SCADA System Cyber Security – A Comparison of Standards

Teodor Sommestad, Göran N. Ericsson, *Senior Member, IEEE,* Jakob Nordlander

***Abstract*— Cyber security of Supervisory Control And Data Acquisition (SCADA) systems has become very important. SCADA systems are vital for operation and control of critical infrastructures, such as the electrical power system. Therefore, a number of standards and guidelines have been developed to support electric power utilities in their cyber security efforts.**

This paper compares different SCADA cyber security standards and guidelines with respect to threats and countermeasures they describe. Also, a comparison with the international standard ISO/IEC 17799 (now ISO/IEC 27002) is made. The method used is based on a comparison of use of certain key issues in the standards, after being grouped into different categories. The occurrences of the key issues are counted and comparisons are made.

It is concluded that SCADA specific standards are more focused on technical countermeasures, such as firewalls and intrusion detection, whereas ISO/IEC 17799 is more focused on organizational countermeasures.

***Index Terms*— SCADA systems, Control systems, Cyber Security, Standards, Smart Grids.**

I. Introduction

SCADA (Supervisory Control And Data Acquisition) systems have been in use more than 30 years, and have become more advanced and complex as computer technology has advanced. They are today vital for operating critical infrastructures, such as electric power systems.

The development of SCADA system started before the wide-spread use of Internet, in a period of time when the need for IT-security mostly consisted of protecting the physical access to the computers of the system. During the last ten years, the number of connections to SCADA systems and the use of internet-based techniques have increased rapidly. SCADA systems have also moved from using proprietary protocols and software to using the same standards and solutions as administrative IT systems. This trend is also likely to continue as Electric Power Utilities (EPUs) move towards the vision of a smart grid [1] [2] [3].

As a consequence, SCADA systems are now being exposed to threats and vulnerabilities they have never been exposed to before, and to a much greater extent than earlier. In addition, conventional security solutions are not always applicable to SCADA systems, since performance and availability requirements differ for administrative IT systems and SCADA systems.

Since the beginning of the new millennium, the need for treating Information Security for EPUs has become more evident among utilities, vendors, consultants, standardization bodies, and regulatory bodies around the globe. For example, this has been stressed within Cigré, where two main working groups on information security have been launched: JWG B3/C2/D2 [4] and WG D2.22 [5]. The list of organizations that publish documents on how to secure SCADA systems include [6][7]: American Gas Association (AGA) , the National Institute of Standards and Technology (NIST), Centre for the Protection of National Infrastructure (CPNI) , International Electrotechnical Commission (IEC), the North American Electric Reliability Corporation (NERC) and IEEE.

A. Purpose

This paper analyzes the content of commonly used SCADA standards and guidelines in terms of recommendations that are given to improve security, and the threats that are discussed. The purpose is to identify how much focus these SCADA standards place on different recommendations and threats. A comparison is also made with ISO/IEC 17799 [8] (now ISO/IEC 27002 [9]) to identify the differences to security management in general.

B. Outline

The paper is structured as follows. Section two provides an overview of related work. Section three presents the method applied when analyzing recommendation in existing standards. Section four presents the result of applying this method to SCADA specific standards, and section five compares the recommendations in SCADA specific standards with those in ISO/IEC 17799. In section six a discussion is given and in section seven conclusions are drawn.

II. Related work: SCADA specific security

It is often argued that SCADA system security is special and different from traditional information security or information technology security because of the environment

This work was supported in part by the Swedish Emergency Management Agency (now the Swedish Civil Contingencies Agency), and supported by Svenska Kraftnät.

T. Sommestad is with the Royal Institute of Technology (KTH), Osquldas vag 10, 100 44 Stockholm, Sweden; phone: +46-8-790-6920; fax: +46-8-790-6839; e-mail: Teodor.Sommestad@ics.kth.se.

G. Ericsson is with Svenska Kraftnät, P.O. Box 1200, 17224 Sundbyberg, Sweden; e-mail: Goran.Ericsson@svk.se.

J. Nordlander is with Cygate AB, Dalvägen 28, 169 56 Solna, Sweden; e-mail: jakob.nordlander@cygate.se.

the SCADA systems are used within, and the requirements placed on them. As a consequence, a large number of recommendations, guidelines and regulations (hereafter collectively referred to as *standards*) that describe matters specifically related to SCADA security has been developed. See for example [10-23]. Overviews of existing standards and other initiatives can be found in [6] and [7].

It is sometimes stated that while the prioritization in traditional information security is CIA (Confidently, Integrity, and Availability) the prioritization for SCADA systems is typically AIC (Availability, Integrity, Confidently) [17]. Hence, electric utilities set higher priority to having the system functioning, than preserving confidentiality of information in it.

Several of the standards provide elaborate descriptions of these differences in terms of requirements that are placed on the system. For example, [17] points out that one such difference is performance requirements: control systems are time-critical and real-time whereas information technology systems only require consistent response times and are not real-time. Such differences are also described in other literature. See for example [24] [25].

