Key Vulnerabilities of Industrial Automation and Control Systems and Recommendations to Prevent Cyber-Attacks

http://dx.doi.org/10.3991/ijoe.v12i01.4888

I. Calvo[1], I. Etxeberria-Agiriano[1], M.A. Iñigo[2], P. González-Nalda[1]
[1] University of the Basque Country (UPV/EHU), Vitoria-Gasteiz, Spain
[2] University of the Basque Country (UPV/EHU), Bilbao, Spain

***Abstract*—Until recently, Industrial Automation and Control Systems (IACS) were largely isolated from corporate systems by means of proprietary protocols, which facilitated their protection against cyber-attacks under the principle of security through obscurity. However, the widespread adoption of the new communication technologies, such as the Internet protocols and wireless communications has changed this scenario.**

In recent years there have been many evidences of cyber-attacks to IACS that exploit their vulnerabilities. Unfortunately, these attacks have increased significantly during the last five years, and quite clearly only the tip of the iceberg comes to the public knowledge.

The purpose of this article is twofold: (1) to raise awareness about the security vulnerabilities that most companies are facing at their IACS and (2) to propose a roadmap that seeks to guide designers and programmers in the new and complex world of industrial cyber-security.

***Index Terms*—Cyber-security, Cyber-attacks, Vulnerabilities, Industrial Automation, Industrial Communications.**

I. INTRODUCTION

Industrial Automation and Control Systems (IACS) cover various types of control systems including Supervisory Control And Data Acquisition (SCADA) and Distributed Control Systems (DCS) that acquire data from industrial processes by means of different specific devices such as Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs) or other Intelligent Electronic Devices (IEDs) that collect data from production processes.

The introduction of new technologies and different types of communication systems in industrial environments has produced a significant progress in the field of Automation and Control. They have significantly improved the possibilities of SCADA systems for monitoring many critical infrastructures in real time in different domains such as energy, transport, water, chemical processing, oil and gas. The landscape has been expanded by offering communication and connectivity to any industrial device, especially with the introduction of Internet technologies [1, 2]. With regards to connectivity through wireless networks, according to Boyes [3] they were used by 43% of the operators in 2011. Their installation was forecast to grow a 20% in three years.

The introduction of the so-called Information and Communications Technologies (ICT) in the industrial sector has become a challenge for engineers and researchers who have been actively seeking and developing Internet-based solutions while improving the automation processes in operational terms [4], including, the remote supervision and monitoring of the industrial processes guaranteeing the flow of information and real-time performance [1, 2].

In this scenario, new solutions based on the Cloud-Computing paradigm allow researchers to work by using Service-Oriented Architecture interfaces. These approaches introduce new concepts and paradigms identified as Internet of Things (IoT) aimed at connecting ICT infrastructure with different devices including industrial sensors, smart meters, Radio-Frequency Identifiers (RFID) and smartphones by means of different wireless technologies [5].

These new settings have promoted modifications in the creation and management of industrial networks. Traditionally, automation systems were isolated from the outside world and the Internet so that the information transmitted from process networks to office networks was minimal [6]. However, the increasing demand for these services regardless of the access point (e.g. remotely) as well as the total connectivity inside the enterprise systems has compromised the security of IACS. As a consequence, in former systems the adoption of proprietary hardware and software ensured a high degree of data security. Nowadays, on the contrary, IACS networks must face similar threats to those found at corporate systems while satisfying more stringent requirements in terms of performance (e.g. alarm distribution). Figure 1 shows a typical scenario where production networks are connected to the corporation network [7].

Unfortunately, the situation is quite complex and the security measures needed in modern IACS may not be the same as in corporate network systems, due to the special real-time and performance requirements of production systems. For example, full availability 24/7 of the equipment, which is a typical requirement in some installations, complicates certain security measures such as software updates, since they may require system stops and/or reboots.

There are also threats caused by the misuse of the equipment by internal staff. One example was the incident after infection with the Mariposa botnet through a USB connection which took three weeks to recover the plant

[8]. This is why a comprehensive security plan that involves all the company staff is required.

