

# Managing Information Security in an Electric Utility

Dr. Göran Ericsson

On behalf of JWG D2/B3/C2-01 Security for Information Systems and Intranets in Electric Power Systems

## Summary

This paper gives an overview of the efforts of the Cigré Joint Working Group (JWG) D2/B3/C2-01 “Security for Information Systems and Intranets in Electric Power Systems.” It stresses the importance of handling information security within an electric utility. Various threats and vulnerabilities are discussed. The evolution of Power Utility Information Systems from isolated to fully integrated systems is described. The concept of security domains for dealing with information security within an electric utility is presented. It is emphasized that collaboration is needed to cope with information security on a wide scale. Some other committee works are highlighted. Directions for further works of the JWG are given.

## 1 Introduction

Computers of various kinds are used on all levels of power system and business operations within an electric utility. For example, they are used for primary operation such as relay protection schemas, secondary operation such as SCADA/EMS, power plant operations, market and business operations, and for administrative purposes such as word processing and spreadsheet calculations in an office PC.

Over time these various systems have been introduced and built as separate computerized islands. However now, these different islands are getting closer interfacing between some islands and by part/true integrations between others. Hence, an event occurring in a SCADA system part may have impact on a word processing document, and vice versa. Therefore, from an information security perspective, a security “hole” in one system part could, and probably will, affect another part of the electric power system.

Currently, no comprehensive solution exists to protect information-, control and diagnostic systems and intranets in electric power systems, hereafter referred to as *power utility information systems* (PUIS), from attack and to protect data from improper use. Implementation is reliant on an adequate and a cost-effective solution for:

- A secure scheme that addresses confidentiality and integrity, which is needed to strengthen access control to all sources of mission-critical information.
- A secure scheme that addresses confidentiality and integrity, which is needed to protect mission-critical data transmitted over, and stored on company intranets and other communication channels.
- A secure scheme that addresses availability of mission-critical information.

These system components would be the fundamental support used for handling of information security. They should provide the capability: to identify, authorize, and validate the source of information, control the right of access to the information, to control the use of the information, and to protect the data at rest as well as in transit. Also, a cost benefit analysis is required, addressing issues such as: “what is the potential cost of an event,” and “what is the investment needed to protect the data.”

## **1.1 Joint Working Group D2/B3/C2-01 Security for Information Systems and Intranets in Electric Power Systems**

The issue of proper handling of information security has been raised within Cigré on a broad basis [1]. A Joint Working Group (JWG) D2/B3/C2-01 “Security for Information Systems and Intranets in Electric Power Systems” has been formed, with members from three Study Committees, namely:

D2 – Information Systems and Telecommunication for Power Systems

B3 – Substations

C2 – Systems Operation and Control

The scope of the JWG is to identify and define information security issues for the electric power industry, such as main domains for Utility Intranets and Information Systems, Telecontrol (control centre and substations). Also, general IT security issues should be addressed, as they impact power utility information systems, such as secure Internet connections.

Within the JWG of Cigré, the standards of [3, 4, 5, 6] are used to define the fundamental principles of proper handling of information security for an electric utility. These principles define the parameters for the preservation confidentiality, integrity, and availability of information. A PDCA model (Plan-Do-Check-Act) to establish and maintain an effective Information Security Management System is described in BS 7799-2 [6]. ISMS is that part of the overall management system based on a risk approach, to establish, implement, operate, monitor, review, maintain, and improve information security. To what extent the 17799 standard will be adopted by the Cigré JWG for Security Management will be concluded in a forthcoming paper.

The work of the JWG began in 2003. The JWG shall deliver results by the SCD2 meeting in 2005. A part of the work is to author 5-6 papers on the subject of information security in electric utilities, where this paper is the first deliverable from the JWG.

It should here be noted that, prior to the first meeting of the JWG, a paper on the subject of information security was published in *Electra*, February 2003 [2]. That paper was on behalf of the Cigré WGD2.13 and some parts from that paper are found and further developed here in this paper, especially the issues of different security domains.

## **1.2 Purpose**

The purpose of this paper is to give an overview of the information security problem for an electric utility and to raise the awareness of the need to implement security to mitigate attacks on information systems and intranets. Hence, the paper is addressing the question of “Why is Information Security important for the electric power industry?” Also, guidance for how to solve the problem is discussed; it is proposed that security is treated from a *domain* point of view, instead of a traditional hardware perspective. Conceptually, this approach of using domains and sub domains has been a useful mechanism to study the attacks on information systems and intranets.

