C. Alcaraz, et al., "Secure Management of SCADA Networks", *Novatica, New Trends in Network Management*, vol. 9, pp. 22-28, 2008.
NICS Lab. Publications: https://www.nics.uma.es/publications

Secure Management of SCADA Networks

Cristina Alcaraz, Gerardo Fernandez, Rodrigo Roman, Angel Balastegui, Javier Lopez

Departamento de Lenguajes y Ciencias de la Computación, Universidad de Málaga

{alcaraz, gerardo, roman, balastegui, jlm}@lcc.uma.es

Abstract

When a SCADA (*Supervisory Control and Data Acquisition*) system monitors and manages other complex infrastructures through the use of distributed technologies, it becomes a critical infrastructure by itself: A failure or disruption in any of its components could implicate a serious impact on the performance of the other infrastructures. The connection with other systems makes a SCADA system more vulnerable against attacks, generating new security problems. As a result, it is essential to perform diverse security analysis frequently in order to keep an updated knowledge and to provide recommendations and/or solutions to mitigate or avoid anomalous events. This will facilitate the existence of a suitable, reliable, and available control network.

Keywords

SCADA network management, Supervisory Control and Data Acquisition Systems, Security Analysis.

1.- Introduction

A SCADA system (or control system) is a complex system capable of controlling and managing other complex system whose resources are considered critical (such as water, gas, oil or electricity). In general, these control systems have evolved over time and are, at present, based on distributed environments. They are composed by very varied (hardware and software) components, being most of their logical components COTS (*Commercial-Off-The-Shelf*) so as to reduce cost of implementation and maintenance. However, both the interaction among different components and the new connection towards external networks, such as Internet, involve multiples and diverse problems of security. Moreover, a failure or disruption in any of their components could involve an important impact on the performance of other infrastructures, affecting on the economy of a region, a nation or nations [1].

As a result, the industrial sector needs to collaborate with the research community and diverse institutions, in order to discover how to enforce certain essential security properties of these critical systems, such as availability. In fact, there are several technical documents and scientific articles dealing with security issues in critical systems (cf. [2][3][4]). However, as none of them provide a complete solution for the problem on these types of infrastructures, it is important to keep an updated knowledge on the subject with technical-scientific procedures, policies and standards, as well as to identify and to describe new vulnerabilities and solutions, considering futures anomalous actions and alternatives. In fact, the main goal of this paper is to make a deep security analysis in the control and access (both physical and logical access) points of

the system, providing an up-to-date overview of new problems, schemes, and solutions, in order to improve the availability and management of a SCADA network.

2.- SCADA Network Architecture and Problems

A SCADA network architecture is composed by two types of foundation networks (both are depicted in the figure 1): the corporative network and the control network. In the corporative network, the operations are more related to the general supervision of the system and the contractors/employees require of strong authentication procedures to interact with the databases (historical, alarms, etc.) and critical servers. On the other hand, the control tasks (as for example, to open/close a pump or to retrieve a measurement) are carried out in the control network. All these tasks are managed by a HMI (Human Machine Interface) localized in the principal SCADA control centre or remote substations, and transmitted to certain field devices which are usually located in the industrial plants or substations.

A field device (such as a RTU – Remote Terminal Unit) is a device with constrained capabilities but autonomous and independent enough to be able to process data and to identify which sensor or actuator is the responsible of executing an order in a substation. Moreover, they are able to establish connections with other substations, other RTUs and other field devices such as PLCs (Programmable Logic Controllers). Furthermore, they can simultaneously process and respond to several messages transmitted by multiple sources since they can support multiples sessions with TCP/IP. Some RTUs can even support Linux/Unix or Microsoft Windows to provide Web applications with graphical interfaces to generate the reports.

Nowadays, numerous industrial and proprietary protocols coexist and work in a same system. Most of them work with the TCP/IP standard: Modbus/TCP [5], DNP3.0 [6] or ICCP [7]. Alternatively, there are other protocols, such as the protocols corresponding to the Common Industrial Protocol (CIP) family supported by *Open DeviceNet Vendors Association* (ODVA) [8]: Ethernet/IP, DeviceNet, CompoNet and ControlNet. These protocols are useful for the control process, but they lack of protection mechanisms, hence they could open new and important security holes that can affect the security of the system.

