# Table Of Contents

Executive Summary 3
Key Takeaways 3
ICS Architectural Components 4
An Attacker’s Perspective on Targeting ICS 5
Breakdown of an ICS Breach 6
The Adversarial-Driven Defence Approach 7
About Smokescreen 8
Executive Summary

With the risk of causing business destabilising kinetic damage, SCADA / ICS cybersecurity has become a hot-button issue.

However, most defences that are implemented are not based on actual attack patterns of these systems in the real world.

Smokescreen regularly conducts red-team attack simulations of these environments for customers, and our team has a 100% penetration success rate.

We fundamentally understand how to breach process control systems.

This white-paper explains how attackers target control systems in the real world, and describes an attack pattern driven approach to defending these systems that actually works.

“Most defences that are implemented are not based on actual attack patterns of SCADA systems in the real world.”

Key Takeaways

- ICS control systems are often under the control of process control engineering departments, not traditional corporate IT.

- Shadow IT results in numerous pivot points to the ICS network that IT security is often unaware of.

- Attackers prefer not to attack the ICS environment directly, but instead target the process control engineering teams on the corporate LAN.

- Deception defences around ICS that focus on low-level protocol emulation such as Modbus or DNP3 are likely to go untouched.

- Attackers will use the process control team’s HMI interfaces to interact with the ICS environment as this is the easiest and most stealthy route to the target.

- When building ICS defences, a custom adversarial driven approach is essential. There is no ‘one size fits all’ solution.
ICS Architectural Components

In order to understand attacker target selection, it’s important to understand the components that make up an ICS environment, and the roles that each of them play. What follows is a high-level overview of common ICS components.

1. Human-machine Interface (HMI)
   As the name suggests, the HMI provides the operating personnel with the ability to visually monitor and control the entire process control system. This is where bits and bytes hit meatspace. It is also a prime target for attackers for the same reason. The HMI may also include a historian service to gather time-series data for trending and alarm generation.

2. PLCs / RTUs
   Interfaces the SCADA to the physical objects being monitored / controlled. They can collect telemetry data or modify settings. RTUs are typically used for wider geographical telemetry due to their wireless communication capability; PLC functionality includes process / relay and motion control. They have multiple inputs and outputs. Often, defenders focus heavily on PLC security, despite the fact that directly targeting them is less likely.

3. Supervisory computers
   The core of the SCADA system that gather data on the process and send commands to the field devices. The HMI interfaces with the supervisory system, and in smaller deployments, may be hosted on a single workstation. Distributed architectures are more common in larger environments.

4. Communications protocols
   ICS environments rely on a number of specific wired / wireless protocols, including SONET, Profibus, Modbus, BACnet etc. The focus of this white-paper will be on attacks against IP driven protocols such as Modbus over TCP / UDP. ICS also uses a number of well-known network protocols such as SNMP, FTP, HTTP and IPMI.
An Attacker’s Perspective on Targeting ICS

Due to the fact that ICS systems run exotic, vulnerable and ill-designed protocols for security. A lot of emphasis goes towards defending these systems. This is also because the security community has focused research around the protocols in this area.

However, from an attacker’s perspective, direct protocol attacks are not the most likely chosen attack vector. Post the Stuxnet incident, SCADA protocol parsing has been introduced into most intrusion detection systems, including open-source platforms such as Bro-IDS. It is also extremely easy for companies to detect attempted lateral movement activity and scans for these protocols, making this a non-stealthy attack vector.

The HMI controllers, however, are the prime target for the attacker.

As they are ultimately where the process control engineers monitor and control the overall system, they are the perfect place to attack the network.

The following types of attacks can be conducted by targeting the HMI:

- Alarm suppression attacks which prevent email or visual alarms being raised on the HMI.
- Data manipulation attacks to corrupt historian trending or misinform the process control engineers about the current state of the system.
- Process manipulation attacks to actually change parameters on the controllers, which can lead to kinetic damage, process destruction or intermittent failures.

Additionally, the HMI is most likely to be accessible through either an engineer’s workstation (which may be multi-homed) or through a jump-point on the corporate LAN. As attackers usually have easy exploitation vectors to the corporate LAN (for example, through spear-phishing), this becomes their logical starting point to attack the network.

