A Concise Model to Evaluate Security of SCADA Systems based on Security Standards

Nasser Aghajanzadeh
School of Electrical and Computer Engineering,
Shiraz University, Shiraz, Iran

Alireza Keshavarz-Haddad
School of Electrical and Computer Engineering,
Shiraz University, Shiraz, Iran

ABSTRACT
SCADA systems are essential for the critical infrastructures, such as electric power, oil, and gas production and distribution systems. Hence, incapacitation or destruction of SCADAs would have a debilitating impact on the defence or economic security of organizations and states. In this paper, we study fifteen SCADA cyber security standards and also assess the security of ten widely-used SCADA systems. Our investigation leads to a comprehensive categorized list of security solutions for SCADAs. This list is used to evaluate and compare security of the SCADA systems; also it will be used as model to improve the security of new SCADA systems.

Keywords
Supervisory Control and Data Acquisition, SCADA, Cyber Security, Security Standard,.

1. INTRODUCTION
Supervisory Control and Data Acquisition (SCADA) systems are Industrial Control Systems (ICS) that are geographically distributed over a large region and typically controlled from a centralized location. SCADA Systems are wildly deployed over real-time infrastructure sectors such as water distribution and wastewater collection systems, oil and gas pipelines, electrical utility and distribution, rail and public transportation systems. These systems collect the information that is distributed over different locations and process to the main station, and monitor and control SCADA network devices using incoming/outgoing signals over a communication network such as Internet, Public Telephone Switching Network, Cellular Wireless Networks, Communication satellites, and so on.

SCADA systems have been used since more than 50 years ago. However, the researchers and system developers have started to seriously pay attention to the cyber security of SCADAs only recently, after experiencing several cyber incidents and attacks on these systems. In the past few years, many organizations have developed cyber security standards and guidelines for SCADAs used in various industries such as electrical power, chemical plants, oil and gas industries, nuclear plants. On the other hand, SCADA system developers have been also trying to improve security of their systems by adding some new security features. In this paper, we take a unifying approach to investigate cyber security of SCADAs based on the security standards and implemented security features in SCADA systems.

This investigation allows us to understand the gaps between the standards and practical systems which can aim to evaluate and improve the security of SCADA systems. We study security solutions suggested in fifteen major security standards and guidelines for SCADA systems. Also, we assess the implemented security solutions in ten widely used SCADA systems in the world. Next, we categorize, list, and prioritize all the security solutions. This categorized list can help us to concisely assess and compare security of the SCADA systems. In fact, our proposed collective model tries to use the experience and knowledge on the developers of security standards and SCADA systems to improve the security of the existing or new SCADAs systems.

The rest this paper is organized as following. In section 2, we review some related works. The security standards and guidelines are introduced and studied in section 3. The security feature of SCADA systems of major SCADA developers are described in section 4. In section 5, we analyze the gathered information from the standards and SCADA systems. Finally, we conclude the paper in section 6.

2. RELATED WORK
In the past few years, the security concerns of SCADA systems have been paid attention by governments, organizations, and academia. Many documents have been published to highlight the cyber threats, vulnerabilities, and solutions to improve cyber security in these systems. Here, we focus on some systematic and scientific researches to advance cyber security in SCADA systems.

In [1] Shahzad and Musa propose cryptographic algorithms to implement SCADA systems in cloud environment and performance of these algorithms are analyzed.

In [2] Lynch provides some security solutions according to the dependencies of physical, specifications of virtual, geographical and logical space and also the complexity of interaction of the various system components for improving security in SCADA systems. Some important security issues and risks in SCADA systems are described in [3]. The paper investigates many existing vulnerabilities SCADA systems according to the transition from old control systems to newer computer network based systems. Cagalaban investigates security of various protocols in SCADA's networks and infrastructures [4]. The paper also evaluates the reliability and accessibility of these systems. In [5] Valli states some basic practices in protecting the security of industrial networks and suggests the use of some technologies such as firewalls for improving the security networks of SCADA. Anokas provides some solutions for making a safe and sound communication in SCADA's systems and by the purpose of creating a new way for combining multiple communication channels like optical fiber, satellite networks and G2/3G/4G for creating a safe and fast relational solution [6]. In [7] Kumar introduces a variety of warnings and some solutions according to the technology of SCADA's module's connection and has investigated analog sensors with communication protocols by evaluating their role and has introduced some solutions for a more safe connection in SCADA's modules.