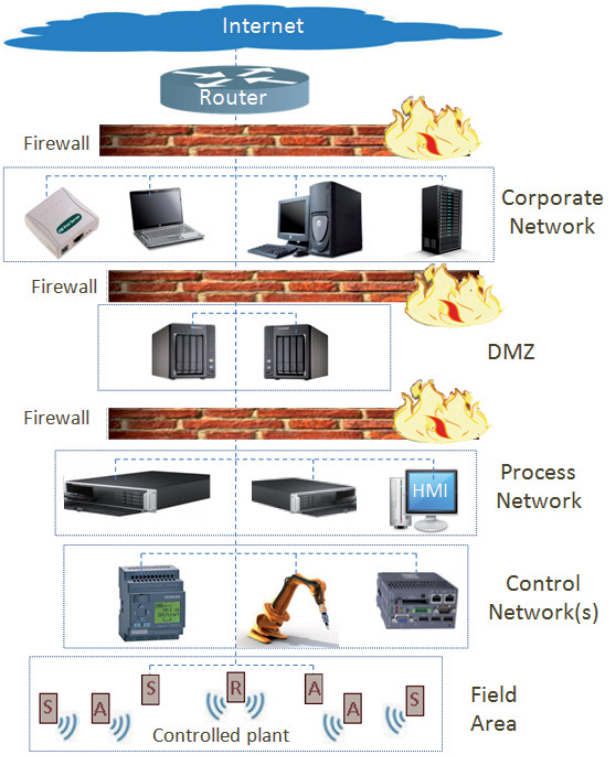

Figure 1. Typical communications of IACS with corporate networks and the Internet

In the following sections we analyze the peculiarities of IACS communications, identifying major key vulnerabilities regarding cyber-attacks. A series of countermeasures are proposed in order to provide greater security in the operation of such systems. The article ends up with final conclusions.

II. INDUSTRIAL COMMUNICATIONS

This section describes the hierarchical structure of industrial networks and its communication requirements.

A. Features

IACS are typically structured hierarchically in several layers according to the automation pyramid (Figure 2). Each layer must guarantee different requirements in terms of operation and performance, both for the systems themselves and the communication protocols. This was established as the ISA-95 standard [9], which integrates different kind of networks, some of them proprietary, such as field and control networks, with IP-based networks, local area networks and Internet [10].

Communication protocols use as reference the basic 7 level OSI (Open System Interconnection) model architecture, ISO/IEC 7498-1 [11], developed by the International Standards Organization. Conversely, the communications protocols used in industrial systems are typically proprietary and specific depending on the automation pyramid level where they are used.

Broadly speaking, these protocols can be classified into the following hierarchy:

- *Plant level*, connecting network segments at supervision level, monitoring and corporate systems.
- *Control level*, distributing information from field devices to controllers and from the drivers themselves.
- *Device-field level*, distributing data from sensors and actuators to controllers and field devices.

Network architectures used in industrial automation systems differ from those used at office. For example, at the lowest levels, a multitude of protocols and/or physical means are used. Even when they are similar or identical to those used in office networks, gateways are required in order to facilitate the communication with upper layers. On the contrary, in management systems the protocols and physical media used tend to be less diverse.

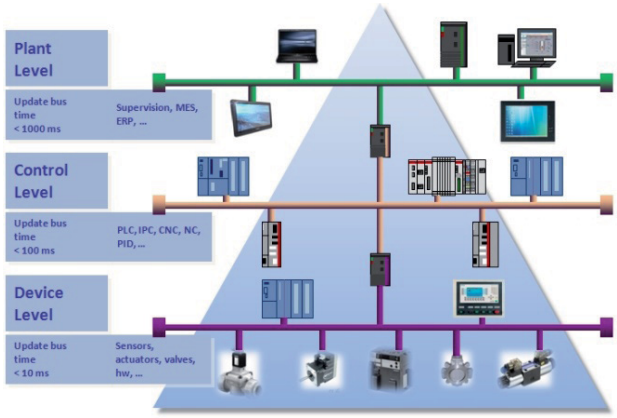

Figure 2. Automation pyramid

B. Special requirements of IACS protocols

Most industrial protocols have to satisfy real-time requirements, which may be classified as:

- *Soft*, with scalable cycle time used in the plant level and process automation when no severe consequences if deadlines are not met
- *Hard*, with cycle times of between 1 and 10 ms [12] used for closed loop time-critical control
- *Isochronous*, with cycle times of 250µs to 1ms, with severe restrictions on the fluctuation (typically less than 1µs), that are used for motion control applications

These real-time requirements depend on the performance of the communication protocols, which in turn depend on the following four parameters:

- *Latency*: time taken by a packet to traverse a network
- *Jitter*: latency variability in time
- *Throughput*: amount of data delivered per unit of time
- *Bandwidth*: maximum possible throughput according to the network capacity

Typically, IACS networks are required to be predictable, so they must provide:

- Low latency
- Constant and low jitter

Unfortunately, some measures introduced to improve the IACS security needs can significantly affect the performance of these parameters.

III. VULNERABILITIES OF IACS

According to a report generated for IACS by the ICS-CERT (Industrial Control Systems Cyber Emergency Response Team), the number of incidents in 2012 increased fivefold since 2010 [13] as illustrated in Figure 3. One of the most notorious cases was the Stuxnet worm discovered in 2010. This malware operated for three years without being detected, inducing physical damage to industrial infrastructure [14]. The potential of cyber-attacks to modern cars has been analyzed at [15]. Another study carried out over several (exactly 291) USA energy sector companies, showed that 76% of them suffered one or more security incidents in 2010 [16]. These and other incidents have led governments, communities and researchers to begin paying special attention to security in IACS.

