Chapter 17

CREATING A EUROPEAN SCADA SECURITY TESTBED

Henrik Christiansson and Eric Luiijf

Abstract Supervisory control and data acquisition (SCADA) systems are commonly used to monitor and control critical infrastructure assets. However, over the past two decades, they have evolved from closed, proprietary systems to open networks comprising commodity platforms running common operating systems and TCP/IP stacks. The open architecture and increased connectivity provide more functionality and reduce costs, but they significantly increase the vulnerabilities and the exposure to threats. Since SCADA systems and the critical infrastructure assets they control must have 24/7 availability, it is imperative to understand and manage the risk. This paper makes the case for a European SCADA security testbed that can be used to analyze vulnerabilities, threats and the impact of attacks, ultimately helping design new architectures and robust security solutions. The paper also discusses testbed requirements, deployment strategies and potential hurdles.

Keywords: SCADA systems, risk assessment, security testbed

1. Introduction

Process control systems – often referred to as supervisory control and data acquisition (SCADA) systems – are commonly used to monitor and control industrial processes. SCADA systems have three main functions: (i) obtaining data from sensors, switches and other devices, (ii) managing industrial processes that are supervised and operated by humans, and (iii) adjusting process parameters by changing the states of relays, switches and actuators (e.g., opening a valve to increase gas flow, which raises the process temperature).

SCADA systems are used in practically every critical infrastructure asset. The term "critical infrastructure" is defined as "those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments" [11]. SCADA

Christiansson, H. and Luiijf, E., 2008, in IFIP International Federation for Information Processing, Volume 253, Critical Infrastructure Protection, eds. E. Goetz and S. Shenoi; (Boston: Springer), pp. 237–247.

systems come in myriad types, sizes and applications. They may monitor only a few devices as in a manufacturing plant or tens of thousands of sensors as in an oil or gas pipeline. They may coordinate a multitude of actuators, each controlling a different physical process as in a petrochemical refinery. The controlled processes may require monitoring cycles varying from milliseconds (e.g., in the power sector) to an hour or longer (e.g., at a sewage treatment facility). SCADA systems differ from "normal" information and communication technology (ICT) systems in that they must operate reliably and provide 24/7 availability. Moreover, their depreciation is much higher and their lifecycles are longer, with eight to fifteen years being quite common [4].

SCADA security is a growing concern; organizational, architectural, technical and implementation vulnerabilities abound [1, 2, 20]. Parks and Duggan [18] observe that the first principle in waging a cyber war is to have a "kinetic effect" such as shutting down an electrical substation or opening the spill gates in a dam. Such attacks can be perpetrated quite effectively by manipulating SCADA systems – the severity of an attack depends on the criticality of the infrastructure asset and the damage characteristics (nature, extent, duration, etc.). Indeed, the effect of an attack can range from a nuisance event to a major national disaster.

It is imperative to analyze the risk to SCADA systems in terms of vulnerabilities, threats and potential impact. This paper argues for the creation of a European testbed for understanding and analyzing the risk to SCADA systems used in critical infrastructure assets. The paper also discusses testbed requirements, deployment strategies and potential hurdles.

2. Problem Description

This section discusses security issues related to SCADA systems and the risk in terms of threats, vulnerabilities and potential impact.

2.1 SCADA Security

Since the early 1990s, proprietary, hard-wired automation systems used in critical infrastructure components have increasingly been replaced by modern SCADA systems [7]. Many of these modern systems incorporate commercial-off-the-shelf ICT solutions, including commodity computing and network equipment, standard operating systems, Internet protocols and open software.

This trend raises serious security issues concerning SCADA systems and the critical infrastructure assets they control. Asset owners and operators are generally unprepared to deal with information security in SCADA environments either due to a lack of expertise or an absence of security functionality and tools. Meanwhile, vulnerabilities in ICT components are becoming part of the SCADA environment. Advanced operator functionality and web-based control interfaces make it easy to change vital SCADA settings deliberately or by accident. Indeed, critical processes can no longer be controlled manually.