3. CYBER SECURITY STANDARDS FOR SCADA SYSTEMS

In this section, we study cyber security standards and guidelines for SCADA systems. First the security standards are introduced and then the security solutions are identified and the standards are compared with each other based on the proposed security recommendations.

3.1 Cyber Security Standards

Here, we briefly introduce main standards and guidelines for cyber security of SCADA systems [8]. These documents have been published by different organizations and some have focused on certain infrastructures. Some of the standards are more significant; though, we introduce them here in alphabetic order.

- **AGA**

AGA is the abbreviation for the American Gas Association. AGA was founded in 1918 and represents 202 local energy companies that deliver natural gas throughout the United States.

- **AGA 12 part 1**

The scope of AGA 12 part 1 is to describe the need for SCADA systems protection. It suggests some steps to define security goals and fundamentals. Moreover, the document defines the cryptographic system requirements and constraints, and a cryptographic test plan [9].

- **CPNI**

CPNI is the abbreviation for Center for the Protection of National Infrastructure. CPNI is a British agency that was created in 2007 [10]. Good Practice Guide, Process Control and SCADA Security This document aims to provide good practice principles for process control and SCADA systems security.

- **DHS**

DHS is the abbreviation for Department of Homeland Security. DHS is an US government agency created in 2002. The agency was formed from 22 other agencies [11].

Cyber Security Procurement Language for Control Systems

This document is supposed to give guidance to people that are either procuring a new system or procuring an update for an existing system. It summarizes which security principles must be considered when designing or procuring a new system [12]. Catalog of Control Systems Security: Recommendations for Standards Developers. This document is designed to provide various industry sectors the framework needed to develop sound security standards, guidelines, and best practices. It contains a listing of recommended controls for a number of resources. The main goal of this document is to be able to balance security while operating within resource limits [13].

- **DOE**

DOE is the abbreviation for Department of Energy which is a US federal agency. It was formed on in 1977 as a merge of the Federal Energy Administration, the Energy Research and Development Administration, the Federal Power Commission, and parts and programs of several other agencies [14].

21 steps to Improve Cyber Security of SCADA Networks

This is a short but very informative document summarizing 21 items that is important when securing SCADA systems. Some of the subjects brought up are: i) Identify all connections to SCADA networks ii) Do not rely on proprietary protocols to protect your system iii) Establish a network protection strategy based on the principle of defence-in-depth strategy vi) Establish system backups and disaster recovery plans [15].

- **GAO**

GAO is the abbreviation for Government Accountability Office which is an independent, nonpartisan agency that works for US Congress [16].

Cyber security for Critical Infrastructure Protection

This is a general document about critical infrastructure protection focusing on: i) What are the key cyber security requirements in each of the critical infrastructure protection sectors? ii) What cyber security technologies can be applied to critical infrastructure protection? [17]

- **IEEE**

IEEE used to be the abbreviation for Institute of Electrical and Electronics Engineers, now a days the organizations scope of interest has expanded into so many related areas [18], [19].

IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities

This standard deals with the cyber security of IEDs in substations. It gives requirements in four main areas. Electronic access control, audit trail, supervisory monitoring and control and configuration software [20].

IEEE Guide for Electric Power Substation Physical and Electronic Security

This standard discusses security issues related to human intervention during the construction, operation (except for natural disasters), and maintenance of electric power supply substations. It mainly deals with physical security as well as electronic security [21].

- **IEC**

IEC is the abbreviation for International Electro technical Commission. The IEC was founded in 1906 and is the leading global organization that prepares and publishes standards for electric, electronic and related technologies. IEC along with ISA (as we describe next) have published standards on cyber security of SCADA systems.

- **ISA**

ISA is the abbreviation for The Instrumentations, Systems, and Automation Society. ISA was founded in 1945.

ANSI/ISA–99.00.01–2007 Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models (equivalent with IEC 62443)

The scope of this document is to define the concepts and models for SCADA systems. It establishes the basis for the remaining standards in the ISA99-series [22].

ANSI/ISA-TR99.00.01-2007 Security Technologies for Industrial Automation and Control Systems

The scope of this document is to provide an assessment of security tools, mitigations, countermeasures and technologies that may be used in SCADA systems. The standard is divided into different areas with each area divided into different techniques. Each technique is divided into 8 sections, introduction, vulnerabilities addressed, typical deployment, known issues and weaknesses, how it is used in SCADA systems today, future directions, recommendations and guidance, references [23].

