WHAT IS SPECIAL ABOUT SCADA SYSTEM CYBER SECURITY?

A COMPARISON BETWEEN EXISTING SCADA SYSTEM SECURITY STANDARDS AND ISO 17799

Jakob Nordlander

KTH Electrical Engineering

Master Thesis
Stockholm, Sweden 2009

XR-EE-ICS 2009:005

WHAT IS SPECIAL ABOUT SCADA SYSTEM CYBER SECURITY?

A COMPARISON BETWEEN EXISTING SCADA SYSTEM SECURITY STANDARDS AND ISO 17799

Jakob Nordlander

A Master Thesis Report written in collaboration with
Department of Industrial Information and Control Systems
Royal Institute of Technology
and
Svenska Kraftnät
with financial support from
MSB - the Swedish Civil Contingencies Agency
Stockholm, Sweden

02, 2009

Abstract. During the past couple of years the amount of connections into SCADA (Supervisory Control And Data Acquisition) systems has increased rapidly. At the same time SCADA systems have gone from using proprietary protocols and software to using the same standard solutions as administrative IT systems. As a consequence the 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. To help make the work with SCADA security easier several standards and guidelines have been developed. There also exist general information security standards that are being used; however there exists no overview of how these standards/guidelines prioritize countermeasures and how SCADA specific standards differ from the general information security standards. This thesis investigates which SCADA security standards/guidelines that exist and try to measure how they prioritize countermeasures. This is then compared to the general information security standard ISO 17799. A delimitation of this thesis is to not deal with the physical security of the systems. The execution of this thesis includes the following five steps:

- Identification of standards and guidelines
- Gathering of attacks and countermeasures mentioned in the documents
- Dividing of the attacks and countermeasures into groups
- Identification of keywords associated with each group
- Compilation of the results when searching for the keywords

The results show that there exist three prominent standards, DHS, NIST Guide and ISA. Some of the more important areas of countermeasures are cryptography, authentication, authorization, firewall, intrusion detection. The comparison with ISO 17799 shows that the SCADA specific standards lack focus in the area of non-technical countermeasures. One conclusion is that all the standards have the same core information but they all have different focus, in some cases the difference can be substantial. Therefore the choice of which standards to use should be carefully considered. If ISO 17799 is the standard that is currently being used then the technical countermeasures is most likely the area where the most work is needed.

Keywords. SCADA Security Standards, Prioritization of countermeasures, Comparison between standards, ISO 17799

Table of Contents

Figures and Tables

1 Introduction

This chapter will give the background to this master thesis and present the purpose and goals. It will also give the delimitations of the thesis and an outline to this report.

1.1 Background

SCADA (Supervisory Control And Data Acquisition) systems are used to supervise and control infrastructure. These systems have existed for a long time and have developed as computer capacity has increased. As computers have become more advance and complex, so have SCADA systems. The development of SCADA started before the time of the Internet in a period of time when the IT-security needed mostly consisted of protecting the physical access to the computers of the system. During the last ten years the number of connections into SCADA systems and the use of Internet based techniques have increased rapidly. SCADA systems have also gone from using proprietary protocols and software to using the same standard solutions as administrative IT systems. As a consequence the 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. To make things even more troublesome, normal state of the art security solutions are not always applicable to SCADA systems. One reason for this is the different requirements on for example performance between administrative IT systems and SCADA systems. Even though SCADA systems resemble administrative IT systems there are some important differences. SCADA systems are for example more time critical, have higher demand on availability and are often more difficult to upgrade. [46]

To help make the work with SCADA security easier several standards and guidelines have been developed. There exist several organisations that work with this, including: AGA, NIST, CPNI, IEC and NERC. Some of these organizations, like NIST, develop several different standards and guidelines dealing with different areas of SCADA security, while others, like AGA, focus on specific areas. In the US some standards are mandatory, amongst these NERC CIP 002-009 [41].

This thesis is sponsored by Svenska Kraftnät (SvK) and the Swedish Civil Contingencies Agency (MSB). SvKs activities stretch over several areas such as

- Administration and operation of the Swedish power grid
- Responsibility of the balance and security within the power grid
- Coordination of the electricity supply in crisis situations
- Telecommunication necessary to remotely supervise and operate the power grid

Central to SvKs operation is the SCADA systems used to control and supervise the power grid in real time. The system supervises and controls components spread over a large geographical area. Since SvKs SCADA system is necessary to ensure continued electric distribution in Sweden there is great reason to protect the system from external and internal threats. SvK is currently using the general information security standard ISO 17799.

1.2 Purpose and goals

The purpose of this master thesis is to improve knowledge in the area of IT security standards and guidelines for SCADA systems and to gain a better understanding of what can be done in addition to the various measures suggested by ISO 17799.

The goals of this master thesis:

- To create an inventory of available standards and guidelines and measure their level of density
- To discover the prioritization of countermeasures in the standards and guidelines
- To compare a selected group of these standards and guidelines against ISO 17799 and be able to show the differences between them

1.3 Delimitation

The physical security of the system is important but it is not the focus of this thesis. Therefore physical countermeasures are not a part of the prioritization and it has not been considered when trying to measure the level of density for the standards and guidelines.

1.4 Outline

1. Introduction:

This first chapter gave an introduction to this thesis, explaining the

- Background
- Purpose
- Goals
- Delimitations

2. Background on SCADA systems:

The second chapter contains an introduction to SCADA systems, an overview of the differences between SCADA systems and other IT systems described in other works. This chapter also contains a part in which the different organizations that writes standards and guidelines and the standards and/or guidelines that they have written are presented.

3. Method:

The third chapter explains the method used throughout this thesis. It explains how the standards and guidelines that are a part of this thesis were selected. Furthermore it explains how the attacks and countermeasures were found, how they were divided into groups and how they were prioritized.

4. Data:

The fourth chapter presents the data that is relevant to the analysis.

5. Result and Analysis:

The fifth chapter analyzes the data that was presented in chapter four. The analysis tries to answer such questions as which standards and guidelines have the highest level of density, why is the focus of the standards on countermeasures, which countermeasures are the most prioritized and what is the difference between ISO 17799 and the SCADA specific standards and guidelines.

6. Conclusion:

This chapter draws conclusions based upon the analysis in chapter 5.

2 Background on SCADA systems

This chapter aims to give background information useful when reading this thesis. This chapter includes an overview of SCADA systems, an overview over the standardization work done so far and a description of the differences between SCADA systems and normal IT systems based on the description in NIST [46].

2.1 Overview of SCADA systems

A SCADA system is a system used to supervise and control infrastructure such as electrical power grids, dams, telecommunications etc. Differential for this critical infrastructure is the demands on real time operation and very high availability. If something goes wrong in these systems it may have serious consequences like human injury, death or environmental damages [46].

History[1]

When SCADA systems were first used in the 1930s their main use was to save in on the amount of personnel needed on the field and to get a better overview of the process. As technology evolved so did the SCADA systems. Computer capacity increased which gave the system the ability to manage more data. In the 1960s and 1970s the main challenge was to manage large amount of data while keeping performance high and to handle the high complexity of the systems. In those days the starting point was that only people with physical access to the system had access to the data and even if someone got access to the data they would not know what it meant. Computer security was not prioritized.

During the 1980s the development continued, even more computer capacity led to more advance functions in the system. This in turn led to the possibility to push the power systems closer to the limit of what was physically possible. The main use of the systems evolved from being a way to save in on personnel to being necessary for normal operation.

About this time the available bandwidth started to increase. This made it possible to introduce more measuring points into the system which in turn led to the introduction of more components. To decrease the dependency on specific vendors the communications between the central server and the components of the system was standardized. In particular the communications to the remote terminal units (RTUs) were standardized by IEC. In this standardization no attention was directed to the security issues. The communications were not encrypted and could easily be eavesdropped on.

In the end of the 1990s the rapid development of the IT area created many new possibilities for what could be done with IT systems. It became popular to connect systems and this led an increase in the number of connections into the SCADA systems, this included an increase in the number of connections to the internet. Along with this the use of standardized protocols and software solutions increased. The use of standardized protocols and software solutions led to an increase in the number of known vulnerabilities of the systems, the SCADA systems were suddenly vulnerable to the same exploits as ordinary IT systems. This has become very clear with some of the latest years incidents with computer viruses and worms spreading to the systems [50]. Some of these vulnerabilities are extra troubling in SCADA systems because some of the solutions applied in the general IT world can

[1] The information in this section is a summary of chapter 2.1 - 2.4 from [32]

not be applied in SCADA systems. The reason for this is the difference in demands between ordinary IT systems and SCADA systems [46]. For more about this see chapter 2.2.

The use of SCADA Systems

SCADA systems range from being relatively simple to extremely complex. The system can contain thousands of different assets capable of measuring and/or controlling the process. The different assets are usually geographically dispersed, sometimes over thousands of square kilometers. The communication between the assets and the control system can range from high speed communication such as WAN to low speed communication such as through the telephone system. [46]

SCADA systems perform two main tasks. They perform centralized monitoring of the system and they control it. Data from all parts of the system is sent to the central SCADA server. The data is collected, stored in long time storage and interpreted in aspect of different set points that has been set by human operators. If anything unusual is detected the system can take action, either by sending commands itself or by alerting a human operator. [46]

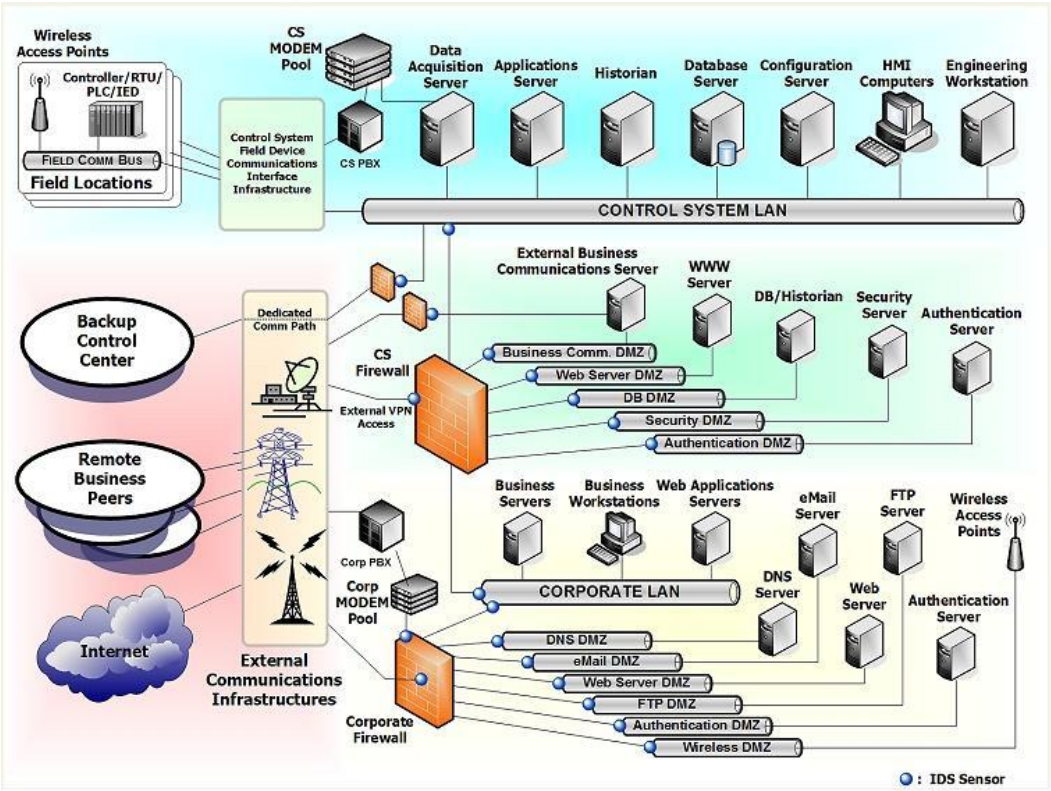

Figure 1 – A SCADA System, [http://csrp.inl.gov/Secure_Architecture_Design.html]

SCADA System Components

SCADA systems consist of many components, some of the more important are:

SCADA Server or Master Terminal Unit (MTU). A MTU acts as the master in a SCADA system. The RTUs and PLCs usually act as slaves. [46]

Remote Terminal Unit (RTU). A RTU is a data acquisition and control unit often used in power stations. RTUs often have the possibility to use wireless communications in case cabled communication is not available. [46]Modern RTUs may for example also have Ethernet ports available and be capable of running web servers [35].

Programmable Logic Controller (PLC). A PLC is a computer used to provide system control of industrial processes. It is designed to perform the logic functions executed by electrical hardware such as relays, switches, and mechanical timer/counters. PLCs are often used instead of RTUs because they are more flexible and economical. [46][12]

Intelligent Electronic Devices (IED). IEDs are sometimes referred to as intelligent end devices. An IED could also be said to be an intelligent sensor/actuator capable of collecting data, processing that data and use it to control the local process and communicating with other devices. [46][12]

Human-Machine Interface (HMI). HMIs are the bridge between human and machines. The data from the SCADA system needs to be presented in a way that a human can understand. That is the job of the HMI. A human can also control the process by using the HMI. Sometimes HMI are also capable of other functions, like showing historical data. [46][12][40]

Data Historian. The data historian saves all process information in a central server. The data can be used to perform analyses. The data is often accessed from both the control network and the corporate network making the data historian server a possible way to gain access to the control system. [46]

Communications Routers. Routers connect separated networks and forwards traffic between them for example by connecting a LAN to a WAN. [46][12]

Modems. Modems are used to provide long-distance communications through the telephone network. They are often used to connect field stations with the central server. Modems are often overlooked when it comes to security and are often used as backdoors into the system. [46][12]

2.2 Differences between SCADA systems and administrative IT systems

In the beginning SCADA and administrative IT systems had little in common, however during the last years that has changed. During the last decade SCADA systems have gone from using proprietary protocols and specialized hardware and software to using standardized protocols and equivalent hardware and software as used in administrative IT systems [46][12][29]. At the same time the connectivity between SCADA systems and other systems has increased dramatically [46][29]. The effect of this is that SCADA systems resemble ordinary IT systems and share the same vulnerabilities. Security solutions exist that can protect administrative IT systems but these can not always be applied to SCADA systems. The reason is that SCADA systems have other requirements [46]. In the following chapter some of the differences between SCADA systems and ordinary IT systems will be explained.

In general IT security it is usually said that there are three things you want to protect. Confidentiality, integrity and availability, this is commonly referred to as CIA. In short to protect the systems confidentiality is to protect the information in the system from disclosure. To protect the integrity of the system is to protect it from unauthorized changes. To protect the availability of the system is to make sure it is possible to use the data and/or resources of the system when requested [3]. In administrative IT systems these are usually prioritized as CIA while in SCADA systems they might instead be prioritized as AIC [46]. One reason for this is that SCADA systems work with actual

physical processes and loss of availability could have serious impacts on the physical world. The consequences include endangerment to human life and loss of equipment. The typical IT system has no interaction with physical processes [46].

The performance requirements of SCADA systems and administrative IT systems differ quite a lot [46]. SCADA systems are time-critical and delay or jitter can not be accepted, the throughput on the other hand does not need to be as high. In administrative IT systems it is usually the other way around. Another effect of the performance requirements is that in an administrative IT system the time it takes for an operator to respond to an event might not be critical. In a SCADA system it might be crucial that an operator is able to respond right away. It is very important that security measures in no way prevent the operator from executing critical commands. An example would be the use of passwords on machines that are used to respond to critical events from the system.

Today many SCADA systems are partially built on so called legacy systems. A legacy system is an old system that continues to be used due to some reason it is problematic to replace it. A problem with legacy systems is that they may for example lack the possibility to do encryption or use password protection making it impossible to implement security measures. [46]

Change management in general is more difficult in SCADA systems than in administrative IT systems. For example in administrative IT systems it might not be a disaster if the system crash after being patched. In a SCADA system this would be unacceptable, one reason being the high demands on availability. System patches and all other changes need to be thoroughly tested before they can be applied. Some SCADA components might use software that is no longer supported by the vendor effectively leaving them with security holes that can never be fixed. Also the components of ICS might not always be that easy to access making it harder to update them regularly. [46]

Further problems are that all vendors of SCADA systems might not allow the installation of third party applications on the system (or it might lead to the loss of support on the system). This would prevent the installation of for example antivirus on ICS. Also the lifetime of ICS is also longer than most administrative IT systems, usually 15-20 years (in other words there might be systems from the 80s still being used today). [46]

Table 1 – The differences between administrative IT systems and SCADA systems [46]

Category	**Information Technology System**	**Industrial Control System**
Performance Requirements	Non-real-time Response must be consistent High throughput is demanded High delay and jitter maybe acceptable	Real-time Response is time-critical Modest throughput is acceptable Delay and/or jitter is not acceptable
Availability Requirements	Responses such as rebooting are acceptable Availability deficiencies can often be tolerated, depending on the system's operational requirements	Responses such as rebooting may not be acceptable because of process availability requirements Availability requirements may necessitate redundant systems Outages must be planned and scheduled days/weeks in advance High availability requires exhaustive pre-deployment testing

Risk Management Requirements	Data confidentiality and integrity is paramount Fault tolerance is less important – momentary downtime is not a major risk Major risk impact is delay of business operations	Human safety is paramount, followed by protection of the process Fault tolerance is essential, even momentary downtime may not be acceptable Major risk impacts are regulatory non-compliance, environmental impacts, loss of life, equipment, or production
Architecture Security Focus	Primary focus is protecting the IT assets, and the information stored on or transmitted among these assets. Central server may require more protection	Primary goal is to protect edge clients (e.g., field devices such as process controllers) Protection of central server is also important
Unintended Consequences	Security solutions are designed around typical IT systems	Security tools must be tested (e.g., off-line on a comparable ICS) to ensure that they do not compromise normal ICS operation
Time-Critical Interaction	Less critical emergency interaction Tightly restricted access control can be implemented to the degree necessary for operations	Response to human and other emergency interaction is critical Access to ICS should be strictly controlled, but should not hamper or interfere with human-machine interaction
System Operation	Systems are designed for use with typical operating systems Upgrades are straightforward with the availability of automated deployment tools	Differing and possibly proprietary operating systems, often without security capabilities built in Software changes must be carefully made, usually by software vendors, because of the specialized control algorithms and perhaps modified hardware and software involved
Resource Constraints	Systems are specified with enough resources to support the addition of third-party applications such as security solutions	Systems are designed to support the intended industrial process and may not have enough memory and computing resources to support the addition of security capabilities
Communications	Standard communications protocols Primarily wired networks with some localized wireless capabilities Typical IT networking practices	Many proprietary and standard communication protocols Several types of communications media used including dedicated wire and wireless (radio and satellite) Networks are complex and sometimes require the expertise of control engineers

Change Management	Software changes are applied in a timely fashion in the presence of good security policy and procedures The procedures are often automated	Software changes must be thoroughly tested and deployed incrementally throughout a system to ensure that the integrity of the control system is maintained ICS outages often must be planned and scheduled days/weeks in advance
Managed Support	Allow for diversified support styles	Service support is usually via a single vendor
Component Lifetime	Lifetime on the order of 3-5 years	Lifetime on the order of 15-20 years
Access to Components	Components are usually local and easy to access	Components can be isolated, remote, and require extensive physical effort to gain access to

2.3 Overview of SCADA Security Standards and Guidelines

In this chapter an overview of the different organizations that create standards and guidelines for SCADA systems will be given. There will also be a brief introduction to the standards and guidelines that exist. This is not all the available standards but rather a selection made from a Swedish perspective. Those who have knowledge about the different organizations and the standards they have written can skip this part without omitting necessary information.

Table 2- The organization and standards/guidelines presented in chapter 2.3.

AGA	AGA 12 Part 1
CPNI	Good Practice Guide, Process Control and SCADA Security
DHS	Cyber Security Procurement Language for Control Systems Catalog of Control Systems Security: Recommendations for Standards Developers
DOE	21 steps to Improve Cyber Security of SCADA Networks
GAO	Cyber security for Critical Infrastructure Protection
IEC	Power system control and associated communications – Data and communication security (62210) Power systems management and associated information exchange – Data and communications security, Part 1: Communication network and system security - Introduction to security issues 62351-1
IEEE	IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities IEEE Guide for Electric Power Substation Physical and Electronic Security
ISA	ANSI/ISA–99.00.01–2007 Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models ANSI/ISA-TR99.00.01-2007 Security Technologies for Industrial Automation and Control Systems ANSI/ISA—TR99.00.02—2004 Integrating Electronic Security into the Manufacturing and Control Systems Environment
ISO	17799: Information technology — Security techniques — Code of practice for information security management
KBM	Aspekter på Antagonistiska Hot mot SCADA-system i samhällsviktiga verksamheter Vägledning till ökad säkerhet i digitala kontrollsystem i samhällsviktiga verksamheter
NERC	CIP-002-1 - CIP-009-1
NIST	System Protection Profile - Industrial Control Systems Field Device Protection Profile for SCADA Systems In Medium Robustness Environments Guide to Industrial Control Systems (ICS) Security
SÄPO	Säkerhetsskydd – en vägledning

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. AGAs vision is

"To be the most effective and influential energy trade association in the United States while providing clear value to its membership" [2]

AGAs mission statement is

"The American Gas Association represents companies delivering natural gas to customers to help meet their energy needs. AGA members are committed to delivering natural gas safely, reliably and cost-effectively in an environmentally responsible way. AGA advocates the interests of its members and their customers, and provides information and services promoting efficient demand and supply growth and operational excellence in the safe, reliable and efficient delivery of natural gas." [2]

AGA 12 part 1

The scope of AGA 12 part 1 is to describe the need for SCADA systems protection. This document proposes steps to define cyber security goals and cyber security fundamentals. More significantly AGA 12 part 1 defines the cryptographic system requirements and constraints, and a cryptographic test plan. The purpose of the document is to save SCADA system owners' time and effort by proposing a comprehensive system designed specifically to protect SCADA communications. [1]

CPNI

CPNI is the abbreviation for Center for the Protection of National Infrastructure. CPNI is a British agency that was created on first of February 2007. CPNI is a merge of the National Infrastructure Security Co-ordination Centre (NISCC) and the National Security Advice Centre (NSAC, a part of MI5) [7]. NISCC used to provide advice and information regarding computer network defense and other information assurance issues while NSAC provided advice on physical security and personnel security issues [7].

"CPNI provides integrated (combining information, personnel and physical) security advice to the businesses and organizations which make up the national infrastructure. Through the delivery of this advice, we protect national security by helping to reduce the vulnerability of the national infrastructure to terrorism and other threats." [7]

Good Practice Guide, Process Control and SCADA Security

They state in the document that their aim is "to provide good practice principles for process control and SCADA security". In the document good practice is defined as

"The best of industry practices such as strategies, activities, or approaches, which have been shown to be effective through research and evaluation."

To do this they have identified seven different areas. [6]

- Understand the business risks
- Implement secure architecture

- Establish response capabilities
- Improve awareness and skills
- Manage third party risks
- Engage projects
- Establish ongoing governance

DHS

DHS is the abbreviation for Department of Homeland Security. DHS is an US government agency created in 2002 in the aftermath of September 11. The agency was formed from 22 other agencies. It has about 180,000 employees [13]. DHS assignment is basically to protect the US.

"This Department of Homeland Security's overriding and urgent mission is to lead the unified national effort to secure the country and preserve our freedoms. While the Department was created to secure our country against those who seek to disrupt the American way of life, our charter also includes preparation for and response to all hazards and disasters. The citizens of the United States must have the utmost confidence that the Department can execute both of these missions" [14].

Cyber Security Procurement Language for Control Systems

This document is supposed to give advice to people that are either procuring a new system or procuring an update for an existing system. It summarizes which security principles that should be considered when designing or procuring new systems. It consists of twelve chapters; each chapter consists of eight parts. First there is a summary that motivates why the subject is included in the document, next there are two sections on the language to be used when procuring the system. It continues with FAT and SAT measures and ends with a maintenance guide, references and dependencies. The document deals with such areas as hardening, firewalls and auditing. [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 several resources. The document is divided into 18 separate chapters, the goal is to be able to balance security while operating within resource limits. Some examples of areas that the document deal with are Security Policy, Configuration Management, Security Awareness and Training and Access Control. At the very end of the document there is a table comparing the content of this document against the content of other standards [11].

DOE

DOE is the abbreviation for Department of Energy. DOE is a U.S. federal agency. It was formed on October the first 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 [10].

"The Department of Energy's overarching mission is to advance the national, economic, and energy security of the United States; to promote scientific and technological innovation in support of that mission; and to ensure the environmental cleanup of the national nuclear weapons complex." [9].

21 steps to Improve Cyber Security of SCADA Networks

This is a short but very informative document summarizing twenty-one items that is important when securing SCADA systems. Some of the subjects brought up are [44]

- Identify all connections to SCADA networks
- Do not rely on proprietary protocols to protect your system
- Establish a network protection strategy based on the principle of defense-in-depth
- Establish system backups and disaster recovery plans

GAO

GAO is the abbreviation for Government Accountability Office. GAO is "an independent, nonpartisan agency that works for Congress. Often called the "congressional watchdog," GAO investigates how the federal government spends taxpayer dollars" [51]. GAO was formed in 1921 and currently employs about 3000 employees [52].

"Our Mission is to support the Congress in meeting its constitutional responsibilities and to help improve the performance and ensure the accountability of the federal government for the benefit of the American people. We provide Congress with timely information that is objective, fact-based, nonpartisan, nonideological, fair, and balanced" [51].

Cyber security for Critical Infrastructure Protection

This is a general document about critical infrastructure protection focusing (according to the document itself) on:

1. What are the key cybersecurity requirements in each of the critical infrastructure protection sectors?
2. What cybersecurity technologies can be applied to critical infrastructure protection? What technologies are currently deployed or currently available but not yet widely deployed for critical infrastructure protection? What technologies are currently being researched for cybersecurity? Are there any gaps in cybersecurity technology that should be better researched and developed to address critical infrastructure protection?
3. What are the implementation issues associated with using cybersecurity technologies for critical infrastructure protection, including policy issues such as privacy and information sharing? [53]

IEC

IEC is the abbreviation for International Electrotechnical Commission. The IEC was founded in 1906 and is the leading global organization that prepares and publishes standards for electric, electronic and related technologies.

The Commission's objectives are to [22]:

- Meet the requirements of the global market efficiently
- Ensure primacy and maximum world-wide use of its standards and conformity assessment systems
- Assess and improve the quality of products and services covered by its standards

- Establish the conditions for the interoperability of complex systems
- Increase the efficiency of industrial processes
- Contribute to the improvement of human health and safety
- Contribute to the protection of the environment

Power system control and associated communications – Data and communication security (62210)

This report deals with security aspects related to communication protocols used within and between systems specializing in computerized supervision, control, metering and protection in electrical utilities. The report identifies some threats and vulnerabilities that can be found in SCADA systems. It also gives directions to other IEC documents where countermeasures to these problems can be found. Finally the report gives recommendations for further security work [23].