Regarding remote controlling from any geographic localization point, it is necessary that diverse communication infrastructures interact with each other, such as Ethernet, dial-up, Satellite, microwave, optical fiber, WiFi, WiMAX, etc. Some SCADA systems could also provide Web and mobile (GSM or TETRA) services in order to reduce maintenance tasks and increase performance and availability of the system.

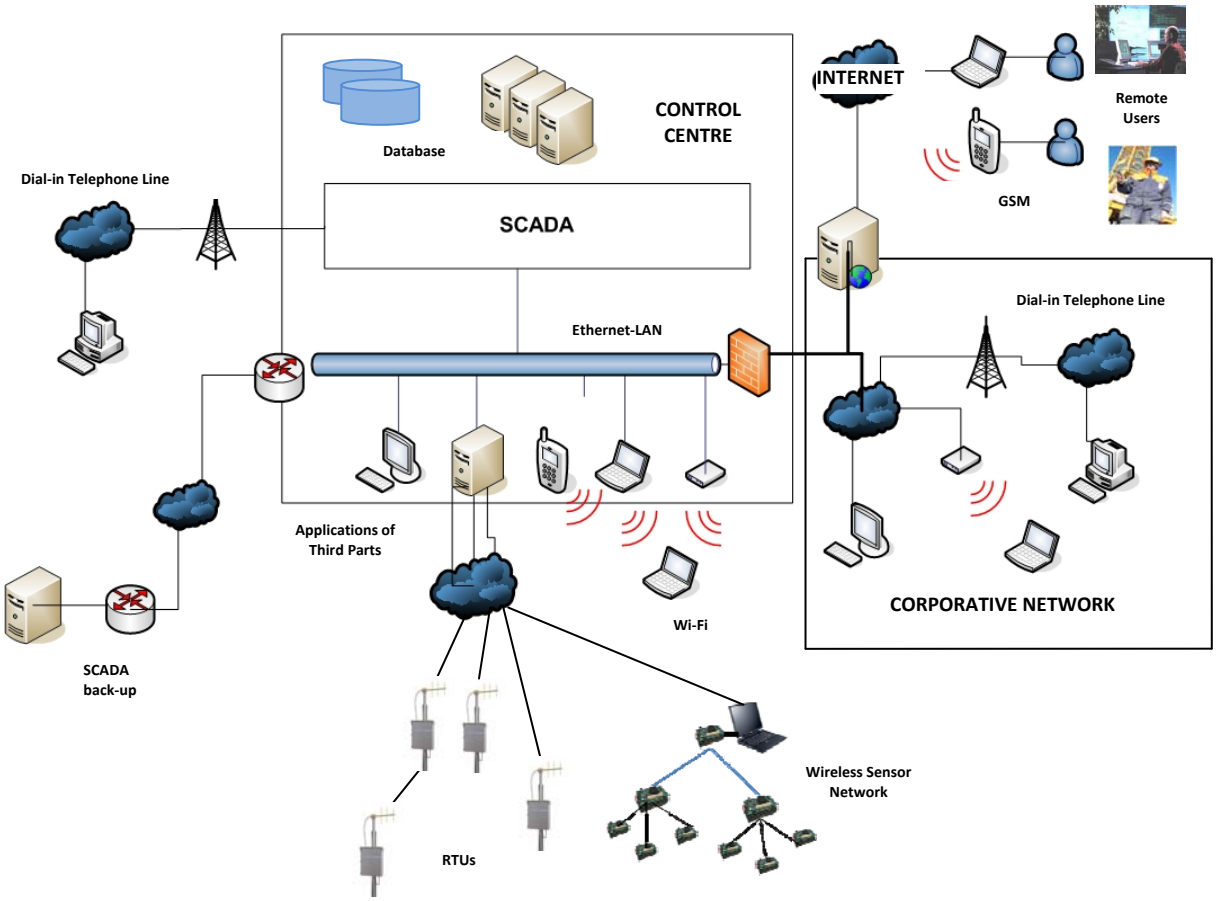

Figure 1: SCADA Network Architecture

A SCADA network, which is depicted in the figure 1, has multiple potential security holes, since internal and external attacks could appear in any point of the system. Internal attacks are associated to (intentioned or not intentioned) human actins, while external attacks are more related to the vulnerabilities corresponding to the standard TCP/IP, as well as the use of new technologies (for example, RFID or Wireless Sensor Network) and COTS components [9]. At present, many of these vulnerabilities are registered in public databases, such as CERT [10] or BICT (*British Columbia Institute of Technology*) [11]. CERT has approximately 2.500 vulnerabilities identified and 150 technical reports published since 1998. Similarly, BICT has the database ISID (*Industrial Security Incidents Data*), which was utilized by Byres et.al [12] to make a statistical study about the type of security problems in critical environment. They concluded that the external vulnerabilities had just started to emerge since 2001, rising every year.

3.- Identification and Authorization in SCADA System

In order to establish a security perimeter between unauthorized personnel and critical components and installations in a SCADA system, it is necessary to define strong access control policies. Said policies must include in their specification both mechanisms of security and electronic devices, such as: biometric systems, magnetic-trip cards, smart cards, RFID, video camera, or even specialized software to carry out the authorization processes from a HMI. In case that these security systems stop working, the most appropriate course of action is to keep active a manual procedure to

complete provisionally the control processes. In effect, these manual procedures must work as a second alternative since they depend on unsecure and unreliable mechanisms, such as a simple key (possibly electronic) or a control list managed by a human being.

