DOI: http://dx.doi.org/10.14236/ewic/ics-csr2014.4

SCADA Laboratory and Test-bed as a Service for Critical Infrastructure Protection

Antonio Sánchez Aragó
Cyber security expert
José Aguado, 41, León, Spain
antonio.sanchez@inteco.es

Enrique Redondo Martínez
Project co-ordinator
José Aguado, 41, León, Spain
enrique.redondo@inteco.es

Sandra Salán Clares
Cyber security expert
José Aguado, 41, León, Spain
sandra.salan@inteco.es

This paper presents a framework able to assess remotely the security level of Industrial Control Systems (ICS) housed in critical infrastructures. This proposal is an extension of the development of a customized testing methodology to be followed in order to receive the final results of each evaluation almost automatically. In addition, the technical and procedural steps required are also identified and implemented.

Keywords: SCADA and ICS security. SCADA and ICS Vulnerability assessment. Testing methodology.

1. INTRODUCTION

As is well known, there is growing interest in security testing for industrial control systems. In the past, such devices and architectures were designed and implemented to work only in isolated networks. However, these isolated systems are being connected to open networks, such as the Internet. This brings huge benefits, but it also increases the number of serious and high level threats, including cyber-terrorism

> ICS is a general term that comprises several different types of control systems, including Supervisory Control and Data Acquisition systems (SCADA), Distributed Control Systems (DCS) and other field devices such as Programmable Logic Controllers (PLC), Remote Terminal Units (RTU) or Intelligent Electronic Devices (IED). In this document, when SCADA is mentioned it will be referred to as ICS.

An ENISA report called *Protecting Industrial Control Systems. Recommendations for Europe and Member States* (European Union Agency for Network and Information Security, 2011) describes the current situation of security in ICS and proposes seven recommendations to improve it. In particular, in its recommendation number 5, it highlights the lack of specific initiatives on ICS security and the need for independent evaluations and tests of ICS security products. In this regard, ENISA encourages the establishment of test-beds. They make use of realistic environments with the appropriate resources for conducting tests permitting independent verification and validation.

This recommendation is a clear illustration of how European organizations are concerned about security in ICS environments.

SCADA LAB (SCADA Laboratory and Test-bed as a Service for Critical Infrastructure Protection) is a project financed by the European Commission which main purpose is to create a test environment which will be able to assess remotely the security level of an ICS, or any part of it. To accomplish this purpose, the SCADA LAB framework is split into two main areas: the laboratory and the test-bed.

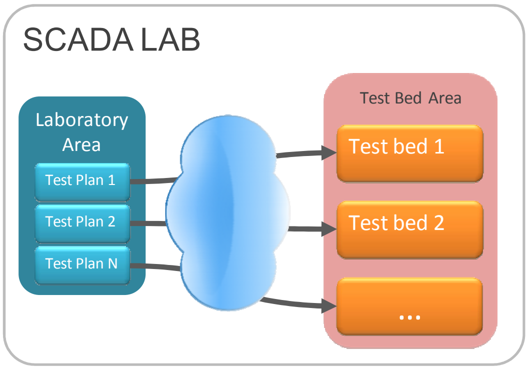


Figure 1: *Main Areas in SCADA LAB.*

The Laboratory Area includes the hardware and software needed to launch a security assessment against a test-bed.

The Test-Bed Area is the target of the test. This area includes: Physical and systems real-time systems and, auxiliary components.

The Test-Bed Area is housed in the headquarters of Telvent Energy, in Seville. The Laboratory is housed in the Data Centre of INTECO, León.

2. TESTING METHODOLOGY

The first activity undertaken was the development of a testing methodology (SCADA LAB Consortium, 2013). The main aim of this methodology is to provide a set of guidelines to facilitate security assessments.

2.1. Key Points

Conceptually, this testing methodology is based on the following key points:

2.1.1. Basic Architecture of an Industrial Control System

The first point taken into account was the minimum set of components for an ICS environment. The basic architecture of an ICS consists of three main levels:

(i) Field and control level: this contains RTUs, PLCs, IEDs, actuators, sensors, associated communications, and related elements.

(ii) Communication interface: this connects the Field Site to the Control Centre.

(iii) Supervisory level: this is where processes are measured or monitored. This level can contain the Human Machine Interface (HMI), SCADA Servers, the Data Historian, and similar items.

2.1.2. Requirements

Fifty-eight requirements were identified and each requirement had a priority assigned to it: high, medium or low. The idea was for the pilot version to meet as many requirements as possible.