Table 1. Risk handling in ICT and SCADA environments.

	ICT Environment	**SCADA Environment**
Reliability	Occasional failures are tolerated	Outages are not tolerated
	Beta test in the field is acceptable	Thorough *quality* assurance testing is expected
Risk Impact	Loss or unauthorized alteration of data	Loss of production, equipment and/or lives; potential for environmental damage; disruptions to the critical infrastructure
	Loss of data privacy and confidentiality	
Information Handling	High throughput is demanded	Modest throughput is acceptable
Performance	Delays and jitter are accepted	Delays are a serious concern
Risk Management	Recovery by rebooting	Fault tolerance is essential
	Safety is not an issue	Explicit hazard analysis *related to the physical process* is expected

Therefore, if a SCADA system fails, the industrial process it controls is rendered non-operational or worse.

Limited emphasis has been placed on SCADA security because it is generally assumed that SCADA systems are based on proprietary hardware and software, and obscure protocols. Other common assumptions are that SCADA systems are isolated from ICT assets and that they operate in benign (if not trusted) environments. However, all these assumptions have been shown to be unwarranted [7, 14].

It is also incorrect to assume that techniques and tools designed to mitigate risk in ICT environments can be directly transferred to SCADA environments. Table 1 (based on [6] with our comments provided in italics) identifies the major differences in handling risk in ICT environments as opposed to SCADA environments. The concept of thorough quality assurance testing for SCADA systems typically focuses on safety and functionality instead of information security [4]. Also, hazard analysis in SCADA environments is generally related to the physical processes being controlled. These issues are not relevant to ICT environments.

2.2 Understanding the Risk

Establishing a suitable SCADA security framework requires an understanding of the risk in terms of threats, vulnerabilities and potential impact. Most SCADA personnel have backgrounds in automation and safety with little, if any,

formal training in information security. ICT security staff often view SCADA systems simply as equipment with valves, switches and sensors.

The primary reason for the general lack of awareness about SCADA security is the scarcity of well-documented incidents. One exception is the British Columbia Institute of Technology's industrial security incident database, which contains data about 94 SCADA incidents from the period 1982 through 2004 [5]; however, details about the incidents are confidential and are released only to authorized entities. Another problem is the lack of a structured repository about specific SCADA vulnerabilities (some information about general vulnerabilities is available; see, e.g., [22]). Moreover, very little is known about attackers and their techniques and tools.

The following are some of the most widely publicized SCADA incidents [14, 15, 21, 24]:

- In January 1998, hackers seized control of GazProm's gas pipeline system. The attack was most likely launched in an attempt to extort money.
- Between January and April 2000, Vitek Boden, a disgruntled former contractor manipulated the SCADA system of Hunter Watertech in Maroochy Shire, Australia a total of 46 times. He released one million liters of untreated sewage to the environment.
- In November 2001, a SCADA software error in The Netherlands caused natural gas to be produced with the incorrect composition; 26,000 Dutch households were unable to heat their homes and cook food for three days.
- In January 2003, the SQL/Slammer worm shut down communications at an electric power substation in the United States. The same worm affected the telemetric system of a SCADA/energy management facility and attacked a security display station at the Davis-Besse nuclear power plant. These systems were unusable for more than five hours.
- The U.S. Department of Energy reported to the U.S. House of Representatives that it had identified several scenarios for unauthorized entry into SCADA systems in the power sector. It reported eight successful penetrations of SCADA systems in eight attempts.
- In January 2005, approximately 15,000 households in Weert, The Netherlands lost electrical power due to a failure in a SCADA system.
- In July 2005, a lack of situational awareness in a SCADA/emergency management system caused an explosion when a ground-wired switch at a new substation was connected to a 150 kV circuit.

We have learned that numerous SCADA security incidents in critical infrastructure facilities have gone unreported by asset owners and operators. These include processing plants being shut down by worms, a penetration testing team inadvertently causing a blackout, and hackers penetrating systems controlling refineries and electrical power transmission substations [14].