Basically, most of the actual SCADA systems are designed under complex and automated authentication mechanisms based on user and password. The assertion of a new user will depend on two important factors: i) responsibility area and privileges of an operator, and ii) time of activity and functionality according to the contract. For controlling both active and inactive (considering expiration account or inactive contract) user accounts, the system will have to periodically check the viability of the security credentials. Any change associated to the user must be registered in the respective databases. Similarly, any type of activity in a session must also be registered to facilitate other types of analysis processes (as for example, statistical or forensic investigations). The security credentials will have to be frequently updated following security patterns and strong access control policies. The system will have to limit the number of sessions by user and to block all those accounts that exceed a maximum of failed attempts.

As already aforementioned, a Web service can be offered by a SCADA network for entering to the system from the Internet and managing in real time the control operations (such as, to receive measurements or to send control orders) from any HMI. The official websites will interact with the relational databases to manage the authorization process. In the case that these services present important security deficiencies, said databases could be compromised. Therefore, development methods must be applied to avoid future attacks, as well as tools to delete diverse implementation errors, as for example DEADBOLT for C and C++ [13]. Nonetheless, all these methods and tools are not enough to achieve a suitable security in the implementation, since the system can be compromised by social engineering or brute force attacks. As a result, it is also important to define and implant a suitable security policy.

4.- Security Policies in SCADA Systems

In any SCADA system is essential to define a set of security policies. These policies help to enforce the security and reliability requirements of an SCADA system by means of a set of audit procedures. The scope of the security policies is very wide, i.e. these define what actions can be executed by a physical (e.g. operator) element and by a logical (e.g. communication subsystems) element, the steps to follow in the maintenance operations and incidence managements, in addition to identify responsibilities.

It is recommendable for the development of a security policy to utilize generic security control standards for information systems, such as NIST 800-53 [14], ISO/IEC 17799 [15] or COBIT [16]. Nonetheless, the specific requirements of the SCADA systems (i.e., high availability, reliability and reaction time) require of a set of rules and policies adapted according to necessities [9]. For them, existing standards have been extended [14], as for example the NIST 800-82 [17], defining diverse schemes of security policies in the academic environment [18].