From these differences, some direct impact on the security recommendations can also be inferred as they constrain the security recommendations that can be given. The requirements on efficiency and safety are for example in conflict with rigid password protection [17], and cryptographic techniques might degrade the performance to an unacceptable level [26].

Although ISO/IEC 17799 [8] is not focused on SCADA systems it is a commonly used security standard in the electric utility industry. Methods to efficiently use ISO/IEC 17799 for security management in electric utilities [26][28] as well as using ISO/IEC 17799 for security assessments of power communication has been proposed [29]. Hence, this general purpose security standard is also used a basis for policies and practices applied to SCADA systems in EPUs. Yet, there has been no comprehensive analysis of how recommendations given in SCADA standards differ from those given in the more general security standards. This paper presents such an analysis by quantitatively reviewing the content of some of the most widely used standards for SCADA security and ISO/IEC 17799.

III. Method

The method comprise of three phases. First, the standards to compare were chosen based on a set of criteria. Secondly, these standards were studied in-depth to extract information on security recommendations and attacks described in them. The extracted information was thereafter grouped, and each group was associated with a number of keywords and phrases that represented its content. Finally, the keywords and phrases have been used to quantify the standards' focus on different security recommendations and threats.

A. Selection of standards

There exist a large number of standards and recommendations that is of relevance to those concerned about SCADA security. This study started with a comprehensive search for documents produced by standardization bodies and governmental agencies. In this search the following criteria was used to determine if a standard would be included or not:

[1] The standard is available in English.

[2] The standard is published by a standardization body or governmental agency.

[3] The standard must focus on SCADA system security (not IT or information security in general)

[4] The standard/guideline must focus on SCADA systems as a whole. Hence, it should not focus on sub systems or components, such as intelligent electronic devices.

The rationale for the second criterion is to include all those standards that are produced by authorities in the field, and thereby makes them widely recognized. The third criterion serves to eliminate those standards that do not represent the requirements and prioritizations that are directly applicable for SCADA systems. The fourth criterion serves to include those standards that cover all parts of SCADA systems. A standard which only focus on one sub-component of the SCADA system could, due to this sub-components characteristics, skew the result to certain countermeasures and threats.

Eight standards and guidelines, or groups thereof, were found to comply with these requirements. These are described in TABLE 1.

TABLE 1 – INCLUDED STANDARDS

Document(s)	Publisher
Good Practice Guide, Process Control and SCADA Security [20]	Centre for the Protection of National Infrastructure (CPNI)
Cyber Security Procurement Language for Control Systems [11]	Department of Homeland Security (DHS)
21 steps to Improve Cyber Security of SCADA Networks [21]	U.S. Department of Energy (DOE)
CIP-002-1 - CIP-009-1 [22]	North American Electric Reliability Corporation (NERC)
Guide to Industrial Control Systems (ICS) Security [17]	National Institute of Standards and Technology (NIST)
System Protection Profile - Industrial Control Systems [23]	National Institute of Standards and Technology (NIST)
ANSI/ISA–99.00.01–2007 Part 1-3 [14][15][16]	The International Society of Automation (ISA)
Cyber security for Critical Infrastructure Protection [18]	U.S. Government Accountability Office (U.S. GAO)

B. Grouping of recommendations and threats

After identifying relevant documents, these were studied and security recommendations as well as threats described were extracted from them. This yielded a substantial number of phrases such as: "Implement firewalls" (recommendation from [21]) and "Malicious code" (threat from [11]).

To enable comparison, the recommendations and attacks extracted from the different documents were grouped according to their objective. For instance, recommendations related to firewalls were grouped in one group of recommendations and threats related to various kinds of malicious software were grouped together. This yielded 26 groups of security recommendations and 14 groups of threats.

C. Quantifying focus of standards

To compare these 26 groups of security recommendations and 14 groups of threats, a number of keywords and key phrases were associated to each group. The keywords and phrases were identified by reading the documents again using the extracted phrases as a starting point. TABLE 2 shows the keywords associated with the groups "Firewall" and "Malicious code". A complete list of keywords can be found in Appendix.

TABLE 2
EXAMPLES OF KEYWORDS AND GROUPS

Firewall	**Malicious code**
Firewall	Malicious code
Packet filtering	Malicious software
Stateful inspection	Virus
Application proxy	Worm
Boundary protection	Trojan
	Malware
	Logic Bomb

When keywords were identified, the number of occurrences of each keyword and phrase in each of the included documents was counted. The number of occurrences for a group was calculated as the sum of its keywords. The number of occurrences of these keywords and phrases was also counted in ISO/IEC 17799 [8] and aggregated using the same procedure.

To enable comparison between ISO/IEC 17799 and the SCADA standards and guidelines the result is normalized with the total number of keyword occurrences in the compared texts. The normalized values thus represent the part of the total requirements that is associated with each group. This normalized value is hereafter referred to as *focus*. This comparison is made for the 26 groups of countermeasures. When comparing SCADA standards internally, each text's focus was normalized with the number of keyword occurrences in this particular text.