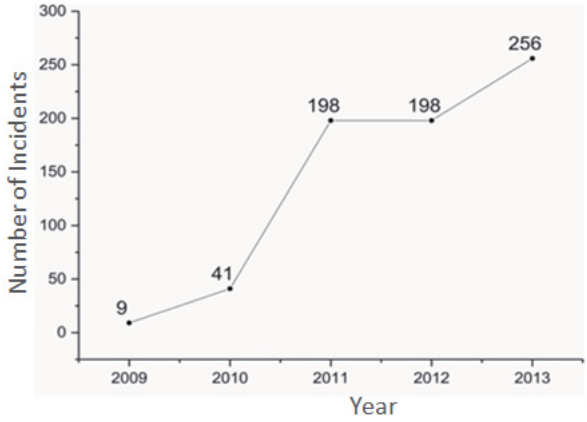

Figure 3. Evolution of the number of incidents [17]

It is important to note that cyber-attacks on industrial equipment refer to security issues and not safety [18], although obviously security failures may also cause safety failures. In many cases these cyber-attacks exploit IACS vulnerabilities, which can be classified into the following categories based on [19] and [20]:

- Policies and procedures
- Platform and applications
- Network
- Communication Protocols

A. Security Management Policies and Procedures

Vulnerabilities related to policies and procedures for IACS are related to:

- Poor or inadequate management of the security policy for the IACS, with no specific documented procedures
- Nonexistent formal definition of an awareness program and safety training aimed at the company staff
- Inadequate or deficient security guidelines to implement the IACS
- Insufficient or nonexistent IACS technology audit
- Lack of contingency planning in case of a disaster
- Change management of the specific IACS configurations

B. Hardware and Software Platform and Applications

Platform vulnerabilities are due to hardware, software and malware protection software of the platform. The most prominent vulnerabilities are related to:

- Outdated equipment and software, often more than 15 years old [6]
- Use of default settings
- Lack of backups of the critical configurations
- Configuration loss due to several reasons such as power outages, surges or spikes
- Inappropriate configuration for remote access
- Inadequate authentication control at equipment and software level (e.g. nonexistent access control or ill-defined passwords)
- Flaws in the platform software components that may produce buffer overflow [21] or Denial-of-Service (DoS) [22] vulnerabilities
- Inadequate or nonexistent measures to protect from malware
- Improper configuration of the operating system, e.g. bad memory management or activation of unnecessary services (daemons)
- Bad application design

C. Network Configuration

Network vulnerabilities may be caused by the network configuration, hardware, perimeter monitoring, communications authentication or wireless connections, as follows:

- Ill-designed network architecture without adequate security measures
- Not stored network settings or lack of backup
- Absence or poor authentication mechanisms at the protocol level (e.g. between the wireless client and the access point)
- Bad management of network passwords: use of defaults; unencrypted passwords; not changed periodically
- Use of insecure physical ports
- No definition of the security perimeter
- Missing or improperly configured firewall
- Network control settings not adequate for the IACS requirements
- Nonexistent network traffic monitoring
- Use of standard protocols such as Telnet or FTP without encryption mechanisms
- Nonexistent integrity checking (i.e. non allowed devices)
- Absence of protocol encryption for data protection (e.g. in wireless connections)

D. Protocols

It is important to note that some of the network vulnerabilities are intrinsic to the protocols used in wired and wireless communications, such as:

- Lack of message authentication
- Lack of message encryption
- Denial-of-Service (DoS) attacks
- Buffer overflow
- Man-in-the-Middle (MitM) attacks

Since some of these vulnerabilities are specific from the computer science domain and may be not common for control engineers, a short explanation is provided below.

A *DoS attack* occurs when a malicious event threatens the availability of a resource. It is a very broad category of attack that can range from the loss of communication with a device to inhibiting or crashing specific services within the device itself (such as storage or I/O processing). DoS attacks on corporate systems have significant negative consequences; indeed, a well-directed DoS system can disconnect and cause system shutdown.

A buffer is a continuous memory allocated for a process where its data is stored. A *Buffer overflow* occurs when written data corrupts the values of adjacent addresses to the allocated buffer due to insufficient space. This allows overwriting the data path control logic programming to hijack the program and run the attacker program.

MitM attacks are one of the most popular and challenging threats in computer systems. A lot of research has been dedicated to the detection and analysis of the different forms of these attacks [23, 24, 25, 26, 27]. In a MitM attack an intruder intercepts messages exchanged between two parties being able to read and write on them without either party being aware of it. This mode of attack has evolved with new technological advances.