Power systems management and associated information exchange – Data and communications security, Part 1: Communication network and system security - Introduction to security issues 62351-1

The scope of the IEC 62351 series is information security for power system control operations. This document 62351-1 is supposed to provide an introduction to the remaining parts of the standard by introducing various aspects of information security as applied to power system operations.

The report starts by giving some background where it is explained why it is necessary to address these issues. It continues by discussing the different threats against the system. These include inadvertent threats as equipment failure and advertent threats such as viruses. The report goes deeper into the different attacks that exist and divide them into categories. For each category they then state a number of countermeasures that could be applied to reduce this threat. There is also a section on the challenges with applying these security measures to power systems. Finally there is an overview of the rest of the series [24].

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 fields it is simply referred to as IEEE (pronounced Eye-triple-E) [17]. IEEE is a non profit organization, one of the worlds leading professional associations for the advancement of technology. IEEE was formed on first of January 1963 from a merge between the AIEE (American Institute of Electrical Engineers) and IRE (Institute of Radio Engineers). Today IEEE has more than 375 000 members in more than 160 countries [16].

"IEEE's core purpose is to foster technological innovation and excellence for the benefit of humanity" [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. Electronic access control requirements specify how the access to the IEDs should work. It is specified amongst other things that there should be a password and an access time-out. Audit trail specifies how the IED shall be audited. It is said that the record should be stored in a sequential circular buffer that is capable of saving at least 2048 events before it overwrites old events. The supervisory and monitoring requirements specify how the IED should monitor the security related activities and make them available in real time to a supervisory system. The configuration and

software requirements are there to make sure that it is not possible to make changes to the configuration without being properly authenticated [20].

IEEE Guide for Electric Power Substation Physical and Electronic Security

This standard discuss "security issues related to human intervention during the construction, operation (except for natural disasters), and maintenance of electric power supply substations". This standard deals with physical security as well as electronic security. The report starts by defining different sort of intrusions that can occur at a substation. Electronic intrusion is specified as one way to intrude on a substation. The report continues with parameters that might affect intrusion and possible consequences. Further the report discuss different countermeasures, first physical, then electronic. The electronic countermeasures include computer security measures which consist of amongst other things dial-back verification and virus scans. Finally a survey is presented where the effectiveness of the countermeasures presented in the standard have been measured. [18]

ISA

ISA is the abbreviation for The Instrumentations, Systems, and Automation Society.ISA was founded on 28 April 1945 in the US.

"The mission of ISA as the global society for instrumentation, systems, and automation is to [31]:

- Maximize the effectiveness of ISA members and other practitioners and organizations worldwide to advance and apply the science, technology, and allied arts of instrumentation, systems, and automation in all industries and applications.
- Identify and promote emerging technologies and applications.
- Develop and deliver a wide variety of high-value information products and services to the global community.

ANSI/ISA–99.00.01–2007 Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models

The scope of this document is to define the terminology concepts and models for SCADA systems. It establishes the basis for the remaining standards in the ISA99-series. It addresses questions such as

- What are the major concepts that are used to describe security?
- What are the important concepts that form the basis for a comprehensive security program?

It also describes a series of models that can be used when designing a security program [28].

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 cyber security tools, mitigations, counter-measures and technologies that may be used in SCADA systems. The document 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. [29]

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 of creating a security program. It continues by specifying the different activities associated with the systems security life cycle. These activities include but are not limited to assessing and defining the existing system, define component test plans, define system validation test plan, routine security reporting and analysis [30].

ISO

ISO is the abbreviation for International Organization for Standards. ISO 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 is a non-governmental organization that was founded in 1946 on a conference in London. Some of ISOs current goals are [27]

- Facilitation of global trade
- Improvement of quality, safety, security, environmental and consumer protection as well as the rational use of resources
- Global dissemination of technologies and good practices

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 Maintainance
- Information Security Incident Management
- Business Continuity Management
- Compliance

In each area a control objective is defined stating what is to be achieved. Then the different controls that can be used to reach the objective are defined. For each control it is described how the control will satisfy the objective, how to implement it and in the end there is additional information if it is needed (for example legal requirements) [26].

KBM

KBM is the abbreviation for Krisberedskapsmyndigheten. KBM is a Swedish government agency assigned to coordinate the efforts in developing the management of serious crisis in the Swedish society. This includes many task one of them being to supply knowledge; this is done for example by conducting and supporting research [33]. Please note that according to a Swedish parliament decision KBM, Räddningsverket and ”Styrelsen för psykologiskt försvar” will be terminated and form a new agency named “Myndigheten för samhällsskydd och beredskap” (MSB). This decision is effective as of January 1, 2009 [34].

Aspekter på Antagonistiska Hot mot SCADA-system i samhällsviktiga verksamheter

There exists both a Swedish and an English version of this report. The English title is “**Guide to Increased Security in Process Control Systems for Critical Societal Functions”**. The purpose of this report is to give a first overview of the need for SCADA security and to try and show how the vulnerabilities in these systems have been created. The report also describes the different activities carried out internationally. This report is not supposed to give deep technical insight but only a overview. [32]

Vägledning till ökad säkerhet i digitala kontrollsystem i samhällsviktiga verksamheter

This document is available in both Swedish and English. It is mainly built upon the following documents

- NERC CIP-002-1 till CIP-009-1
- NIST SP 800-82 – Guide to Industrial Control Systems (ICS) Security
- CPNI Good Practice Guide Process Control and SCADA Security
- 21 Steps to Improve Cyber Security of SCADA Networks
- Krav til informasjonssikkerhetsnivå i IKT-baserte prosesskontroll-, sikkerhetsog støttesystemer
- Cyber Security Procurement Language for Control Systems

The document is divided into three parts. The first part is about background, why security in industrial control systems is important, the difference between security in industrial control systems and regular IT systems and some summarizing recommendations on how to do industrial control system security. The second part is more detailed recommendations on how to create secure industrial

control systems. There is fifteen different subjects amongst them defense-in-depth, how to perform risk analysis and hardening of an industrial control system. The third part is a list of the documents that been used as reference and some comments to each document [35].

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 U.S. Federal Energy Regulatory Commission and governmental authorities in Canada. NERCs mission is to ensure the reliability of the bulk power system in North America. To achieve this NERC:

"Develops and enforces reliability standards; assesses adequacy annually via a 10-year forecast and winter and summer forecasts; monitors the bulk power system; audits owners, operators, and users for preparedness; and educates, trains, and certifies industry personnel" [41]

CIP-002-1 - CIP-009-1

CIP stands for Critical Infrastructure Protection. Power companies in the US are required to comply with the CIP standards[1]. 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. [43]

- **CIP 001-1:** Sabotage Reporting
- **CIP 002-1:** How to identify your critical cyber assets and how to document them.
- **CIP 003-1:** Which security management controls should be used and how should they be used.
- **CIP 004-1:** How to train your personnel to become more security aware and how to make treat personnel risks.
- **CIP 005-1:** How to secure your critical cyber assets with the help of a electronic perimeter
- **CIP 006-1:** Physical Security
- **CIP 007-1:** System security management, how to patch, how to do anti virus etc.
- **CIP 008-1:** Incident planning and documentation
- **CIP 009-1:** Recovery plan

NIST

NIST is the abbreviation for National Institute of Standards and Technology. NIST is a US non-regulatory federal agency founded in 1901.

"NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life." [39]

NIST consists of different programs one of them being the NIST laboratories. One of the laboratories is the Information Technology Laboratory who amongst other things conducts research on computer security [37]. Their research also includes control system security. NIST for example hosts the Process Control Security Requirements Forum (PCSRF) [38].

[1] CIP-001-1 not included

Field Device Protection Profile for SCADA Systems In Medium Robustness Environments

This document specifies minimum security requirements for SCADA field devices. The document lists some threats against SCADA systems and describes some security objectives. There are functional and assurance requirements and a rational for that these are complete. [8]

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 ICS, tries to identify the threats against an ICS are and the vulnerabilities of an ICS. It also brings up the subject of how to develop and deploy and ICS security program. This includes such aspects as how to use business cases, how to obtain support from senior management and how to create security teams. The document also gives suggestions on how to construct the network. It gives examples and brings up the pros and cons of them. The document finally gives more SCADA specific instructions on how to solve the different security problems in for example the following areas [46]:

- Risk Assessment
- Personnel Security
- Incident Response
- Identification and Authentication

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. The document lists a set of threats that should be addressed by security controls implemented by the STOE. It identifies the risks to the STOE and defines the security objectives. There are functional and assurance requirements that must be satisfied by the STOE, derived from CC part 2 and 3. [40]

SÄPO

SÄPO is the abbreviation for Säkerhetspolisen. SÄPO is the Swedish security police. The Swedish security police was first formed in 1914, it has existed in its current form since 1989 [47]. SÄPOs task is to prevent and expose crime against national security. Further SÄPO shall fight terrorism and protect the central government. The purpose is to protect the democratic system, the rights of the citizens and the national security [48].

Säkerhetsskydd – en vägledning

This document discusses general information security. The discussion is linked to which parts of the Swedish law that affects it. The document gives some general directions, deals with information security for secret documents in writing or pictures, deals with information security for secret documents in IT systems. It also gives advice on how to restrict admittance to secure sites and how to perform record checks.

3 Method

In this chapter the method used throughout this thesis will be presented. This includes how the selection of standards and guidelines was done, how the attacks and countermeasures were identified, how they were divided into groups, how the keywords were selected and how the results were compiled

3.1 Workflow

The work in this thesis has basically been conducted in the five steps as shown in **Figure 2**. A more exhaustive description of each step can be found below.

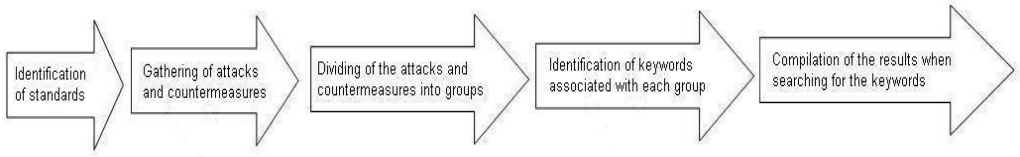

Figure 2 – The workflow of this thesis

Identification of standards and guidelines

The first step was to create an inventory of the available standards and guidelines. The starting point of this inventory was a list of known standards and guidelines. These standards and guidelines were studied and by following the references made within them further standards and organizations writing standards were identified. There exists articles where they have summarized some of the standardization work that is currently being done [5][21]; this was another source of information. This process continued in parallel with other activities. Since not all of the standards and guidelines found seemed relevant the selection process described in chapter 3.2 was performed.

Gathering of attacks and countermeasures

To be able to find out how the standards and guidelines prioritize the countermeasures the countermeasures must first be identified. This process started by simply searching each standard and guideline for all possible mentioning of countermeasures and attacks. When an attack or countermeasure was found it was given a number, a name, if needed a description and the page where it was found was noted. This was an iterative process that was performed several times. Each time a mentioning of a countermeasure is found it is possible that new information is discovered that can be used to find more information in other standards and guidelines.

Dividing of the attacks and countermeasures into groups

When all the attacks and countermeasures had been found they were divided into groups. The reason for this is that there are so many attacks and countermeasures that it is hard to work with them. The attacks or countermeasures placed within the same group have the same objective, for example

authentication, password authentication and biometric authentication are all placed within the authentication group. The groups and a short description of their content can be found in chapter 4.1.

Identification of keywords associated with each group

The next step was to identify keywords that could be associated with each group. This was done by following all the references that belongs to each group. For each reference, keywords that could be associated with that particular countermeasure / attack was identified. One important property for a keyword is that it is not too general since this will generate false hits. An example of a group and some of its keywords is shown in **Table 3**.

Table 3 – Group three and some of its keywords

3	**Firewall**
	Firewall
	Packet Filtering
	Stateful Inspection
	Application Proxy

Compilation of the results when searching for the keywords

When the steps above had been completed it was time to search each standard and guideline for the keywords that had been identified. The data was compiled per group and per standard/guideline. The number of hits per standard was used to compare the level of density between the standards and help us to reach the first goal of this thesis. The number of hits per group was used to compare the different groups and decide how the groups are prioritized thereby helping us reach the second goal of this thesis. Since all of the above has been completed for ISO 17799 these results can be used to reach the third goal of this thesis as well.

Comparing the number of hits it is obvious that there can be quite a big difference in the number of hits for certain standards/guidelines. The reason is that the standards and guidelines are not equally long. The shortest standard/guideline studied in this thesis is ten pages long while the longest is 287 pages. This makes it hard to compare the standards and guidelines just counting keywords. To be able to create a comparison, the number of hits is also divided by the number of pages. The number of hits per page is more comparable between standards than the number of hits in total as it better reflects the prioritization among countermeasures in the standards/guidelines.

To be able to compare the results for a specific group in the SCADA specific standards against a specific group in ISO 17799 and DHS Catalog the results need to be normalized. The normalization is done by dividing the number of hits per page by the total number of hits. The result is a measurement of how many percent each group stands for. This number is then used to compare the SCADA specific standards against ISO 17799 and DHS Catalog.

Survey investigating the prioritization of countermeasures according to experts

After analyzing the results from the standards it felt like it could be interesting to find out how these countermeasures are prioritized by people who actually work with this area. Therefore it was decided to create a survey that investigates this. It was decided that in order to make things easier a tool named “Focal Point” would be used.

Focal Point is a tool that let an administrator create objects and then make it possible to compare these objects. The objects are compared pairwise and based on this data Focal Point uses something called "Analytical Hierarchical Process" to create a prioritization between all of the objects. For this to work a minimum amount of comparisons need to be completed and the more comparisons the more accurate result. In this case the objects were countermeasures that were identified by their names and the keywords associated with them. The survey was sent to 20 people that all work with SCADA system security.

3.2 Selection of Standards

In this section all the standards and guidelines that have been found will be listed. When working with these documents some standards are treated as one. The ISA 99 documents are all a part of ISA 99 and will be treated as one document. The documents from IEC are related and will also be treated as one. The same goes for the documents from KBM.

To select which standards and guidelines that were to be a part of this thesis three properties were taken into consideration.

1. The standard/guideline must be available
2. The standard/guideline must focus on SCADA system security, not general information security
3. The standard must focus on SCADA systems as a whole; it should not focus on sub systems for example IEDs

In **Table 4** it is shown which standards and guidelines that fulfil which criteria. To be a part of the investigation a standard/guideline must fulfil all three criteria. The exception is ISO 17799 that will be included as a comparison. The standards that do not fulfil all three criteria have not been given an abbreviation.

Table 4 – This table shows which standards that fulfill which criteria for selection

Number	Short name	Reference	Name	Available	Focus on SCADA security	Focus is on the system as a whole
1.	AGA 12	[1]	AGA 12 Part 1	X	X	X
2.	CPNI	[6]	Good Practice Guide, Process Control and SCADA Security	X	X	X
3.	DHS	[12]	Cyber Security Procurement Language for Control Systems	X	X	X
4.	DOE	[44]	21 steps to Improve Cyber Security of SCADA Networks	X	X	X
5.	IEC	[23]	Power system control and associated communications – Data and communication security (62210)	X	X	X
		[24]	Power systems management and associated information exchange – Data and communications security, Part 1: Communication network and system security - Introduction to security issues 62351-1	X	X	X
6.	NERC	[43]	CIP-002-1 - CIP-009-1	X	X	X
7.	NIST, Guide	[46]	Guide to Industrial Control Systems (ICS) Security	X	X	X
8.	NIST, SPP	[40]	System Protection Profile - Industrial Control Systems	X	X	X
9.	ISA	[28]	ANSI/ISA–99.00.01–2007 Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models	X	X	X
		[29]	ANSI/ISA-TR99.00.01-2007 Security Technologies for Industrial Automation and Control Systems	X	X	X
		[30]	ANSI/ISA—TR99.00.02—2004 Integrating Electronic Security into the Manufacturing and Control Systems Environment	X	X	X

10.	GAO	[53]	Cyber security for Critical Infrastructure Protection	X	X	X
11.	KBM	[32]	Aspekter på Antagonistiska Hot mot SCADA-system i samhällsviktiga verksamheter	X	X	X
		[35]	Vägledning till ökad säkerhet i digitala kontrollsystem i samhällsviktiga verksamheter	X	X	X
12.	ISO 17799	[26]	17799: Information technology — Security techniques — Code of practice for information security management	X		X
13.	DHS Catalog	[11]	Catalog of Control Systems Security: Recommendations for Standards Developers	X	X	X
14.	N/A		API 1164 – "SCADA Security"		X	X
15.	N/A	[8]	Field Device Protection Profile for SCADA Systems In Medium Robustness Environments	X	X	
16.	N/A	[20]	IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities	X	X	
17.	N/A	[18]	IEEE Guide for Electric Power Substation Physical and Electronic Security	X	X	
18.	N/A	[49]	Säkerhetsskydd – en vägledning	X		

3.3 Validity and Reliability

The selection of standards will affect the final result. In this thesis the selection is based on distinct criteria documented in chapter 3.2. It is possible that not all available standards are a part of this investigation but the most common ones are. The selection process has been very thorough and it has also taken help from other documents that investigates which standards that exists [5][21]. One standard that could have been relevant to include is Catalog of Control Systems Security: Recommendations for Standards Developers from DHS however this standard is not intended to be used as a regular standard, but as a help for people writing standard. Therefore it has been used to make a comparison instead.

The gathering of attacks and countermeasures is not based on any particular method but was performed very thoroughly in an iterative process. The dividing of the countermeasures and attacks into groups and the selection of keywords associated with each group also affects the result. There is no obvious best way to do this. The countermeasures could have for example been divided by which threat they mitigate, in this case it was chosen to divide them by their security goal. Similar ways of dividing attacks and/or countermeasures have been used in other reports [36][40]. It would have been possible to choose an already existing taxonomy such as the headers of ISO 17799, this would however not catch the things specific to SCADA systems. The selection of both attacks/countermeasures and keywords is based upon the preferences of the performer; however the author have studied these documents very thoroughly and has a high the knowledge of what is actually written in the documents. Furthermore the selection of attacks and countermeasures was performed by two people.

Concerning the reliability everything produced is traceable. There is some subjectivity in the selection of keywords that represents the countermeasures and attacks; however given the chosen keywords the reliability is good. Overall everything is traceable, from the selection of standards, to the selection of attacks and countermeasures, to the dividing of attacks and countermeasures into groups, to the selection of keywords and finally to the measuring of the keywords. The exact data for each keyword can be found in Appendix 2.

The survey was sent out to 20 experts, unfortunately there was not enough time to wait for all the results and therefore only six answers were received. Out of these five responses completed at least the 55 comparisons required to create a valid prioritization. The sixth response completed 28 comparisons. Even though there is not enough data to draw any reliable conclusions the data can still be used to show a trend and to analyze this trend, the data that has been collected it reliable in itself. Focal Point assumes that the objects that are compared are independent from each other; this is not the case in this survey. For example authentication is dependant on cryptography and this might affect the final outcome. Some of the experts made complaints that it was hard to prioritize the countermeasures in the way they were categorized. Therefore the expert survey is treated as a supplement to the standard comparison.

4 Data

In this chapter the data gathered will be presented. First the groups of countermeasures and attacks will be defined. Then the data will be shown. The data is divided into three different groups. First there is the data that is used to show the level of density, then the data that is used to prioritize between different groups. Finally the data used to create a comparison with ISO 17799 is presented.

4.1 Description of Groups

Table 5 – Groups of countermeasures, the keywords associated with each group can be found in Appendix 2

1	Network Security	Network security contains countermeasures aimed at securing the remote connection to the system. This group includes the security of modems, wireless connections, etc. This group also includes measures to protect TCP/IP and DNS.
2	Separation of Network	Separation of network contains countermeasures that help separating the control network from other networks. This group includes such techniques as DMZ and VLAN.
3	Firewall	Firewall contains explanations on how to use a firewall in control systems and suggestions on how to configure and maintain it.
4	Intrusion Detection	Intrusion detection contains explanations of the different intrusion detection systems that exist. It also contains other ways to detect intrusions such as honey pots and profile based anomaly detection.
5	Cryptography	Cryptography contains advice on how to handle encryption in the system. It deals with all cryptographic countermeasures including digital signatures and certificates and similar.
6	Authorization	Authorization contains advice on how to authorize the users of the system. It includes techniques as role based access control and give advice on how to set access rules.
7	Authentication	Authentication contains countermeasures that deal with the authentication of users. It deals with a lot of different techniques such as passwords, biometric authentication, location based authentication etc.
8	Hardening	Hardening contains countermeasures designed to reduce the attack surface of the system. This includes advice on how to remove unnecessary services and how to manage the use of default accounts.

9	Antivirus	Antivirus contains countermeasures that deal with the detection of and protection from malicious software such as viruses, worms etc.
10	Patch Management	Patch management gives information on the problems with patch management in today's control systems. It also gives suggestions on how the process of patch management can be improved.
11	Change Management	Change management contains countermeasures that give advice on how to handle changes in the system. Change management deal with changes to configurations, hardware, software, policies, etc. The main goal is to always maintain the security of the system.
12	Auditing and vulnerability scanning	Auditing and vulnerability scanning contains the countermeasures that are supposed to help in finding flaws in the security design of the system. Auditing also deals with logging the events and actions in the system.
13	Inventory and Overview	Inventory and overview contains advice on how to perform an inventory of the system. This includes all the connections to the system. It also suggests the use of network diagrams.
14	Risk Assessment and Management	Risk assessment and management contains countermeasures that deal with risk assessment and management of risk. It includes finding the risks and how to mitigate them.
15	Security Organization	Security organization contains advice on how to form security teams, who should be included, what competence is needed and more.
16	Training and Awareness	Training and awareness deal with the training of personnel. It also includes suggestions on how to raise security awareness.
17	Personnel Management	Personnel management contains countermeasures used to reduce the security risks that can be associated with personnel. This includes defining security roles for personnel and to have policies about hiring and to remember security in employment contracts.
18	Incident planning and handling	Incident planning and handling deals with what should be done when something has happened. The intrusion detection system might have detected something or a user might have reported suspicious activity. This includes planning, handling and reporting of incidents.
19	Business Continuity and Contingency planning	Business continuity and contingency planning contains countermeasures that are supposed to help when dealing with a disaster. This includes having disaster recovery plans and to test them to make sure they work.
20	System Resilience	System resilience contains countermeasures that increase the resilience of the system. For example having redundant systems and try to avoid having single points of failure.

21	Backup	Backup deal with the issues of creating backups and making sure they work.
22	Third party collaboration	Third party collaboration contains countermeasures that are supposed to reduce the risk that might be introduced by a third party. This includes continuous cooperation and communication. It also gives the advice to use security solutions approved by the vendor.
23	Business Management Commitment	Business management commitment gives advice on how to make sure management is committed to creating a secure system. This includes creating business cases to make it easier to explain to management why security is important.
24	Policies and Standards	Policies and standards contain advice on how to create policies and how to maintain and update them. It also gives advice on what different policies might be needed in the system.
25	Security Principles	This group contains countermeasures such as defense in depth.
26	System administration tools	This group contains tools that help in the administration of the system.

Table 6 – Groups of attacks

1	Denial of Service (DOS)	This group contains all sorts of DOS attacks. It includes both intentional and unintentional DOS and DOS against all parts of the system.
2	Malicious Software	This group contains attacks by malicious software and also discusses how malicious software might get into the system. It also discusses what kind of malicious software there is.
3	Spoofing	This group contains attacks that include some sort of spoofing. It can be IP spoofing, spoofing to perform man-in-the-middle etc.
4	Threats from employees	This group contains attacks that can be made by employees. This includes intentional attacks such as introducing malicious code and unintentional attacks such as issuing the wrong command.
5	Information Gathering	This group contains attacks that try to gather information about the system for example by listening to and analyzing the traffic or by visual observation.
6	Social Engineering	This group contains attacks where the attacker interacts with employees and either tries to gain information from them or tries to trick them into doing something they should not do. An attacker might for example convince an employee to turn off the security system.

7	Remote Connections	This group contains attacks that try to gain access to the system by the remote connections. This includes access through modems (for example war-dialing) and connections from third parties.
8	Replay, interception and modification of data	This group contains attacks that attack the data that is being transmitted in the system. This is done by for example replaying the data or by modifying it.
9	Software flaws	This group contains attacks that try to take advantage of flaws in the software of the system. An example of a common bug is buffer overflow.
10	Web-attacks	This group contains attacks that are usually performed within the web-browser. Examples of this type of attacks are remote file include and cross site scripting.
11	Password stealing/guessing	The attacks in this group try to find out a users password by stealing or guessing it. Guessing of passwords often succeed because passwords are too weak and stealing of passwords might be possible if they are sent in clear text.
12	Non-repudiation attacks	The attacks in this group are aimed at destroying the trace of other malicious activity. This can for example be done by destroying logs.
13	Network Separation	The attacks in this group aim to exploit poorly configured networks to produce broadcast storms or gain access to parts of the network they should not have access to.
14	Attacks against cryptography	The attacks in the group try to break the cryptographic protection of the system.

4.2 Level of density per standard

This data is used to show the level of density for different documents. The method to obtain this data has been described in chapter 3.1.

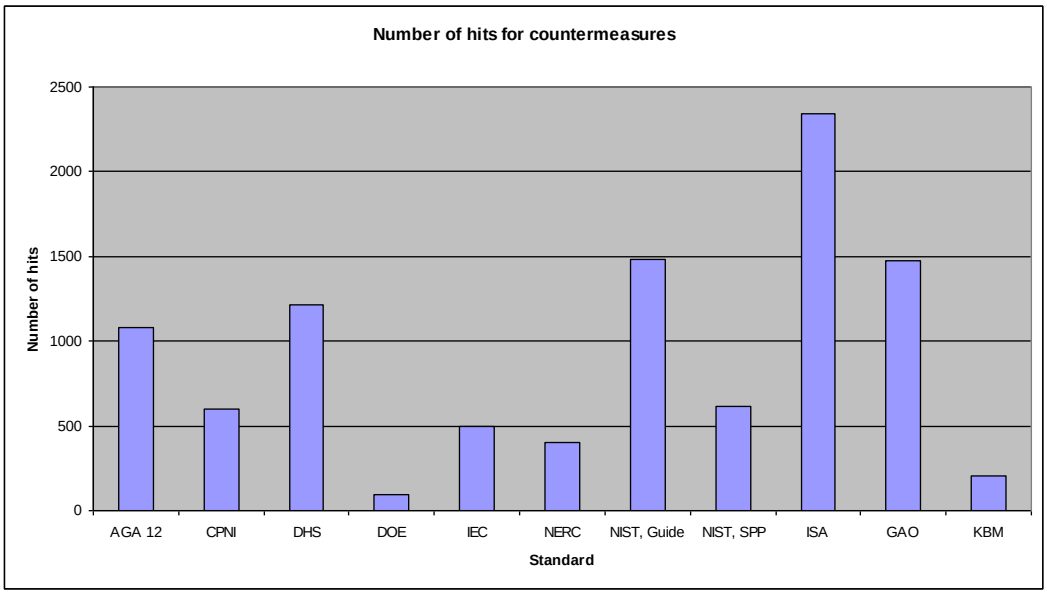

Figure 3 - The number of hits generated by each standard when searching for countermeasures

As can be seen in **Figure 3** the document with the highest amount of hits using this method is the ISA document. The document with the least amount of hits is DOE. An ordered list of the result can be found in **Table 7**.