The areas covered are: Authentication and authorization, Filtering/Blocking/Access control, Encryption and Data Validation Management, Audit, Measurement and Detection

Tools, Industrial Automation and Control Systems Computer Software, Physical Security Controls

ANSI/ISA—TR99.00.02—2004 Integrating Electronic Security into the Manufacturing and Control Systems Environment

The purpose of this document is to present a consistent approach for developing, implementing and operating a program that addresses security for SCADA systems. It starts out with the basic process for creating a security program [24].

- **ISO**

ISO is the abbreviation for International Organization for Standards which is the world largest developer and publisher of standards. ISO is a network of national standard institutes and can be found in 157 countries [25].

ISO 17799: Information technology—Security techniques—Code of practice for information security management

This standard deals with general information security. The document contains best practices of controls in the following areas Security Policy Organizing, Information Security, Asset Management, Human Resource Security, Physical and Environmental Security, Communications and Operations Management, Access Control, Information Systems Acquisition, Development and Maintenance Information Security, Incident Management, Business Continuity Management. In each area a control objective is defined stating what is to be achieved. Then the different controls that can be used for the objective are presented [26].

- **NERC**

NERC is the abbreviation for North American Electric Reliability Corporation. NERC was founded in 1968 and is a self-regulatory organization, subject to oversight by the US Federal Energy Regulatory Commission and governmental authorities in Canada.

CIP-002-1 - CIP-009-1
CIP stands for Critical Infrastructure Protection. Power companies in the US are required to comply with the CIP standards1. There are eight standards providing a cyber-security framework for identification and protection of critical cyber assets. The purpose is to support reliable operation of the bulk electric system [27].

Guide to Industrial Control Systems (ICS) Security
The purpose of this document is to provide guidance for securing SCADA systems. The document provides an overview of SCADA systems, tries to identify the characteristics of an industrial control system (ICS), threats and the vulnerabilities. It also brings up the subject of how to develop and deploy and ICS security program.

System Protection Profile - Industrial Control Systems
A system protection profile is a document providing an implementation independent set of security requirements. This document does that for a generic industrial control system and lists a set of threats that should be addressed by security controls.

3.2 Security Solutions Recommended in the Standards

After introducing the standards and guidelines on SCADA cyber security, we study briefly review and categorize the security solutions. First, we provide a complete list of the proposed security solutions for SCADA systems. Then, we will use the list to concisely compare the standards based on the security solutions that they offer.

- Network security
- Network separation
- Risk management of security organization
- Firewall
- Education and knowledge
- Influence recognition
- Personnel's Management
- Encryption
- Programming for services after accidents and incidents
- Access permission
- Continuing business
- Authentication
- System flexibility
- Ant viruses
- Backup
- Management of security patches
- Managing Corporation with contractors
- Managing changes
- Standards and Politics of security system region
- Auditing and scanning of vulnerabilities
- Security basics
- System managing instruments
- Assets and properties

3.3 Comparing the Standards based the Security Solutions

By considering experience and knowledge of standards developers, this list specifies what security solutions have had most importance degree for them. From their point of view using these solutions for SCADA systems is an advantage for them as shown in Figure 1.

4. SECURITY OF SCADA SYSTEMS OF WELL-KNOWN DEVELOPERS

In this section, we study the security solutions used by ten well-known SCADA system developers in the world for creating and increasing security in these systems. In this level, our listed SCADAs will be studied and security solutions used by them will be categorized in separated lists for more concentration in addition to the searching in the main site of company and the brochure of this product had been checked. Also available versions of these products had been downloaded and rechecked

4.1 Security Solutions in various SCADA Systems

Here, we introduce ten well-known SCADAs and security solutions that are implemented in them. Table 1 describes a list of security solutions in these SCADA products