IV. SECURITY GUIDELINES

This section introduces some guidelines aimed at highlighting which security aspects should be considered during the design process of automation systems. Should security not taken into account at this stage (i.e. security by design), it becomes an often-tried and often-fail trial an error process. However, it is important to be fully aware that it is impossible to produce a totally secure system against any type of cyber-attack.

Much research is being carried out in this area. The NIST standards organization provides some design strategies in this respect [19]. Risks and vulnerabilities are studied in [20]. In the USA the ICS-CERT [13] aims at reducing risks within and across all critical infrastructure sectors. Similarly, in the UK the Centre for the Protection of National Infrastructure (CPNI) provides protective security advice [32].

The adoption of the Industrial Internet around the world is being studied by the Industrial Internet Consortium. In [33] it is presented a document intended to broaden understanding about the major architectural issues and to create consensus with particular attention on security, trust and privacy in industrial environments.

These cyber-security guidelines are aimed to technical and non-technical profiles in order to show with a clear and easy-to-understand language which are the major points to consider, from the cyber security perspective, when building IACS.

There are several ways to protect IACS from external threats related to the above-described vulnerabilities. We have classified them into the following blocks:

- Network architecture
- Firewall configuration
- Access control and secure communications
- Monitoring IACS networks
- Malware prevention
- Policies and procedures
- Security Audit

A. Network architecture

As depicted in Figure 1, corporate and IACS networks must be separated in order to improve computer security using different configurations. These require the use and implementation of one or more firewalls and the creation of a Demilitarized Zone (DMZ) [28].

A *DMZ* is an isolated area that corresponds to a private network between the corporate network and the outside. When properly configured, DMZs prevent external users from directly accessing the computational resources inside this area, providing higher security, control and filtering capability.

For an acceptable security solution two areas may be implemented using two firewalls but they must be deployed with extreme caution. The most secure, manageable and scalable solution for the segregation of an IACS and a corporate networks is typically based on the creation of at least three areas, incorporating one or more DMZs as shown in Figure 4.

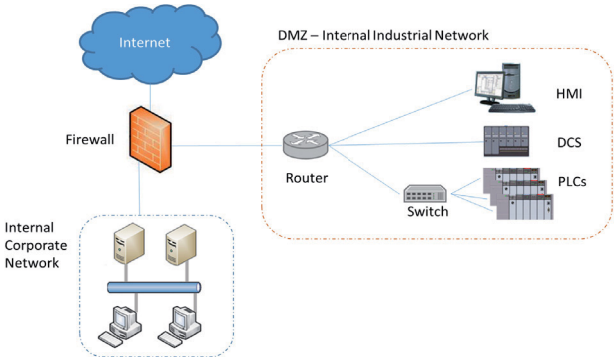

Figure 4. Basic scheme of a DMZ with Firewall.

B. Firewall configuration

A properly configured firewall can greatly restrict unwanted access to and from computers and host controllers of the IACS, improving safety and potentially improving the responsiveness of a control network by eliminating non-essential network traffic.

Its configuration allows the creation of rules for specific services such as DNS, HTTP, FTP or TFTP, Telnet, SMTP, SNMP, DCOM, SCADA and industrial protocols. For IACS a number of issues related to the firewall configuration must be considered, such as remote access, multicast traffic, single points of failure, MitM attack prevention, fault tolerance and redundancy.

A very basic configuration that works in many cases, in spite of the performance penalty caused by the firewall, includes the following rules:

- Denying all communications except those marked as known and accepted
- Specifying source and destination IP addresses
- Using inspection data to monitor active connections and decide which packages are authorized
- Using deep packet inspection to monitor the content of the communication traffic and not just the headers

Using different protocols in separate networks when possible, e.g. between the corporate network and the DMZ and between the DMZ and the IACS networks as shown in Figure 5.

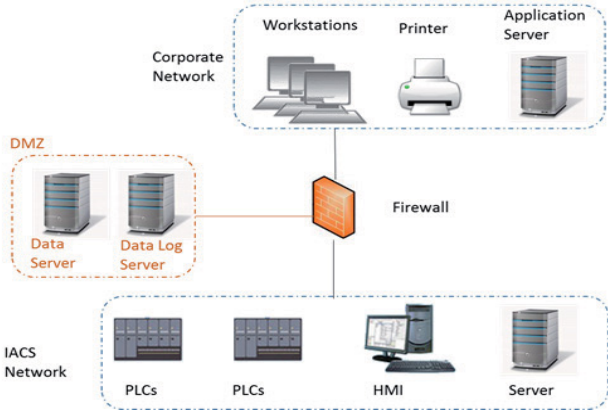

Figure 5. Firewall with DMZ between Corporate and IACS Network [19]

C. Access control and secure communications

Access control includes authentication and authorization policies in order to manage network access and secure remote access. Another important issue is the introduction of encryption techniques for sending critical data.

Authentication and authorization policies introduce protection mechanisms in applications by verifying the user's unique identity (authentication) and granting access to devices and operations (authorization).