Table 7 - Number of hits per standard in regard of countermeasures

ISA	2339
NIST, Guide	1485
GAO	1476
DHS	1216
AGA 12	1081
NIST, SPP	612
CPNI	600
IEC	497
NERC	403
KBM	202
DOE	91

Table 8 - The number of pages in each document

	AGA 12	CPNI	DHS	DOE	IEC	NERC	NIST, Guide	NIST, SPP	ISA	GAO	KBM
Pages	123	130	90	10	88	37	157	151	287	223	50

In **Table 8** the different lengths of the documents are shown. ISA and GAO are the two longest. To be able to compare the different documents in terms of density the number of hits needs to be set in proportion to the number of pages. As described in chapter 3.1 the number of hits is divided by the number of pages. The result can be seen in **Figure 4**.

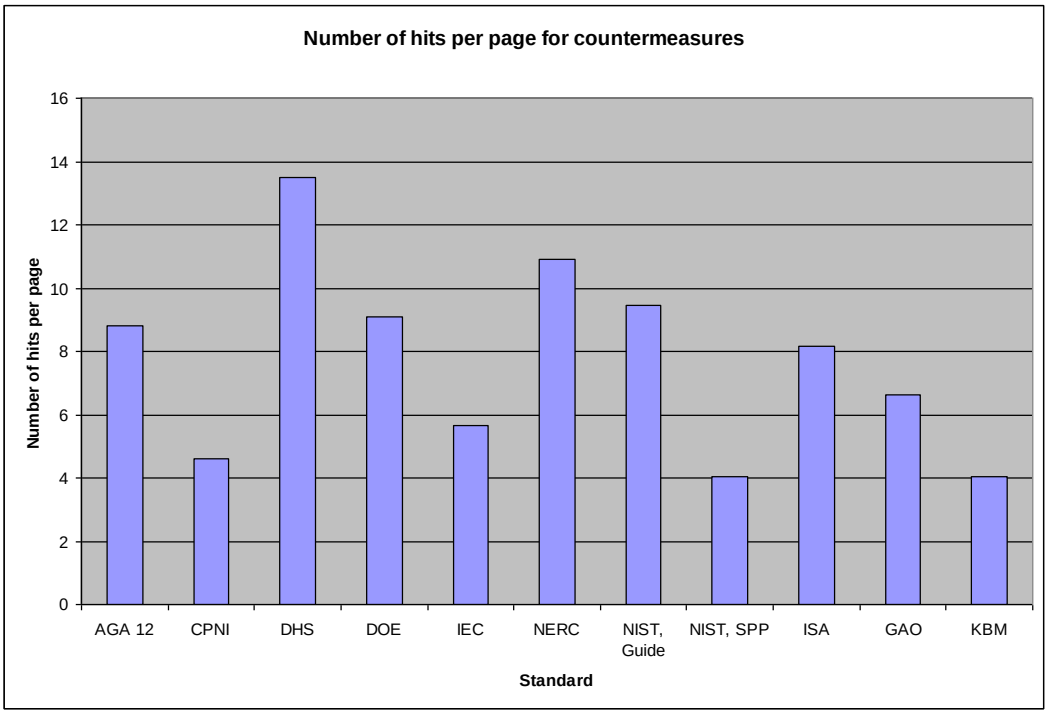

Figure 4 - The number of hits generated by each standard per page when searching for countermeasures

As can be seen in **Figure 4** the weighting of the number of hits against the number of pages give a different view of the level of density for the standards. According to this way of measuring ISA and GAO receives much lower scores compared to the other standards while documents as DHS and NERC receive the highest scores. An ordered list of the result can be found in **Table 9**. This shows the level of density for the different standards in regard of countermeasures.

Table 9 – Number of hits per page in regard of countermeasures

DHS	13.2
NERC	10.89
NIST, Guide	9.46
DOE	9.1
AGA 12	8.79
ISA	8.15
GAO	6.62
IEC	5.65
CPNI	4.84
NIST, SPP	4.05
KBM	4.02

Figure 5 shows the number of hits per standard for attacks. The result is similar to the result for countermeasures with a few exceptions. First of all it should be pointed out that neither DOE nor NERC bring up attacks; therefore they are not represented in the attack data. ISA gets the most hits with NIST Guide coming in second and GAO third. This data might not be the best to use for comparison; data that is better to compare can be seen in **Figure 6**.

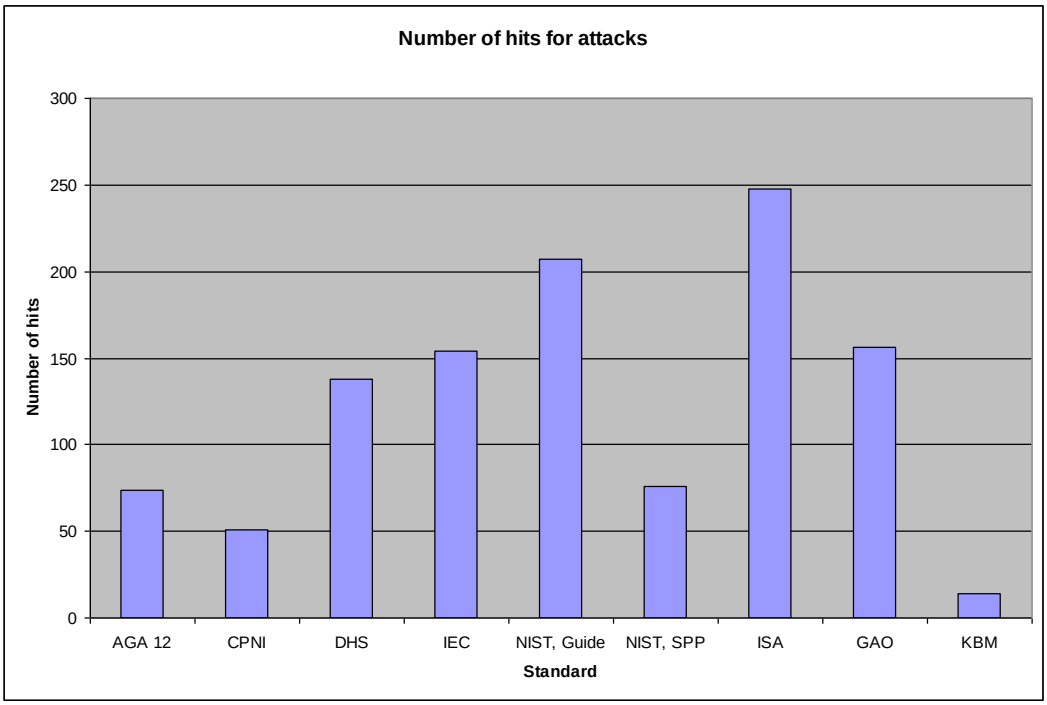

Figure 5 - The number of hits generated by each standard when searching for attacks

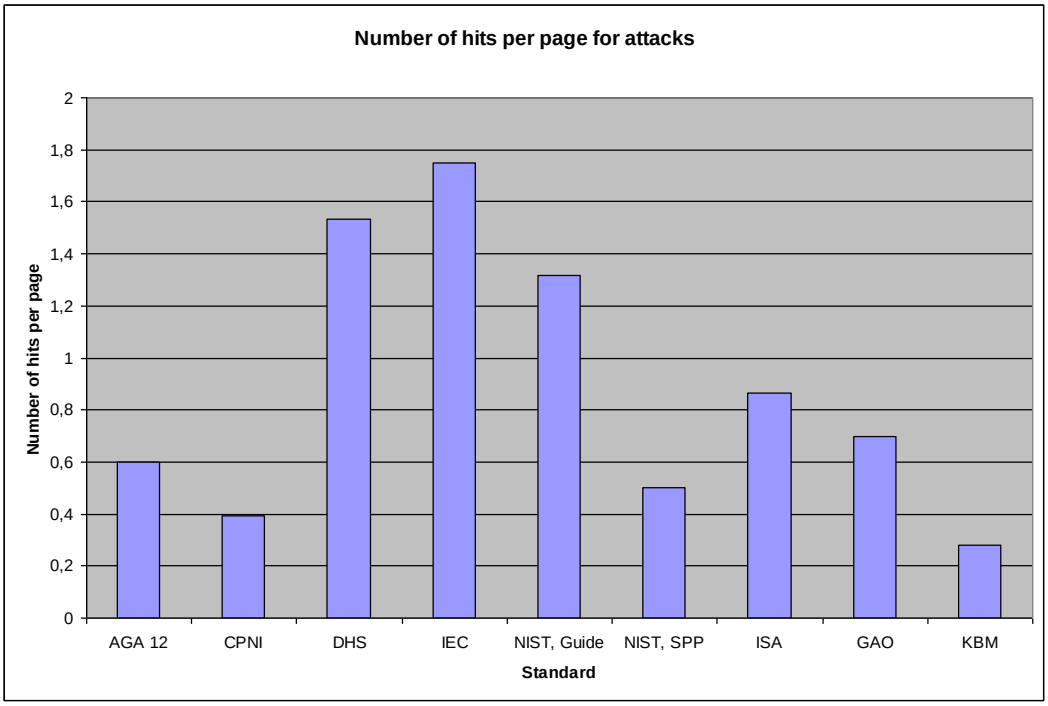

Figure 6 - The number of hits generated by each standard per page when searching for attacks

Table 10 – Number of hits per page in regard of attacks

IEC	1.75
DHS	1.533333
NIST, Guide	1.318471
ISA	0.864111
GAO	0.699552
AGA 12	0.601626
NIST, SPP	0.503311
CPNI	0.392308
KBM	0.28

The level of density for a standard should be measured not just by the density of countermeasures but by the density of countermeasures and attacks combined. This is done by adding the number of hits per page for countermeasures and the number of hits per page for attacks. Since attacks are of so low significance the result will be very similar to the result of countermeasures alone. The result can be seen in **Figure 7**.

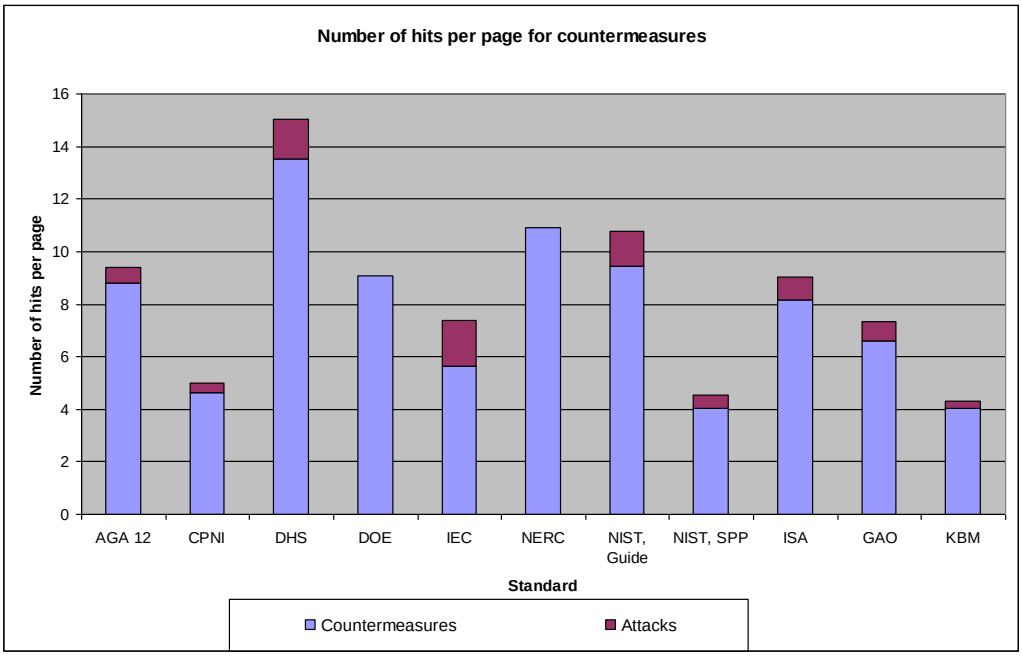

Figure 7 - Number of hits per page in regard of both countermeasures and attacks

A sorted list of the result is found in **Table 11**. The only differences between this list and the list in **Table 9** is that AGA 12 and DOE switched places and so did IEC and GAO. The list in **Table 11** shows the level of density for the standards after adding the results for countermeasures and attacks.

Table 11 - Sum of number of hits per page for countermeasures and number of hits per page for attacks

Standard	Total	Countermeasures	Attacks
DHS	14.73	13.2	1.53
NERC	10.89	10.89	0
NIST, Guide	10.77	9.46	1.32
AGA 12	9.39	8.79	0.6
DOE	9.1	9.1	0
ISA	9.01	8.15	0.86
IEC	7.4	5.65	1.75
GAO	7.31	6.62	0.7
CPNI	5.23	4.84	0.39
NIST, SPP	4.56	4.05	0.5
KBM	4.3	4.02	0.28

To get a more fair comparison the number of hits is put in relation to the number of hits per page. In this diagram the upper right corner is considered the "best" position.

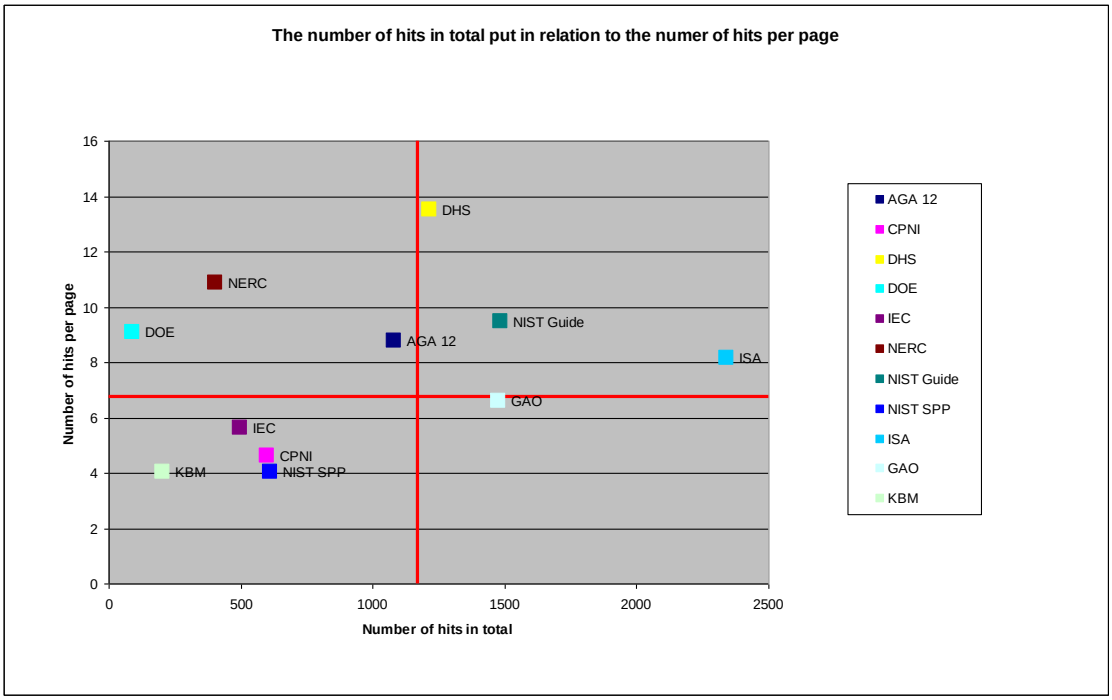

Figure 8 – The number of hits in relation to the number of hits per page

Table 12 – Compilation of the results for standards

	Number of hits for countermeasures	Number of hits for attacks	Number of hits per page for countermeasures	Number of hits per page for attacks	Number of hits per page for countermeasures and attacks combined
AGA 12	1155	123	8.79	0.60	9.39
CPNI	651	130	4.84	0.39	5.23
DHS	1354	90	13.2	1.53	14.73
DOE	91	0	9.1	0	9.1
IEC	651	88	5.65	1.75	7.4
NERC	403	0	10.89	0	10.89
NIST, Guide	1692	157	9.46	1.32	10.77
NIST, SPP	688	151	4.05	0.50	4.56
ISA	2587	287	8.15	0.86	9.01
GAO	1632	223	6.62	0.70	7.31
KBM	215	50	4.02	0.28	4.3

4.3 Data to compare groups

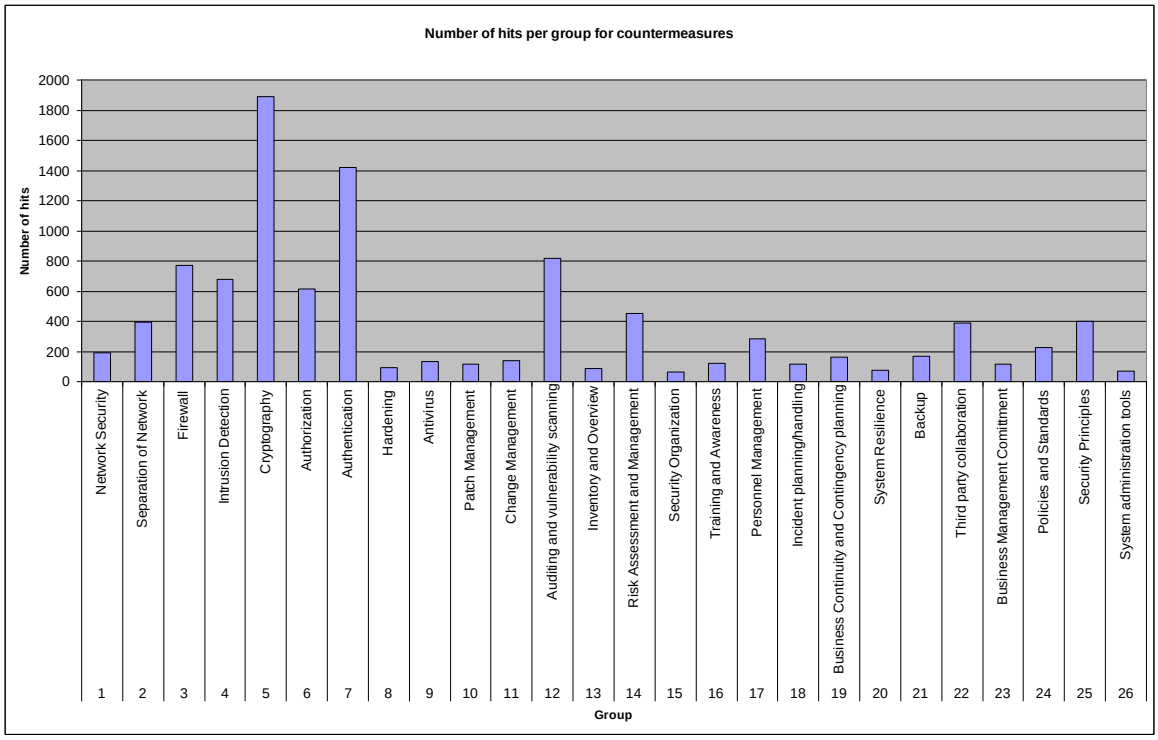

Figure 9 - Number of hits per group in regard of countermeasures

For countermeasures it is possible to see three different levels of magnitude. The groups that got more than 600 hits, the groups that got between 200 and 600 hits and the groups that got less than 200 hits.

- Number of hits>600 Group: 3, 4, 5, 6, 7, 12 a total of six groups
- 600 > Number of hits > 200, Groups: 2, 14, 17, 22, 24, 25 a total of six groups
- 200 > Number of hits, Groups: 1, 8, 9, 10, 11, 13, 15, 16, 18, 19, 20, 21, 23, 26 a total of fourteen groups

To create a prioritization of the groups the method described in chapter 3.1 was used; the result can be seen in **Figure 9**. The figure shows the number of hits per group in regard of countermeasures. It is clear that the two groups with the most hits are cryptography and authentication with about 1800 and 1400 hits respectively. An ordered list can be found in **Table 13**.

Table 13 - Number of hits per group in regard of countermeasures

Cryptography	1891
Authentication	1419
Auditing and vulnerability scanning	816
Firewall	773
Intrusion Detection	680
Authorization	616
Risk Assessment and Management	454
Security Principles	401
Separation of Network	392
Third party collaboration	391
Personnel Management	286
Policies and Standards	224
Network Security	193
Backup	166
Business Continuity and Contingency planning	164
Change Management	141
Antivirus	135
Training and Awareness	122
Patch Management	118
Incident planning/handling	116
Business Management Commitment	115
Hardening	92
Inventory and Overview	88
System Resilience	76
System administration tools	71
Security Organization	62

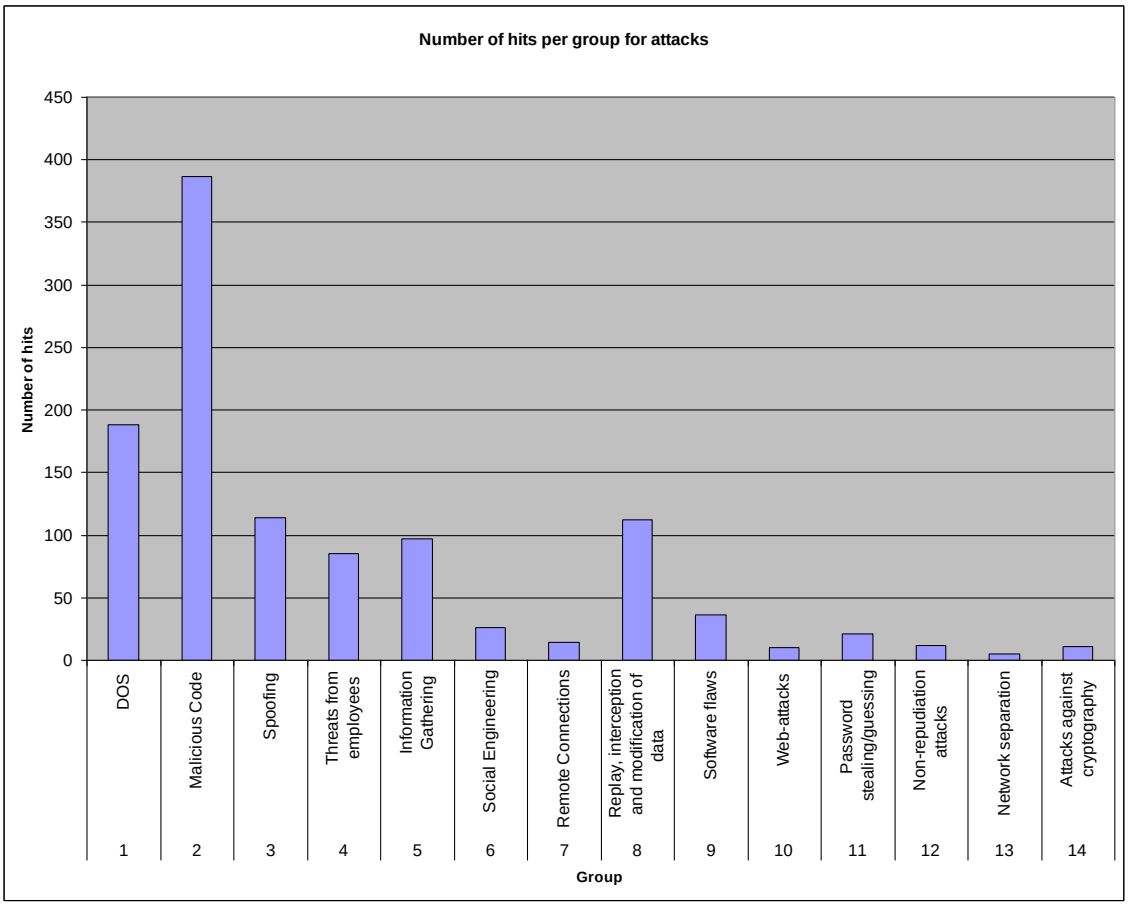

Figure 10 - Number of hits per group in regard of attacks

As with countermeasures it is possible to see three different levels of magnitude. The groups that got more than 300 hits, the groups that got more than 100 hits and the groups that got less than a 100 hits.

- Number of hits > 300, Groups: 2, a total of one group
- 300> Number of hits > 100, Groups: 1, 3, 8, a total of three groups
- 100 > Number of hits, groups 4, 5, 6, 7, 9, 10, 11, 12, 13, 14, a total of ten groups

It is clear that malicious software is the most prioritized group within these standards with almost twice as many hits as the closest.

Table 14 - Number of hits per group in regard of attacks

Malicious Code	387
DOS	188
Spoofing	114
Replay, interception and modification of data	112
Information Gathering	97
Threats from employees	85
Software flaws	36
Social Engineering	26
Password stealing/guessing	21
Remote Connections	14
Non-repudiation attacks	12
Attacks against cryptography	11
Web-attacks	10
Network separation	5

To be able to compare these values against ISO 17799 the results are divided by the total number of pages. The total number of pages is 1346. It should be noted that ISO 17799 does not deal with attacks and therefore there is no reason to show this information for attacks. That information can be found in Appendix 1for those interested.