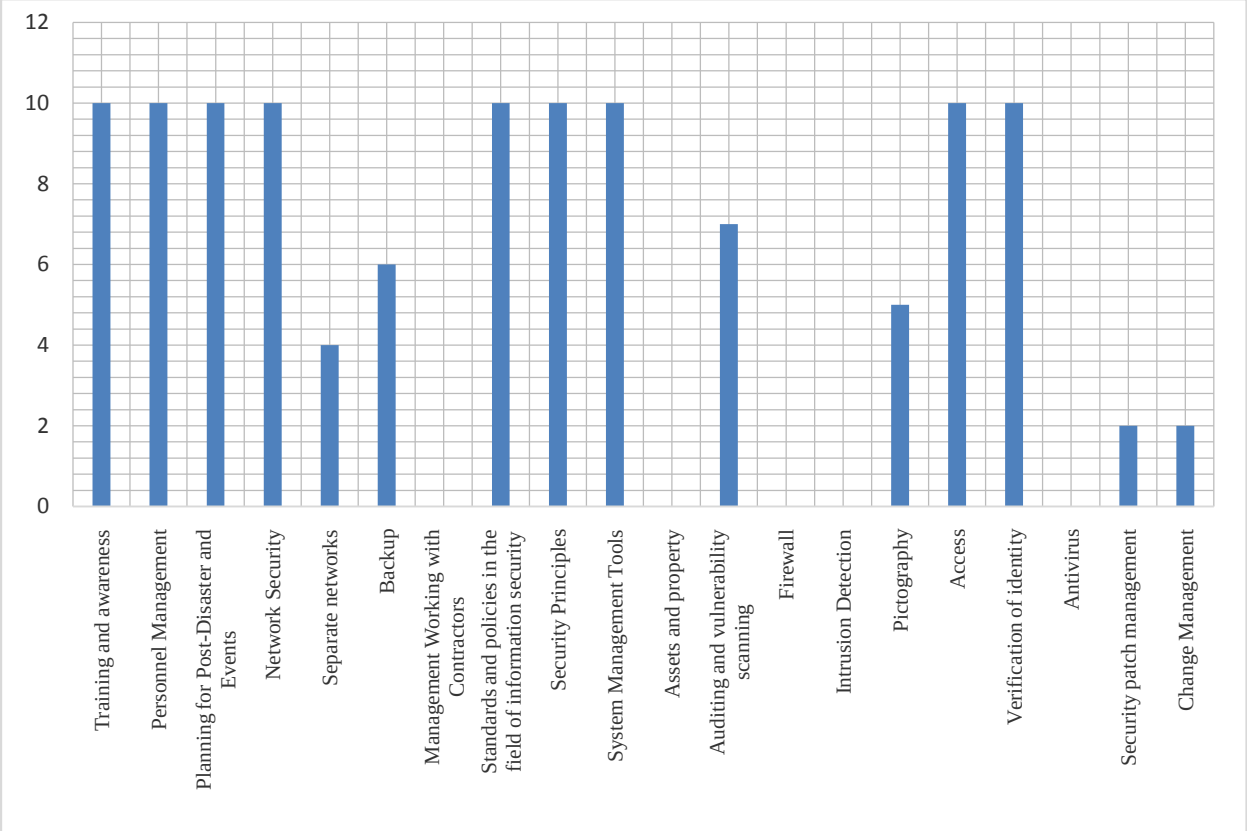

Figure 1: Number of standards that recommend a particular security solution

Table 1: The information related to SCADA's security systems

Name	Security solutions
Broadwin SCADA	*Using passwords *Making usernames *Individual virtual networks *Safe node's connection system *Security's region and levels
General Electric proficy CIMPLICTY	*Keeping a long history of transactions for visiting and checking *Access to APIs for doing special actions *Using biometric technology *electronically signature *Allowance for using system only by allowed connections *Encrypting data *Creating domain group and access permission *Using multiple parallel servers
Proficy HMI/SCADA–iFIX 5.5	*Keeping a long history of transactions for visiting and checking *Using biometric technology *Electronic signature *Allowance for using system only by allowed connections *Encrypting data

	*Creating domain group and access permission *Using multiple parallel servers
IGSS	*Keeping and fixing preventative integrated system *Using multiple parallel servers *Using username and access levels *Documentation of group members *Controlling work stations *Security layers *Auditing user's activity *Integrated system of safe order executive management *Individual virtual networks *Access to remote system
ICONICS GENESIS 32	*Categorizing personnel *Creating individual limitation *User's entrancing system *Auditing system
Ignition	*Using multiple parallel servers *Using SSL like banks and Financial Transactions *Reporting system of auditing *Acting specific commands after employer's verification *Encryption *User authentication *Creating access permission
RealFlex 5.2	*Encryption *Using multiple parallel servers * Management of security patches *Backup system and automatic performance in time of problems *Repeating data and attachment of additional data in communication time for data correction in error times of data communication
RealWin	*Encryption *Using multiple parallel servers * Management of security patches *Backup system and automatic performance in time of problems *Repeating data and attachment of additional data in data communication time for data correction in error times of data communication
OPC system NET	*Username and access point *Categorizing personnel *Auditing system

4.2 Categorizing security solutions in SCADA systems

We identified the security solutions used in the well-known SCADA systems in Table 1. Here we categorize the solutions and provide a list below. Note that the repeated solutions are omitted and similar solutions are stated in one category.