Those requirements were identified based on criteria such as: The implementation should be as similar as possible to a real system; the components of the test bed may be implemented and shared from geographically diverse networks to enable remote tests; the SCADA LAB implementation has to be aligned with the SCADA LAB Testing Methodology and so on.

2.1.3. Analysis of Existing Methodologies

Proverbially, one should not re-invent the wheel. Hence the main existing testing methodologies for ICS, standards and related documentation were analysed. The conclusion was that there was no testing methodology that fully met the aims of the project. It was thus decided to develop such a methodology. Nevertheless, some key points were considered:

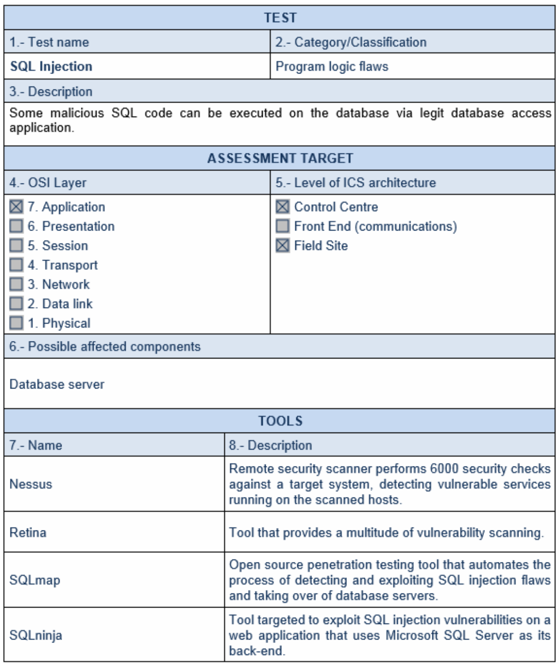
- The general structure of the methodology is based on the assessment process specified in *Cyber Security Assessments of Industrial Control Systems. Good Practice Guide* (Centre for the Protection of National Infraestructure, 2010).
- The attack vectors were defined according to the guidelines specified in *Commercially Available Penetration Testing.* (Centre for the Protection of National Infraestructure, 2006).
- The TOEs (Targets of Objective) and Test Procedures used in the proposed testing methodology are based on the specifications contained in *Vendor System Vulnerability Testing* (Idaho National Engineering and Environmental Laboratory, 2005).
- The proposed methodology could potentially be made compatible with the Common Criteria (AVA class – Vulnerability Assessment) in order to allow future certifications of services or products based on the SCADA LAB testing methodology (Common Criteria Recognition Arrangement, 2012).

2.1.4. Type of Security Assessment

The purpose of any security testing method is to ensure the strength of a system in the face of malicious attacks or regular software failures. This is usually accomplished by performing security tests. The methodology comprises three main types of security assessment: black box, grey box and white box testing.

2.1.5. An Approach to a Test Inventory

The methodology also provides an initial test inventory.



TEST	
1.- Test name	2.- Category/Classification
SQL Injection	Program logic flaws
3.- Description	
Some malicious SQL code can be executed on the database via legit database access application.	
ASSESSMENT TARGET	
4.- OSI Layer	5.- Level of ICS architecture
☒ 7. Application □ 6. Presentation □ 5. Session □ 4. Transport □ 3. Network □ 2. Data link □ 1. Physical	☒ Control Centre □ Front End (communications) ☒ Field Site
6.- Possible affected components	
Database server	
TOOLS	
7.- Name	8.- Description
Nessus	Remote security scanner performs 6000 security checks against a target system, detecting vulnerable services running on the scanned hosts.
Retina	Tool that provides a multitude of vulnerability scanning.
SQLmap	Open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers.
SQLninja	Tool targeted to exploit SQL injection vulnerabilities on a web application that uses Microsoft SQL Server as its back-end.

Figure 2: *Example of details of one test.*

2.1.6. Roles

The roles required during a security assessment are included in the methodology, together with clearly identified responsibilities and the relationships between them. The roles are:

- Sponsor.
- Developer / Vendor.
- Analysts.
- Evaluation Authority.
- Test-bed manager.