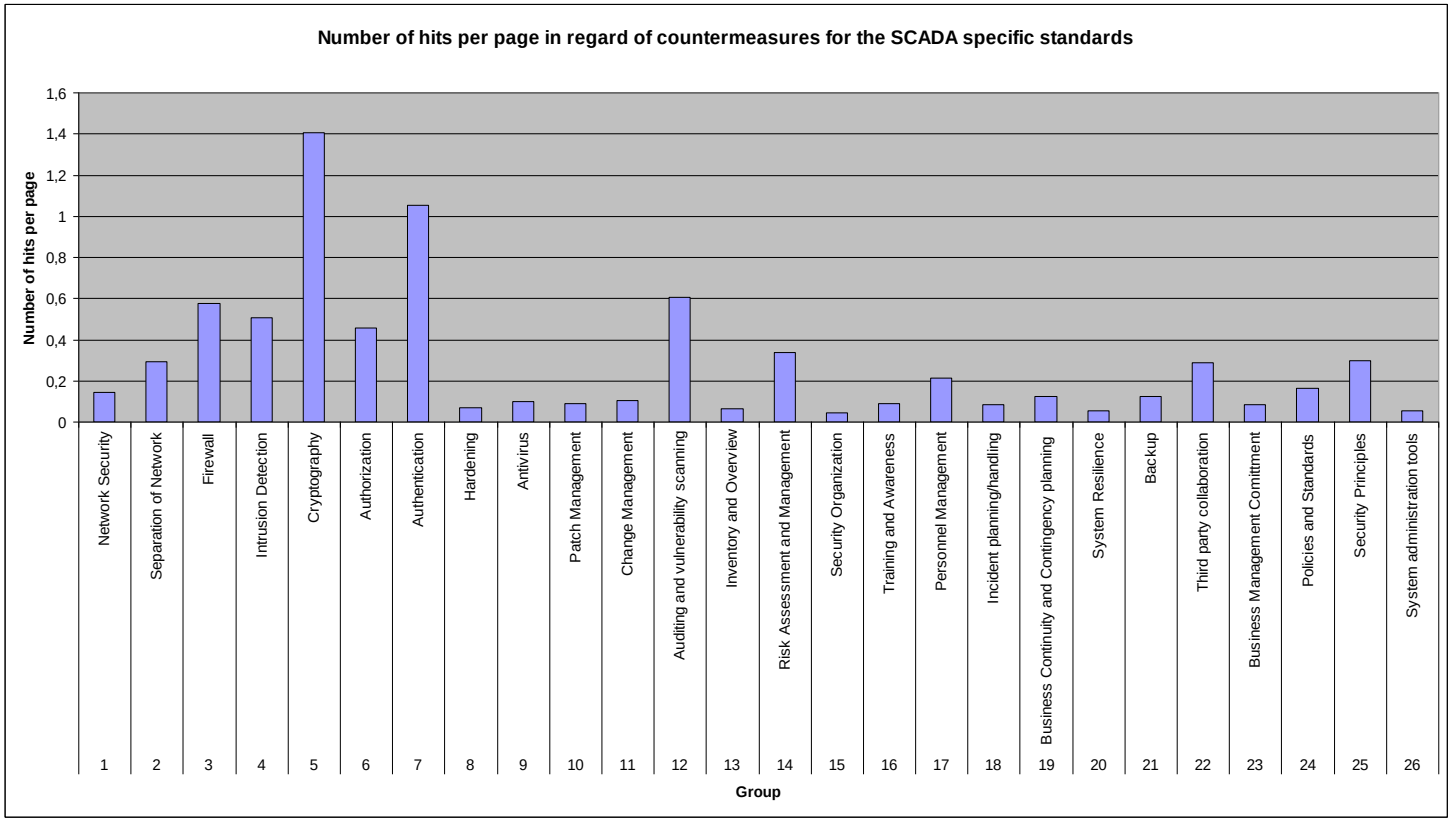

Figure 11 - Number of hits per page in regard of countermeasures for the SCADA specific standards

The same groups of magnitude can of course be found here but with the following border values.

- Number of hits > 0.4
- 0.4 > Number of hits > 0.14
- 0.14 > Number of hits

These values can be used to create the same groups of magnitude for ISO 17799.

4.4 Data for ISO 17799

In **Figure 12** the number of hits per page is shown. The result is similar to the other standards in some ways and different in others. To be able to compare the prioritization of countermeasures between ISO 17799 and the SCADA specific standards the results need to be normalized. This is done by dividing the number of hits per page per group with the total number of hits per page. The result can be seen in **Figure 13**.

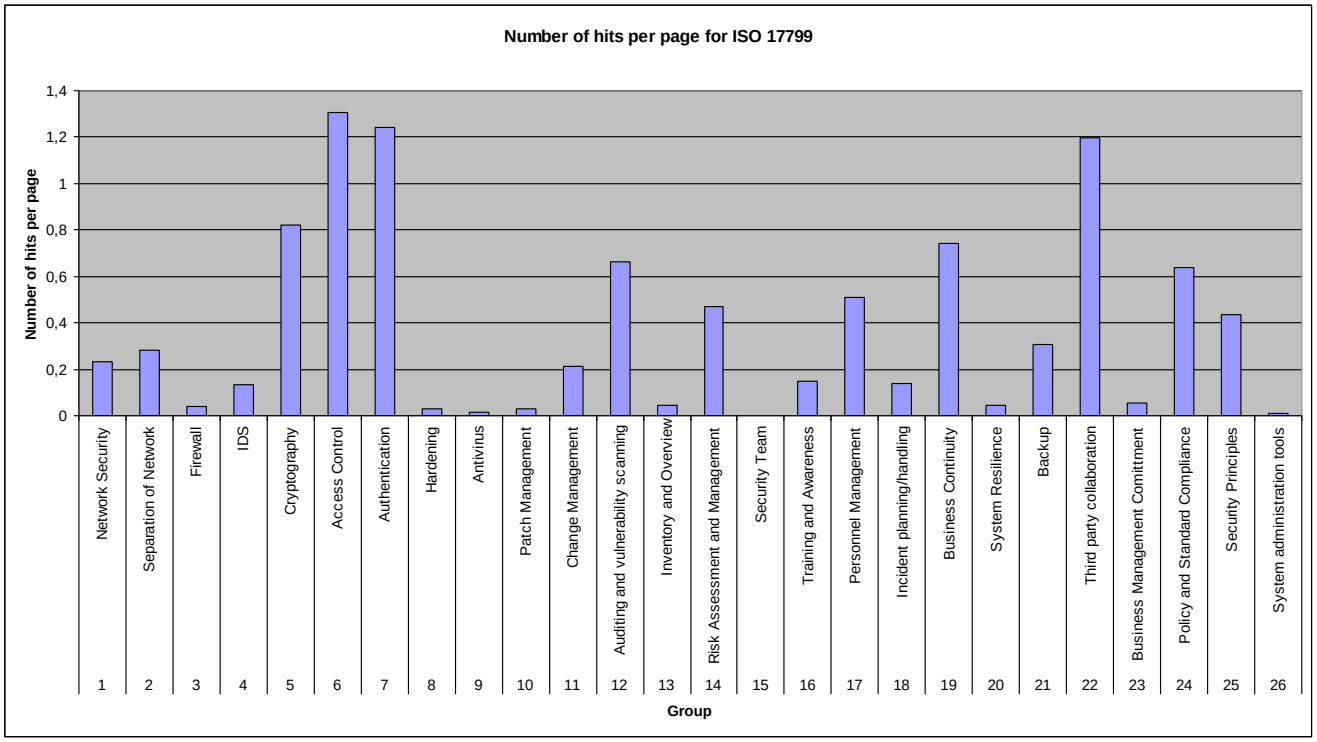

Figure 12 - Number of hits per page in regard of countermeasures for ISO 17799

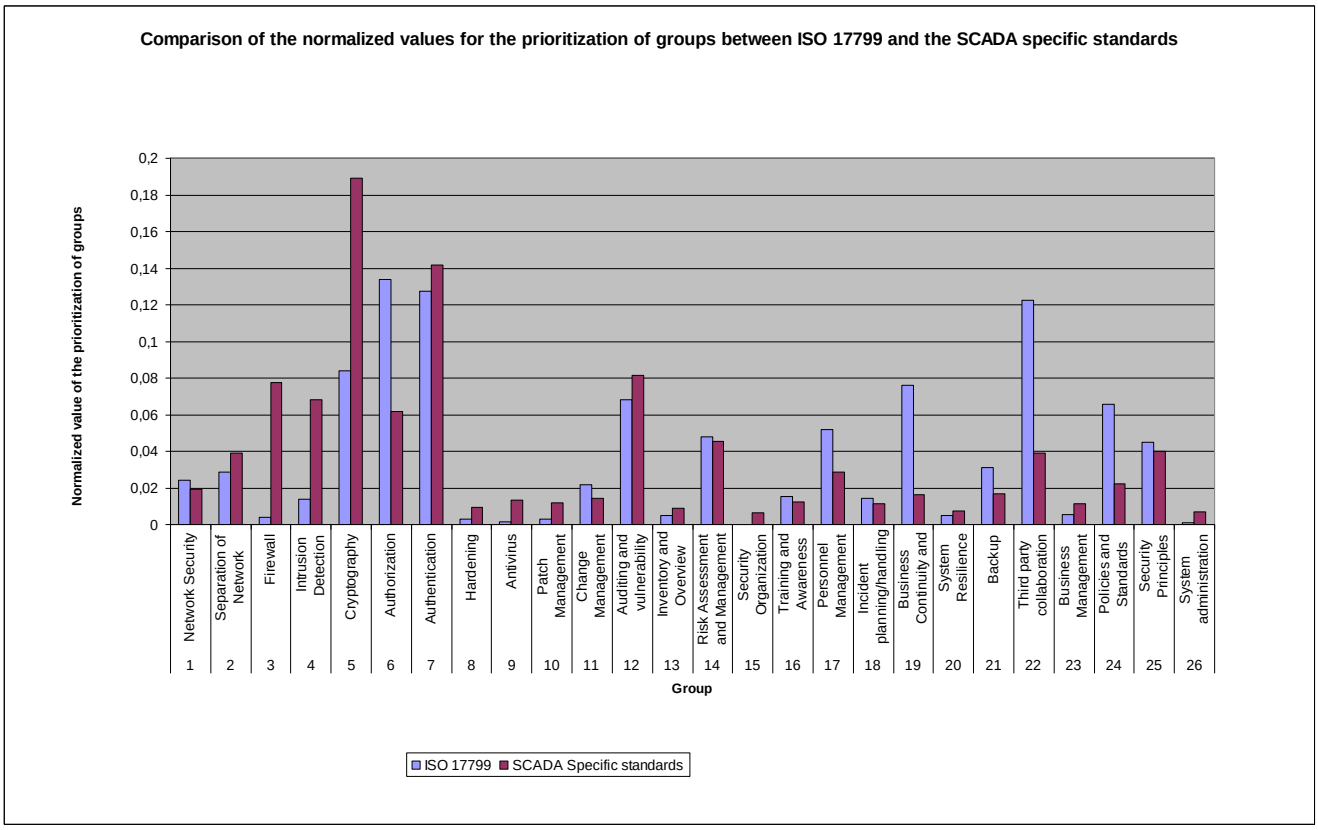

Figure 13 - Number of hits per page - ISO 17799 versus SCADA Specific Standards

It is possible to create the same groups of magnitude as for the SCADA specific standards by using the same border values; they are 0.06 and 0.02

- Number of hits > 0.06, Groups: 5, 6, 7, 12, 19, 22, 24 a total of seven groups
- 0.06 > Number of hits > 0.02, Groups: 1, 2, 11, 14, 17, 21, 25 a total of seven groups
- 0.02 > Number of hits, Groups: 3, 4, 8, 9, 10, 13, 15, 16, 18, 20, 23, 26 a total of twelve groups

Table 15 - Number of hits per page (Normalized) - ISO 17799

6	Access Control	0.133814
7	Authentication	0.127404
22	Third party collaboration	0.122596
5	Cryptography	0.084135
19	Business Continuity	0.076122
12	Auditing and vulnerability scanning	0.068109
24	Policy and Standard Compliance	0.065705
17	Personnel Management	0.052083
14	Risk Assessment and Management	0.048077
25	Security Principles	0.044872
21	Backup	0.03125
2	Separation of Network	0.028846
1	Network Security	0.024038
11	Change Management	0.021635
16	Training and Awareness	0.015224
18	Incident planning/handling	0.014423
4	IDS	0.013622
23	Business Management Comittment	0.005609
13	Inventory and Overview	0.004808
20	System Resilience	0.004808
3	Firewall	0.004006
8	Hardening	0.003205
10	Patch Management	0.003205
9	Antivirus	0.001603
26	System administration tools	0.000801
15	Security Team	0
	Total	1

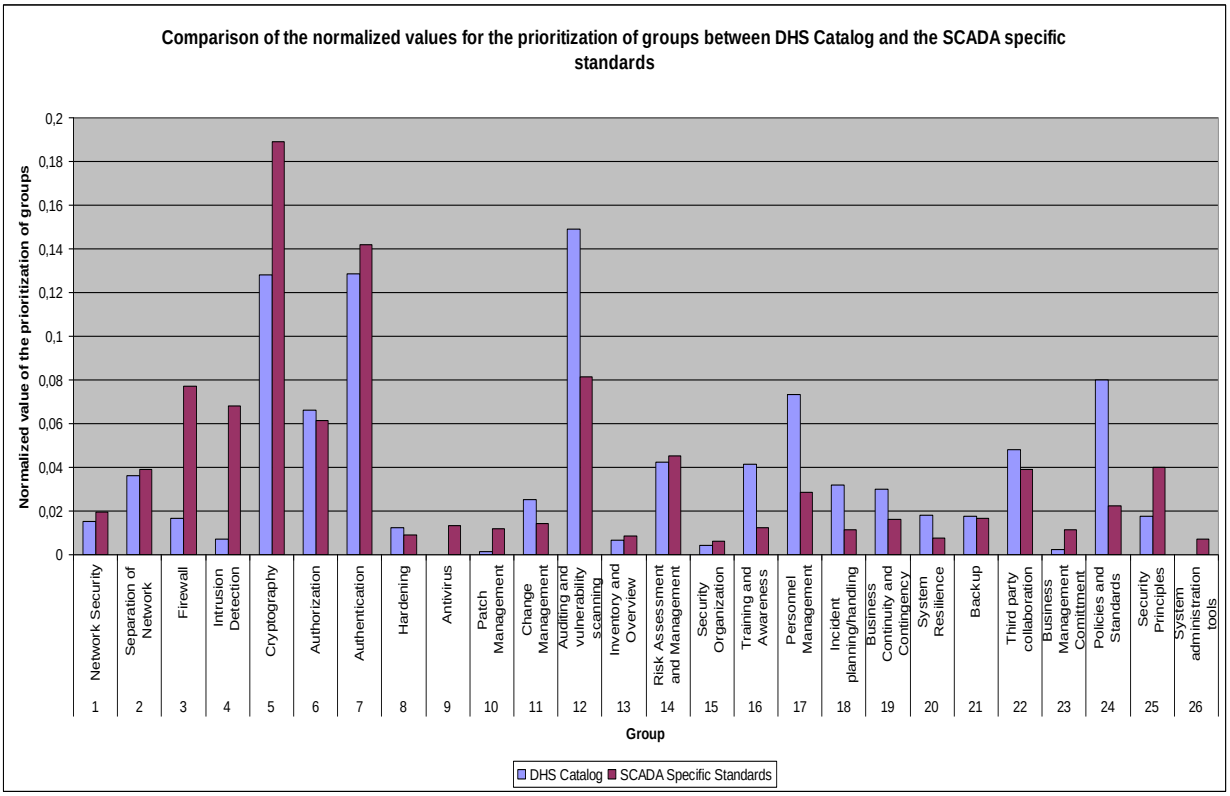

Figure 14 – Data to be able to compare DHS Catalog against the other standards and guidelines

4.5 Data from experts

This chapter shows the data from experts.

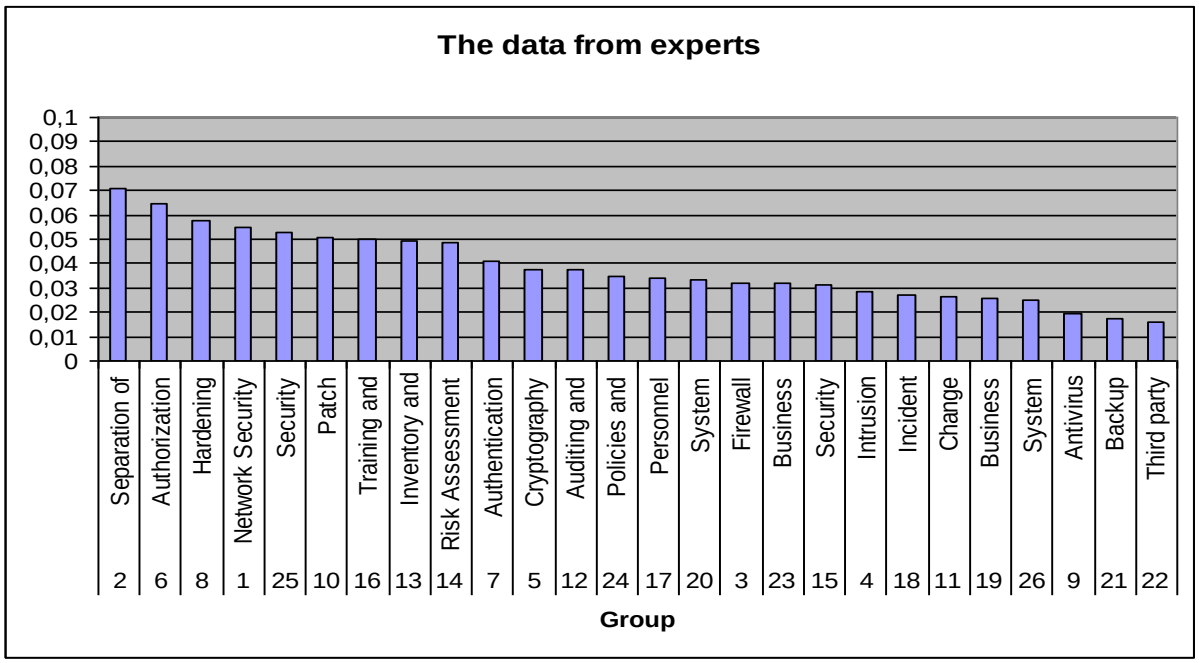

Figure 15 – The data from experts sorted

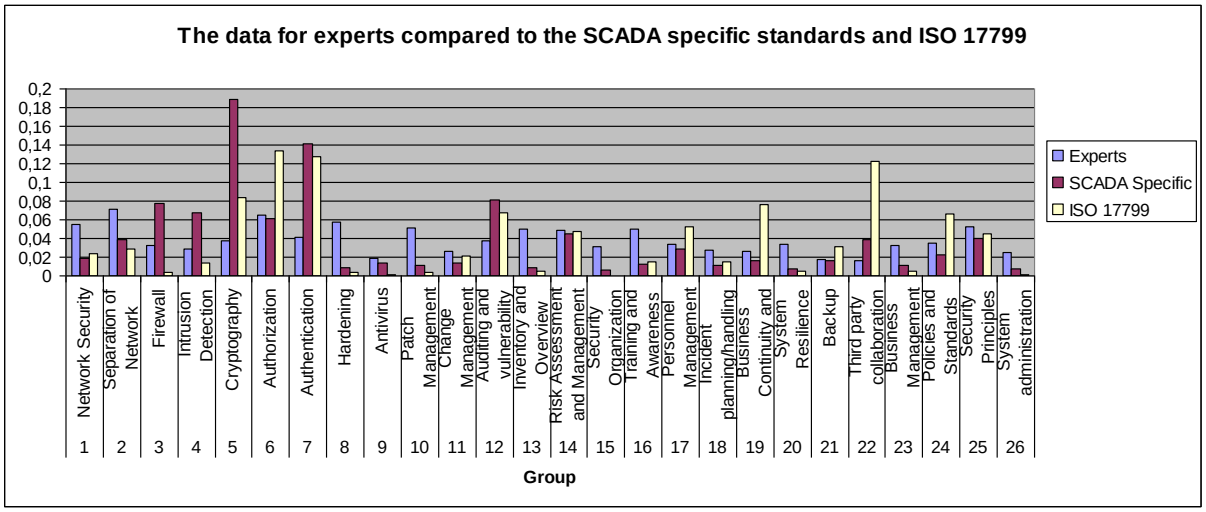

Figure 16 – The data from experts compared with the data for the SCADA specific standards and ISO 17799

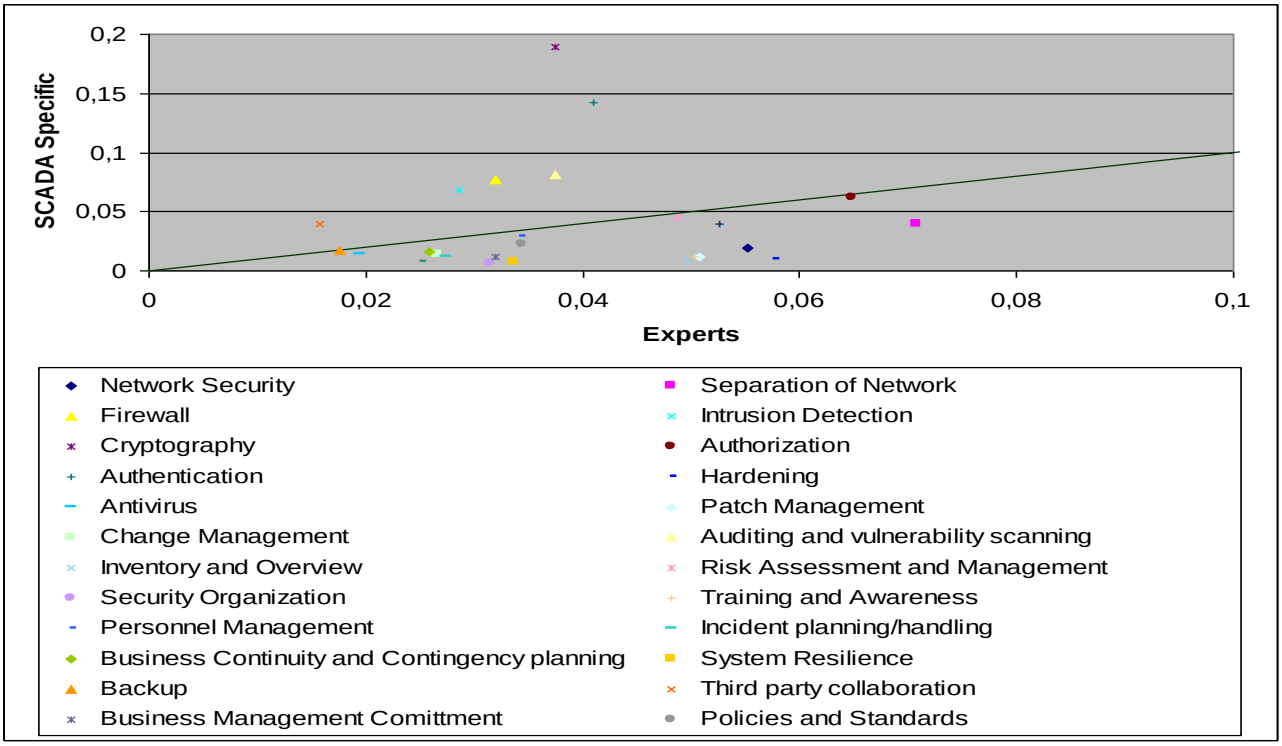

Figure 17 – The data from experts put in relation to the data from the SCADA specific standards

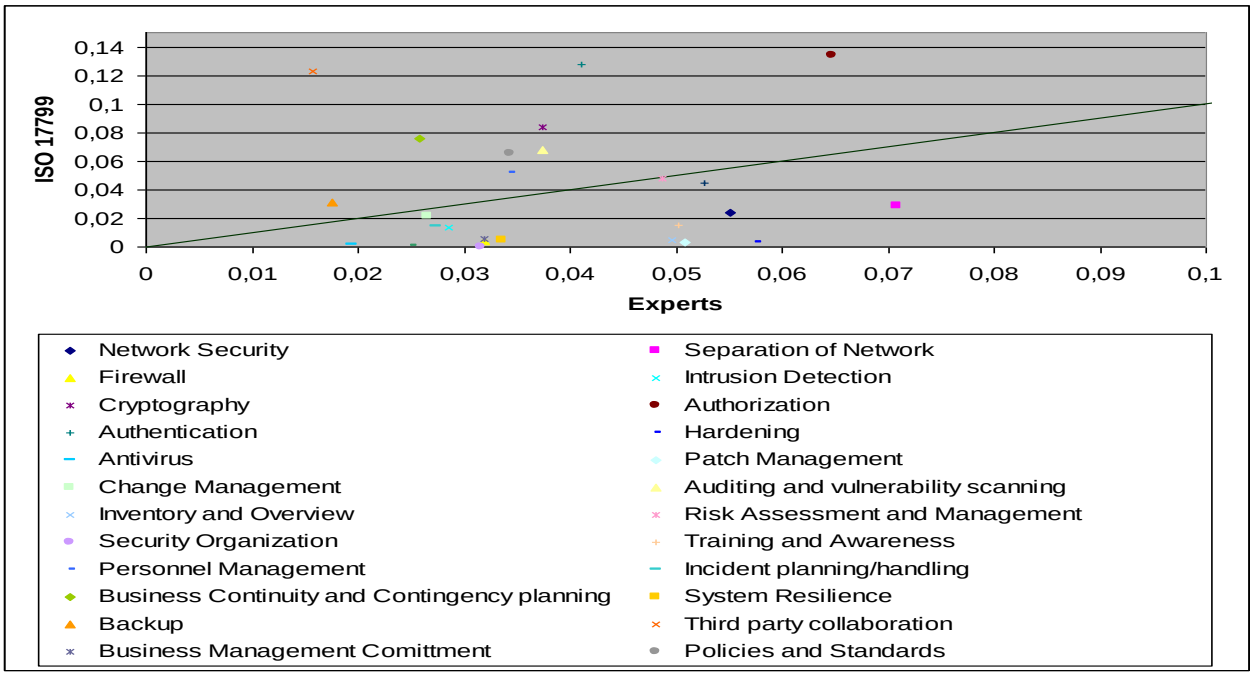

Figure 18 – The data from experts put in relation to the data from ISO 17799

5 Results and Analysis

In this chapter the data presented in chapter 4 is analyzed.

5.1 Analysis of data for standards

In this chapter the data for standards will be analyzed. Some of the questions that will be discussed are

- Why certain standards/guidelines receives the most number of hits
- Why cryptography is the most "important" countermeasure
- What the focus of the standards/guidelines seems to be

The standard with the highest level of density in regard of countermeasures

The way to measure the level of density for a standard is described in chapter 3.1. As shown in **Figure 3** and **Table 7** ISA get the highest amount of hits closely followed by NIST Guide and GAO. This data is a way to show which standard contains the most information in total. In other words it is ISA contains the most information in regard of the groups described in chapter 4.1. There might be a simple reason as to why ISA get the highest number of hits. ISA is the longest standard/guideline; there is more text where it is possible to find hits. As described in chapter 3.1 the number of hits is divided by the number of pages. The result can be seen in **Figure 4**; this shows the number of hits per page. In this case standards/guidelines like ISA and GAO get a lower value and instead DHS and NERC receive the highest number of hits per page. This way of measuring can be interesting to for example find out which standard requires the least amount of reading but still contain a lot of information.

The standard with the highest level of density in regard of attacks

It is possible to make the same analysis but for attacks instead. This data is shown in **Figure 5** and **Figure 6**, an ordered list of the number of hits per page can be found in **Table 10**. There is a similar pattern as for countermeasures. When it comes to the number of hits in total ISA get the highest number of hits but when divided it by the number of pages it is clear that IEC and DHS are the documents with the highest level of density. It is also clear that the focus of the standards/guidelines is countermeasures and not attacks, more about that later. The fact that ISA, GAO and NIST Guide have a high number of hits can most likely be deduced to their advantage in the number of pages. It is a little surprising that NIST SPP is not further up on these lists since it is one of the documents that deal with attacks explicitly. This may partially be because NIST SPP deals with attacks in a very structured way using a language that does not generate many hits.

The standard with the highest level of density in total

The data in **Figure 7** and **Table 11** shows a merge of the results for attacks and the results for countermeasures. It shows the level of density based on the number of hits per page. Since attacks generates a lot less hits per page than countermeasures this result is similar to the result for countermeasures. There are a few differences, but DHS is still the document with the highest level of density according to this way of measuring.