For every SCADA system, it is important to take into account the following security policies [18]: data protection (access and storage), hardware and software configuration (virus, intrusion detection, access control and codification), security in the

communication (wireless access, local, remote), human resources (use of the system, preparation and recycling), audits, physical security (access to equipment, material destruction), and manual operations execution in failure case. All these security policies are influenced by the following factors: the existing interdependences of the organization, the roles of the diverse human resources, the information system architecture, the data managed in SCADA and the risks associated to the system.

A clear example of such policies is incidence management, since a SCADA system must recover its performance in a crisis situation as soon as possible. For this policy, it is necessary to define how to store and how to access to the events that occurred in the system. The events have to be visible for those operators with determined privileges, and these operators must have enough information (for example, telephone number, email, cryptographic key and instructions for verifying its identity) to contact with the responsible in charge of treating the incidence occurred. Finally, determined accessories (alongside with recuperation procedures and the appropriated practice) must exist to recompile and analyze evidence proofs, which could be used in legal actions.

5.- SCADA Communication Networks Protection

A SCADA system requires of secure network management processes, which must identify and manage all connections from the Internet towards the SCADA network – and vice versa -, and from the corporative network towards the control network. Said processes are under specialized and restrictive mechanisms, such as: firewalls, IDS (Intrusion detection system), IPS (Intrusion Prevention Systems), antivirus, RADIUS servers or VPN (Virtual Private Networks) protocols. Every one of these components will have to be configured and distributed strategically to reach a strong protection and a defense-in-depth [19]. In addition, the accesses from the corporative network towards the control network and towards diverse critical servers must also be controlled. The communication channels have to be protected by means of tunneling services, key management systems and specialized tools, as for example SecSS (Security Services Suite) [20].

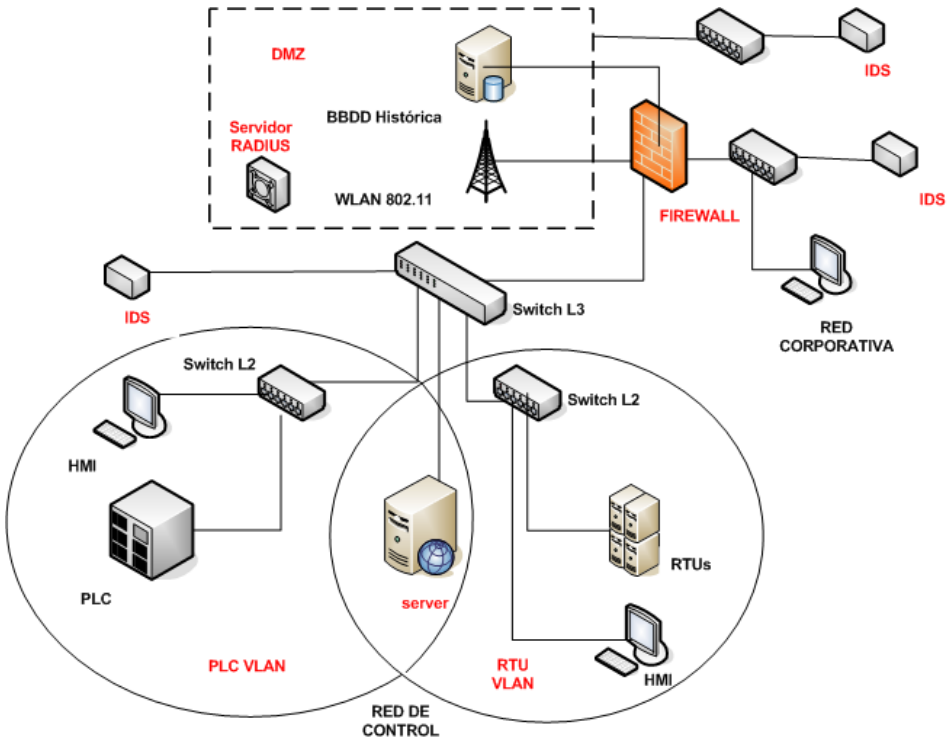

Figure 2: SCADA network architecture proposed by NISCC

In case of existing devices with wireless communication (Bluetooth, Rogue APs o WiFi), the access control policies must be very restrictive. The inactive ports and the broadcast of the SSID (Service Set IDentifier) should be closed, and the communication channel must be protected with cryptographic mechanisms. Also, it is recommendable in these scenarios to employ WPA-Radius and TLS. Finally, within this category the Wireless Sensor Networks play an important role in the control processes, since they are considered a perfect candidate in the critical infrastructure protection in general [21]. In fact, nowadays, there are several initiatives [22][23] to standardize their communications in the industrial control processes.

