

# SCADA Security Testing - without breaking it!

## Why us?

- The #1, largest provider of penetration and security testing in Europe
- Over 50 testers, able to react quickly to your requirements
- Largest team of CHECK and CREST qualified testers in the UK
- 100% ethical - a stable PLC listed on the London Stock Exchange with robust vetting of all staff

Migration of legacy serial SCADA networks to the all pervasive IP, creates a whole new set of security challenges.

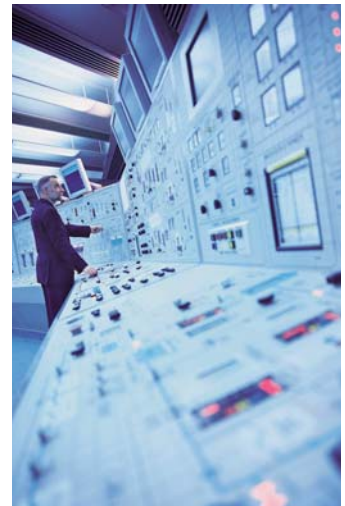
Conventional penetration tests simply break SCADA networks, so you need one of our SCADA dedicated testing experts to test it safely.

We are a recognised expert in this field, having tested SCADA environments for over 20 of the UK utilities companies, we also speak widely on the subject at utility industry forums.

### The risks

Although most SCADA systems were originally built before and are often separate from other corporate networks, they are often bridged to them using IP technology to enable easy visibility of management information and remote access. They can therefore be accessed through corporate networks or from remote access points leaving them vulnerable to unauthorised access and control.

The use of internal firewalls and intrusion detection systems (IDS) and strong password policies to protect the new access points created by network connection is essential, yet these controls are frequently applied inconsistently and/or ineffectively leaving SCADA systems exposed to attack from internal and external sources.



## Our Expertise

### Penetration Testing:

Network Infrastructures  
Web applications  
Compiled applications  
Wireless networks  
Laptops and mobile devices  
Remote access  
Databases and mainframes  
Forensics

### Managed Security Monitoring Service:

Daily assurance that your networks and applications stay secure through the provision of more scanning and tailored alerting services

### PCI DSS Services:

Gap Analysis  
PCI Audit  
Quarterly ASV scanning  
PCI workshops

### Social Engineering:

We test organisations to see where 'people' and physical weaknesses lie

*"We have information, from multiple regions outside the United States, of cyber intrusions into utilities, followed by extortion demands,"*

Senior CIA Analyst Tom Donahue said, according to a statement posted by the SANS Institute.

*"We have information that cyber attacks have been used to disrupt power equipment in several regions outside of the United States. In at least one case, the disruption caused a power outage affecting multiple cities. We do not know who executed these attacks or why, but all involved intrusions through the Internet."*

### The threats

SCADA systems utilise arcane technology which only a small and diminishing number of specialists are expert in. Many believe this makes these systems inherently secure as they are difficult for hackers to access and control.

However, organisations which use SCADA systems are likely targets of coordinated attacks by 'cyber-terrorists' who are highly motivated, well-funded and could have insider knowledge.

Furthering this risk is the increasing availability of published information describing the operations of SCADA systems to support competition in product choices and enable improved maintenance and connectivity.

Finally, efforts to make efficient use of SCADA system information company-wide had led to the development of 'open' standard SCADA systems where security is only as strong as that of the corporate network. While RTUs on a network may be difficult to access outside dedicated serial lines, it is less difficult to penetrate the control panel for the SCADA manager through the corporate network and quickly 'learn' commands by watching actions that are carried out on the screen.

**Book a 1 day SCADA security workshop with one of our SCADA security testing consultants, call us now on 0161 209 5111**

0161 209 5111  
securetest@nccgroup.com

## How we can help

As a leading provider of penetration and security testing and training services, we know how these systems work and have extensive experience in testing these systems.

We will test your SCADA/Control Systems interfaces and control processes using our unique SCADA experience and skill set to identify the risks posed.

We will conduct a three-stage attack, customised to suit your organisation, following a detailed scoping discussion:

### Stage One

A comprehensive documented security review of your SCADA/Control System infrastructure, examining in particular where it touches your corporate network and any IP networks. The output is a detailed report including clear recommendations, with good practice guides.

### Stage Two

A physical test of your SCADA, Control System or Development system covering each individual component (e.g. RTU, Serial Devices, Control System) resulting in specific instructions where changes to the live system are required.

### Stage Three

A physical test of the live SCADA environment - a highly complex test which is only undertaken under very specific circumstances to test factors which cannot be replicated sufficiently in the test environment.

We also recommend social engineering, focusing on the 'human element' of the threat of hackers gaining access to any part of your physical network (e.g. example sub-stations) and the steps you should take to mitigate this risk.

## About NCC Group Secure Test

Secure Test, the penetration and security testing division of NCC Group, is a leading independent provider of expert security testing and training services, with over 500 clients across the private, public and not for profit sectors.

Our mission is to provide the highest quality security testing and training services, whilst advancing the understanding of security vulnerabilities throughout the IT industry and amongst our clients.

We are 100% ethical - all security testing consultants undergo a rigorous security clearance, sponsored by CESG, the Government information security body. Many of our consultants are accredited to the highest levels, allowing them to work on high-level Government security projects of critical national importance.

The reason for our success is simple - we meet and exceed expectations - as a result we have very happy clients from all market sectors, including finance, local & central government, gaming/gambling and service sectors.

NCC Group is a leading global provider of independent IT assurance, security and consultancy services. As a trusted advisor, we help over 15,000 public, private and not for profit sector organisations, including 94 of the FTSE 100, to make the most efficient use of information and technology and to manage the associated risks.



Call us now: 0161 209 5111

- Speak with a SCADA security expert
- Book a SCADA security workshop
- Read a sample SCADA report
- Read a SCADA research paper
- Request an invite to a SCADA security event

## Our accreditations:



# CLAS

CESG Listed Adviser Scheme



# CHECK

IT Health Check Service