The question is which way of measuring to use, the number of hits or the number of hits per page. The number of hits per page is more comparable but the question is if it gives a fair result. The main issue is if the shorter documents get an unfair advantage. Take DOE as an example. In regard of

actual hits DOE get the lowest amount. Looking at the hits per page DOE suddenly has the fifth highest level of density. But DOE still contains the same amount of information no matter which way of measuring that is used. Having many hits per page does not mean DOE is a better standard/guideline. It just means it requires less reading to receive as much information. For example the total amount of information in ISA is still (most likely) higher then for DOE (unless ISA is all repetition). To get a more fair comparison the number of hits is set in relation the number of hits per page. The result can be found in **Figure 8**.

This result shows which standards that have the combination of a high number of hits and many hits per page. The best position to be in is the upper right corner. There are three standards that are clearly inside this area. These are DHS, NIST Guide and ISA.

This is a summarization of the results concerning which standard that got the highest level of density.

- The number of hits shows that ISA and NIST Guide have the highest level of density (**Table 7**).
- The number of hits per page shows that DHS and NERC have the highest level of density (**Table 9**).
- A combination of the results above shows that DHS, NIST Guide and ISA have the highest level of density (**Figure 8**).

Which of these results to use when choosing which standard to read depend upon the goal with reading the standard/guideline. For example if it is important to gain information as fast as possible it might be best to use the number of hits per page. If it is important to really understand the area of cyber security in SCADA system it might be better to use a document with a lot of information. The suggestion of the author would be to use either DHS or NIST Guide.

Focus on countermeasures

In the data it can be seen that the number of hits per page is much lower for attacks. The highest number of hits per page is found in IEC with 1.75 hits per page. This is less than half the number of hits that KBM (the standard/guideline with the lowest level of density in regard of countermeasures) got in regard of countermeasures. In **Table 16** the quotient between the number of hits per page for countermeasures and the number of hits per page for attacks is shown.

Table 16 – Number of hits per page in regard of countermeasures divided by number of hits per page in regard of attacks

Standard	Quotient	Number of hits per page in regard of countermeasures	Number of hits per page in regard of attacks
IEC	3.23	5.65	1.75
NIST. Guide	7.17	9.46	1.32
NIST. SPP	8.05	4.05	0.50
DHS	8.61	13.51	1.53
ISA	9.43	8.15	0.86
GAO	9.46	6.62	0.70
CPNI	12.33	4.62	0.39
KBM	14.36	4.04	0.28
AGA 12	14.61	8.79	0.60
Average	9.69	7.21	0.88

The average quotient is 9.69; in average there are almost 10 more hits per page for countermeasures when compared with attacks. It is evident that the standards focus on countermeasures and not attacks.

The standards have different focus

It seems like the standards focus on different aspects of the security. There are three groups that can be identified. Data for the number of hits per group for each standard can be found in Appendix 3.

1. There are standards that focus on technical countermeasures. These standards include GAO, DHS, NIST Guide, ISA
2. There are standards that focus on non-technical countermeasures. These standards include DOE, CPNI, NERC
3. There is a standard that focus on cryptography, AGA.
4. Finally NIST SPP, KBM and IEC do not seem to have a clear focus.

Table 17 – Shows which countermeasures that are technical and which are non-technical

		Technical	Non-technical
1	Network Security	X	
2	Separation of Network	X	
3	Firewall	X	
4	Intrusion Detection	X	
5	Cryptography	X	
6	Authorization	X	
7	Authentication	X	
8	Hardening	X	
9	Antivirus	X	
10	Patch Management	X	
11	Change Management		X
12	Auditing and vulnerability scanning	X	
13	Inventory and Overview		X
14	Risk Assessment and Management		X
15	Security Organization		X
16	Training and Awareness		X
17	Personnel Management		X
18	Incident planning/handling		X
19	Business Continuity and Contingency planning		X
20	System Resilience	X	
21	Backup	X	
22	Third party collaboration		X
23	Business Management Comittment		X
24	Policies and Standards		X
25	Security Principles		X
26	System administration tools		X

Table 18 – The percent each group of focus has in the respective areas

	Technical standards	Non-technical standards	Standard with focus on cryptography	Remaining
Technical countermeasures	0.56	0.22	0.05	0.16
Non-technical countermeasures	0.29	0.50	0.04	0.17
Cryptography	0.44	0.001	0.41	0.14

The number of hits per page for the countermeasures that are considered to be technical shows that group 1 stands for 56 % of the hits, group 2: 22 %, group 3: 5 % and group 4: 16 %. The number of hits per page for countermeasures that are considered non-technical shows that group 1 stands for 29 %, group 2: 50 %, group 3: 4 % and group 4: 17 %. Finally the number of hits per page for the countermeasure that the specialized standard focuses on (in this case it is cryptography), shows us that group 1 stands for 44 % of the number of hits, group 2: 0.1 %, group 3: 41 % and group 4: 14 %.

It is interesting to see that the standards that focus at non-technical countermeasures write almost nothing about cryptography. As seen in chapter 5.2 cryptography is the most important countermeasure (or at least the countermeasure that generates most hits). One explanation could be that cryptography is very technically oriented. It is also interesting that the standards that focus on technical countermeasures and the standards that focus on non-technical countermeasures stands for over 50 % of the number of hits per page in their respective focus area. This indicates that it can be quite important which standard that is used especially if only certain aspects of SCADA system security are of interest. It also shows that it is probably best to not only use one standard/guideline but rather several to be able to cover all areas. Further it is interesting that one standard is able to generate 41 % of this number of hits per page for cryptography. This might push the results towards being too concentrated on cryptography.

5.2 Analysis of data for groups

In this chapter the data for groups will be analyzed. The way the data was generated is described in chapter 3.1. The result can be seen in **Figure 9** and an ordered list can be found in **Table 13**.

Cryptography, the most important countermeasure

The group that gets the most hits is the group that contains cryptographic countermeasures. These countermeasures include all sorts of encryption, digital signatures, certificates and so on. One explanation to cryptographies large number of hits is that it is used as a part of many other countermeasures. For example cryptography is often mentioned when discussing such subjects as secure login and protection of data. This has the effect that the keywords for cryptography are mentioned in connection with these subjects as well which has the effect that it generates more hits. Another explanation to the large amounts of hits for cryptography is that one of the standards (AGA) is aimed at cryptographic countermeasures and generates a third of the hits alone.

Properties that affect the importance of countermeasures

As could be seen in chapter 4.3 the countermeasures can be divided into three groups of magnitude. These are:

- Number of hits per page >0.4 Group: 3, 4, 5, 6, 7, 12 a total of six groups
- 0.4 > Number of hits per page > 0.14, Groups: 2, 14, 17, 22, 24, 25 a total of six groups
- 0.14 > Number of hits per page, Groups: 1, 8, 9, 10, 11, 13, 15, 16, 18, 19, 20, 21, 23, 26 a total of fourteen groups

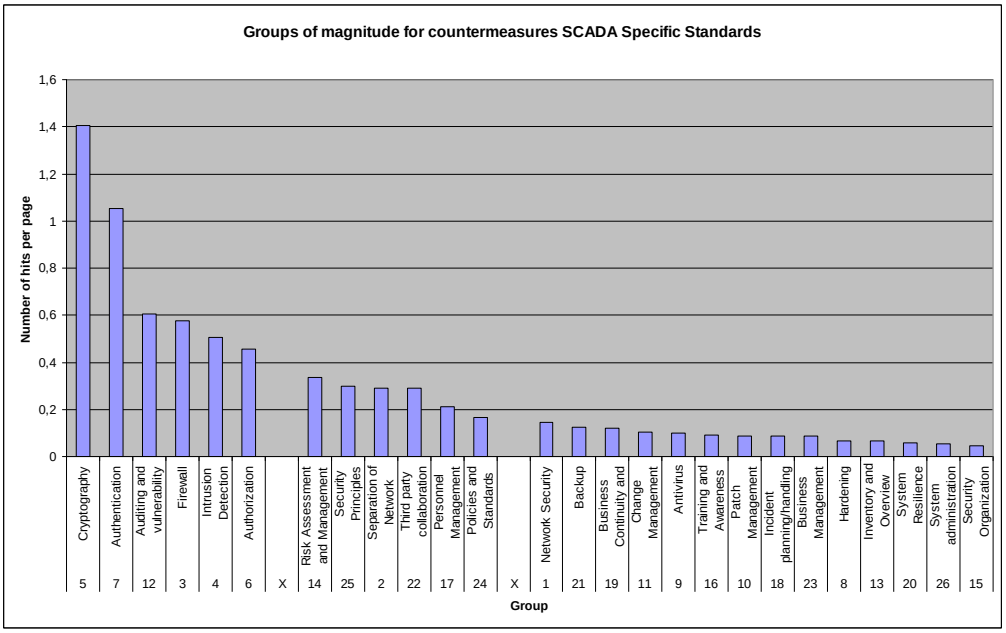

Figure 19 - The groups of magnitude for countermeasures for SCADA specific standards

Examining the group with over 0.4 hits per page all of these countermeasures are technical. A technical countermeasure (sometimes referred to as logical) is a countermeasure that is used to "protect the C.I.A. of sensitive information. Examples include logical access systems, encryptions systems, antivirus systems, firewalls, and intrusion detection systems." This is in contrast to non-technical countermeasures (administrative) that contains policies, personnel security, training and awareness and so on. [45]

Another thing is that all of these countermeasures are rather broad in the way that they can be used in several ways and in different parts of the system. As already explained cryptography for example can be a part of many other countermeasures and auditing and vulnerability scanning includes logging which is used within all parts of the system.

Continuing to the groups with over 0.14 hits per page it can be seen that they are a mix of technical and non-technical countermeasures. As with the groups that got more than 0.4 hits per page these countermeasures are rather broad. For example Risk assessment and management, Security Principles and Policies and Standards are all used to support other countermeasures.

Finally looking at the groups with less than 0.14 hits per page they are a mix of technical and non-technical countermeasures but most of these countermeasures got specific subjects. For example backup, patch management and system administration tools are all rather specific.

Considering this there seems like there are two things that can be identified that influence the number of hits a group get.

1. How broad a group is
2. How technical a group is

There are of course exceptions to this, for example antivirus is a very technical countermeasure and it is as general as firewalls and intrusion detection but it still only get 0.099 hits per page compared to firewalls 0.574 or intrusion detections 0.505.

Malicious software the biggest threat

Continuing with the data for attacks the number of hits per group can be seen in **Figure 10**. It is quite clear that malicious software is the attack with the most hits. An explanation to this could be that malicious software is an obvious threat against SCADA systems; there exists a couple of known incidents were SCADA systems have been affected by malicious code [50]. An ordered list of the result can be found in **Table 14**.

Properties that affect the importance of attacks

In chapter 3.1 it was said that the attacks could be divided into three groups of magnitude as follows

- Number of hits > 300, Groups: 2, a total of one group
- 300> Number of hits > 100, Groups: 1, 3, 8, a total of three groups
- 100 > Number of hits, groups 4, 5, 6, 7, 9, 10, 11, 12, 13, 14, a total of ten groups

For countermeasures there were some patterns for which countermeasure received most hits, there is nothing similar for attacks. This might be because the focus of these standards is on countermeasures. There is not enough data to find a pattern.

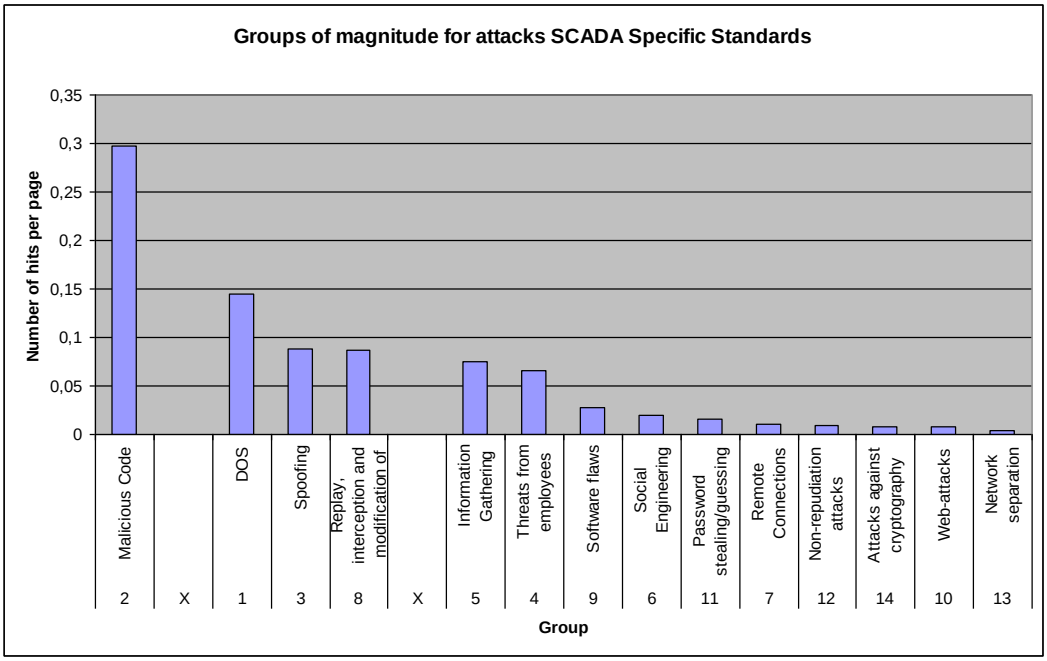

Figure 20 - The groups of magnitude for attacks for SCADA specific standards

Malicious software, biggest threat but not most prioritized

Considering the content of the groups it is interesting to see that malicious software is the biggest group amongst attacks, but antivirus is not one of the biggest groups amongst the countermeasures. Antivirus is not even in the top ten but can be found on seventeenth place. This seems odd but there can be a few explanations for this. Antivirus protection in SCADA systems is special. It is not possible to install any antivirus software and see what happens. First of all some vendors might not continue to give support if third party software such as antivirus is installed on your system [46]. Antivirus software can sometimes be very resource demanding making it impossible to install on systems with limited resources and high availability demands. Another problem with antivirus software is that some parts of SCADA systems often are so called legacy systems where it might no even be possible to install updated antivirus software. There exists a document that deals solely with host based antivirus in SCADA environments [15].

The mapping between attacks and countermeasures is in general not very easy to see. The standards do not contain much information about this subject with a few exceptions. NIST SPP has one section about it and IEC brings it up to some extent. It would be good if there existed a mapping from attacks to countermeasures to consequences. That way it would be possible to know what the consequence of not applying a countermeasure would be which could greatly reduce the difficulty of performing risk assessments. In the case of malicious code as in the example above it is obvious that antivirus is one countermeasure that could help but it is not as obvious that for example authentication could also help preventing malicious code.

5.3 Comparison with ISO 17799

Please note that this comparison is done as to see which of the subjects brought up in the SCADA specific standards are also brought up in ISO 17799. This data may not show the entire picture of which subjects that ISO 17799 consider as important. To begin the data for ISO 17799 will be analyzed by itself. This data can be seen in **Figure 12**. An ordered list of the result can be seen in **Table 15**.

Properties that affect the importance of countermeasures for ISO 17799

To be able to compare the groups of magnitude with the ones of the SCADA specific standards the normalized results have to be used. With the same border values as for the other standards the following groups are created:

- Number of hits > 0.06, Groups: 5, 6, 7, 12, 19, 22, 24 a total of seven groups
- 0.06 > Number of hits > 0.02, Groups: 1, 2, 11, 14, 17, 21, 25 a total of seven groups
- 0.02 > Number of hits, Groups: 3, 4, 8, 9, 10, 13, 15, 16, 18, 20, 23, 26 a total of twelve groups

Looking for patterns as done for the other standards there are two things that can be seen. The first thing is that most of the groups with over 0.06 hits per page have in common is that they are general. The second thing is that all the groups contain a mix of technical and non-technical countermeasures.

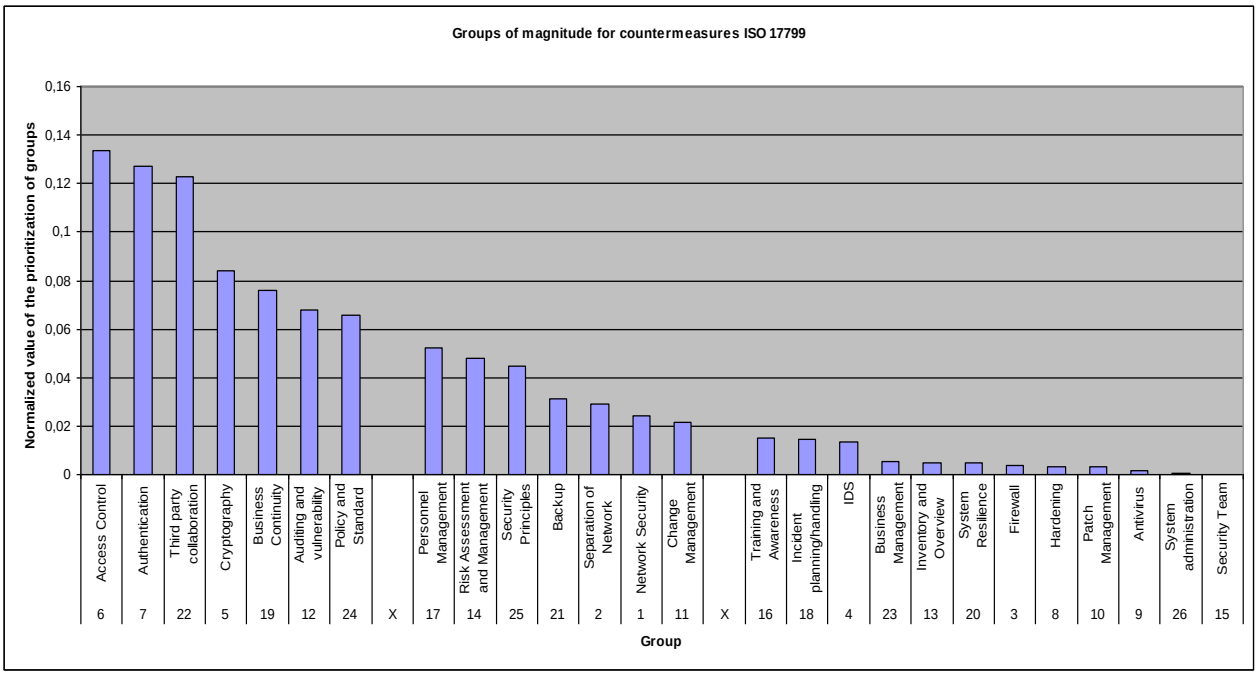

Figure 21 - The groups of magnitude for countermeasures for ISO 17799

Comparison between patterns for SCADA specific standards and ISO 17799

Comparing the patterns found for SCADA specific standards with the ones found for ISO 17799 it is seen that the generality of groups is important to receive hits in both cases. On the other hand in the SCADA specific standards the technical countermeasures seems to get more hits than the others but in ISO 17799 the technical countermeasures receives less hits (with some exceptions). In general ISO 17799 have more groups with the highest level of magnitude. All of the levels of magnitude in ISO 17799 contain a mix of technical and non-technical countermeasures. The fact that ISO 17799 contains more groups with the highest level of magnitude could be interpreted as that ISO 17799 is broader than the SCADA specific standards. It gives a more complete picture of what needs to be done even though it still miss some areas as will be shown later in this chapter.

Comparing this result with the result for the SCADA specific standards there are both differences and similarities. In **Figure 13** the results are shown side by side. One thing that is clear is that the technical countermeasures get less priority in ISO 17799. There is especially a big difference in the amount of hits per page for firewalls and intrusion detection. There is also quite a big difference in how many hits cryptography gets. ISO 17799 put more focus on the non-technical countermeasures. Some groups that stand out when compared to the other standards are personnel management, third party collaboration and policies and standards.

Difference in the number of hits

The idea with making this comparison is to be able to see which groups of countermeasures that are considered important in the SCADA specific standards but are not considered important in ISO 17799. To be able to do this the quotient between the number of hits per page for the SCADA specific standards and the number of hits per page for ISO 17799 is used. When calculating the quotient the normalized values seen in **Figure 13** are used. The result can be seen in **Table 19**. All the

groups with a quotient greater than or equal to two are considered groups that are more important in the SCADA specific standards than in ISO 17799.

Table 19 - Quotient between number of hits per page for SCADA specific standards and number of hits per page for ISO 17799

			ISO 17799	SCADA Specific standards
3	Firewall	19.29	0.004	0.077
26	System administration tools	8.86	0.001	0.007
9	Antivirus	8.42	0.002	0.013
4	IDS	4.99	0.014	0.068
10	Patch Management	3.68	0.003	0.012
8	Hardening	2.87	0.003	0.009
5	Cryptography	2.25	0.084	0.189
23	Business Management Commitment	2.05	0.006	0.011
13	Inventory and Overview	1.83	0.005	0.009
20	System Resilience	1.58	0.005	0.008
2	Separation of Network	1.36	0.029	0.039
12	Auditing and vulnerability scanning	1.20	0.068	0.082
7	Authentication	1.11	0.127	0.142
14	Risk Assessment and Management	0.94	0.048	0.045
25	Security Principles	0.89	0.045	0.040
18	Incident planning/handling	0.80	0.014	0.012
1	Network Security	0.80	0.024	0.019
16	Training and Awareness	0.80	0.015	0.012
11	Change Management	0.65	0.022	0.014
17	Personnel Management	0.55	0.052	0.029
21	Backup	0.53	0.031	0.017
6	Access Control	0.46	0.134	0.062
24	Policy and Standard Compliance	0.34	0.066	0.022
22	Third party collaboration	0.32	0.123	0.039
19	Business Continuity	0.21	0.076	0.016
15	Security Team	∞	0.000	0.006

The groups with a quotient greater or equal to two are:

- Firewall
- Intrusion Detection
- Cryptography
- Hardening
- Antivirus
- Patch Management
- Business Management Commitment
- System Administration tools

Trying to secure a SCADA system currently protected according to ISO 17799 these are the areas that need the most extra attention. The next section gives suggestions on which standards to use to find more information on these areas.

Why are these groups not as represented in ISO 17799 as in the SCADA specific standards? Firewalls, intrusion detection, cryptography, antivirus and patch management are all extra problematic in SCADA systems and this could be the reason they receive more attention in the SCADA specific standards. These countermeasures also require quite specific configurations depending on the system they are used in which make it quite hard to write about in a standard that is supposed to be general. ISO 17799 is not only supposed to be written for general systems, ISO 17799 also considers information security rather than computer security or SCADA security. One difference that comes from this is that ISO 17799 is concerned about the security of data regardless of if the information is stored electronically or printed on paper. Also the priorities differ between information security and SCADA security.

It is also possible to look at the quotient in the opposite way. The groups with a very low quotient are most likely dealt with in a sufficient way in ISO 17799. If the quotient is 0.5 or lower that means that there is at least twice as many hits in ISO 17799.

- Policy and Standard Compliance
- Third party collaboration
- Business Continuity

If ISO 17799 is currently in use but there is a plan to start using a SCADA specific standard then there might not be as much need to work with these areas since they are probably already dealt with in a satisfying way. This being said there might still be some SCADA specific questions that are dealt with in the SCADA specific standards so there is still reason to read through these sections of the SCADA specific standards you choose to use.

Suggestion on standards to use to improve security in addition to ISO 17799

The specific data for number of hits per standard per group can be found in Appendix 3, this data is the foundation for this suggestion. For each area the three standards with the most number of hits have been picked out.

Table 20 - Which standards to use to learn more about certain areas

Firewalls	GAO, ISA, NIST Guide
Intrusion Detection	DHS, GAO, ISA
Cryptography	AGA, DHS, ISA
Hardening	DHS, NIST Guide, KBM
Antivirus	NIST Guide, DHS, GAO
Patch management	GAO, NIST Guide, DHS
Business Management Commitment	NERC, CPNI, NIST Guide
System Administration Tools	GAO, IEC, NIST Guide

My personal opinion on the list in **Table 20**.

For firewalls all of these documents are good. GAO is most basic and brings up what a firewall is and what it is used for. ISA and NIST Guide can be used for more specific advice on the use of firewalls in SCADA systems. Also worth mentioning is "Good Practice Guide on Firewall deployment for SCADA and Process Control Networks" from NISCC (CPNI) [4]. When it comes to intrusion detection all of the documents are good, GAO is more basic, DHS is aimed at procurement of systems and ISA is more detailed. AGA is focused on cryptographic countermeasures in SCADA systems and is the best document to get to know more about cryptography. For hardening the best suggestion is to use DHS since it is the only document that lets hardening have its own section. There is also an interesting part of KBM about the removal of unnecessary connections. As described in chapter 5.2 antivirus is not dealt with to a great extent in any standard. All of the documents in the list are equally good even though GAO might still be more basic. It is also once again worth mentioning the document about antivirus in SCADA environments [15].

5.4 Comparison with DHS Catalog

The document DHS Catalog is supposed to be a framework to help in the development of sound security standards/guidelines. As such it could be interesting to compare what this document considers important to the other standards.

In general the numbers are similar to the ones from the SCADA specific standards/guidelines. As in the comparison with ISO 17799 the DHS Catalog seems to put more focus on the non-technical countermeasures although not as much as ISO 17799. Also similar to ISO 17799 is the difference in the numbers for the intrusion detection and firewall groups. These are lower for DHS Catalog. Also worth mentioning is the fact that DHS Catalog receives no hits at all for antivirus; this is a trend for all of the standards/guidelines. The fact that the data is similar for the SCADA specific standards and DHS Catalog indicates that the SCADA specific standards deal with the issues that DHS would like them to deal with.

5.5 Completeness of standards in regard of countermeasures

The completeness of a standard can be measured by checking how many of the groups of countermeasure the standard covers. The result can be seen in **Table 21**. Two of the standards can be said to be complete in the sense that they somehow deal with all of the groups of countermeasures; these are NIST Guide and ISA. It is interesting that DHS, the document that has been determined to have the highest level of density only covers 22 of the 26 areas. One of the groups that DHS does not cover is training and awareness which might be a little surprising since all the other standards cover it in some way.

On the other end of the scale there is NIST SPP that covers only 18 of the 26 groups and then there is DOE and IEC that both cover 21 groups. In the case of NIST SPP it might be interesting to note that it does not cover the area of network security which is covered by all of the other standards. It is also interesting that neither DOE nor NERC deals with cryptography which has been shown to be the most important area in total. DOE also does not deal with authorization while NERC does not deal with firewalls both groups that are considered to be amongst the more prioritized countermeasures.