IV. Focus in SCADA security standards

Using the method described above, the included SCADA standards has been analyzed. This analysis has identified how much attention is given to the groups of countermeasures and threats. Two of the standards (ANSI/ISA Part 1-3 [10-12] and NIST's Guide to Industrial Control Systems Security [17]) cover all groups of countermeasures. No document covers all groups of threats. The standards' focus on the 26 countermeasure-groups and the 14 threat-groups is described below.

A. Countermeasures

The keywords and phrases associated with the 26 groups of countermeasures occurred in total 8222 times in the eight SCADA standards. Fig. 1 show the number of occurrences for each group normalized with the total number of occurrences in all standards. As depicted in Fig. 1 countermeasures related to *authentication* accounts for 14.5 percent of the occurrences followed by countermeasures related to *cryptography* with 13.6 percent of the occurrences.

On the other end of the scale, measures related to how to set the *security organization*, how support can be gained from *system management tools*, how to create *system resilience* to attacks and recommendations on *hardening* of computers and services are found.

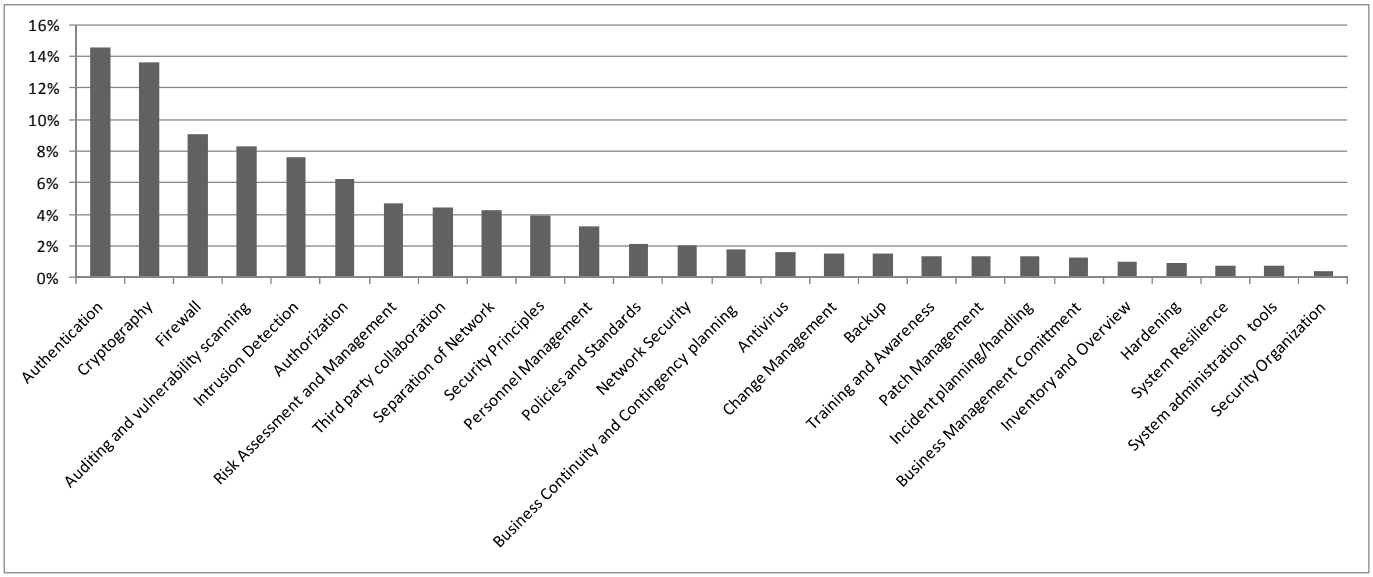

Fig. 1 Focus of SCADA standards and guidelines on countermeasure-groups, normalized.

The focus on these groups differs among standards. Let the focus on group i in standard j be $F_{i,j}$ and let M_i be the arithmetic mean of all standards focus on group i.

With n standards the absolute mean deviation for a group i, D_i, can then be obtained as:

$$D_i = \sum_{j=1}^{n} \frac{\|M_i - F_{i,j}\|}{n}$$

The mean of D_i over the 26 countermeasure-groups (mean absolute mean deviation) is 2.50 percent. This should be compared to the mean focus on groups in general, which is approximately 3.86 percent (1/26). Hence, the standards included in this comparison do to a large extent deviate when it comes to the number of times different types of countermeasures are mentioned in text. In TABLE 3 the arithmetic mean of the focus of the eight SCADA standards is shown together with the mean average deviation (MAD) of their focus. Also shown is the quotient between these, i.e. how much standards deviate in their focus compared to their mean focus on the countermeasure group.