Security measures should provide any kind of network access authentication mechanisms. Frequently, IACS devices only include low authentication capacity mechanisms. A higher security level should include not only the use of something the user knows (e.g. a password) but also something the user has or is (such as certificates or any biometric characteristic) in order to ensure that the user is really who claims to be.

Access control must allow identifying the access mode and origin, by following the recommendations of unique identification, role-based authorization and principle of least privilege with limited connections, filtering by ports, applications and users, and encrypted communications.

In this scenario, the creation of Virtual Private Networks (VPNs) is recommended to secure the traffic between end points and thus prevent information from being captured. In such networks it is necessary to encrypt data going from one point to another. Encryption is a transformation process using an algorithm that provides information that can only be decrypted by means of a key. VPNs may be based on IPSec [29] as well as other mechanisms described in [30]. Also, the use of secure protocols such as SSH or SFTP is recommended for all connections.

It is recommended to use most frequent industrial protocols without sending and receiving information to/from the corporate network. The creation of different work areas with rules through Firewalls and traffic monitoring would allow access control.

Special caution should be exercised with encryption mechanisms since they may overload processing elements and cause DoS of the involved devices. In addition, the effects of the introduced latency and jitter must be considered to meet the requirements of real-time applications.

D. Monitoring IACS networks

Aggressors may attack some specific field devices of an IACS (weak points) in order to collect information not only from this process device but the network itself, compromising the whole system. In most cases, the steps carried out by the attacker typically generate network and device activity, which can be tracked by specialized systems.

Intrusion Detection Systems (IDS) allow monitoring networks to detect misuse or abnormal operations. In the first case network connections are compared with large databases of known attack signatures. In the second case a baseline is defined comparing its performance with other network segments to detect abnormalities.

In any case, it must be defined which are the patterns to monitor, analyze logs and compare and make decisions. Some classic rules include the following:

- Blocking all datagrams of IACS network protocols with wrong size or length
- Blocking of all network traffic incoming/outgoing from/to any area that is not expected or not allowed
- Blocking of IACS network protocol packages that are detected in an area where they are not expected or allowed
- Alerting of failed authentication attempts and abnormal situations

E. Malware prevention

Malware is any malicious or annoying software that can be installed in computer systems to perform actions without the knowledge of the users. There are different types of malware, including viruses, worms, Trojan horses, spyware and adware.

Antimalware packages analyze files on storage devices and compare them with an inventory of known malware signature files. Antimalware software can be deployed on workstations, servers, firewalls and handhelds. Their use in IACS requires the adoption of special practices, including compatibility checks, change management and performance impact metrics.

Special care should be taken with conventional antimalware software to avoid compromising the real time responsiveness of the systems. Only specific solutions should be considered for this kind of systems.

Inside of an IACS network, the introduction of Malware should be centralized by means of a Malware o Antivirus server in DMZ as shown in Figure 6. The configuration of the devices could be grouped so it would be possible to easily separate critical and non-critical devices and analyze.

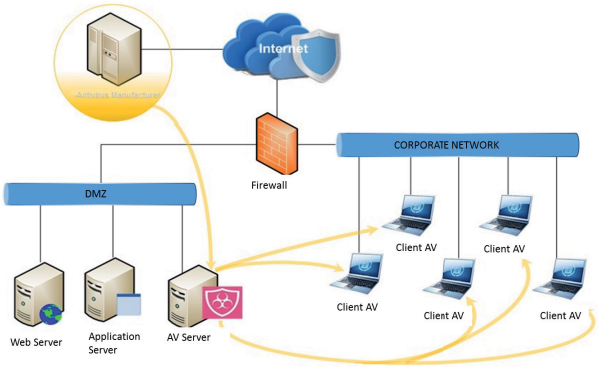

Figure 6. Scheme of centralized Antivirus. (Based on [31])

F. Policies and procedures

For a successful security strategy in IACS the policies and procedures for deployment and use must be documented and disseminated among employees with at least an annual review. It should be the first step to ensuring IACS networks. Sometimes, in order to secure IACS networks, similar policies to those used for securing corporate information systems can be directly applied.

An effective security policy it must be practical, applicable and should not significantly impact productivity, with no prohibitive cost or lack of support. Moreover, IACS system administrators must have technical knowledge but also need authorization and management support to implement these policies.

The issues to consider in a policies and procedures document are the following:

- Definition of aims, scope and duration
- Definition of the security responsibilities for every role and user
- List of devices with their functionalities and installed software
- Definition of network architecture and firewalls as well as developed rules
- List of users, roles and access privileges
- Description of vulnerabilities and prevention plan
- Definition of a hardware and software updating plan
- Definition of a backup and recovery plan
- Definition a safety training plan.