Table 21 – The completeness of the SCADA specific standards

		AGA 12	CPNI	DHS	DOE	IEC	NERC	NIST Guide	NIST SPP	ISA	GAO	KBM	
1	Network Security	X	X	X	X	X	X	X		X	X	X	**10**
2	Separation of Network	X		X	X	X	X	X	X	X	X	X	**10**
3	Firewall	X	X	X	X	X		X	X	X	X	X	**10**
4	Intrusion Detection	X	X	X	X	X	X	X	X	X	X	X	**11**
5	Cryptography	X	X	X		X		X	X	X	X	X	**9**
6	Authorization	X	X	X		X	X	X	X	X	X	X	**10**
7	Authentication	X	X	X	X	X	X	X	X	X	X	X	**11**
8	Hardening		X	X	X	X	X	X		X	X	X	**9**
9	Antivirus		X	X		X	X	X		X	X		**7**
10	Patch Management		X	X		X	X	X		X	X	X	**8**
11	Change Management	X	X	X	X	X	X	X	X	X	X	X	**11**
12	Auditing and vulnerability scanning	X	X	X	X	X	X	X	X	X	X	X	**11**
13	Inventory and Overview	X	X	X	X		X	X		X	X	X	**9**
14	Risk Assessment and Management	X	X	X	X	X	X	X	X	X	X	X	**11**
15	Security Organization	X	X		X			X		X		X	**6**
16	Training and Awareness	X	X		X	X	X	X	X	X	X	X	**10**

17	Personnel Management	X	X	X	X	X	X	X	X	X	X	X	**11**
18	Incident planning/handling	X	X	X	X		X	X	X	X	X	X	**10**
19	Business Continuity and Contingency planning	X	X		X		X	X	X	X	X	X	**9**
20	System Resilience	X	X	X	X	X		X	X	X	X	X	**10**
21	Backup	X	X	X	X	X	X	X	X	X	X	X	**11**
22	Third party collaboration	X	X	X	X	X	X	X	X	X	X	X	**11**
23	Business Management Commitment	X	X		X		X	X		X	X		**7**
24	Policies and Standards	X	X	X	X	X	X	X	X	X	X	X	**11**
25	Security Principles	X	X	X	X	X	X	X	X	X	X	X	**11**
26	System administration tools			X		X	X	X		X	X		**6**
	Total	**22**	**24**	**22**	**21**	**21**	**22**	**26**	**18**	**26**	**25**	**23**	

5.6 Analysis of data from experts

The first thing that is striking is that the data from the experts is much more evenly spread. This might be due to the method that focal point uses to create the prioritization from the pairwise comparisons. However the experts seem to believe that technical countermeasures are more important since the four countermeasures in the top all are technical. It is very interesting to see that these are not at all the same countermeasures that are on top for the SCADA specific standards. The experts seem to worry more about the countermeasures that protect the network having both separation of network and network security amongst the top four countermeasures. Also hardening includes such tasks as making sure there exist no unnecessary connections into the system. Other technical countermeasures such as firewalls and intrusion detection are considered less important compared to the SCADA specific standards.

6 Conclusions

Based on the results in chapter 4 and 5 it seems reasonable to assume that which standard to use depend heavily upon the desired outcome. The standards all have different focus and even though the core is very similar they all add their own contribution. The data presented in this report shows that standards with the highest level of density are DHS, NIST Guide and ISA, however DHS was shown to be less complete than NIST Guide and ISA.

It is quite hard to say which countermeasures are the most important. Only looking at the number of hits it is easy to see that cryptography is frequently occurring, so is also authentication, firewalls, intrusion detection and authorization. On the other hand as discussed in chapter 5.2 there is a gap between which attacks are considered important and which countermeasures that are considered important. Based on the importance of attacks antivirus is an important area but it is not considered important if you look at the data for countermeasures. Since the focus of the standards is on technical countermeasures the non-technical countermeasures might need more attention. The connection between attacks and countermeasures need more study and a clear mapping between this would provide excellent rationale for which countermeasures to use considering which attacks you want to protect yourself from. It would also ease risk analysis since it would be possible to see which attacks you leave yourself vulnerable to if you do not implement a certain countermeasure.

Looking at the comparisons with ISO 17799 and DHS Catalog it is clear that if you are currently using ISO 17799 the areas that need the most focus are technical countermeasures. Some of the more important areas to consider are firewalls, intrusion detection and cryptography. The best standards to use can be found in **Table 20**. Another area that receives a low priority in ISO 17799 is antivirus, however antivirus is not prioritized in the SCADA specific standards either.

The expert and SCADA specific standards agree that technical countermeasures are more important but disagree on which countermeasures that are the most important. The experts focus is to protect the network. The experts agree with ISO 17799 by giving countermeasures such as firewall and intrusion detection a low priority.

The title of this thesis asks the question what is special about SCADA system cyber security. Compared to other areas of IT security there seems to be a greater focus on technical countermeasures, this takes its form in for example a lot of information about cryptography, firewalls and intrusion detection systems.

7 REFERENCES

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

[2] AGA. *About AGA*. AGA, http://www.aga.org/About/ [Accessed 17 December 2008]

[3] Bishop, M. *Introduction to Computer Security*. Addison-Wesley, Third Printing October 2006

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

[5] Carlson, R., Dagle, J., Shamsuddin, S., Evans, R. *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

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

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

[8] Digital Bond. *Field Device Protection Profile for SCADA Systems In Medium Robustness Environments Version 0.71*. National Institute of Standards and Technology, May 2006

[9] Department of Energy (DOE) . *About DOE*. DOE, http://www.energy.gov/about/index.htm [Accessed 17 December 2008]

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

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

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

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

[14] DHS. *Strategic Plan*. DHS, http://www.dhs.gov/xabout/strategicplan/ [Accessed 17 December 2008]

[15] Falco, J., Hurd, S., Teumim, D. *Using Host-Based Antivirus Software on Industrial Control Systems: Integration Guidance and a Test Methodology for Assessing Performance Impacts*. National Institute of Standards and Technology, September 2006

[16] IEEE. *A brief history of the IEEE*. IEEE, http://www.ieee.org/web/aboutus/history/index.html [Accessed 17 December 2008]

[17] IEEE. *About IEEE*. IEEE, http://www.ieee.org/web/aboutus/home/index.html [Accessed 17 December 2008]

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

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

[22] International Electrotechnical Commission (IEC). *Mission and Objectives*. IEC, http://www.iec.ch/about/mission-e.htm [Accessed 17 December 2008]

[23] IEC. *Power system control and associated communications – Data and communication security First Edition*. IEC, May 2005

[24] 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, May 2007

[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] ISO *ISO Strategy and policies*. ISO, http://www.iso.org/iso/about/iso_strategy_and_policies.htm [Accessed 17 December 2008]

[28] 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

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

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

[31] ISA. *ISA's History*. ISA, http://www.isa.org/Content/NavigationMenu/General_Information/About_ISA1/ISAs_History/ISAs_History.htm [Accessed 17 December 2008]

[32] Johansson, E., Christiansson, H., Andersson, R., Björkman, G., Vidström, A. *Aspekter på Antagonistiska Hot mot SCADA-system i samhällsviktiga verksamheter*. Krisberedskapsmyndigheten (KBM), 2007

[33] KBM. *Krisberedskapsmyndighetens uppgifter*. KBM, http://www.krisberedskapsmyndigheten.se/templates/EntryPage____1184.aspx [Accessed 17 December 2008]

[34] KBM. *Om Krisberedskapsmyndigheten*. KBM, http://www.krisberedskapsmyndigheten.se/templates/Page____4.aspx [Accessed 17 December 2008]

[35] KBM. *Vägledning till ökad säkerhet i digitala kontrollsystem i samhällsviktiga verksamheter*. KBM, 2008

[36] Kungliga Tekniska Högskolan (KTH). *Assessment of Enterprise Information Security How to Make it Credible and Efficient*. KTH, October 2005

[37] National Institute of Standards and Technology (NIST). *Computer Security Division*. NIST, http://csrc.nist.gov/index.html [Accessed 17 December 2008]

[38] NIST. *Computer Security Division Industrial Control System Security (ICS) Detailed Overview*. NIST, http://csrc.nist.gov/groups/SMA/fisma/ics/overview.html [Accessed 17 December 2008]

[39] NIST. *General Information*. NIST. http://www.nist.gov/public_affairs/general2.htm#Organization [Accessed 17 December 2008]

[40] NIST. *System Protection Profile - Industrial Control Systems Version 1.0*. NIST, April 2004

[41] North American Electric Reliability Corporation (NERC). *About Compliance*. NERC, http://www.nerc.com/page.php?cid=3|249 [Accessed 7 February 2009]

[42] NERC. *About NERC*. NERC, http://www.nerc.com/page.php?cid=1 [Accessed 17 December 2008]

[43] NERC *CIP-001-1 - CIP-009-1*. NERC, 2006

[44] 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

[45] Purcell, J. *Security Control Types and Operational Security*. Global Information Assurance Certification, http://www.giac.org/resources/whitepaper/operations/207.php [Accessed 18 December 2008]

[46] Stouffer, K., Falco, J., Scarfone, K. *Guide to Industrial Control Systems (ICS) Security Special Publication 800-82 SECOND PUBLIC DRAFT*. National Institute of Standards and Technology, September 2007

[47] Säkerhetspolisen. *Historik*. Säkerhetspolisen, http://www.sakerhetspolisen.se/omsakerhetspolisen/historik.4.7671d7bb110e3dcb1fd800010243.html [Accessed 17 December 2008]

[48] Säkerhetspolisen. *Om Säkerhetspolisen*. Säkerhetspolisen, http://www.sakerhetspolisen.se/omsakerhetspolisen.4.3b063add1101207dd46800055415.html [Accessed 17 December 2008]

[49] Säkerhetspolisen. *Säkerhetsskydd – en vägledning*. Säkerhetspolisen, May 2008

[50] Turk, R. *Cyber Incidents Involving Control Systems*. Idaho National Laboratory, October 2005

[51] United States General Accounting Office (GAO). *About GAO*. GAO, http://www.gao.gov/about/index.html [Accessed 17 December 2008]

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

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

8 Appendix 1

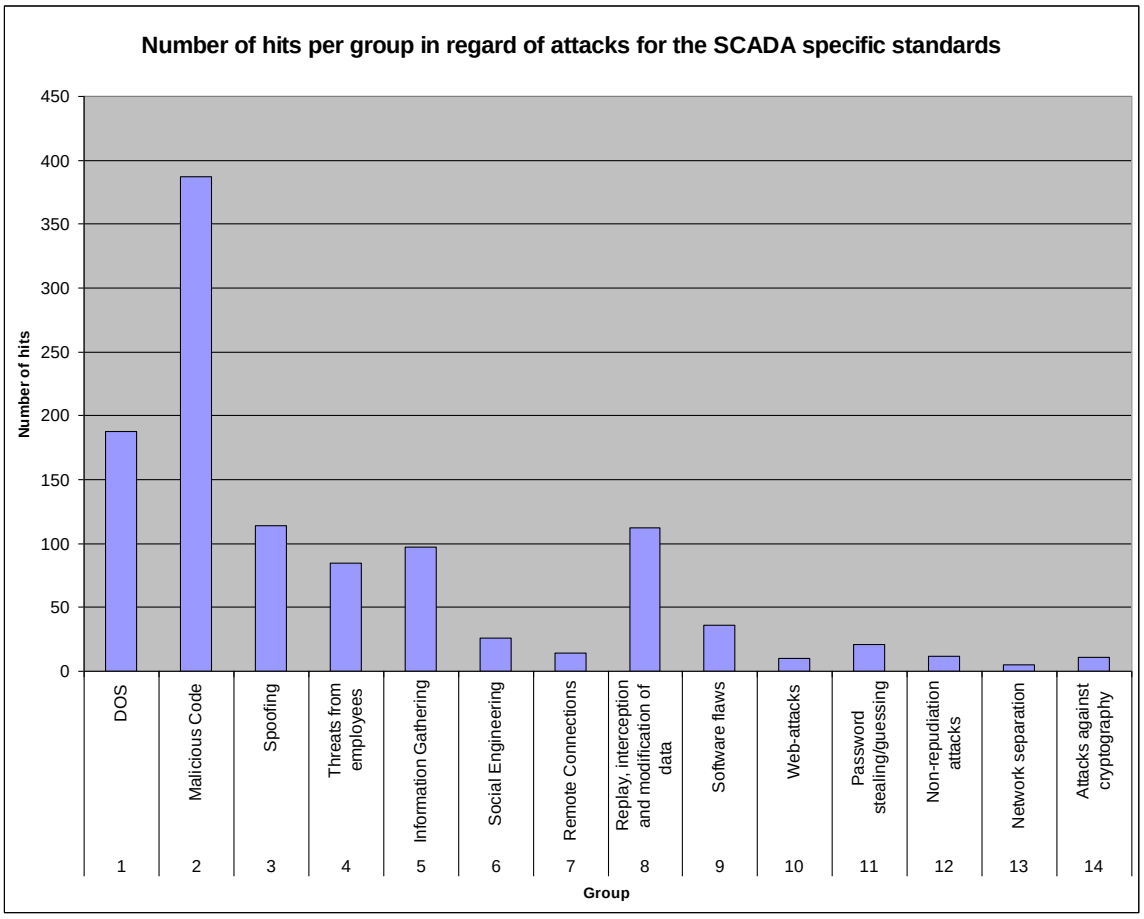

Figure 22 – The number of hits per group for attacks

9 Appendix 2

Table 22 – The number of hits for each keyword per group of countermeasures, per keyword and per standard.

		1	2	3	4	5	6	7	8	9	10	11		
		AGA 12	CPNI	DHS	DOE	IEC	NERC	NIST Guide	NIST SPP	ISA	GAO	KBM		
1	**Network Security**													
	Dial-up Modem	1		7			1	7		2				**18**
	Dial-back modem	1		1										**2**
	Remote Support Connection		3											**3**
	Remote Support Access							2						**2**
	Wireless polic(y)(ies)													**0**
	Wireless network security							5						**5**
	Wireless security					1				1	12			**14**
	Dedicated line			8										**8**
	Web-based interface			9										**9**
	DNS			41				13		1	3	1		**59**
	TCP/IP	2	1	12		16		7		5	24			**67**
	Callback system				1			1						**2**
	MAC address locking							4						**4**
	Total	**4**	**4**	**78**	**1**	**17**	**1**	**39**	**0**	**9**	**39**	**1**		**193**

		1	2	3	4	5	6	7	8	9	10	11		
		AGA 12	CPNI	DHS	DOE	IEC	NERC	NIST Guide	NIST SPP	ISA	GAO	KBM		
2	**Separation of Network**													
	Separate security domain	1												**1**
	Separat(e)(ion)(ing)	8		14		3		18	3	15	6	10		**77**
	Isolat(e)(ation)			3	2	4		12		15		3		**39**
	DMZ			34	1			51		11		4		**101**
	Demilitarized zone			2	1			5		6				**14**
	Electronic security perimeter			10		1	88					6		**105**
	VLAN			4				19		28				**51**
	Virtual Local Area Network							2		2				**4**
	Total	**9**	**0**	**67**	**4**	**8**	**88**	**107**	**3**	**77**	**6**	**23**		**392**
		1	2	3	4	5	6	7	8	9	10	11		
		AGA 12	CPNI	DHS	DOE	IEC	NERC	NIST Guide	NIST SPP	ISA	GAO	KBM		
3	**Firewall**													
	Firewall	6	37	77	3	11		164	3	215	183	11		**710**
	Packet Filtering			1				3		3				**7**
	Stateful Inspection			1				6		2	14			**23**
	Application Proxy							1		1	13			**15**
	Boundary protection								5		13			**18**
	Total	**6**	**37**	**79**	**3**	**11**	**0**	**174**	**8**	**221**	**223**	**11**		**773**

		1	2	3	4	5	6	7	8	9	10	11		
		AGA 12	CPNI	DHS	DOE	IEC	NERC	NIST Guide	NIST SPP	ISA	GAO	KBM		
4	**Intrusion Detection**													
	Intrusion detection	11	3	33	5	11		27	5	44	33	9		**181**
	Intrusion prevention		1	6				3		3	14			**27**
	HIDS			21						15		1		**37**
	NIDS			34						16		1		**51**
	IDS	6	1	81	2	6		29	10	82	69	3		**289**
	Canar(y)(ies)			10								1		**11**
	Honey pot			1								2		**3**
	Security status monitoring			2			2							**4**
	Replay detection								2					**2**
	Detection of modification								2					**2**
	Security alarms								3					**3**
	Anomaly detection			1					2	1	1			**5**
	Potential violation analysis								3					**3**
	Content management										7			**7**
	Security event correlation tool										15			**15**
	Traffic monitoring			4				1		3				**8**
	Forensics and analysis tools									4				**4**
	Attack heuristics								4					**4**
	Integrity checker			1							23			**24**
	Total	**17**	**5**	**194**	**7**	**17**	**2**	**60**	**31**	**168**	**162**	**17**		**680**

		1	2	3	4	5	6	7	8	9	10	11		
		AGA 12	CPNI	DHS	DOE	IEC	NERC	NIST Guide	NIST SPP	ISA	GAO	KBM		
5	**Cryptography**													
	Encrypt(ion)	152	1	80		46		67	2	133	84	1		**566**
	Cryptograph(y)(ic)	413	0	4		6		37	37	97	75			**669**
	Decryption	31		1				4		29	26			**91**
	TLS	1				25		8		5	1			**40**
	Digital Signature	13				11				10	38			**72**
	PKI	5		3		5				10	9			**32**
	Public key infrastructure	2						1		2	5			**10**
	Confidentiality during transition								1					**1**
	IPSEC	1		5		4		11		18	9			**48**
	SSL	8		3		2		11	8	17	11			**60**
	SSH			3				4		6	1			**14**
	Certificate(s)	12		5		8				8	11			**44**
	VPN	4	1	31		16		24	2	81	41			**200**
	Virtual private network	2		6		6		4		5	14			**37**
	Kerberos									8				**8**
	Total	**644**	**2**	**141**	**0**	**129**	**0**	**171**	**50**	**429**	**325**	**1**		**1892**
		1	2	3	4	5	6	7	8	9	10	11		
		AGA 12	CPNI	DHS	DOE	IEC	NERC	NIST Guide	NIST SPP	ISA	GAO	KBM		
6	**Authorization**													
	RBAC	6		12		7		6	2	24				**57**
	Access Control	14	1	66		17	10	42	35	61	21	1		**268**

	Session Management			4										**4**
	Access rights		1			2	6			1	1			**11**
	Electronic access						14					2		**16**
	Account Management	3		19			2			3				**27**
	Management of TSF data								1					**1**
	Rights and privileges										11			**11**
	Authorization	5		12		7	8	14	7	64	20			**137**
	Access control list			2		5		3		1				**11**
	Least privilege	1		2				3			2			**8**
	Separation of duties							1	1	1	2			**5**
	Password policy			1				2			1			**4**
	Key management	24				10		7	1	11	3			**56**
	Total	**53**	**2**	**118**	**0**	**48**	**40**	**78**	**47**	**166**	**61**	**3**		**616**
		1	2	3	4	5	6	7	8	9	10	11		
		AGA 12	CPNI	DHS	DOE	IEC	NERC	NIST Guide	NIST SPP	ISA	GAO	KBM		
7	**Authentication**													
	Authentication	77		120	1	95	3	119	72	299	74	3		**863**
	Single Sign-On	1		9						1				**11**
	Password	27	2	86		15	6	112	13	204	53	4		**522**
	Identification									18		1		**19**
	Time-limited								2					**2**
	Session locking							1	1					**2**
	Total	**105**	**2**	**215**	**1**	**110**	**9**	**232**	**88**	**522**	**127**	**8**		**1419**

		1	2	3	4	5	6	7	8	9	10	11		
		AGA 12	CPNI	DHS	DOE	IEC	NERC	NIST Guide	NIST SPP	ISA	GAO	KBM		
8	**Hardening**													
	Harden(ing)		5	12	1			3		6	2	12		**41**
	Unnecessary hardware can be physically disabled			1										**1**
	Protect the BIOS			1										**1**
	Heartbeat signals			7										**7**
	Disabling, Removing or modifying well-known or guest accounts			13										**13**
	Disconnect unnecessary connections to the SCADA network				2							1		**3**
	Default account			4			3							**7**
	Default password			3		1		4		3	1	1		**13**
	Media Protection							6						**6**
	Total	**0**	**5**	**41**	**3**	**1**	**3**	**13**	**0**	**9**	**3**	**14**		**92**
		1	2	3	4	5	6	7	8	9	10	11		
		AGA 12	CPNI	DHS	DOE	IEC	NERC	NIST Guide	NIST SPP	ISA	GAO	KBM		
9	**Antivirus**													
	Antivirus		1	3				39		10	24			**77**
	Anti-virus		10	2		4	4	1		4				**25**
	Malware Detection			28										**28**
	Malware Prevention						4							**4**
	Total	**0**	**11**	**33**	**0**	**4**	**8**	**40**	**0**	**14**	**24**	**0**		**134**

		1	2	3	4	5	6	7	8	9	10	11		
		AGA 12	CPNI	DHS	DOE	IEC	NERC	NIST Guide	NIST SPP	ISA	GAO	KBM		
10	**Patch Management**													
	Patch management		1	10		1	3	9		7	24			**55**
	Apply patch		1											**1**
	Patching		10	6				3		5	1	2		**27**
	Security update			1						2				**3**
	Security patch		1	5			7	12		4	3			**32**
	Total	**0**	**13**	**22**	**0**	**1**	**10**	**24**	**0**	**18**	**28**	**2**		**118**
		1	2	3	4	5	6	7	8	9	10	11		
		AGA 12	CPNI	DHS	DOE	IEC	NERC	NIST Guide	NIST SPP	ISA	GAO	KBM		
11	**Change Management**													
	Change control		11			1	6	1	1	3				**23**
	Configuration management	1		3	4		6	8	12	9	18	1		**62**
	Change management							9		24		8		**41**
	Management of change		2					1		10	1	1		**15**
	Total	**1**	**13**	**3**	**4**	**1**	**12**	**19**	**13**	**46**	**19**	**10**		**141**

		1	2	3	4	5	6	7	8	9	10	11		
		AGA 12	CPNI	DHS	DOE	IEC	NERC	NIST Guide	NIST SPP	ISA	GAO	KBM		
12	**Auditing and vulnerability scanning**													
	Audit(ing)	50	25	15	6	29	21	41	92	107	31	7		**424**
	Understand the vulnerabilities	4	1											**5**
	Post implementation review		2											**2**
	Security review		10	1										**11**
	Security test (Test security before system go live)	1	15	2		1	2	8		5	6	6		**46**
	Self-assessments		3		4			1		1		1		**10**
	Vulnerability assessment	1	1				18	10	9	20	31			**90**
	Monitoring Electronic Access						1							**1**
	Security Assessments		1	1		4		8		3	1			**18**
	User identity association								2					**2**
	Test plans	24						3	2	28		1		**58**
	System validation							1		12				**13**
	Scanner			3				8		39	72			**122**
	Timestamp					1			8			1		**10**
	Log auditing									4				**4**
	Total	**80**	**58**	**22**	**10**	**35**	**42**	**80**	**113**	**219**	**141**	**16**		**816**

		1	2	3	4	5	6	7	8	9	10	11		
		AGA 12	CPNI	DHS	DOE	IEC	NERC	NIST Guide	NIST SPP	ISA	GAO	KBM		
13	**Inventory and Overview**													
	Inventory	1	30	2	1			12		28	1	3		**78**
	Understand the system		1											**1**
	Identify all connections				2							1		**3**
	Identified critical asset						1							**1**
	Network diagrams		2					1		1				**4**
	Identify assets										1			**1**
	Total	**1**	**33**	**2**	**3**	**0**	**1**	**13**	**0**	**29**	**2**	**4**		**88**
		1	2	3	4	5	6	7	8	9	10	11		
		AGA 12	CPNI	DHS	DOE	IEC	NERC	NIST Guide	NIST SPP	ISA	GAO	KBM		
14	**Risk Assessment and Management**													
	Risk assessment	13	30		4	6	18	28	24	33	53	5		**214**
	Understand (the) vulnerabilities	4	3											**7**
	Understand (the) threats	1	3			1					1			**6**
	Understand (the) impacts		3											**3**
	Understand (the) risks		1							1	1			**3**
	Assessment of business risk		3											**3**
	Risk reduction workshop		3											**3**
	Mitigation Controls							4		1				**5**
	Risk analysis	8	1		2			5	7	17	6	15		**61**

	Define risks									5				**5**
	Risk goals	2								12				**14**
	Risk Management		2		5	3		14	30	7	18	7		
	Mitigate Risk			2				1		11	3			
	Risk mitigation													
	Risk based						6	4			12	2		
	Identify risk			1				1	1					
	Total	**28**	**49**	**3**	**11**	**10**	**24**	**57**	**62**	**87**	**94**	**29**		**454**
		1	2	3	4	5	6	7	8	9	10	11		
		AGA 12	CPNI	DHS	DOE	IEC	NERC	NIST Guide	NIST SPP	ISA	GAO	KBM		
15	**Security Organization**													
	Security team	1	3					12						**16**
	InfoSec team	24												**24**
	Security Response Team		8											**8**
	Red Team	1			4			1				1		**7**
	Cross-Functional Team							4		3				**7**
	Total	**26**	**11**	**0**	**4**	**0**	**0**	**17**	**0**	**3**	**0**	**1**		**62**
		1	2	3	4	5	6	7	8	9	10	11		
		AGA 12	CPNI	DHS	DOE	IEC	NERC	NIST Guide	NIST SPP	ISA	GAO	KBM		
16	**Training and Awareness**													
	Training and Awareness	3	1					3						**7**
	Awareness and Training		5					10		1				**16**
	Awareness programme		13											**13**

	Coach IT personnel		1											**1**
	Information Awareness				1									**1**
	Security Training		4			1	2	4		1	1			**13**
	Training program						6	6	1	8				**21**
	Security Awareness		15				4	10	8		10	3		**50**
	Total	**3**	**39**	**0**	**1**	**1**	**12**	**33**	**9**	**10**	**11**	**3**		**122**
		1	2	3	4	5	6	7	8	9	10	11		
		AGA 12	CPNI	DHS	DOE	IEC	NERC	NIST Guide	NIST SPP	ISA	GAO	KBM		
17	**Personnel Management**													
	Contract	8	31	38		5	7	10	7	26	11			**143**
	Improved relationships		1											**1**
	Separation Agreement			3										**3**
	Security roles				2			1	14			1		**18**
	Personnel Risk Assessment						17							**17**
	Personnel Security		18					9	3	12				**42**
	Hiring	1						1		10				**12**
	Conditions of Employment							1		6				**7**
	Roles and responsibilities	1	5		2		4	5	5	2	5	5		**34**
	Security organization				2			3		3	1			**9**
	Background Checks													**0**
	Total	**10**	**55**	**41**	**6**	**5**	**28**	**30**	**29**	**59**	**17**	**6**		**286**