TABLE 3
FOCUS DEVIATIONS IN SCADA STANDARDS

GROUP	MAD	MEAN	MAD / MEAN
Security Organization	0.011	0.009	1.294
System administration tools	0.006	0.006	1.090
Inventory and Overview	0.015	0.014	1.070
Business Management Commitment	0.017	0.018	0.925
System Resilience	0.008	0.009	0.900
Hardening	0.011	0.012	0.896
Network Security	0.016	0.018	0.891
Separation of Network	0.046	0.053	0.872
Business Cont, and Contingency planning	0.026	0.031	0.842
Incident planning/handling	0.016	0.020	0.827
Training and Awareness	0.015	0.019	0.789
Security Principles	0.040	0.052	0.765
Cryptography	0.069	0.095	0.723
Third party collaboration	0.036	0.054	0.678
Authentication	0.072	0.108	0.671
Policies and Standards	0.015	0.024	0.643
Antivirus	0.009	0.014	0.638
Backup	0.013	0.021	0.612
Patch Management	0.008	0.013	0.604
Intrusion Detection	0.039	0.067	0.589
Firewall	0.040	0.070	0.582
Authorization	0.031	0.056	0.552
Personnel Management	0.023	0.044	0.520
Risk Assessment and Management	0.029	0.061	0.468
Change Management	0.009	0.020	0.430
Auditing and vulnerability scanning	0.030	0.093	0.316

All groups are mentioned in all standards. NERC CIP [22] does for instance place 21.8 percent of its focus on "Separation of networks" while CPNI's "Good Practice Guide" [20] does not use a single keyword associated with that group. Also when they all mention words associated with a particular group there is difference with regard to the focus placed on it. The focus on authentication is for example 23.3 percent in ISA's three documents [14][15][16]; 1.1 percent in DOE's "21 steps to Improve Cyber Security of SCADA Networks" [21]; and only 0.3 percent in CPNI's "Good Practice Guide" [20].

B. Threats

The standards included in this study have a focus on countermeasures and recommendations on how to secure SCADA systems. The keywords and phrases associated with the 14 groups of threats occurred in total 876 times in the documents. The threats the standards focus on can be seen in Fig. 2, here normalized with the total number of occurrences in all standards.

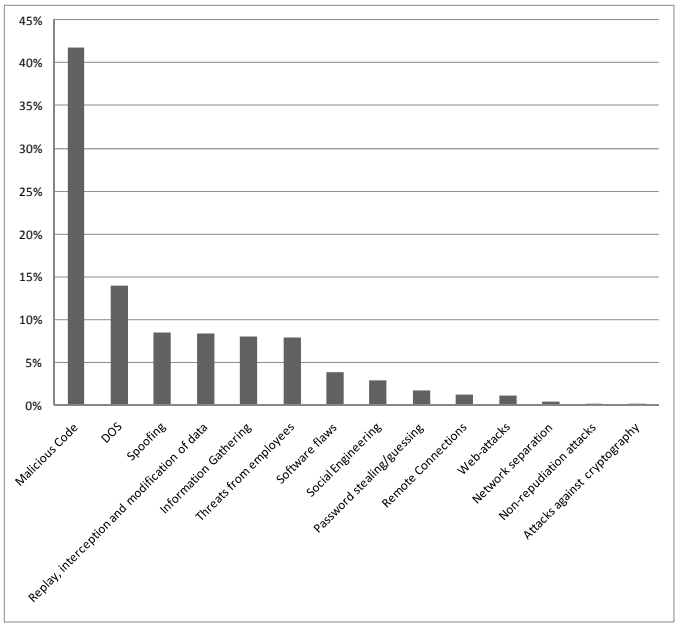

Fig. 2 Focus of SCADA standards and guidelines on threat-groups, normalized.

More than 40 percent of the occurrences of threats mentioned belong to the group *Malicious code* (described in TABLE 2). Denial of service attacks with the keywords "DOS", "DDOS", "Denial of Service", "Syn flood" and "Resource Exhaustion" is the second most mentioned attack with 14 percent of the hits.

Threats against data communication are also given much attention, here represented by *Spoofing* (e.g. "man-in-the-middle") and *Replay, interception and modification of data* (e.g. "message replay"). On fifth place, threats related to *information gathering* are found, for example "war dialing" and "traffic analysis".

Threats from employees and *Social engineering* attacks are more related to the human element of cyber security. These are given modest attention with focus of 7.9 and 3.0 percent respectively.

Also with regard to threats there is a difference in how much attention they are given in the included standards. The mean absolute mean deviation with regard to threats in the standards (mean of D_i over the 14 threat-groups), is 3.9. This could be compared to the mean focus of groups, which are 6.1.

NERC CIP 002-009 [22] does not contain any of the keywords related to threats. In [20] 78 percent of the occurrences are related to *Malicious code*, while in [18] this quotient is 50 percent. The same quotient in the System Protection Profile (published by NIST) [23] is less than eight percent. Further, the system protection profile [23] focus to 42 percent on *DOS* while the guide published by the same organization ("Guide to Industrial Control Systems (ICS) Security" [17]) only focus 10 percent of the attention on this threat.