- User authentication
- maintenance of integrated preventative
- Creating access permission for users
- Performance management of essential orders
- Documentation of member's group activity
- Auditing systems
- Creating security levels
- Creating individual limitations
- Isolated system network
- Using SSL
- Access to remote control
- Using multiple parallel servers
- Encryption
- Determining identified connections for access
- Error correlation systems in data communication
- Encryption
- Individual virtual networks
- Managing security patches
- Determining limited performance for special node
- Using biometric technology
- Electronically signature

4.3 Emphasis on security solutions in SCADAs systems

Provided information in Table 1 for each SCADA is evaluated here to analyze the number of security mechanisms. By experience and knowledge of developer's considerations, this shows which SCADA systems implement more solutions. As shown in Figure 2, IGSS uses the highest number of security recommendations.

4.4 Use of recommended solutions by standards in SCADA systems

Here we analyse how many recommended security solutions by the standards and guidelines are have been implemented in the SCADA systems. By considering experience and high knowledge of standards creators in the world, this can indicate which SCADA system has higher security. As shown in Figure 2, CIMPILICITY, iFIX5.5, RealFlex 5.2 and RealWin mostly use security recommendations Figure 2: Number of different security solutions in the SCADA systems

Figure 3: Number of recommended solutions by the standards in SCADA systems

4.5 Comparing used rate of categorizing security solutions

Here the gathered information about SCADA systems is evaluated to obtain that each SCADA's security solutions rate as depicted in Figure 3. This list specifies what security solutions have higher importance degree for the SCADA developers. From their point of view using these solutions for SCADA's systems is an advantage for them.

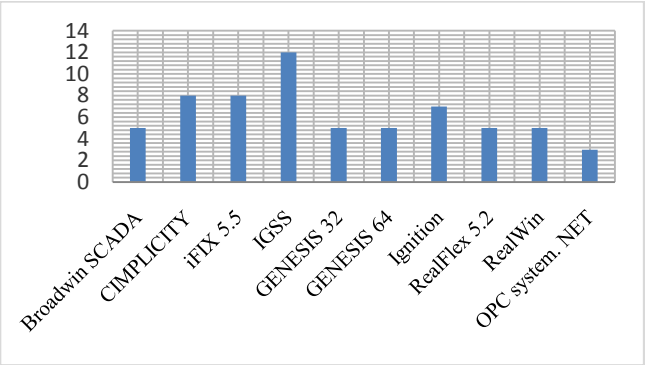

Figure 2: Number of different security solutions in the SCADA systems

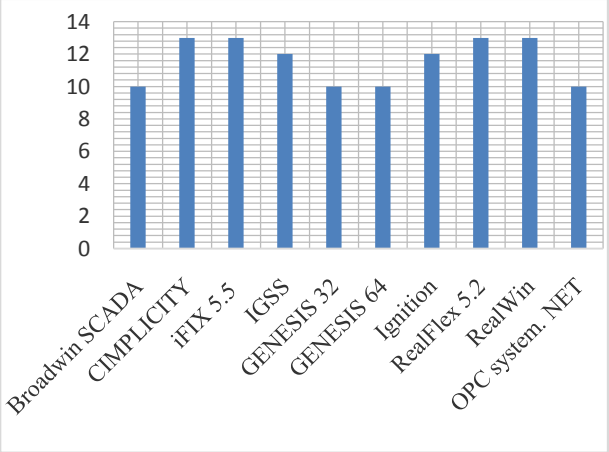

Figure 3: Number of recommended solutions by the standards in SCADA systems

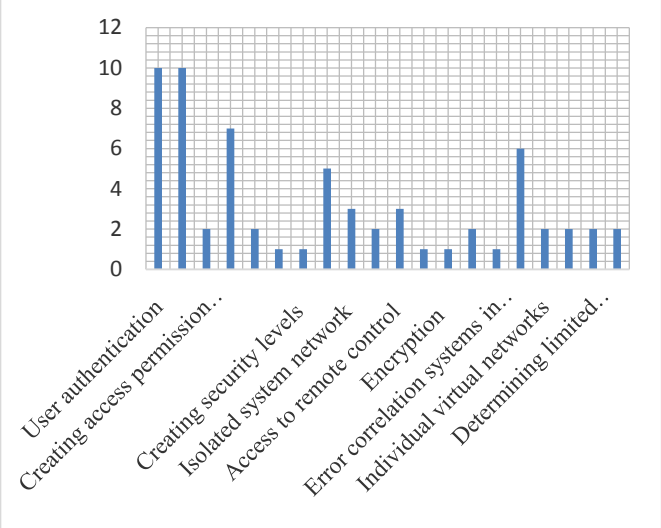

Figure 3: Security solutions used in various SCADA systems

5. ANALYZING SECURITY SOLUTIONS IN THE STANDARDS VS. SCADA SYSTEMS

The information provided in this section is a combination of last two sections. Here, we provide a list of total interactive and preventative security solutions which mentioned in the security standards and implemented SCADA systems. This list can be used as a model in developing SCADA systems or when SCADA systems are compared in term of their security.