On the threat side of the risk spectrum, more than twenty nation states currently possess advanced cyber attack capabilities [16]. Seven types of actors are deemed to constitute a threat to SCADA systems [16, 20]:

- Nation states seeking to add electronic attacks on critical infrastructure assets to their set of capabilities
- Radical activists and terrorists intending to impact society by attacking critical infrastructure assets
- Activists seeking to publicize their cause by disrupting critical infrastructure services
- Criminal organizations intending to extort money from critical infrastructure asset owners and operators
- Virus/worm writers interested in demonstrating their ability to shut down critical infrastructure assets
- Insiders seeking revenge on their employers by attacking critical infrastructure assets
- Script kiddies experimenting with tools that could affect critical infrastructure assets

However, it is difficult to assess the expertise of potential attackers. The main reason is the absence of well-documented incidents (at least in the open literature). At a minimum, qualified attackers should have substantial expertise about: (i) physical systems and processes managed by SCADA systems, (ii) technical and operational aspects of SCADA systems, and (iii) techniques for circumventing security measures.

It would appear that attacking SCADA systems is a difficult task because of the complex knowledge, advanced skills and access needed for successful penetration. But the reality is that asset owners and operators have a distinct disadvantage. It is well-known that they operate SCADA systems to control important societal resources. Detailed information about SCADA architectures, protocols and configurations is freely available on the Internet or is obtainable from other sources; and system vulnerabilities and code for exploiting weaknesses are public knowledge. The geographic scale, remoteness and limited physical security of many critical infrastructure assets allow them to be penetrated quite easily. Finally, even when SCADA systems are designed to be isolated, the need to share information for business purposes or to perform remote maintenance results in interconnections with public networks, including the Internet.

3. Establishing a SCADA Security Testbed

A SCADA security testbed can be used to analyze vulnerabilities, threats and the impact of attacks. This section discusses the requirements of a testbed and makes a case for deploying a European SCADA testbed.

Table 2. Penetration testing in ICT and SCADA environments.

Activity	ICT Environment	SCADA Environment
Enumeration and identification of hosts, nodes and networks	Perform a ping sweep (e.g., nmap)	Examine channel access method (CAM) protocol tables on switches Examine router configuration files and router tables Verify physical configuration Perform passive scanning or intrusion detection (e.g., snort)
Identification of vulnerabilities in services	Perform a port scan (e.g., nmap)	Verify local ports (e.g., netstat) *Perform port scan of duplicate, development or test system*
Identification of services on hosts, nodes and networks	Perform a vulnerability scan (e.g., Nessus, ISS)	Capture local banners using version lookup in a CVE database *Perform scan of duplicate, development or test system*

3.1 Assessing SCADA Security

Several challenges are encountered when attempting to perform security-related analyses of SCADA systems. The following sections describe the primary challenges, all of which can be addressed using a well-designed SCADA security testbed.

Penetration Testing of Live Systems Penetration testing of live systems is an effective technique for discovering vulnerabilities and assessing attack impact. Unlike their ICT counterparts, SCADA systems control physical processes and have real-world consequences associated with their actions. Consequently, it is very dangerous to perform penetration tests on live SCADA systems; a SCADA testbed is most appropriate for this purpose.

According to [10], a penetration test of ICT systems involves three steps: (i) identification of hosts, nodes and networks; (ii) identification of services available on hosts, nodes and networks; and (iii) identification of possible vulnerabilities in services. However, performing penetration testing of SCADA systems requires a different approach, which is highlighted in Table 2 (our comments are italicized for emphasis).

Penetration testing techniques for SCADA environments are more complex because they must incorporate damage control and mitigation activities. Some researchers (e.g., [23]) have used active penetration methods on live systems, but this is not well advised [10, 14]. At best, passive penetration tests are recommended for operational SCADA systems. Active tests should be performed only on development systems or testbeds.