5.1.- The First Defense Line

The *National Infrastructure Security Co-ordination Centre* (NISCC) [24] of BCIT presented by means of a guide the foundations for the configuration and management of firewalls corresponding to control systems in 2005. In the guide, a possible secure and scalable architecture is described based on a division in three main zones (see figure 2), being the first defense line: the firewall, IDSs and DMZ (Demilitarized Zone).

The firewall has to filter the network addresses, considering that every SCADA component has an IP address and one or more TCP/UDP ports, and also all the high risk services in the network including the services of the SCADA. At present, there are several firewalls exclusives for industrial environment, such as MODBUS-aware [25], developed by *Cisco Systems Critical Infrastructure Assurance Group* (CIAG), or Vattenfall **[**26] for the IEC 60870-5 (101, 103 y 104) family [27]. In addition, the NISC proposed in the guide the development of embedded firewalls for the field devices, known as micro-firewalls. However, a micro-firewall requires certain computational capabilities which cannot always be supported by the field devices, thus it is necessary to continue researching in this area.

With regard to the IDS, they assume the responsibility for monitoring the network traffic. They are composed on patterns, rules and a knowledge source based on evidences occurred in the past (vulnerabilities and attacks). Said knowledge needs to be kept up-to-date, and for a critical network such as SCADA, this may be unpractical. There are several IDS tools for critical environment as [28][29][30], and any type of detected incidence must be registered for future forensic researches.

Finally, it is important to comment that the rules configured in the firewalls may not be always accurate, mainly due to incorrect configuration or changes made by an IPS. A possible solution would be to install a tool that analyzes in real time whether the rules of the firewall coincide with those specified in the security policy, such as APT (Access Policy Tool) [31].

5.2.- Protection in the Communication Channels

The control operations have to be managed from any connection point and geographic localization in order to assure the availability of a SCADA system. Independently of the network, the encryption and authentication processes must be strong and restrictive, respectively. If the control network has direct connection to Internet, it is necessary to implement a VPN using standard protocols such as SSL and IPsec.

Generally, the protocols responsible of transmitting the control operations to the field devices (e.g. Modbus or DNP3 protocols) lack of security mechanisms. Depending on the underlying communication mechanisms and protocols the system will have to have implemented a determined security mechanism. For example, if the communication is serial, the system should configure a Bump-in-the-Wire [32] device between the EIA-232 port of the RTU and the modem to manage the encryption operations. Otherwise, if the communication is using the TCP/IP standard, it would only be necessary to install and configure those security mechanisms associated to the standard.

The previous control operations can also be transmitted between SCADA systems by means of specific protocols, such as ICCP/TASE 2.0. Although, ICCP provides both high availability and performance in the data transference, it lacks of security mechanisms. For resolving this problem the TC57 defined the standard IEC-62351 [33] to include the TLS/SSL protocols (they offer interoperability between SCADA systems), MMS/IEC-62351-4 and a bilateral table to register the corresponding associations to a system. As a result, the system could provide support for certification, message authentication code, key interchange (at least 1024 bits), RSA and DSS. This standard offers the port TCP 3782 to establish secure communications.

Other important aspect for the protection in the communication channels is the cryptography and the key management systems. One of the first technical documents that described a cryptographic implementation for critical systems was proposed by *American Gas Association* (AGA) with AGA-12 Part 1 [34]. Later, they presented AGA-12 Part 2 [35] to describe a specification of cryptographic implementation in serial communication channels, including a protocol based on sessions with authentication services by means of symmetric keys generated by AES and SHA-1. At present, there are two reports still pending of publishing, which are AGA-12 Part 3 and Part 4. Both of them specify the network protection and the security of the embedded devices in SCADA components.