C. Comparison to ISO/IEC 17799

In terms of security, EPUs must cope with both "traditional, administrative office IT" requirements and "SCADA specific" requirements. Several utilities use the generic standard ISO/IEC 17799 [8] (now ISO/IEC 27002 [9]) as a basis for security management. It is therefore interesting to compare SCADA standards with ISO/IEC 17799 to clarify the difference and coverage in terms of security requirements.

Fig. 3 show normalized values of how much focus that is placed on countermeasures in SCADA standards and ISO/IEC 17799. It can be seen here that ISO/IEC 17799 puts significantly stronger emphasis on *Security organization*, *Business continuity and contingency planning*, *Policies and standards,* and *Third party collaboration*. The quotient between ISO/IEC 17799 focus on these countermeasures and the SCADA standards' focus on them is 10.5, 4.3, 3.1 and 2.8 respectively. More emphasis is also placed on *Authorization* (quotient 2.1), *Backups* (2.0), *Personnel management* (1.6) and *Change management* (1.4).

Thus, ISO/IEC 17799 focus more on administrative and organizational measures than SCADA standards. SCADA standards focus more on *Firewalls*, *System administration tools*, *Antivirus* and *Intrusion detection*. The quotient for these is: 0.044, 0.10, 0.10 and 0.19 respectively. Hence, SCADA standards place more than 22 times more focus on *Firewalls* than ISO/IEC 17799, and 10 times as much focus on *System administration tools* and *Antivirus*.

Other countermeasures that are mentioned more often in SCADA standards are: *Patch Management* (quotient 0.23), *Hardening* (0.34), *Business Management Commitment* (0.45), *Inventory and Overview* (0.47), and *System Resilience* (0.61). In addition, the keywords associated with the group Security principles are not mentioned in ISO/IEC 17799, but constitute 4.0 percent of the SCADA standards' recommendations.

The other countermeasure groups receive similar focus in both ISO/IEC 17799 and the SCADA standards. Their quotient is within the range 0.67 and 1.38. *Risk management* and *Incident planning/handling* has the quotients closest to one (1.02 and 1.03 respectively) and thus receive similar focus in both SCADA standards and the more general ISO/IEC 17799.

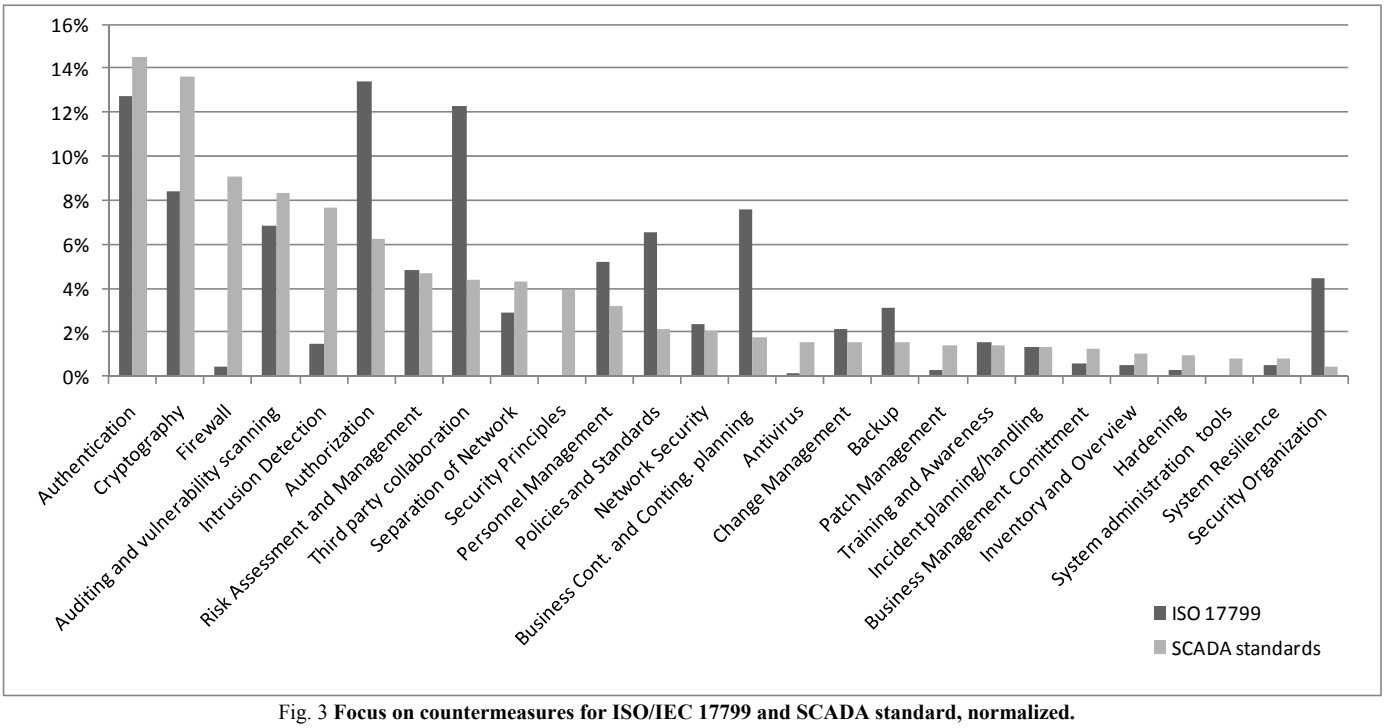

Fig. 3 **Focus on countermeasures for ISO/IEC 17799 and SCADA standard, normalized.**