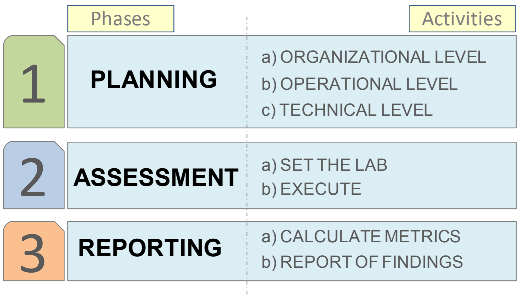
2.2. Phases in the Methodology

When operators request an assessment, three phases will need to be undertaken: Planning, Assessment and Reporting.

2.2.1. Phase I, Planning
This phase includes a set of actions to be performed. During this phase, an environment is prepared on the basis of the type of evaluation being undertaken: the test team, tests of connectivity, and other features.

2.2.2. Phase II, Assessment
Once the tests are planned, appropriate steps are taken to run each test.

2.2.3. Phase III, Reporting
After each test is completed, the results are evaluated and conclusions are drawn.



	Phases	Activities
1	PLANNING	a) ORGANIZATIONAL LEVEL b) OPERATIONAL LEVEL c) TECHNICAL LEVEL
2	ASSESSMENT	a) SET THE LAB b) EXECUTE
3	REPORTING	a) CALCULATE METRICS b) REPORT OF FINDINGS

Figure 3: *Phases in the Testing Methodology.*

3. LABORATORY AND TEST-BED IMPLEMENTATION

In the light of the basic architecture of ICSs, the test-bed includes the three main levels (field and control level, communication interface and supervisory level).

2.1. Design of the Test-Bed Architecture

The laboratory architecture proposed (SCADA LAB Consortium, 2013) includes all the components needed, from the highest-level items located in the Control Centre to the most basic elements sited at the Field Site. It also includes three types of communication channel: Digital and analog input and output signals, ethernet and serial communications. In addition, the main control protocols from the energy sector are represented: DNP 3.0, MODBUS and IEC 104.

Furthermore, in order to carry out tests at all levels of the OSI model, an agent needs to be connected directly to the test-bed. This function is covered by SCADALAB Testing Agent.

2.2. Design of the Laboratory Architecture

The Laboratory Area is responsible for managing test plans, including all the information received from the operator. The main components of the Laboratory are the following:

- SCADALAB Server.
- SCADALAB Front-End.

The SCADA LAB Server manages the test plans, including the setup of the test-bed and tests to be performed. On the other hand, SCADALAB Front-End is the point of contact between the stakeholder and the SCADA LAB Technical Department when requesting and managing security assessments.

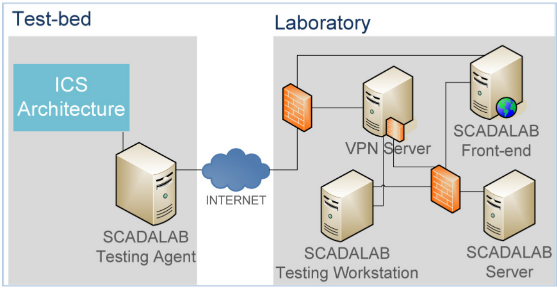


Figure 4: *Laboratory Architecture.*

2.3. Experiments

Once the Laboratory and Test-Bed Areas have been completed, the moment comes to start experiments. A description of the entire process used to perform a security assessment is given below (SCADA LAB Consortium, 2013).

(i) The operator accesses the SCADALAB Front-End component to request authorisation.
(ii) The technician receives a notification about that request.
(iii) The operator is requested via email to send required documentation: NDA, authorization form, etc.
(iv) Once the request is accepted, the technician registers the operator on SCADALAB Server and gets the user configuration file.
(v) The technician also registers the operator on SCADALAB Front-end and uploads the configuration file on the operator workspace. That file includes: user-id, ports used in the test-bed, etc.