Also, AGA was involved in developing standards for key management in control systems, and at present there several work groups working on them, such as *TC57WG15* (IEC62351), *IEEE Power Engineering Society Substations Committee* with P1689 and *DNP3 User Group* (DNP3 v1.0). So far, several security mechanisms have been proposed among them the use of Elliptic Curve Cryptography [36]. Due to the number of security mechanisms and methods for SCADA, it may be necessary to use a methodology [37] to identify and select which of them is the most suitable for a certain design.

6.- Protection of the Information Systems

In this section we will describe those processes that can improve the security of the information systems, focusing on those processes in charge of protecting SCADA systems against possible and future attacks. As of 2008, new attacks have occurred in these types of critical systems [38]. An important factor to take into account is the existing applications that include support for carrying out such attacks [39], as for example Metasploit. As these tools are increasingly easy to use, SCADA systems may become a new target for all those that want to show their malicious abilities.

The protection solutions provide a layer of defense against internal attacks. Generally, internal attacks are possibly one of the most dangerous in these systems because of the intruders' knowledge of the system. Nonetheless, these mechanisms also provide an additional base to face the external attacks, since they could build a scenario to control the impact caused by an intruder.

A fundamental part of the protection of the information systems is to specify the dependences between services and other services/applications installed. Such knowledge can help in the design of isolated execution contexts for the services, reducing their visibility and allowing a better control of both their privileges and their relationships with the other elements of the system. There are several possible technical solutions available for different Operative Systems: group policies and access control rules in Windows, SELinux in Linux or RBAC and Containers in Solaris. In order to facilitate this task, the number of services available in a SCADA system should be reduced to a set of essential services. This also reduces the dependencies between services and potential vulnerabilities that may arise.

The data storage is other aspect that must be taken into account in determined situations. After an attack is carried out, an intruder could break or accede to sensible information such as the privileges of the system. A possible solution would be to adopt existing encryption mechanisms to protect the sensible data of the system. Other solution would be that the database servers may interrupt the access to the files (not encrypted) activating the own encryption mechanisms.

Also, resource monitoring helps to detect anomalous behaviors or prevent a possible failure of the system caused by an attack. A possible solution to know whether the system is being attacked is to check an unjustified overload in the processor, an excess in the network traffic or a drastic reduction on the memory or hard disk. Besides, it is convenient to employ audit solutions/tools in the SCADA network components to track suspicious actions and/or to discover malicious evidences, in addition to determine the scope of the attacks in the critical environments.

The HIDS (Host Intrusion Detection Systems) allow the system to detect and mitigate common attacks through detection of anomalous behaviors. Their main goals are to prevent the execution of suspicious applications, to interrupt any suspicious software that tries to capture information, to avoid any physical access to memory or disk, and so on. Obviously, the application of these solutions in a SCADA system has to be carefully considered, since they could damage the performance of certain essential functionalities. As general rule, most of these solutions include an initial learning mode in order to create a 'right behaviour' baseline configuration, which will provide a set of authorization rules that alert of future anomalous actions.

7.- Conclusions

A SCADA system is considered a critical control system since it monitors and controls the performance and availability of other critical infrastructures, such as transport systems, energy suppliers, water treatment systems or communication systems. A disturbance in any (hardware and software) component because of a failure (technical or human) or an attack (physical or logical) could result in an unforeseen chain of events that affect other infrastructures, expanding towards other sectors and affecting the performance of a region, nation or nations. These effects are caused by the (direct or indirect) interdependencies among infrastructures [1].

It is then necessary and crucial to resolve and mitigate a few problems already identified in these types of control systems, as well as establish mechanisms, policies, standards and security procedures. All of them will make possible the protection of the system from a physical level (installations, communication networks and resources) to a logical level (software and communication channels). Nowadays, several documents and articles have been published describing disadvantages and a few and possible solutions. However, and due to the criticality of these systems, it is necessary to have an updated visualization of new security problems and technical recommendations.