V. Discussion

This study has investigated the differences between the recommendations for securing traditional administrative IT-systems and the recommendations for securing SCADA systems used to operate electrical power processes. The well established best practice standard ISO/IEC 17799 [8] has been used as reference for security requirements placed on systems in general. A difference between this standard and the SCADA standards discussed in this study is that it is concerned with information security, and does not focus solely on information technology (such as SCADA systems). ISO/IEC 17799 is however widely used in the electric utilities to secure information technology systems and also proposed as a tool for securing the SCADA domain in utilities [26][28].

The comparison made here is quantitative and compares the *focus* of SCADA standards and ISO/IEC 17799. The *focus* is defined as the normalized value for the number of occurrences of certain keywords in the compared texts. This method is similar the one presented in [30], where it is used to define the enterprise information security field. To compare texts based on the frequency of different words has weaknesses compared to more qualitative methods, where the semantics of a text would be fully interpreted. However, it yields a traceable result that accurately captures the portion of a text that is devoted to certain countermeasures and threats. Based on the initial literature study the authors also believe that this quantitative method provides a good indication of the texts' content.

With this quantitative method a major difference between SCADA standards and ISO/IEC 17799 is found. While the latter focuses more on administrative and organizational matters (see section IV. C.) SCADA standards focus more on technical countermeasures. This result confirms that SCADA security is more concerned with information technology than ISO/IEC 17799 and that a security manager adopting ISO/IEC 17799 should focus on its technical recommendations. This applies to firewalls, patch management and hardening in particular.

SCADA standards, as well as many other security standards, have a strong emphasis on countermeasures. Keywords associated with countermeasures are mentioned 8222 times while those associated with threats are mentioned 876 times. This difference could perhaps be explained by the uncertainty that exists about the actual threat against SCADA systems. Few confirmed incidents are publically known. However, if the countermeasures suggested in these documents are based on a rational process, a threat analysis would most probably be the basis for the countermeasure-recommendations. From this study it is not apparent that this is the case. For example, malicious code is the most frequently mentioned threat in the SCADA standards and accounts more than 40 percent of the focus. Antivirus, that is an obvious countermeasure to this threat, does however only represent 1.6 percent of the focus when it comes to countermeasures.

VI. Conclusions

This paper has presented a quantitative evaluation of SCADA standards and the comparison to ISO/IEC 17799. It can be concluded that with this ranking method, more than every fourth countermeasure mentioned in the SCADA standards concern cryptography or authentication. Furthermore, the threats most frequently mentioned are those relating to malicious code or denial of service attacks, which together make up 50 percent of the total occurrences of keywords associated with threats. There is also a strong focus on countermeasures in the SCADA standards, hence less focus on threats.

Moreover, it was found that compared to SCADA standards ISO/IEC 17799 focus more on management and organizational issues, and less on technical issues. These results suggest that electric power utilities solely using standards similar to ISO/IEC 17799 for security management should complement its efforts by adapting this to SCADA-specific security requirements. In particular should firewalls, system administration tools, antivirus, and intrusion detection be considered.

References

[1] DOE, "What the smart grid means to you and the people you serve", U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability, USA, 2009

[2] DOE, ""Grid 2030" — A National Vision for Electricity's Second 100 Years", United States Department of Energy, Office of Electric Transmission and Distribution, USA, 2003.

[3] European Commission, "European Technology Platform SmartGrids, Strategic Research Agenda for Europe's Electricity Networks of the Future", EUR 22580, ISBN 92-79-03727-7, Luxembourg, 2007.

[4] G. Ericsson, "Information Security for Electric Power Utilities (EPUs) – Cigré Developments on Frameworks, Risk Assessment and Technology," Paper TPWRD-543-2008, *IEEE Transactions on Power Delivery, Vol. 24, No. 3, July 2009, pp. 1174-1181.*

[5] G.Ericsson, "Towards a Framework for Managing Information Security for an Electric Power Utility – Cigré Experiences," Paper TPWRD-406-2006 published in *IEEE Transactions on Power Delivery, Vol. 22, No. 3, July 2007, pp. 1461-1469.*

[6] R. Carlson, J. Dagle, S. Shamsuddin, and R. Evans, "*A Summary of Control System Security Standards Activities in the Energy Sector,"* Office of Electricity Delivery and Energy Reliability U.S. Department of Energy, October 2005.

[7] V. Igure, S. Laughter, and R. Williams, "*Security issues in SCADA networks,"* Computers & Security 25, (2006) 498 – 506.