5.1 Subsections

This model has experience and knowledge of SCADA's developer and in another way has experience and knowledge of international standards and transactions, it can be a good guidance for our mentioned goals.

- User authentication
- Creating access permission
- Performance management of important transactions
- Auditing system
- creating access levels
- Isolated network system
- Access to remote control
- Encryption
- Specifying allowed connections for access to system
- Individual virtual networks
- Specifying access limitation to a special node
- Documentation of group member's activities
- Creating individual limitation
- Using SSL
- Using multiple parallel servers
- Error correction systems in data transfer
- Managing security patches
- Using biometric technology
- Electronically signature
- Firewall
- Intrusion Detection
- Antivirus
- Managing security patches
- Changing management
- Properties
- Risk management
- Security organization
- Personnel management
- Programming for services after accidents and incidents
- Continuing business
- System flexibility
- Managing corporation with contractors
- Standards and politics of information security region.

5.2 Recommended solutions in standards which not used in SCADA systems

Provided information in the last sections, a list of obtained information that presents security solutions that standards and guidelines of its recommendation was released but do not exist in SCADA systems.

- Firewall
- Instruction detection
- Antivirus
- Security patches management
- Changes management
- Asset and property
- Risk management
- Security organization
- Personnel management
- Programming for proceedings after events and
- Continuing Business
- Flexible system
- Corporation management with contractors
- Standards and politics of information security region

As mentioned earlier, there are 14 cases of security solutions that have been evaluated in the standards; this list can be usable for updating the standards or producing new a standard for improving security level in SCADA systems. By considering experience and knowledge of SCADA systems developers in the world, this list can have a positive role in completing the standards. For understanding importance of this list, we highlight that how many times these solutions have been mentioned in the security standards.

Next, we analyze the importance of these security solutions by paying attention the frequency of their appearance in the documents of standards. As you can see in figure 4, using firewall has the most quantity and we can remark that the most important point of SCADA's system developer's idea that had been remained is using firewall because it is an important point of increasing a SCADA system. Also we can see that security organization is less important point in international standard developer's idea and had been forgotten from the SCADA's system developer's point of view.

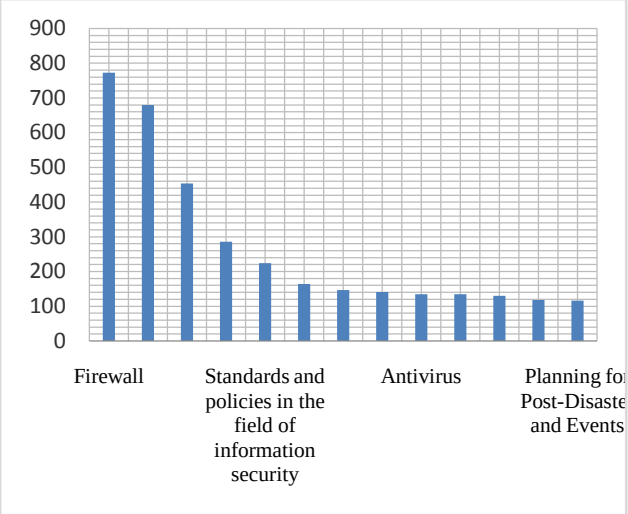

Figure 4: Number of appearances of not implemented SCADA solutions in the standards

5.3 Applied solutions in SCADA systems which not exist in standards

Provided information in the last sections, a list of obtained information that presents security solutions are used in SCADA systems, but there is no recommendation for them. This list gives us good solutions for elevation and increasing of SCADA's development or in preparing a SCADA system and we can provide more security for systems by point's observation. Also this list can be useful for updating standards for security elevation.