		1	2	3	4	5	6	7	8	9	10	11		
		AGA 12	CPNI	DHS	DOE	IEC	NERC	NIST Guide	NIST SPP	ISA	GAO	KBM		
18	**Incident planning/handling**													
	Incident handling			1			1	6						**8**
	Incident management		2					3				5		**10**
	Incident response	1	19		1		17	15	2	7				**62**
	Warning system		2											**2**
	Incident report		3				4	1	1		1			**10**
	Incidents documentation						1							**1**
	Response to security incidents										1			**1**
	Computer forensics tool	1	3	1	1			2		4	10			**22**
	Total	**2**	**29**	**2**	**2**	**0**	**23**	**27**	**3**	**11**	**12**	**5**		**116**
		1	2	3	4	5	6	7	8	9	10	11		
		AGA 12	CPNI	DHS	DOE	IEC	NERC	NIST Guide	NIST SPP	ISA	GAO	KBM		
19	**Business Continuity and Contingency planning**													
	Disaster recovery	1	7		5		2	8	2	7		2		**34**
	Business Continuity	1	7				1	12	4	3	3			**31**
	Recovery plan				5		22	9	1	3		3		**43**
	Contingency	2						19		6	2	9		**38**
	Continuity of operation	1						1	3		13			**18**
	Total	**5**	**14**	**0**	**10**	**0**	**25**	**49**	**10**	**19**	**18**	**14**		**164**

		1	2	3	4	5	6	7	8	9	10	11		
		AGA 12	CPNI	DHS	DOE	IEC	NERC	NIST Guide	NIST SPP	ISA	GAO	KBM		
20	**System Resilience**													
	Redundant	4	1	3		3		19	4	5	5			**44**
	Single points of failure	1			2			2	2					**7**
	Spof								3					**3**
	Fault tolerance							6	1	1	5	2		
	UPS							4						
	Fail-safe	1						2						**3**
	Total	**6**	**1**	**3**	**2**	**3**	**0**	**33**	**10**	**6**	**10**	**2**		**76**
		1	2	3	4	5	6	7	8	9	10	11		
		AGA 12	CPNI	DHS	DOE	IEC	NERC	NIST Guide	NIST SPP	ISA	GAO	KBM		
21	**Backup**													
	Backup	21	8	2	3	10	13	29	31	22	19	8		**166**
	Total	**21**	**8**	**2**	**3**	**10**	**13**	**29**	**31**	**22**	**19**	**8**		**166**
		1	2	3	4	5	6	7	8	9	10	11		
		AGA 12	CPNI	DHS	DOE	IEC	NERC	NIST Guide	NIST SPP	ISA	GAO	KBM		
22	**Third party collaboration**													
	Third party Third parties	11	45	27		6	9	14	3	9	6	2		**132**
	Vendor	12	25	100	7		5	35	2	35	12	41		**274**
	Reuse proven solutions		1											**1**
	Flaw Remediation			11					13					**24**
	Industry forums									2				**2**

	Security requirements in procurement		1											**1**
	Total	**23**	**72**	**138**	**7**	**6**	**14**	**49**	**18**	**46**	**18**			**391**
		1	2	3	4	5	6	7	8	9	10	11		
		AGA 12	CPNI	DHS	DOE	IEC	NERC	NIST Guide	NIST SPP	ISA	GAO	KBM		
23	**Business Management Commitment**													
	Define the cyber security goals and practice	3												**3**
	Business case	2	19					19		5	5			**50**
	Senior management	7	11		1			9		2				**30**
	Senior manager	1	1		1		20							**23**
	Charter and Scope							5						**5**
	Leadership commitment									2	2			**4**
	Total	**13**	**31**	**0**	**2**	**0**	**20**	**33**	**0**	**9**	**7**	**0**		**115**
		1	2	3	4	5	6	7	8	9	10	11		
		AGA 12	CPNI	DHS	DOE	IEC	NERC	NIST Guide	NIST SPP	ISA	GAO	KBM		
24	**Policies and Standards**													
	Security polic(y)(ies)	14	9	1	1	28	23	14	21	66	18	4		**199**
	Develop(ing) polic(y)(ies)		3			1		1		9				**14**
	Compliance with polic(y)(ies)		6											**6**
	Legal requirement		1							3	1			**5**
	Total	**14**	**19**	**1**	**1**	**29**	**23**	**15**	**21**	**78**	**19**	**4**		**224**

		1	2	3	4	5	6	7	8	9	10	11		
		AGA 12	CPNI	DHS	DOE	IEC	NERC	NIST Guide	NIST SPP	ISA	GAO	KBM		
25	**Security Principles**													
	Secure Architecture		34					1				1		**36**
	Write safe code			2										**2**
	Defense in depth	1		2	3			22		12	4			**44**
	Security requirement	9	53	3	3	45		34	66	38	42	19		**312**
	Information protection			1			4							**5**
	Peformance Consideration									2				**2**
	Total	**10**	**87**	**8**	**6**	**45**	**4**	**57**	**66**	**52**	**46**	**20**		**401**
		1	2	3	4	5	6	7	8	9	10	11		
		AGA 12	CPNI	DHS	DOE	IEC	NERC	NIST Guide	NIST SPP	ISA	GAO	KBM		
26	**System administration tools**													
	Host configuration management tools									3				**3**
	Policy enforcement Applications										4			**4**
	Network management			3		6	1	6		7	41			**64**
	Total	**0**	**0**	**3**	**0**	**6**	**1**	**6**	**0**	**10**	**45**	**0**		**71**
		1	2	3	4	5	6	7	8	9	10	11		
		AGA 12	CPNI	DHS	DOE	IEC	NERC	NIST Guide	NIST SPP	ISA	GAO	KBM		
	TOTAL	**1081**	**600**	**1216**	**91**	**497**	**403**	**1485**	**612**	**2339**	**1476**	**202**		

Table 23 - The number of hits for each keyword per group of countermeasures, per keyword and per standard.

		AGA 12	CPNI	DHS	IEC	NIST, Guide	NIST, SPP	ISA	GAO	KBM	
1	**DOS**										
	DOS	17	1	6	2	14	30	6			**76**
	DDOS	2						2	1		**5**
	Denial of Service	6	7	3	29	6	2	23	20		**96**
	Syn flood			1							**1**
	Resource Exhaustion				10						**10**
		25	**8**	**10**	**41**	**20**	**32**	**31**	**21**	**0**	**188**
		AGA 12	CPNI	DHS	IEC	NIST, Guide	NIST, SPP	ISA	GAO	KBM	
2	**Malicious Code**										
	Malicious Code	3	1	2		8		23	17	7	**61**
	Malicious Software	1		3	1	4		2	1	1	**13**
	Virus	1	13	5		19	5	42	25	1	**111**
	Worm	1	16	2		14		7	20	1	**61**
	Trojan		2	3	3	5	1	10	13		**37**
	Malware		8	47	1	45		1			**102**
	Logic Bomb								2		**2**
		6	**40**	**62**	**5**	**95**	**6**	**85**	**78**	**10**	**387**

		AGA 12	CPNI	DHS	IEC	NIST, Guide	NIST, SPP	ISA	GAO	KBM	
3	**Spoofing**										
	Spoof	1		7	9	7	10	10	4		**48**
	Impersonate	2			7		3	2			**14**
	Masquerade	1			10			2	2		**15**
	Man in the middle				10	11		7	2		**30**
	MITM			6							**6**
	Session Hijack			1							**1**
		4	**0**	**14**	**36**	**18**	**13**	**21**	**8**	**0**	**114**
		AGA 12	CPNI	DHS	IEC	NIST, Guide	NIST, SPP	ISA	GAO	KBM	
4	**Threats from employees**										
	Disgruntled Employee	1	1		4	4		2	2		**14**
	Operator error										**0**
	Insider	1	1		10	10	5	21	20		**68**
	human error, theft, fraud					2		1			**3**
		2	**2**	**0**	**14**	**16**	**5**	**24**	**22**	**0**	**85**
		AGA 12	CPNI	DHS	IEC	NIST, Guide	NIST, SPP	ISA	GAO	KBM	
5	**Information Gathering**										
	Eavesdrop	4			9	4		5	5		**27**
	Sniff					1	3	16	4		**24**
	Traffic analysis	2		1	5		1	3			**12**
	Tap	5		1	1			7			**14**

	War dial	1		4		2			2		**9**
	War drive								1		**1**
	Visual observation							2			**2**
	Keystroke					3	2	2	1		**8**
		12	**0**	**6**	**15**	**10**	**6**	**35**	**13**	**0**	**97**
		AGA 12	CPNI	DHS	IEC	NIST, Guide	NIST, SPP	ISA	GAO	KBM	
6	**Social Engineering**										
	Social engineering					7	1	8			**16**
	Phishing					7		3			**10**
		0	**0**	**0**	**0**	**14**	**1**	**11**	**0**	**0**	**26**
		AGA 12	CPNI	DHS	IEC	NIST, Guide	NIST, SPP	ISA	GAO	KBM	
7	**Remote Connections**										
	Rogue access point					1					**1**
	Backdoor				1	7			1	1	**10**
	Uncontrolled external access						1				**1**
	Unknown connection					1				1	**2**
		0	**0**	**0**	**1**	**9**	**1**	**0**	**1**	**2**	**14**

		AGA 12	CPNI	DHS	IEC	NIST, Guide	NIST, SPP	ISA	GAO	KBM	
8	**Replay, interception and modification of data**										
	Replay	9			20	6	11	13	2		**61**
	Intercept			12	9	5		14	6		**46**
	Modify data								1		**1**
	Modification of data		1		1			1			**3**
	(Unauthorised change of setpoints)					1					**1**
		9	**1**	**12**	**30**	**12**	**11**	**28**	**9**	**0**	**112**
		AGA 12	CPNI	DHS	IEC	NIST, Guide	NIST, SPP	ISA	GAO	KBM	
9	**Software flaws**										
	Buffer overflow			7	1	4	1	2			**15**
	Command Injection			5							**5**
	Software bugs							1			**1**
	"illegal" conditions					1					**1**
	Programming errors			1				1	1	1	**4**
	SQL injection			4							**4**
	Software flaw							4	2		**6**
		0	**0**	**17**	**1**	**5**	**1**	**8**	**3**	**1**	**36**

		AGA 12	CPNI	DHS	IEC	NIST, Guide	NIST, SPP	ISA	GAO	KBM	
10	**Web-attacks**										
	Remote File Include			5							**5**
	Cross Site Scripting			5							**5**
		0	**0**	**10**	**0**	**0**	**0**	**0**	**0**	**0**	**10**
		AGA 12	CPNI	DHS	IEC	NIST, Guide	NIST, SPP	ISA	GAO	KBM	
11	**Password stealing/guessing**										
	Stealing password	1									**1**
	Password Guessing					1		1			**2**
	Guessable passwords								1		**1**
	Brute force			1				2			**3**
	Dictionary	5		4		5					**14**
		6	**0**	**5**	**0**	**6**	**0**	**3**	**1**	**0**	**21**
		AGA 12	CPNI	DHS	IEC	NIST, Guide	NIST, SPP	ISA	GAO	KBM	
12	**Non-repudiation attacks**										
	Deleting Records				3						**3**
	Denial of Action				4						**4**
	Claim of Action				4						**4**
	Modify log			1							**1**
		0	**0**	**1**	**11**	**0**	**0**	**0**	**0**	**0**	**12**

		AGA 12	CPNI	DHS	IEC	NIST, Guide	NIST, SPP	ISA	GAO	KBM	
13	**Network separation**										
	Poorly designed network			1							**1**
	Broadcast storm					1		1		1	**3**
	Dual network interface cards (NIC) to connect networks					1					**1**
		0	**0**	**1**	**0**	**2**	**0**	**1**	**0**	**1**	**5**
		AGA 12	CPNI	DHS	IEC	NIST, Guide	NIST, SPP	ISA	GAO	KBM	
14	**Attacks against cryptography**										
	Ciphertext-only attack	1									**1**
	Known-plaintext attack	1									**1**
	Chosen-plaintext attack	2									**2**
	Adaptive-chosen plaintext attack	1									**1**
	Chosen-ciphertext attack	3									**3**
	Adaptive chosen ciphertext attack	1									**1**
	Known-key attack	1									**1**
	Roll back							1			**1**
		10	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**11**