In the following section we will deconstruct a highly-effective, stealthy and reliable attack pattern for compromising an ICS environment without targeting the protocol layer at all. Smokescreen’s adversarial team has been successful with this attack pattern in numerous assessment scenarios.
Breakdown of an ICS Breach

Armed with the knowledge above, the skilled ICS attacker uses an attack pattern that Smokescreen calls the ‘Triple Cycle Pattern’ which modifies an existing privilege escalation and lateral movement pattern used commonly to attack financial institutions and retail environments. It is centred around the exploitation of the corporate LAN, especially the Windows Active Directory environment.

By obtaining an initial intrusion as a low-privilege domain user (through spear-phishing), the attackers escalate privileges to local administrator. Multiple options exist to do this, including:

- Service path vulnerabilities
- Missing patches
- Hot potato
- DLL hijacking
- LLMNR / NBNS / mDNS spoofing
- GPP password use

They then use ‘user hunting’ to identify where domain administrators are logged in. User hunting enumerates logged in users across systems, to identify high value targets. Tools such as BloodHound are designed for efficient, rapid user hunting.

After obtaining domain administrator rights, they hunt process control engineer workstations, or identify pivot points (such as network monitoring systems) that allow access to the HMI. The benefits of attacking the HMI from the workstation of the legitimate engineer are that the attack is extremely stealthy, bypasses access control and monitoring, and gives the attacker a short-path vector to the ICS network. This pattern even works for air-gapped networks through ‘Sneakernet’ pivot points.

Notice that the triple-cycle pattern does not require any targeting of ICS protocols at all!
The Adversarial-Driven Defence Approach

Smokescreen has assessed, penetrated and then secured ICS environments for customers in multiple process control scenarios — ranging from single-instance non-connected plant environments, up to global Fortune 500 SCADA environments spanning continents.

We use deception technology to offer a low-touch, low-false positive approach to detecting and thwarting these threats before they can complete the traditional kill chain, or the triple cycle pattern.

Many deception technologies focus on protocol level decoys, assuming wrongly, that these will provide a measure of detection. The fact is that the attacker uses a completely different compromise path as illustrated above.

Instead, at Smokescreen we developed ICS specific attack trees and ran probability simulations, by assigning weights to different attack paths. The conclusion was simple — in practically every simulation, the triple cycle pattern is the most favoured attack vector, accounting for over 97% of chosen paths.

The next point of consideration is realism — Smokescreen’s IllusionBLACK deception platform has been designed for building customised deception modules.

This means that rather than doing generic decoy implementations, we can develop completely custom decoys that are far more enticing and engaging to the attacker.

We believe that protecting ICS with deception with a ‘one size fits all’ approach that does not consider adversarial simulation will result in a false sense of security. These approaches are either misinformed, due to a lack of exposure to ICS assessment, or are checkbox features that provide little value in the real world.

Smokescreen’s Approach to ICS Defence

Our approach to defending ICS environments can be summed up as follows:

- Focus on prevention of the triple cycle pattern with deception.
- Study the individual ICS environment to understand pivot points and implementation specifics.
- Conduct an adversarial simulation of compromise of the ICS environment.
- Develop deception scenarios around compromise of the HMI and process engineer workstations.
- Develop custom decoys for realism, and advise on placement based on adversarial simulation.
- Avoid ‘one size fits all’ through basic protocol emulation.

Looking to assess or defend your ICS environment?

Click here to talk to us!

www.smokescreen.io
About Smokescreen

At Smokescreen, we use our deep insight into how apex hackers operate to build deception based defences.

Our IllusionBLACK is the industry’s most advanced decoy technology — bringing military deception principles to the digital battlefield.

Smokescreen’s solutions protect some of the most highly targeted organisations globally, including leading financial institutions, and Fortune 500 companies.

Email: info@smokescreen.io
Phone: +91 22 610 63851
Web: www.smokescreen.io

Address
Smokescreen Technologies
Kaledonia D wing, 1st Floor
Sahar Road, Andheri East
Mumbai 400 069, India.