- Newspapers management of essential transactions
- Isolated network system
- Access to remote system
- Determining allowed connection for access to system
- Virtual individual networks
- Determining performance limitation for a special node
- Protection and maintenance of integrated preventative systems
- Creating individual limitations
- Using SSL
- Using multiple parallel servers
- Error correlation systems in data transfer
- Managing security patches
- Electronically signature

These 13 cases can be usable for updating international standards or creating new standards for increasing security level in SCADA systems. By considering experience and high knowledge of SCADA systems of well-known developers in the world, this list can have a positive role in completing standard.

For understanding important rate of this list, we evaluating these solutions in SCADA's systems and the information of this analyze has been shown in figure 5. As shown in the figure, using parallel servers by using 6 times has the most rate and we can mention that the most important point of international standards was missed. By the SCADA systems developers, it is a powerful security point and a good solution opposing attacks. Also, we can see that network isolation, maintain system and integrated fixing, SSL and access to remote system are less important points in SCADA system developer's ideas that had been remained in the standards.

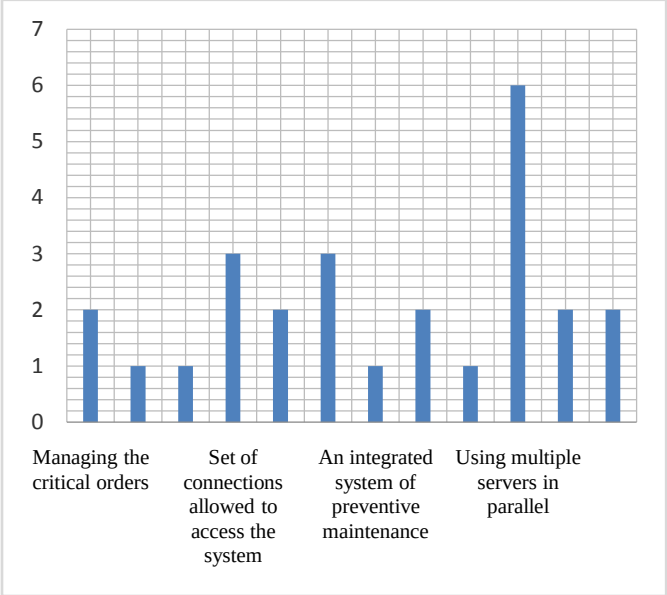

Figure 5: Number of security solutions in SCADAs which not mentioned in the standards

5.4 Comparing security solutions in various SCADA systems

As we mentioned in Figure 2, IGSS system or 12 using points of security solutions provided by SCADA's system developers mostly used it and we can say that it can have the most gain from provided solutions and also it has the most creativity for using security solutions and then General CIMPILICITY and iFIX 5.5 with 8 usage point and at last OPC has the least gain with 3 usage point.

Also, our study indicate that RealWin, CIMPLICITY, iFIX 5.5 and RealFlex systems or 13 using cases of security solutions provided by SCADA's system developers mostly used it. Basically, we can say that it can have the most gain from provided solutions or it has the best quality standard of SCADA's system in data protection and then IGSS and Ignition are placing and again at last OPC has the least gain with 10 usage points. By using provided information in this section and combining the way of using provided solutions, in Figure 6 we find combined information about used solution in SCADA systems and then evaluate the average. As shown in the figure, IGSS has the most average and we can say that by considering both standards has the most usage of security solutions and also in addition to suitable usage of provided solutions, it provided modern solution for improving security. After that CIMPLICITY and iFIX 5.5 have been placed and like other sections, OPC has the last column of the table.

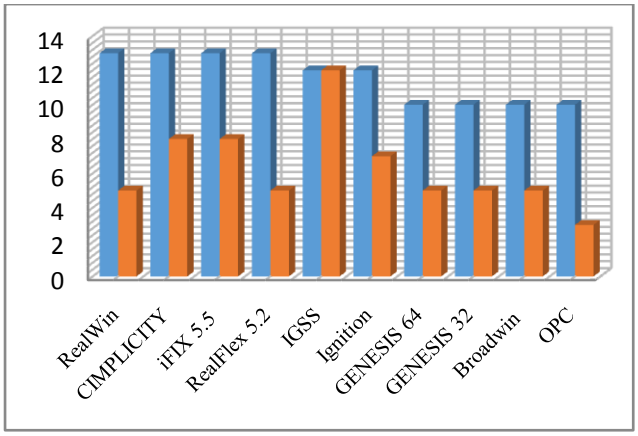

Figure 6: Combined information about SCADA systems, including

Number of security solutions in standards, in SCADA systems.