10 Appendix 3

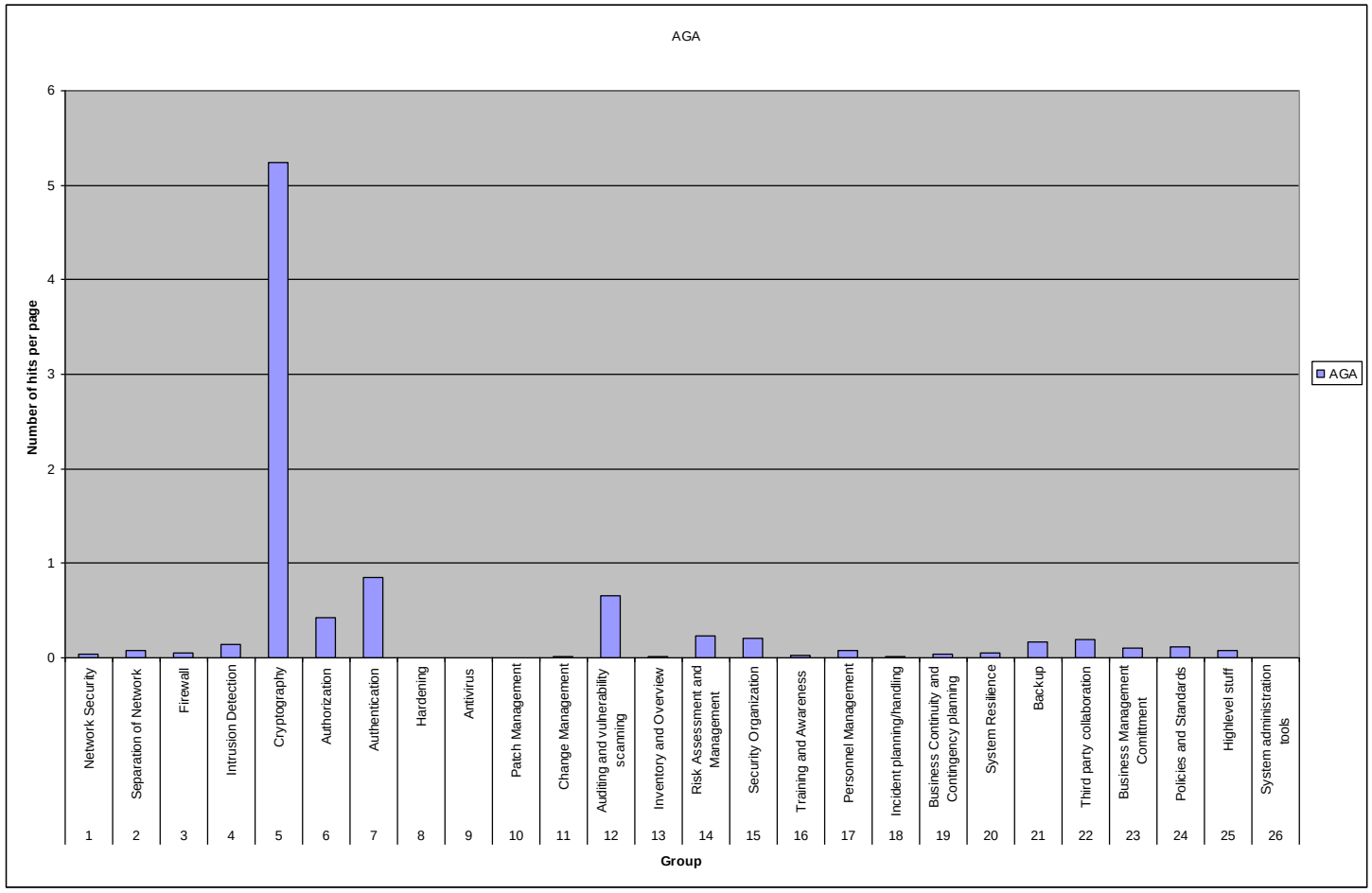

Figure 23 – The number of hits per page per group for AGA 12

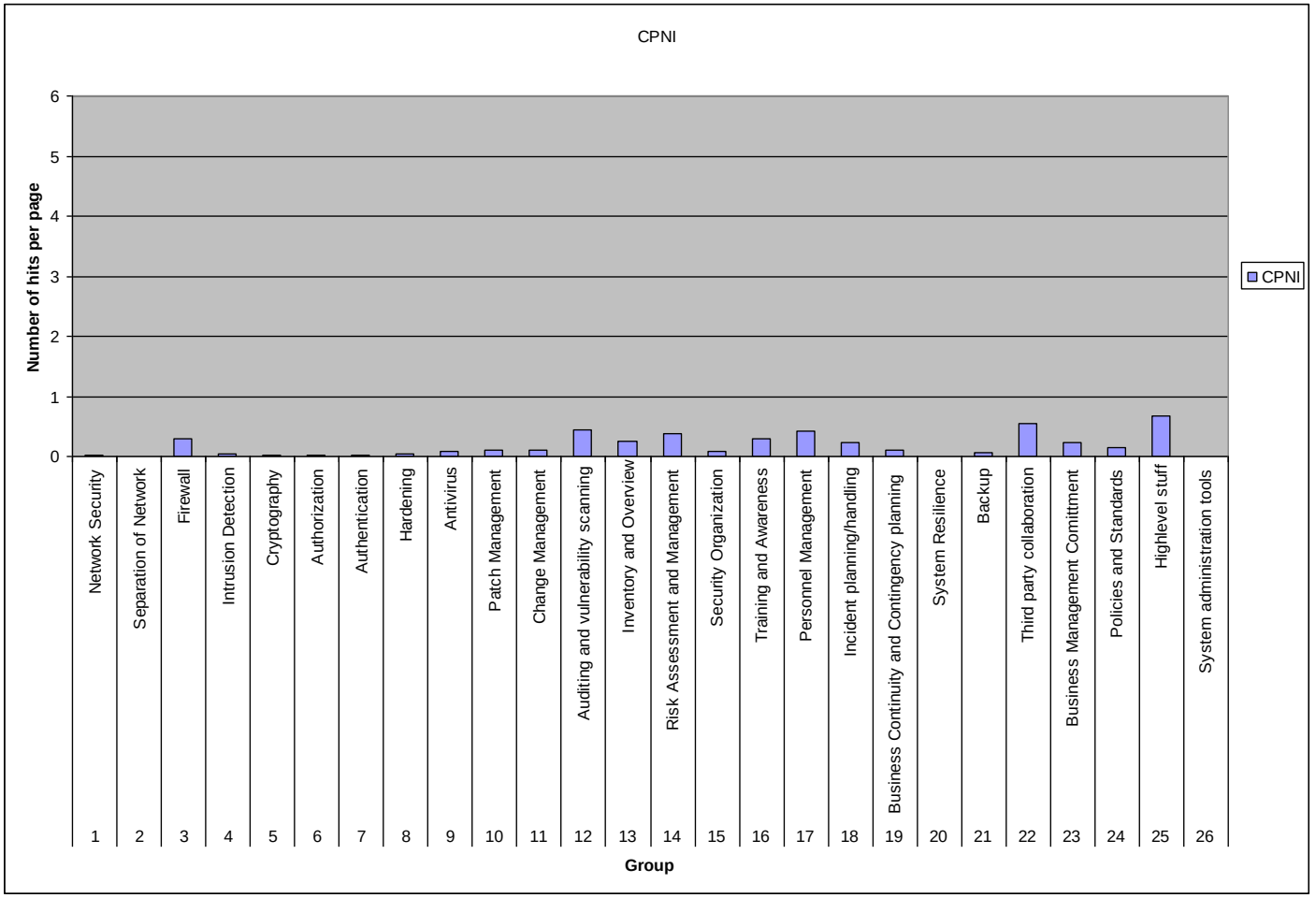

Figure 24 - The number of hits per page per group for CPNI

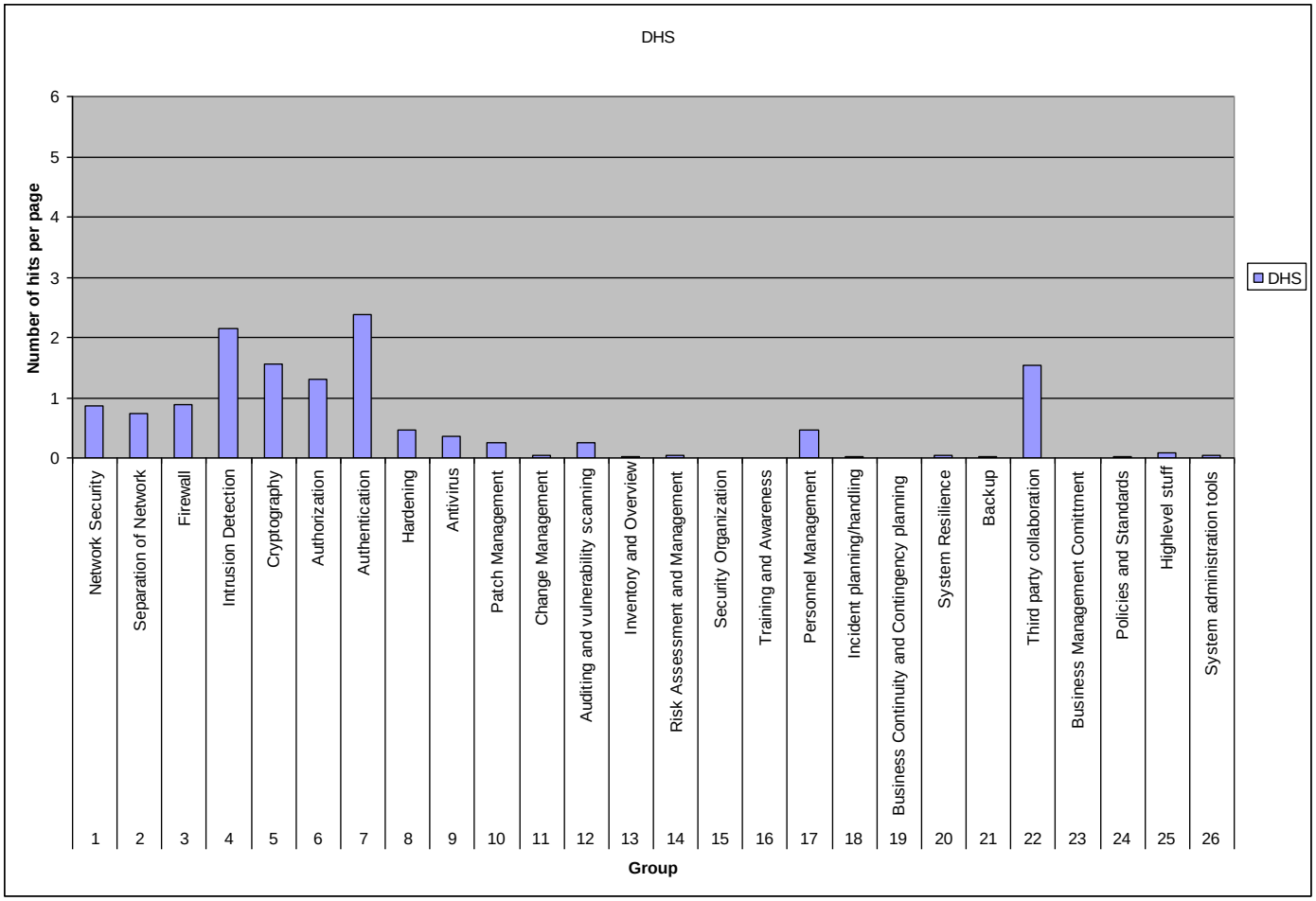

Figure 25 - The number of hits per page per group for DHS

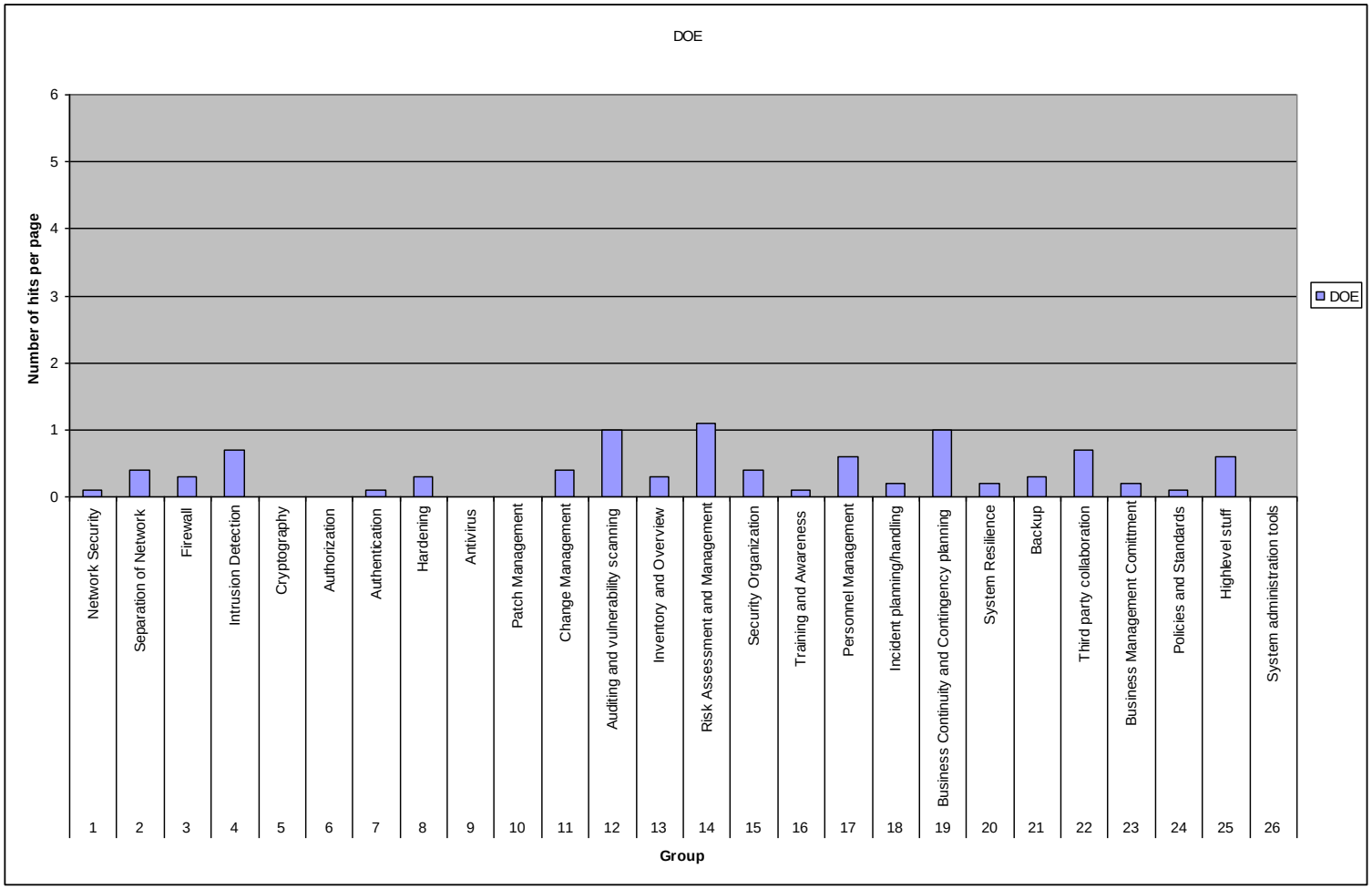

Figure 26 - The number of hits per page per group for DOE

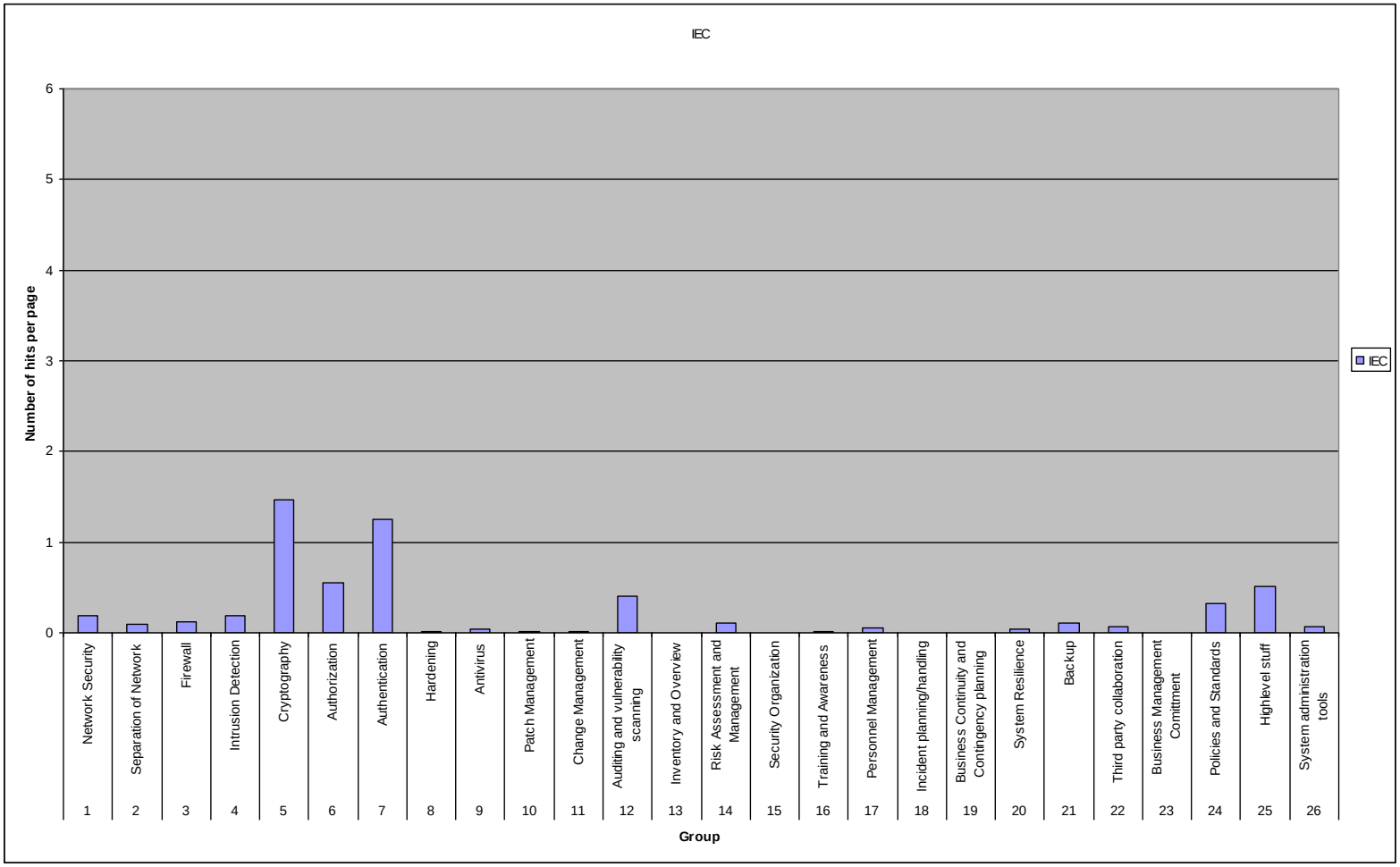

Figure 27 - The number of hits per page per group for IEC

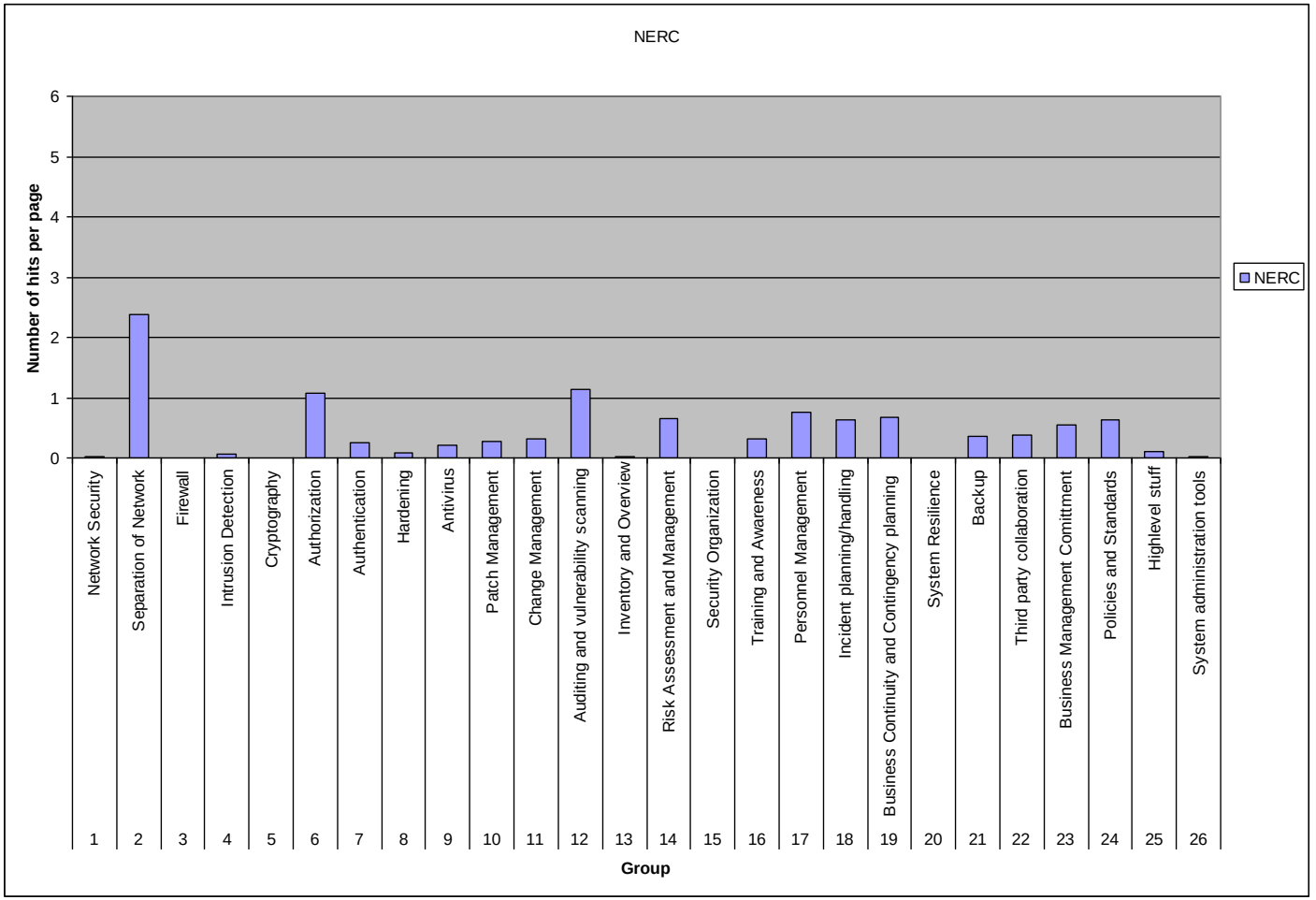

Figure 28 - The number of hits per page per group for NERC

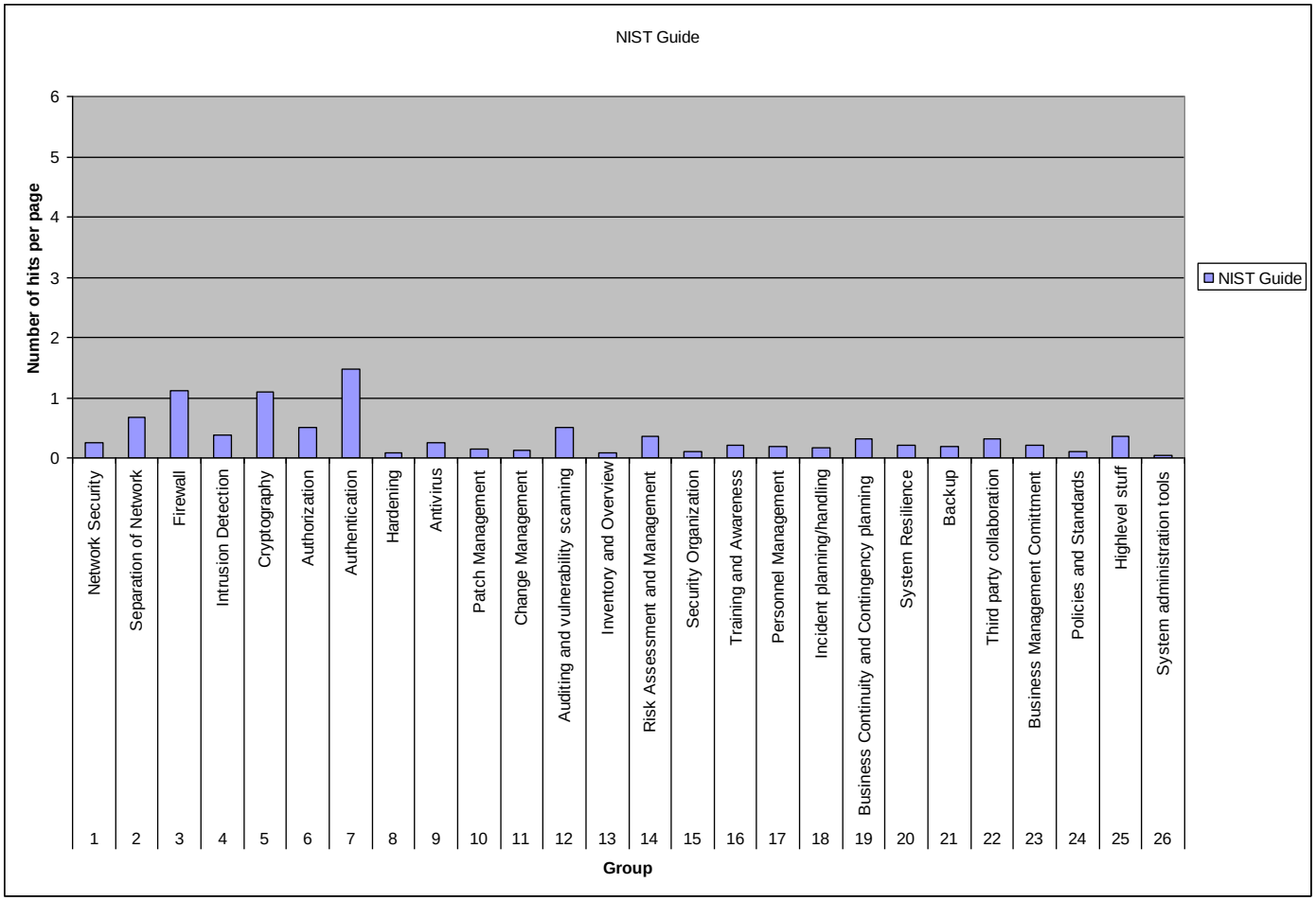

Figure 29 - The number of hits per page per group for NIST Guide

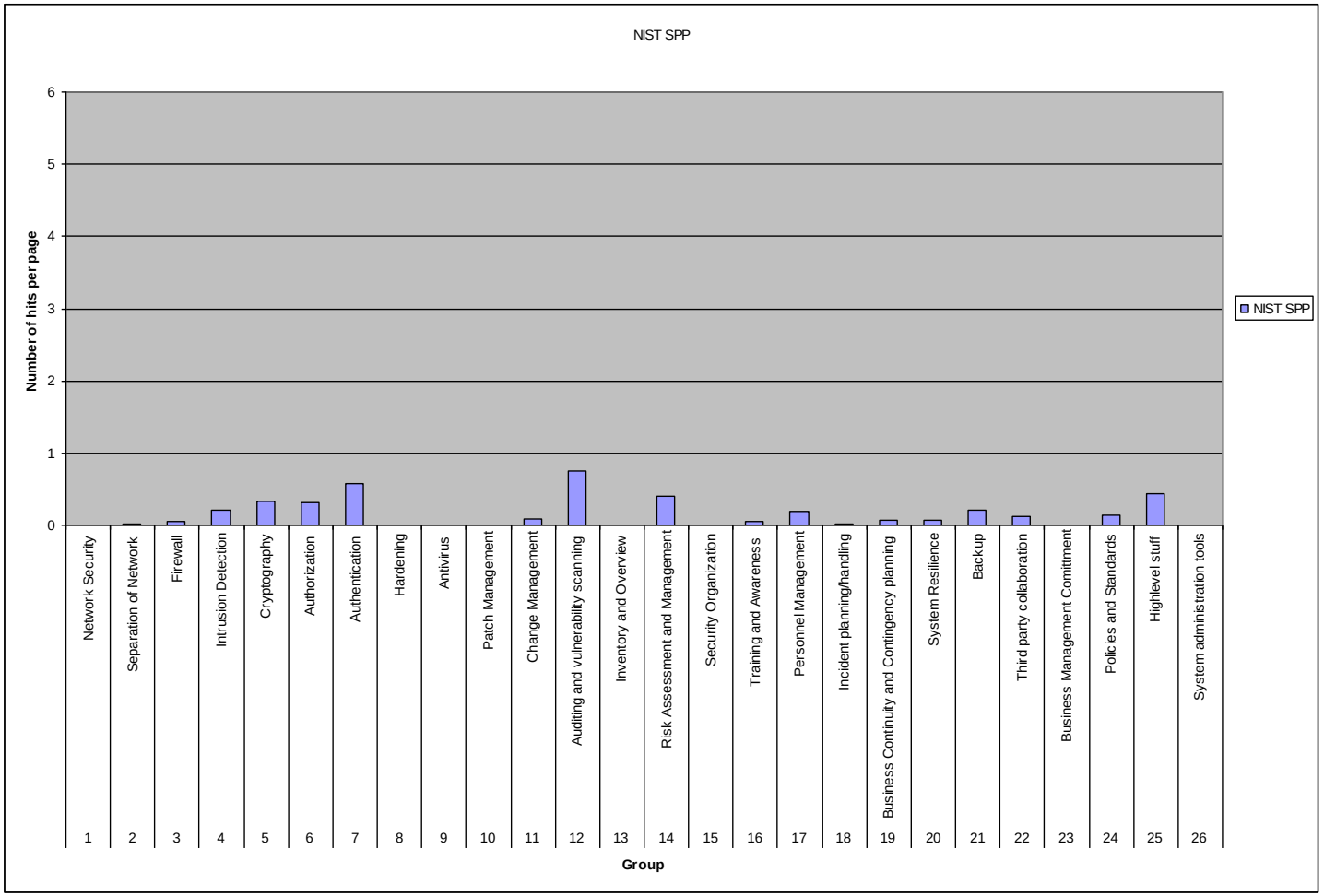

Figure 30 - The number of hits per page per group for NIST SPP

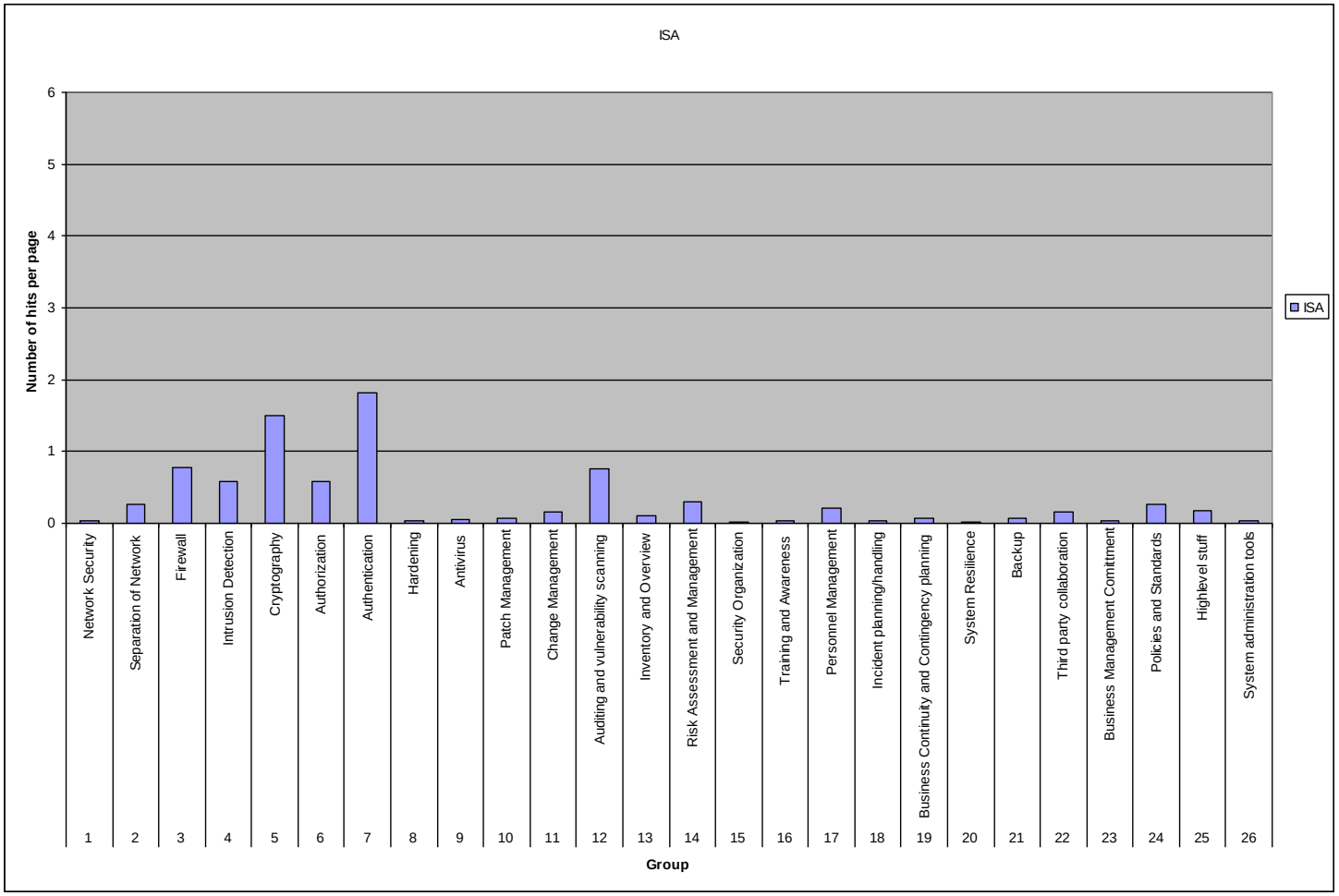

Figure 31 - The number of hits per page per group for ISA

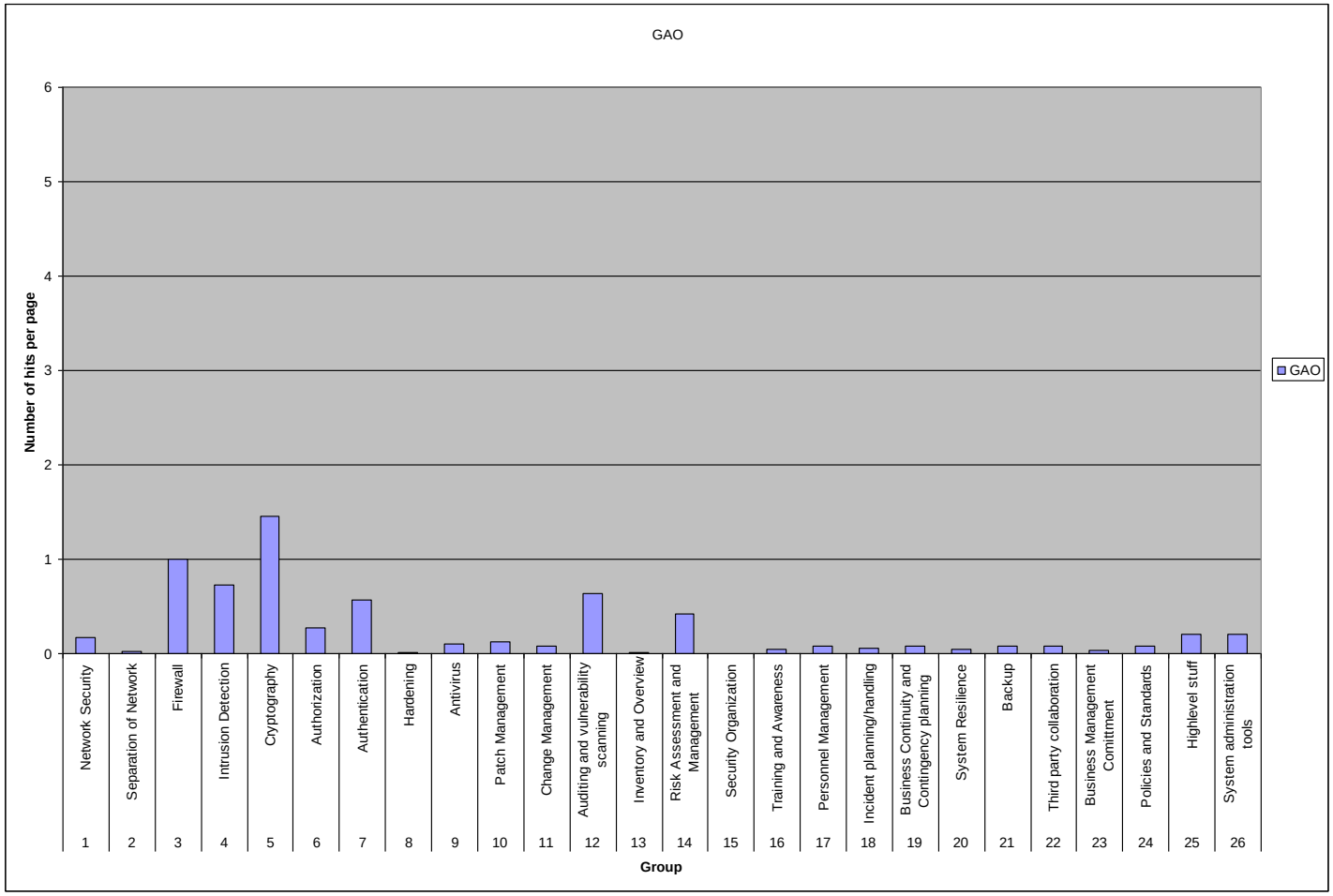

Figure 32 - The number of hits per page per group for GAO

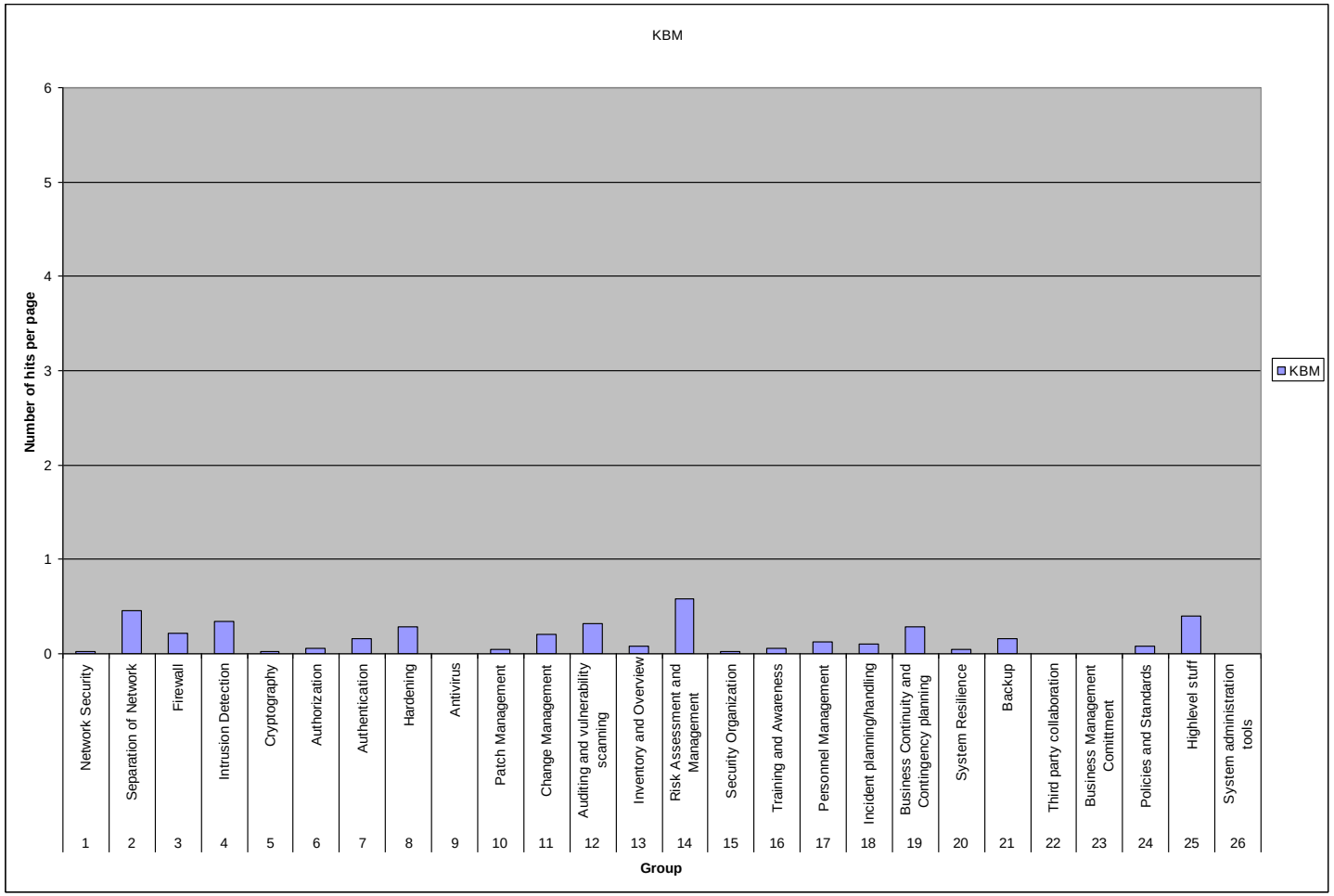

Figure 33 -The number of hits per page per group for KBM