We have identified and described in this paper diverse security management procedures in the SCADA communication networks and access controls, identifying important necessities, such as: specification of standards, security policies, roles and responsibilities, and design and implementation of secure network architectures. Nonetheless, it is very important to take into account other crucial factors in these critical systems: the risk management (a tool could be the RiskMAP to provide support in decision-making and actions [40]), incidence management for future analysis and forensic investigations, document management, evaluation metrics and methodologies, proliferation of training programs, maintenance and inspection.

8.- Acknowledgments

This work has been funded by the Ministry of Education and Science of Spain under the investigation projects CRISIS (TIN2006-09242) and ARES (CSP2007-00004).

References

[1] **James P. Peerenboom and Ronald E. Fisher**, *Analyzing Cross-Sector Interdependencies*, 40th Annual Hawaii International Conference on System Sciences (HICSS '07), IEEE Computer Society, pp. 112-119, 2007.

[2] **V. Igure, S. Laughter and R. Williams**, *Security issues in SCADA networks*, Computers & Security 25, v 25, pp 498-506, num 7, 2006.

[3] **R. Chandia, J. Gonzalez, T. Kilpatrick, M. Papa and S. Shenoi**, *Security Strategies for SCADA Networks*, IFIP International Federation for Information Processing, Critical Infrastructure Protection, Springer Boston, v 253, pp 117-131, 2007.

[4] **M. Hentea**, *Improving Security for SCADA Control System*, Interdisciplinary Journal of Information, Knowledge, and Management, v 3, pp 73-86, 2008.

[5] **Modbus-IDA** the architecture for distributed automation, http://www.modbus.org/, 2005.

[6] **DNP3**, DNP Users Group, http://www.dnp.org, 2008.

[7] **IEC 60870-6**, International Electrotechnical Commission

[8] **ODVA**, Open DeviceNet Vendors Association, http://www.odva.org/, 2008.

[9] **A. Cárdenas, S. Amin and S. Sastry**, *Research Challenges for the Security of Control Systems*, 3rd USENIX Workshop on Hot Topics in Security (HotSec'08), San Jose, USA, 2008,

[10] **CERT**, Carnegie Mellon Software Engineering Institute, CERT/CC Statistics 1988-2008, http://www.cert.org/stats/vulnerability_remediation.html, 2008.

[11] **BCIT**, British Columbia Institute of Technology, http://www.bcit.ca/, 2008.

[12] **E. Byres and J. Lowe**, *The myths and facts behind cyber security risks for industrial control systems*, 'VDE Congress, VDE Association For Electrical, Electronic Information Technologies, British Columbia Institute of Technology and PA Consulting Group, 2004.

[13] **DEADBOLT**, Institute for Information Infrastructure Protectio (I3P), http://www.thei3p.org/docs/publications/factsheet-Deadbolt-2-24-08.pdf, 2008.

[14] **NIST Special Publication 800-53**. *Recommended Security Controls for Federal Information Systems*. Diciembre 2007.

[15] **ISO/IEC 17799:2005**. *Code of Practice for Information Security Management*. 2005.

[16] **ISACA**. *Control Objectives for Information and related Technology, rev 4.1*. 2007.

[17] **NIST Special Publication 800-82**. *DRAFT - Guide to Industrial Control Systems (ICS) Security*. 2007.

[18] **D. Kilman, J. Stamp**. *Framework for SCADA Security Policy*. Sandia National Laboratories report SAND2005-1002C. 2005.

[19] **U.S. Department of Energy**, *21 Steps to Improve Cyber Security of SCADA Networks*, white paper, 2005.

[20] **SecSS**, Institute for Information Infrastructure Protection (I3P), http://www.thei3p.org/docs/publications/factsheet-SecSS-2-21-08.pdf, 2008.

[21] **R. Roman, C. Alcaraz and J. Lopez**, *The role of Wireless Sensor Networks in the area of Critical Information Infrastructure Protectio*n, Information Security Technical Report, Elsevier. Vol 12, no 1, pp 24-31, 2007.