[8] ISO/IEC, *"Information technology — Security techniques — Code of practice for information security management,"* International Organization for Standardization, International Electrotechnical Commission, ISO/IEC 17799:2005, 2005.

[9] ISO/IEC," *Information technology – Security techniques – Information security management systems – Requirements*," International Organization for Standardization, International Electrotechnical Commission, ISO/IEC 27001: 2005.

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

[11] DHS, "*Cyber Security Procurement Language for Control Systems,"* DHS, August 2008.

[12] IEC, *"Power system control and associated communications – Data and communication security," First* Edition, IEC 62210 International Electrotechnical Commission, May 2005.

[13] IEC, *"Power systems management and associated information exchange – Data and communications security, Part 1: Communication network and system security - Introduction to security issues First Edition*," IEC 62351-1, International Electrotechnical Commission, May 2007

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

[15] ISA, *"ANSI/ISA-TR99.00.01-2007 Security Technologies for Industrial Automation and Control Systems*," International Society of Automation (ISA), October 2007

[16] ISA, *"ANSI/ISA—TR99.00.02—2004 Integrating Electronic Security into the Manufacturing and Control Systems Environment,"* International Society of Automation (ISA), October 2004

[17] K. Stouffer, J. Falco, K. Scarfone, "*Guide to Industrial Control Systems (ICS) Security Special Publication 800-82,"* Second public draft, National Institute of Standards and Technology, September 2007.

[18] GAO, *"Technology Assessment - Cybersecurity for Critical Infrastructure Protection,"* U.S. Government Accountability Office, May 2004.

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

[20] CPNI, *"Good Practice Guide, Process Control and SCADA Security,"* Centre for the Protection of National Infrastructure (CPNI), 2005.

[21] DOE, *"21 steps to Improve Cyber Security of SCADA Networks*," Office of Energy Assurance, U.S. Department of Energy, 2002.

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

[23] NIST, "*System Protection Profile - Industrial Control Systems,"* Version 1.0, National Institute of Standards and Technology (NIST), April 2004.

[24] J. Falco, J. Gilsinn, K., and Stouffer, *"IT Security for Industrial Control Systems: Requirements Specification and Performance Testing,"* 2004 NDIA Homeland Security Symposium & Exhibition, Crystal City, VA, 2004.

[25] D. Kilman, and J. Stamp, *"Framework for SCADA Security Policy,"* Sandia National Laboratories Report, SAND 2005-1002C, 2005. http://www.sandia.gov/scada/documents/sand_2005_1002C.pdf

[26] D. Dzung, M. Naedele, T. Von Hoff, and M. Crevatin, , *"Security for Industrial Communication Systems",* Proceedings of the IEEE, Volume 93, Issue 6, 2005, pp. 1152-1177.

[27] G. Ericsson, and T. Torkilseng, "*Management of Information Security for an Electric Power Utility—On Security Domains and Use of ISO/IEC17799 Standard"*, IEEE Transactions on Power Delivery, vol. 20, No. 2, April 2005

[28] W. Jayawickrama, *"Managing Critical Information Infrastructure Security Compliance: A Standard Based Approach Using ISO/IEC 17799 and 27001,"* On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, pp. 565-574, 2006.

[29] L. Nordstrom, *"Assessment of Information Security Levels in Power Communication Systems Using Evidential Reasoning,"* IEEE Transactions on Power Delivery, vol. 23, No. 3, pp. 1384-1391, July 2008.

[30] E. Johansson and P. Johnson, *"Assessment of Enterprise Information Security – An Architecture Theory Definition,"* in Proceedings of the 3rd Annual Conference on Systems Engineering Research (CSER), 2005, pp. 138-146.

Teodor Sommestad received a M.Sc degree in computer science at the KTH – the Royal Institute of Technology, Stockholm, Sweden.

He is currently a PhD student at the department Industrial Information and Control systems at KTH. His research interests are security of industrial control system, primarily the security systems used for power network management.

Mr. Sommestad is a member of ISACA and is chairman of the research and development committee of ISACA's Swedish Chapter.

Göran N Ericsson (S'90 – M'96 – SM'06) was born in Huddinge, Sweden, in 1963. He received the Ph.D. degree from the Royal Institute of Technology (KTH), Stockholm, Sweden, in 1996.

In 1997, he joined Svenska Kraftnät (Swedish National Grid), Sundbyberg, Sweden. During 1997-2006 he held expert and managerial positions within the fields of data- and telecommunications. During 2007 – May 2009, he was the Chief Information and IT Security Officer. He was the convener of CIGRÉ working group D2.22 on information security 2006-2009.

As of June 2009, Dr. Ericsson is the Manager R&D. He is active in IEEE Power & Energy Society PSCC and CIGRÉ SCD2

Jakob Nordlander received an M.Sc degree in computer science at the KTH – the Royal Institute of Technology, Stockholm, Sweden in 2009.

He is currently working as a software engineer at Cygate where he primarily is involved in the development of PKI systems.

Mr. Nordlander is a member of International Society of Automation.