Validating Security Solutions It is important to ensure that classical ICT security solutions (e.g., firewalls, VPNs and anti-virus software) do not adversely impact operations, especially when SCADA environments use specialized protocols such as Modbus or DNP3. This requires the design and deployment of test plans, architectures and configurations, and extensive analysis of test results [12, 19]. Thorough testing is also required to evaluate potential negative side-effects of software updates and patches. These activities can only be performed using a SCADA testbed.

Establishing Risk Analysis Methods Relatively few risk assessment methods are available for SCADA systems. One of the more prominent is the relative risk assessment method developed for water utilities in the United States [26]. The method, which is based on joint assessments by sector experts and SCADA security experts, assumes that the potential consequences of a SCADA system failure are unique to an infrastructure asset. Therefore, risk assessment cannot be performed using generic information related to SCADA system security. As a consequence, developing an effective risk analysis method requires a realistic SCADA security testbed.

Establishing SCADA Security Standards Many ICT security standards such as ISO/IEC 17799:2005 conflict with requirements for SCADA environments [14]. Few security standards have been established for SCADA systems to date; however, recently, there has been a flurry of activity [1]. The risk to SCADA systems is so high that even incompatible and conflicting security standards and best practices are being considered. In the energy sector, for example, emphasis is being placed on addressing the technology gaps before specifying security policies and best practices [8]. The most effective way to address these challenges is to establish a SCADA security testbed.

3.2 Rationale for a European Testbed

The U.S. National SCADA Test Bed (NSTB) has had a major influence in developing security solutions. Testimony at a 2005 congressional hearing highlighted the effectiveness of the NSTB [1], a joint venture involving the national laboratories, and the SCADA and ICT vendor communities. The NSTB has helped identify several SCADA vulnerabilities, which were subsequently fixed by SCADA vendors and integrators. Validation of the fixes was also performed using the NSTB's extensive SCADA testing environment.

Other SCADA testbeds are located at NIST in Gaithersburg, Maryland and at the British Columbia Institute of Technology (BCIT) in Burnaby, Canada. In Europe, testbeds are operational in Grenoble, France; at CERN in Geneva, Switzerland; and at the European Joint Research Centre in Ispra, Italy [13].

Clearly, a large (possibly distributed) SCADA security testbed needs to be established in Europe. Many of the reasons for creating a testbed have already been discussed. Perhaps the most important reason, however, is the fact that the architectures of many European critical infrastructure components are

quite unique. For example, the European power grid has a highly distributed structure with diverse power generation facilities; in contrast, the North American system has deregulated control [3]. A European testbed will help develop, assess and deploy security solutions and best practices that fit the European realm. Moreover, the testbed will help evaluate and frame standards and legislation related to SCADA security and critical infrastructure protection.

4. Towards a European Testbed

This section discusses the deployment strategy and the potential barriers to creating a European SCADA security testbed.

4.1 Strategy

Establishing a European SCADA security testbed requires a coherent strategy that addresses the issues of what to test, how to test, and (eventually) how to disseminate the results. The issue of what to test requires an assessment of what a European testbed can provide to its stakeholders. This requires an examination of the architectural characteristics of European infrastructures.

The NSTB identifies technology security, protocol security and infrastructure security as three major testing areas [17]; these can be used as the basis for a European approach. The NSTB checklist for the strategic impact of assumed attacks or failures [17] is also a good starting point as it prioritizes systems for testing based on aspects such as the extent of use and manufacturer's market share. A consistent and coordinated strategy is required for all SCADA components – from field devices to complex SCADA systems [9]. It is important to note the lack of coherent work conducted in Europe in the area of SCADA security will likely complicate the task of identifying the relevant competencies. Equally important is to identify deficiency areas that should be addressed.

No international standards exist for testing SCADA components and systems. To our knowledge, the only list of security characteristics to be tested is the one employed by the NSTB [25]. The list, which is determined based on risk, ease of attack and attack severity, includes clear text communications, authentication, system integration, web services and perimeter protection.