[22] **ISA100**, Wireless Systems for Automation, http://www.isa.org/MSTemplate.cfm?MicrositeID=1134&CommitteeID=6891, Industrial Automation and Control system (ISA), 2007.

[23] **WirelessHART™ technology**, , HartComm Company

[24] **NISCC**, National Infrastructure Security Co-ordination Centre, *NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks*, British Columbia Institute of Technology (BCIT), 2005.

[25] **Modbus Software**, Linux Firewall for Modbus/TCP protocol, http://sourceforge.net/projects/modbusfw, 2008.

[26] **Vattenfall**, http://www.vattenfall.se/www/vf_se/vf_se/518304omxva/525894stude/525924exame/564400exemp/833879firew/index.jsp, 2007.

[27] **IEC 60870-5**, International Electrotechnical Commission

[28] **EMERALD**, Event Monitoring Enabling Responses to Anomalous Live Disturbances, SRI International, http://www.sdl.sri.com/projects/emerald/, 2007.

[29] **IDS Signatures**, Digital Bond, http://www.digitalbond.com/index.php/research/ids-signatures/, 2007.

[30] **Nessus 3 SCADA**, Tenable Network Security, http://blog.tenablesecurity.com/2006/12/nessus_3_scada_.html, 2006.

[31] **D. Nicol, B. Sanders and M. Seri**, *Access Control Policies and their Impact on Survivability*, Process Control Systems Workshop, The 4th Annual I3P PCS Security, 2008.

[32] **P. Tsang and S. Smith**, *YASIR: A low-latency high integrity security retrofit for legacy SCADA systems*, 23rd International Information Security Conference (IFIC SEC), 2008.

[33] **IEC-62351**, International Electrotechnical Commission.

[34] **AGA-12 Part 1**, *Cryptographic Protection of SCADA Communications Part1: Background, Policies and Test Plan*, 2006.

[35] **AGA-12 Part 2**, M. Hadley, K. Huston, *Performance Test Plan, Pacific Northwest National Laboratories*, 2006.

[36] **R. Lambert**, *ECC and SCADA Key Management*, SCADA Security Scientific Symposium Conference, Digital Bonded., 2007.

[37] **L. Cambacédes and P. Sitbon**, *Cryptographic Key Management for SCADA Systems -Issues and Perspectives*, pp 156-161, IEEE Computer Society, Information Security and Assurance (ISA) 2008.

[38] **D. Morrill**, *Everybody Panic Metasploit does SCADA Hacking*, Information Technology Professional IT Community, http://it.toolbox.com/blogs/managing-infosec/everybody-panic-metasploit-does-scada-hacking-27104, 2008.

[39] **K. Finisterre**, *The Five Ws of Citect ODBC Vulnerability CVE-2008-2639*, http://www.milw0rm.com/papers/221, 2008.

[40] **RiskMAP**, Institute for Information Infrastructure Protection (I3P), http://www.thei3p.org/docs/publications/factsheet-RiskMap-2-22-08.pdf, 2008.

Biographies

Cristina Alcaraz is currently a PhD student and got her MSc degree on Computer Science from University of Malaga in 2006. Her research interests focus on Critical Information Infrastructures Security and control systems security.

Gerardo Fernandez is currently a PhD student and got her MSc degree on Computer Science from University of Malaga in 2006. His research interests focus on intrusion detection and prevention, network security and vulnerabilities management.

Rodrigo Roman received the MSc and PhD degrees in Computer Science from University of Malaga in 2004 and 2008, respectively. His main research interests are WSN and ubiquitous security, as well as Critical Information Infrastructures Security.

Angel Balastegui received the BSc in Computer Science from University of Malaga in 2008. Since 2006 he collaborates as research student in different security projects in the Computer Science Department.

Javier Lopez is full professor in the Computer Science Department, where he joined in 1994. He has leaded different Spanish and European research projects in the area on Information and Communications Security. He is a member of the editorial board of several international publications.