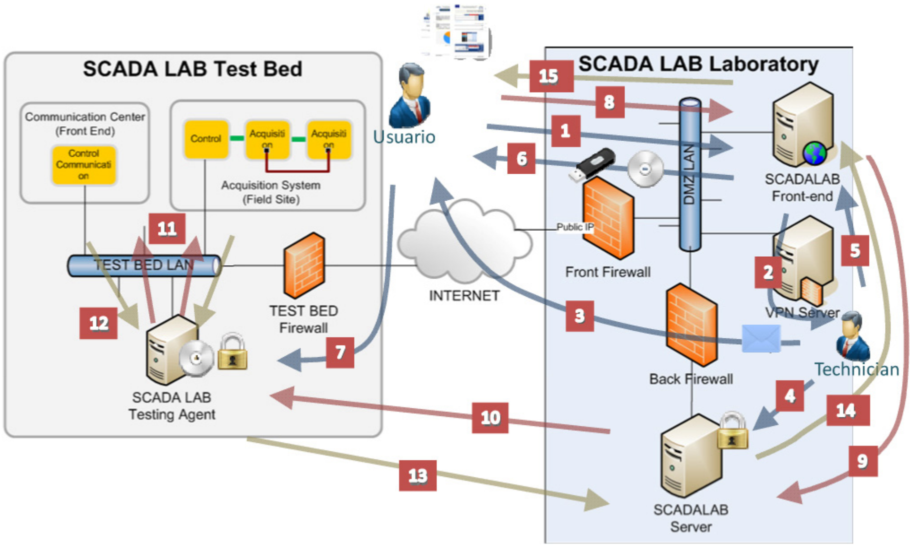


Figure 5: *Workflow for Experiments.*

(vi) The operator downloads both the ISO image and the configuration file.

(vii) The operator installs the ISO image on the SCADALAB Testing Agent component. The configuration file must be also plugged into it, via USB, in order to configure the SCADALAB Testing Agent.

(viii) The operator logs on to the SCADALAB Front-End and following this, he requests new assessment.

(ix) SCADALAB Front-End calls the SCADALAB Server in order to receive further information about the assessment: type of assessment, slot time, target, etc.

(x) SCADALAB Server connects to SCADALAB Testing Agent and sets up the test plan.

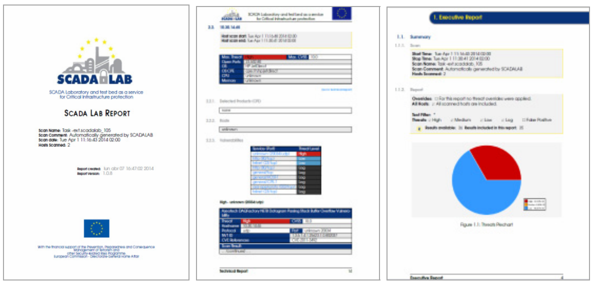
(xi) SCADALAB Testing Agent performs the tests against the target.

(xii) SCADALAB Testing Agent gathers the results of the tests.

(xiii) SCADALAB Testing Agent sends those results to the SCADALAB Server.

(xiv) The SCADALAB Server generates a technical report and it is uploaded to the SCADALAB Front-End. Thereafter the operator will be able to download it.

(xv) Finally, the operator may consult the technical report.


SCADA LAB

SCADA Laboratory and test bed as a service for Critical Infrastructure protection

SCADA LAB REPORT

1. Executive Report

Figure 6: *Vulnerability Assessment Report.*

Steps (ii) and form (ix) to (xiv) are automatic, the rest are manual or semi-automatic.

2.4. Supplementary Documentation

Additionally, a wide variety of documentation is provided: a template for a non-disclosure agreement, an application for authorization form, a template for security tests, and similar materials.

2.5. Lessons learned

The success of the SCADA LAB was largely dependent on the skills and strengths of the people involved. During this project was needed to have a dedicated, talented set of cyber security and industrial skills working towards a proper design of the final test bed and laboratory architecture.

3. CONCLUSIONS

This full solution includes all the technical and procedural features required to perform a remote security assessment against environments based on industrial control systems.

As a result of a security assessment, those responsible for security in critical infrastructures can gather the relevant information for making decisions which minimize the risk of security incidents which might seriously affect the reputation of a company and sometimes even put human life at risk.

In this paper, the aim has been to showcase a framework that is capable of providing a first view of the security level of critical infrastructures, in a detailed, fast and simple way.

3. REFERENCES

Centre for the Protection of National Infrastructure (2006) Commercially available penetration testing. Best practice guide.

Centre for the Protection of National Infrastructure (2010) Cyber security assessments of industrial control systems. Good practice guide.

Common Criteria Recognition Arrangement (2012) CC v3.1 Release 4.

European Union Agency for Network and Information Security (2011) Protecting industrial control systems. Recommendations for Europe and member states, Heraklion, Greece.

Idaho National Engineering and Environmental Laboratory (2005) Vendor system vulnerability testing test plan.

SCADA LAB Consortium (2013) D.2.2 Testing methodology.

SCADA LAB Consortium (2013) D3.1 System architectural design document.

SCADA LAB Consortium (2013) D3.2 Security assessment.