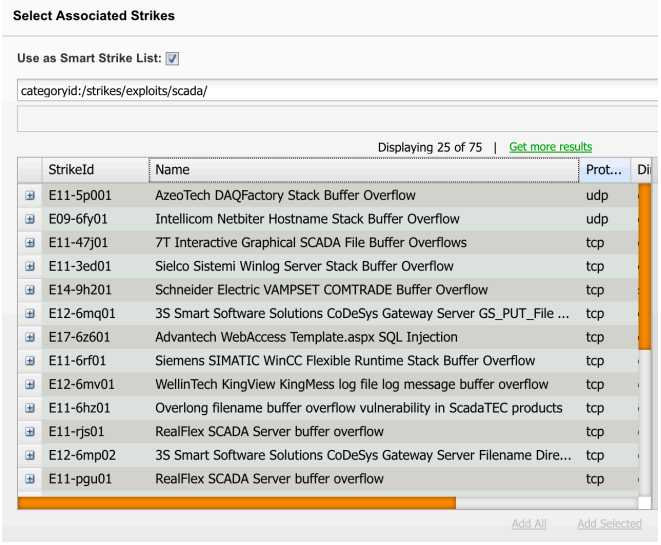
Problem: Every SCADA device or network is customized to suit various deployments. Applications are modified, networks have unique characteristics, and traffic profiles are unique. There is no possibility of creating a one-size-fits-all SCADA test methodology that can service all customers.

Solution: Create realistic application and attack traffic using BreakingPoint—easily parametrize and customize application commands to create your own application variants, recreate propriety traffic with packet replay, and simulate endpoints with the network environment editor. These realistic SCADA test scenarios result in accurate analysis and better understanding of the security posture of ICS networks.

SCADA network design changes/upgrades and patch management

Problem: It's difficult to make changes in a system that's controlling temperature in nuclear plants or maintaining water pressure in a water-treatment plant. A small mistake can result into devastating catastrophes.

Solution: Having a BreakingPoint based test lab means you have an incubation center where you can make changes and test their effects on the infrastructure prior to deployment. This enables you to make changes/update patches and introduce new technologies within your SCADA network with confidence.



Validation in the lab, with real-world application traffic and security attacks, can ensure SCADA networks are resilient and secure.

Use BreakingPoint's pre-packaged SCADA applications and attacks to create test scenarios.

Key BreakingPoint Test Cases

- Mitigate existing and future risks through testing of different normal and abnormal scenarios
- Build highly realistic labs using simulation techniques at a substantially lower cost
- Run customized traffic and attacks replicating the uniqueness of your network without compromising security
- Run regression tests with updated application and attack scenarios to continuously validate the dynamic world of SCADA security and fast-track patch management and updates
- Build SCADA cyber defense training curriculum to train security professionals with scenarios like application traffic management, deploying security policies, and handling breach incidences

Don’t Leave SCADA Network Security to Chance

Organizations are taking notice of the threats to SCADA networks and the possible impacts of breaches. It is also clear that, despite being much farther from the standard network security demarcation zones, SCADA networks continue to be exceptionally vulnerable to cyber-attacks.

Validation in the lab, with real-world application traffic and security attacks, can ensure SCADA networks are resilient and secure. Increasing the attack readiness of both your ICS networks and people will go a long way in increasing the resiliency of the SCADA/ICS systems of today and in the future.

For more information, visit www.ixiacom.com/products/breakingpoint

KEYSIGHT TECHNOLOGIES