A large-scale European testbed should address the needs of SCADA manufacturers, critical infrastructure stakeholders and academic researchers, and should facilitate the testing of new SCADA security architectures and strategies, along with the analysis and evaluation of complex vulnerabilities in real-world environments. The testbed must support iterative, synergistic evaluation efforts and the integration of different competency areas such as infrastructure system engineering, ICT security and physical security.

4.2 Potential Problems

Europe has an excellent track record at running world-class joint research centers ranging from CERN to JET (nuclear fusion). However, a European

SCADA security facility would have a very different political and economical environment from that at CERN or JET (which focus on fundamental research) or at a U.S. SCADA testbed facility (which is managed by one national government). A major complexity arises because a European SCADA security testbed would have to balance the national security interests of multiple nations. Also, the needs of asset owners and operators and SCADA vendors from different countries would have to be balanced. Since a European facility is multinational in nature, the political, financial and strategic issues would have to be addressed to the satisfaction of all the participating entities.

4.3 Requirements

The requirements of a SCADA security testbed are complex, and cover the organizational and technical areas. The organization that operates the testbed should be an independent entity and should be able to handle and safeguard extremely sensitive information related to vulnerabilities, threats and attacks, in addition to proprietary information from owners, operators and vendors. Dissemination of Computer Emergency Response Team (CERT) data about SCADA security must be performed both rapidly and carefully as a release can affect thousands of operational systems around the world. At the same time, unauthorized leaks or the release of incorrect information could create havoc throughout the critical infrastructure, potentially resulting in economic losses, environmental damage and casualties.

A European SCADA testbed must leverage the resources provided by existing testbed facilities; simultaneously, it should identify and initiate efforts in specialty areas. International cooperation will be critical, especially in the areas of testing, research and development, and standards promulgation. Finally, the testbed should be highly reconfigurable and connect to other SCADA facilities using secure, long-haul communication links to create a state-of-the-art distributed testing environment.

5. Conclusions

The architectures of many European infrastructure components are unique. A state-of-the-art European testbed is, therefore, needed to analyze vulnerabilities, threats and the impact of attacks on SCADA systems that control vital infrastructure assets. Since a European facility would be multinational in nature, the political, financial and strategic exigencies will have to be addressed to the satisfaction of all the participating entities. However, given Europe's track record at running world-class research centers such as CERN, a European SCADA security testbed promises to be extremely successful. The testbed would engage industry stakeholders, academic researchers and government scientists, helping design new SCADA security architectures and strategies that would significantly enhance global critical infrastructure protection efforts.

References

[1] K. Ananth, Testimony of Dr. K. P. Ananth, Associate Laboratory Director, National and Homeland Security, Idaho National Laboratory, Idaho Falls, Idaho, Idaho Hearing on SCADA and the Terrorist Threat: Protecting the Nation's Critical Control Systems, House Committee on Homeland Security, Subcommittee on Economic Security, Infrastructure Protection and Cyber Security, October 18, 2005.

[2] M. Assante, R. Wells and W. Pelgrin, The SCADA and process control security procurement project update, SANS Special Webcast, SANS Institute, Bethesda, Maryland, May 18, 2006.

[3] D. Bakken, What good are CIP test beds? And what CIP test beds are good? Some observations from the field, presented at the *Joint U.S.-E.U. Workshop on ICT-Enabled Critical Infrastructures and Interdependencies: Control, Safety, Security and Dependability*, 2006.

[4] K. Barnes, B. Johnson and R. Nickelson, Review of Supervisory Control and Data Acquisition (SCADA) Systems, Technical Report INEEL/EXT-04-01517, Idaho National Engineering and Environmental Laboratory, Idaho Falls, Idaho, 2004.

[5] E. Byres, The British Columbia Institute of Technology's confidential industrial security incident database, presented at the *NISCC SCADA Security Conference*, 2005.

[6] E. Byres, J. Carter, A. Elramly and D. Hoffman, Test your system five ways, *ISA InTech Magazine*, vol. 50(3), pp. 24–27, 2003.