VII. Appendix – Groups and Keywords

This appendix shows the keywords (phrases) associated with each group. A set of letters enclosed by parentheses represent a set of words that were all used in the search. The letters within the parentheses can either be included in the word or left out of it. For example, the keyword "Isolat(e)(ation)" would result in: "Isolate" and "Isolation".

A. Countermeasures

Antivirus: antivirus, anti-virus, malware detection, malware prevention

Auditing and vulnerability scanning: audit(ing), understand the vulnerabilities, post implementation review, security review, security test, self-assessments, vulnerability assessment, monitoring, electronic access, security assessments, user identity association, test plans, system validation, scanner, log auditing

Authentication: authentication, single sign-on, password, identification, time-limited, session locking

Authorization: RBAC, access control, session management, access rights, electronic access, account management, management of TSF data, Rights and privileges, authorization, access control list, least privilege, separation of duties, password policy, key management

Backup: backup

Business Continuity and Contingency planning: disaster recovery, business continuity, recovery plan, contingency, continuity of operation

Business Management Commitment: define the cyber security goals and practice, business case, senior management, senior manager, charter and scope, leadership commitment

Change Management: change control, configuration management, change management, management of change

cross-functional team
Cryptography: encrypt(ion), cryptograph(y)(ic), Decryption, TLS, digital Signature, PKI, public key infrastructure, confidentiality during transition, IPSEC, SSL, SSH, certificate(s), VPN, virtual private network, kerberos
Firewall: firewall, packet filtering, stateful inspection, application proxy, boundary protection
Hardening: harden(ing), unnecessary hardware can be physically disabled, protect the BIOS, heartbeat signals, disabling, removing or modifying well-known or guest accounts, disconnect unnecessary connections to the SCADA network, default account, default password, media protection
Incident planning/handling: incident handling, incident management, incident response, warning system, incident report, incidents documentation, response to security incidents, computer forensics tool
Intrusion Detection: intrusion detection, intrusion prevention, HIDS, NIDS, IDS, canar(y)(ies), honey pot. security status monitoring, replay detection, detection of modification, security alarms, anomaly detection, potential violation analysis, content management, security event correlation tool, traffic monitoring, forensics and analysis tools, attack heuristics, integrity checker
Inventory and Overview: inventory, understand the system, identify all connections, identified critical asset, network diagrams, identify assets
Network Security: dial-up modem, dial-back modem, remote support connection, remote support access, wireless polic(y)(ies), wireless network security, wireless security, dedicated line, web-based interface, DNS, TCP/IP, callback system, MAC address locking
Patch Management: patch management, apply patch, patching, security update, security patch
Personnel Management: contract, improved relationships, separation agreement, security roles, personnel risk assessment, personnel security, hiring, conditions of employment, roles and responsibilities, security organization
Policies and Standards: security polic(y)(ies), develop(ing) polic(y)(ies), compliance with polic(y)(ies), legal requirement
Risk Assessment and Management: risk assessment, understand (the) vulnerabilities, understand (the) threats, understand (the) impacts, understand (the) risks, assessment of business risk, risk reduction workshop, mitigation controls, risk analysis, define risks, risk goals, risk management, mitigate risk, risk based, identify risk
Security Organization: security team, security response team, red team
Security Principles: secure architecture, write safe code, defense in depth, security requirement, information protection, performance consideration
Separation of Network: separate security domain, separat(e)(ion)(ing), isolat(e)(ation), DMZ, demilitarized zone, electronic security perimeter, VLAN, virtual local area network
System administration tools: host configuration management tools, policy enforcement applications, network management
System Resilience: redundant, single points of failure, spoof, fault tolerance, UPS, fail-safe
Third party collaboration: third party, vendor, reuse proven solutions, flaw remediation, industry forums, security requirements in procurement
Training and Awareness: Training and Awareness, Awareness and Training, Awareness programme, Coach IT personnel, Information Awareness, Security Training, Training program, Security Awareness

B. Threats

Attacks against cryptography: roll back
DOS: DOS, DDOS, denial of service, syn flood, resource exhaustion
Information Gathering: eavesdrop, sniff, traffic analysis, tap, war dial, war drive, visual observation, keystroke
Malicious Code: malicious code, malicious software, virus, worm, trojan, malware, logic bomb
Network separation: poorly designed network, broadcast storm, dual network interface cards (NIC) to connect networks
Non-repudiation attacks: modify log
Password stealing/guessing: stealing password, password guessing, guessable passwords, brute force, dictionary
Remote Connections: rogue access point, backdoor, uncontrolled external access, unknown connection
Replay, interception and modification of data: replay, intercept, modify data, modification of data, unauthorized change of set points
Social Engineering: social engineering, phishing
Software flaws: buffer overflow, command injection, software bugs, “illegal” conditions, programming errors, sql injection, software flaw
Spoofing: spoof, impersonate, masquerade, man in the middle, MITM, session hijack
Threats from employees: disgruntled employee, operator error, insider, human error, fraud
Web-attacks: remote file include, cross site scripting