G. Security Audit

An audit is an independent review to assess the adequacy of the safety mechanisms implemented in IACS. Audits also evaluate the compliance of the established policies and operational procedures in order to know their suitability. A study that analyzes the major strengths and weaknesses along with some recommendations must be developed. This study aims at finding any necessary changes in policies, procedures and security measures.

In order to perform the audit it is necessary to carry out the following items:

- List of implemented hardware, software, services, security measures and network architecture
- Review and assess
- Logs of sent and received packages
- Analyze access mode to the devices, applications and services along with the implemented security measures
- Procedure for making backups, upgrades and implementations
- Implementation efficiency in firewalls with rules and IDS.

Finally, in some cases it may be necessary to perform penetration tests in order to know and evaluate the response of the security systems with IACS in operational mode. White hat modalities may be compulsory in safety critical parts, i.e. together with the system designers.

Figure 7 summarizes the major cyber-security guidelines to take into account by any IACS organization. They are grouped in blocks according to the contents of section IV.

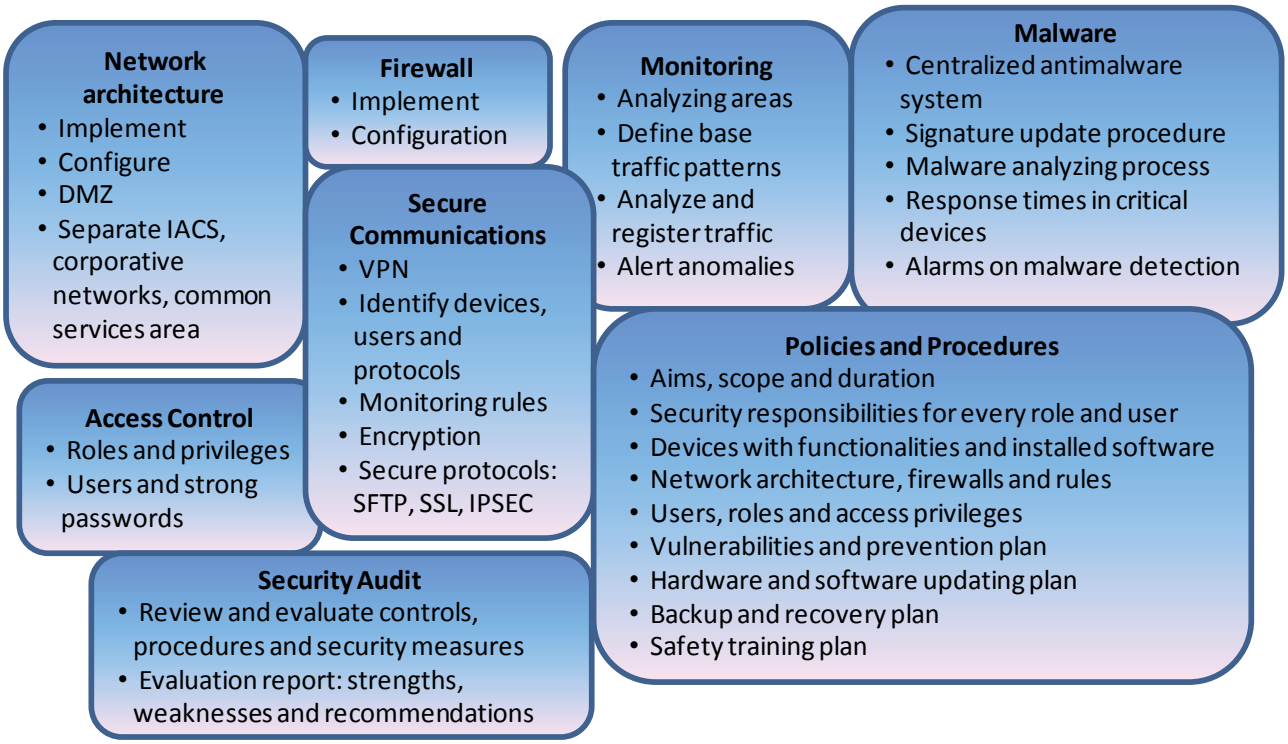

Figure 7. Cyber-Security guidelines for IACS

V. CONCLUSIONS AND FUTURE WORK

The introduction of the newest technologies in the Industrial Automation and Control Systems (IACS), including the emergence of Internet and TCP/IP based solutions, is risking the responsiveness, productivity and continuity of such environments, opening new issues and risks. Too often, these systems are threatened by cyber-attacks due to poor or nonexistent security measures. So far, most approaches have been based on using security by obscurity, implemented due to the isolation of these systems from systems external to them.

This article provides an overview of the topic by analyzing and classifying some of the most common vulnerabilities and types of attacks, such as lack of authentication, lack of message encryption, and Main-in-the-Middle or Denial of Service attacks.