[7] E. Byres and J. Lowe, The myths and facts behind cyber security risks for industrial control systems, presented at the *VDE Congress*, 2004.

[8] R. Carlson, J. Dagle, S. Shamsuddin and R. Evans, A summary of control system security standards activities in the energy sector, National SCADA Test Bed, U.S. Department of Energy, Washington, DC (www.oe.energy.gov/DocumentsandMedia/Summary_of_CS_Standards_Activities_in_Energy_Sector.pdf), 2005.

[9] J. Davidson, M. Permann, B. Rolston and S. Schaeffer, ABB SCADA/EMS System INEEL Baseline Summary Test Report, Technical Report INEEL/EXT-04-02423, Idaho National Engineering and Environmental Laboratory, Idaho Falls, Idaho, 2004.

[10] D. Duggan, M. Berg, J. Dillinger and J. Stamp, Penetration Testing of Industrial Control Systems, Technical Report SAND2005-2846P, Sandia National Laboratories, Albuquerque, New Mexico, 2005.

[11] European Commission, Critical Infrastructure Protection in the Fight Against Terrorism, Communication COM(2004) 702 Final, Communication from the Commission to the Council and the European Parliament, Brussels, Belgium, 2004.

[12] J. Falco, Use of antivirus on industrial control and SCADA systems, presented at the *Process Control Security Requirements Forum Spring Meeting*, 2005.

[13] S. Lueders, Control systems under attack? presented at the *International Conference on Accelerator and Large Experimental Physics Control Systems*, 2005.

[14] H. Luiijf and R. Lassche, SCADA (on)veiligheid: Een rol voor de overhead? TNO-KEMA Report, TNO Defence, Security and Safety, The Hague, The Netherlands, 2006.

[15] M. Naedele and D. Dzung, Industrial information system security – IT security in industrial plants – An introduction, *ABB Review*, issue 2, pp. 66–70, 2005.

[16] National Infrastructure Security Co-ordination Centre (NISCC), The Electronic Attack Threat to Supervisory Control and Data Acquisition Control and Automation Systems, NISCC Briefing 02/04, London, United Kingdom, 2004.

[17] R. Parks, National control system security testing plan, presented at the *SANS Process Control and SCADA Security Summit*, 2006.

[18] R. Parks and D. Duggan, Principles of cyber-warfare, *Proceedings of the IEEE Workshop on Information Assurance and Security*, pp. 122–125, 2001.

[19] R. Parks, J. Hills, S. Smith, T. Davis, A. Baros and P. Cordeiro, Network Security Infrastructure Testing, Version 1.2, Center for SCADA Security, Sandia National Laboratories, Albuquerque, New Mexico (sandia.gov/scada/documents/NSTB_NSIT_V1_2.pdf), 2005.

[20] A. Priore, Hacking for dollars, *Newsweek International*, December 22, 2005.

[21] T. Smith, Hacker jailed for revenge sewage attacks, *The Register*, October 31, 2001.

[22] J. Stamp, J. Dillinger and W. Young, Common Vulnerabilities in Critical Infrastructure Control Systems, Technical Report SAND2002-0435C, Sandia National Laboratories, Albuquerque, New Mexico, 2002.

[23] V. Virta, The red team tool box: A method for penetration tests, *Proceedings of the European Institute for Computer Antivirus Research Conference*, 2005.

[24] J. Visser, M. Berkom, J. Spiekhout, Y. Suurenbroek, J. Wessels, B. Smolders and C. Pietersen, Storing Gasmengstation (Faults in Gas Mixing Stations), Technical Report CB-2-02.060, Raad voor de Transportveiligheid, The Hague, Netherlands, 2002.

[25] R. Wells, Measurements, presented at the *SANS Process Control and SCADA Security Summit*, 2006.

[26] W. Young and J. DePoy, Relative Risk Assessment for Water Utility SCADA Systems, Technical Report SAND2003-1772C, Sandia National Laboratories, Albuquerque, New Mexico, 2003.