6. CONCLUSIONS

In this paper we briefly reviewed security solutions recommended by main security standards of SCADA systems. Also, we studied the implemented security solutions in some widely used SCADA systems in the world. By combining these two, we identified several important security solutions. After analyzing the gathered information, we found that utilizing encryption is one of important solutions to improve the security of SCADA systems. Firewalls and intrusion detection systems, authentication and access rights will be at later stages. Moreover, in terms of compliance with the standards, the well-known SCADA systems can be sorted as following: RealWin, General Electric Proficy CIMPLICITY, Proficy HMI / SCADA - iFIX 5.5 and RealFlex 5.2 and later IGSS and the Standard Ignition.

7. REFERENCES

[1] A. Shahzad and S. Musa, "Cryptography and Authentication Placement to Provide Secure Channel for SCADA Communication", International Journal of Security (IJS), Volume 6, Issue 3, 2012.

[2] K. Lynch, "Improving Security for SCADA Control Systems ", Interdisciplinary Journal of Information Knowledge and Management, Volume 3, 2008.

[3] P. Ralston, J. Graham, J. Hieb, "Cyber security risk assessment for SCADA and DCS networks", ISA Transactions 46, April 2007.

[4] A. Cagalaban, Y. So, S. Kim," SCADA Network Insecurity: Securing Critical Infrastructures through SCADA Security Exploitation", Journal of Security Engineering, Vol.6, No.6, 2009.

[5] C. Valli "SCADA Security – Slowly Circling A Disaster Area", WORLDCOMP 2009, Security and Management Conference 2009. (pp. 613-617) Las Vegas, USA.

[6] J. Ahokas, T. Guday, T. Lyytinen"Secure and Reliable Communications for SCADA Systems" INTERNATIONAL JOURNAL OF COMPUTERS AND COMMUNICATIONS, Issue 3, Volume 6, 2012.

[7] R. Kumar, "Recent Advances in SCADA alarm System", International Journal of Smart Home, Vol.4, No.4, October, 2010.

[8] J. Nordlander, " WHAT IS SPECIAL ABOUT SCADA SYSTEM CYBER SECURITY", Master Thesis, Stockholm, Sweden 2009

[9] American Gas Association (AGA). Cryptographic Protection of SCADA Communications Part 1: Background, Policies and Test Plan (AGA 12, Part 1). AGA, March 2006

[10] CPNI. About CPNI. CPNI, http://www.cpni.gov.uk/aboutcpni188.aspx [Accessed 17 December 2008]

[11] DHS Security. History. DHS, http://www.dhs.gov/xabout/history/ [Accessed 17 December 2008]

[12] DHS Cyber Security Procurement Language for Control Systems version 1.8. DHS, February 2008

[13] Department of Homeland Security (DHS) Catalog of Control Systems Security: Recommendations for Standards Developers. DHS, January 2008

[14] DOE. History. DOE, http://www.energy.gov/about/history.htm [Accessed 17 December 2008]

[15] Office of Energy Assurance, U.S. Department of Energy. 21 steps to Improve Cyber Security of SCADA Networks. Office of Energy Assurance, U.S. Department of Energy

[16] GAO. GAO at a Glance. GAO, http://www.gao.gov/about/gglance.html [Accessed 18 December 2008]

[17] GAO. Technology Assessment - Cybersecurity for Critical Infrastructure Protection. GAO, May 2004

[18] IEEE. About IEEE. IEEE, http://www.ieee.org/web/aboutus/home/index.html [Accessed 17 December2008]

[19] IEEE. IEEE Mission and Vision. IEEE, http://www.ieee.org/web/aboutus/visionmission.html [Accessed 17 December 2008]

[20] IEEE. IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities. IEEE, December 2007

[21] IEEE. IEEE Guide for Electric Power Substation Physical and Electronic Security. IEEE, January 2000

[22] International Society of Automation (ISA). ANSI/ISA–99.00.01–2007 Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models. ISA, October 2007

[23] ISA. ANSI/ISA-TR99.00.01-2007 Security Technologies for Industrial Automation and Control Systems. ISA, October 2007

[24] ISA. ANSI/ISA—TR99.00.02—2004 Integrating Electronic Security into the Manufacturing and Control Systems Environment. ISA, October 2004

[25] International Organization for Standardization (ISO) About ISO. ISO, http://www.iso.org/iso/about.htm [Accessed 17 December 2008]

[26] ISO Information technology — Security techniques — Code of practice for information security management Final Draft. ISO, 2005

[27] North American Electric Reliability Corporation (NERC)., NERC CIP-001-1 - CIP-009-1. NERC, 2006