It is important to note that it is impossible to get a totally secure system against cyber-attacks and, indeed, in the opinion of the authors, it is crucial to be fully aware of this premise. However, a collection of security recommendations have been introduced as a guide to point designers what aspects should be taken into account in the design of automation systems. It is also important to consider that many security measures require the introduction of sophisticated algorithms, such as data encryption, which can affect overall system performance.

However, the application of these measures has some costs: (1) a good approach for security requires rearranging the network architecture isolating those vital parts from possible external attacks when possible; (2) some specific software and hardware equipment must be needed (e.g. monitoring tools, malware prevention and detection systems), which sometimes must be provided by specific vendors; (3) some recommended techniques, such as encryption or deep packet inspection, may be computer intensive requiring the updating of hardware platforms and (4) since the resulting infrastructure is more complex, staff qualified in cyber-security will be increasingly demanded.

The authors are currently working and researching the encoding of different industrial protocols, in particular the effects of using VPN in real time systems, which is the best mode to update and patch management and which are the effects of using anti-virus programs in IACS environments.

As a final remark, it is necessary to implement global and in depth strategies through policies that affect both network and platform levels in order to provide certain security measures that may help control engineers to develop reasonable secure IACS.

REFERENCES

[1] I. Calvo, M. Marcos, D. Orive, I. Sarachaga, "A methodology based on distributed object-oriented technologies for providing remote access to industrial plants," Control Engineering Practice, 14 (8), pp. 975-990, 2006. http://dx.doi.org/10.1016/j.conengprac.2005.05.008

[2] T. Sauter, S. Soucek, W. Kastner, and D. Dietrich, "The evolution of factory and building automation," IEEE Industrial Electronics Magazine, 5 (3), pp. 35-48, 2011. http://dx.doi.org/10.1109/MIE.2011.942175

[3] W. Boyes, "All quiet on the wireless front," Control, August 2011, http://www.controlglobal.com/articles/2011/all-quite-on-the-wireless-front/

[4] M. Jain, A. Jain, and M. Srinivas, "A web based expert system shell for fault diagnosis and control of power system equipment," Proceedings of Intl. Conf. Condition Monitoring and Diagnosis (CMD-08), 2008, pp. 1310–1313. http://dx.doi.org/10.1109/cmd.2008.4580217

[5] S. Li, L.D. Xu, and S. Zhao, "The internet of things: a survey," Information Systems Frontiers, 17 (2), pp. 243-259, 2015. http://dx.doi.org/10.1007/s10796-014-9492-7

[6] K. Fischer and J. Gesner, "Security Architecture Elements for IoT enabled Automation Networks," 17th IEEE Intl. Conf. Emerging Technologies and Factory Automation (ETFA), 2012. http://dx.doi.org/10.1109/etfa.2012.6489651

[7] M. Cheminod, L. Durante, and A. Valenzano, "Review of security issues in industrial networks," IEEE Transactions on Industrial Informatics, 9:1, pp. 277-293, 2013. http://dx.doi.org/10.1109/TII.2012.2198666

[8] P. Sinha, A. Boukhtouta, V.H. Belarde, and M. Debbabi, "Insights from the Analysis of the Mariposa Botnet," 5th IEEE Intl. Conf. Risks and Security of Internet and Systems (CRiSIS), 2010. http://dx.doi.org/10.1109/crisis.2010.5764915

[9] B. Scholten, "The Road to Integration: A Guide to Applying the ISA-95 Standard in Manufacturing," Intl. Society of Automation (ISA), 2007.

[10] C. Schwaiger and A. Treytl, "Smart card based security for fieldbus systems," 5th IEEE Intl. Conf. Emerging Technologies and Factory Automation (ETFA), 2003. http://dx.doi.org/10.1109/etfa.2003.1247734

[11] Standardization, I. O. F. "ISO/IEC 7498-1: 1994 information technology–open systems interconnection–basic reference model: The basic model," International Standard ISOIEC 74981 (1996): 59.

[12] M.S. Branicky, S. M. Phillips, and W. Zhang, "Stability of networked control systems: Explicit analysis of delay," in Proc. American Control Conference (AACC), pp. 2352–2357, 2000. http://dx.doi.org/10.1109/acc.2000.878601

[13] ICS-CERT, "ICS-CERT Monitor Newsletters," October–December 2012. https://ics-cert.us-cert.gov/monitors

[14] G. McDonald, L.O. Murchu, S. Doherty, and E. Chien, "Stuxnet 0.5: The Missing Link," Symantec, Mountain View, California, 2013.

[15] S. Checkoway et al., "Comprehensive experimental analyses of automotive attack surfaces," Proc. 20th USENIX Conf. on Security, 2011.

[16] Ponemon Institute, "State of IT Security. Study of Utilities & Energy Companies", 2011.

[17] W. Yang and Q. Zhao. "Cyber security issues of critical components for industrial control system," Guidance, Navigation and Control Conference (CGNCC), IEEE Chinese, 2014. http://dx.doi.org/10.1109/cgncc.2014.7007593

[18] S. Kriaa et al., "A survey of approaches combining safety and security for industrial control systems," Reliability Engineering & System Safety, 139, pp. 156-178, 2015. http://dx.doi.org/10.1016/j.ress.2015.02.008

[19] K. Stouffer, J. Falco, and K. Scarfone, "Guide to industrial control systems (ICS) security," NIST special publication (2011): 800-82.

[20] E. D. Knapp and J. T. Langill, "Chapter 8 - Risk and Vulnerability Assessments," In "Industrial Network Security," (Second Edition), Syngress, Boston, 2015, Pages 209-260. http://dx.doi.org/10.1016/b978-0-12-420114-9.00008-3

[21] L. Feifei, "The principle and prevention of windows buffer overflow," 7th Intl. Conf. Computer Science & Education (ICCSE), 2012. http://dx.doi.org/10.1109/iccse.2012.6295299

[22] W. Liu, "Research on DoS attack and detection programming," 3rd IEEE Intl. Symp. Intelligent Information Technology Application (IITA), pp. 207-210, 2009. http://dx.doi.org/10.1109/iita.2009.165

[23] N. Asokan, V. Niemi, and K. Nyberg, "Man-in-the-Middle in Tunnelled Authentication Protocols," Security Protocols Workshop, volume 3364 of LNCS, pages 28-41. Springer, 2003. http://dx.doi.org/10.1007/11542322_6

[24] D. Kügler, ""Man in the Middle" Attacks on Bluetooth," Financial Cryptography, volume 2742 of LNCS, pages 149-161. Springer, 2003. http://dx.doi.org/10.1007/978-3-540-45126-6_11

[25] U. Meyer and S. Wetzel, "A man-in-the-middle attack on UMTS," Proc. 3rd ACM Workshop on Wireless Security (WiSe), pp. 90-97, 2004. http://dx.doi.org/10.1145/1023646.1023662

[26] B. Aziz, G. Hamilton, "Detecting man-in-the-middle attacks by precise timing," 3rd IEEE Intl. Conf. Emerging Security Information (SECURWARE), 2009. http://dx.doi.org/10.1109/securware.2009.20

[27] F. Callegati, W. Cerroni, and M. Ramilli, "Man-in-the-Middle Attack to the HTTPS Protocol," IEEE Security & Privacy, 7:1, pp. 78-81, 2009. http://dx.doi.org/10.1109/MSP.2009.12

[28] H. Flynn, *Designing and building enterprise DMZs*, Syngress, 2006.

[29] Y. Heng and H. Wang, "Building an application-aware IPsec policy system," IEEE/ACM Trans on Networking, 15:6 pp. 1502-1513, 2007.

[30] D. Hadziosmanovic, D. Bolzoni, P. Hartel, "A log mining approach for process monitoring in SCADA," Intl. Journal of Information Security (IJIS) 11:4 pp. 231–251, 2012.

[31] INCIBE, "Problemática de los antivirus en entornos industriales." https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/Problematica_antivirus_SCI. [Accessed: 21-Oct-2015].

[32] CPNI. Centre for the Protection of National Infrastructure. http://www.cpni.gov.uk/

[33] S.-W. Lin et al., "Industrial Internet Reference Architecture", Technical Report, Industrial Internet Consortium., 2015. http://www.iiconsortium.org/IIRA.htm

AUTHORS

Isidro Calvo is with the University College of Engineering of Vitoria-Gasteiz, Department of Systems Engineering and Automatic Control, University of the Basque Country (UPV/EHU), Spain, as Senior Lecturer (email: isidro.calvo@ehu.eus).

Ismael Etxeberria-Agiriano is with the University College of Engineering of Vitoria-Gasteiz, Department of Computer Languages and Systems, University of the Basque Country (UPV/EHU), as Senior Lecturer, (e-mail: ismael.etxeberria@ehu.eus).

Miguel Angel Iñigo Ulloa is an R&D project manager at Virtualware. In 2013 he studied Master in Control Engineering, Automation and Robotics at the Faculty of Engineering of Bilbao, University of the Basque Country (UPV/EHU) (email: minigo@virtualwaregroup.com)

Pablo González-Nalda is with the University College of Engineering of Vitoria-Gasteiz, Department of Computer Languages and Systems, University of the Basque Country (UPV/EHU), as Senior Lecturer, (e-mail: pablo.gonzalez@ehu.eus).

This work was supported in part by the University of the Basque Country (UPV/EHU) and the Basque Government (GV/EJ) by projects EHU13/42 and CPS4PSS ETORTEK14/10 respectively.

Submitted, 23 July 2015. Published as resubmitted by the authors on 30 October 2015.