### **1.3 Why is Information Security important for the electric power industry?**

As providers of life-critical products and services, electric power providers need to develop new security systems and procedures that are responsive to the improvements in technology and also recognize the development of threats and attacks. This implies that utilities not only need to deal with physical intrusion, but also and with logical intrusion.

It is essential for electric system providers to recognize that while cyber security is an important component of protecting their systems, it is only one tool from a much larger set of information control techniques. Cyber security is only effective if it is deployed as part of a comprehensive set of security policies, and when it is combined with adequate attention to physical security. Like many security-related issues, operating a reliable information security system requires more than a purely technological fix. Systems are initially compromised by attacks against lax operating procedures and poor implementations.

Furthermore, what is clear is that information (or data) is no longer sent from “here” to “there”, a point-to-point view of data transfer and communication security; but rather data has a point of presence – there is no “there”, the data must be available to all who have a legitimate need for it. Therefore, data needs to be controlled and protected at its source, and a security scheme needs to provide the capability and means to control access to the data, and to control its use. Also, there is a need to attain a more high level view for development of policies spanning the range of risks and threats.

### **1.4 Outline of Paper**

In Section 2, various threats and vulnerabilities are discussed. Especially, the evolution of Power Utility Information Systems is described to emphasize the need for a strategy to handle intrusions. In Section 3, the concept of security domains is presented and further developed from [1, 2]. In Section 4, directions for further works of the JWG are given, together with some concluding remarks. In Section 5, a brief list of different activities within the field of information security is presented together with corresponding references.

## **2 Threats and Vulnerabilities**

The purpose of this section is to describe the development of different data computer networks and systems, and the impact with respect to threats and vulnerabilities. The presentation relates to Figures 1, 2 and 3.

The issues of “threats” and “vulnerabilities” treated here mainly refers to the following definitions adopted from American Gas Association (AGA) [7], namely:

*Threat* – Any circumstance or event with the potential to adversely impact a system through unauthorized access, destruction, disclosure, and/or modification of data or denial of service.

*Vulnerability* – A flaw or weakness in a system’s design, implementation, or operation and management that could be exploited to violate the system’s security policy.

The definitions may be subject to revision, but at this stage they provide adequate support for covering the issues.

Various cyber security intrusion studies by the U.S. Department of Energy (DOE) [7] and by commercial security consultants have demonstrated the cyber vulnerabilities of control systems to unauthorized access. There have been more than forty real-world cases where control systems have been impacted by electronic means [23]. These events have occurred in electric power control systems for transmission, distribution, generation (including fossil, gas turbine, and nuclear, where three plants experienced denial of service events), as well as control systems for water, oil/gas, chemicals, paper, and agricultural businesses. Some of these events have resulted in damage. Confirmed damage from cyber intrusions have included intentionally opening valves resulting in discharge of millions of liters of sewage, opening breaker switches, tampering with boiler control settings resulting in shutdown of utility boilers, shutdown of combustion turbine power plants, and shutdown of industrial facilities.

**2.1 Attackers have a range of capabilities and motives**

Threat agents can arise from many groups of people. These potential attackers will also have a wide range of capabilities, resources, organizational support, and motivations. Fig. 1 includes a brief list of potential attackers, their capabilities and resources, and their motivation to initiate an attack.

<b>Attacker/threat agent</b>	<b>Special capabilities/resources</b>	<b>Motivation</b>
Hackers	Computer, spare time, dedication	Fun, challenge, fame
Employees	Inside knowledge, generally easy access	Desire to do a good job without understanding cyber security vulnerabilities, challenge, experimentation, grievance, profit.
Insiders, contractors, competitors	System access, confidential information, knowledge of operations and default passwords	Revenge, union issue, grievance, profit.
Traders	Computer skill	Financial gain
Foreign governments	System expertise, large computers, cryptographers, intelligence agency, money, military	Strategic military and/or economic damage
Organized crime	Computer skill	Financial gain
Extremist groups	Computer skill, dedication	Harm groups they oppose
Terrorists	Computer skill, spying, money, organization	Terrorize, finance operations, economic damage
Alliances of above groups	Combined resources of any above group	Alliance of convenience to advance own interest

Fig. 1 Capabilities and motivation to initiate an attack

**2.2 Yesterday’s situation**

About 20 years ago, data and computer networks and systems were designed and built for their separate purposes, respectively. See Fig. 2. The administrative network was built to meet the requirements of a computer office system, and handle administrative data. The power system control system was developed to meet the requirements for proper data transfer for adequate and secure process operation, such as SCADA/EMS.

The different kinds of networks were designed and built as separate “islands” of operations. There were no interconnections and no data was interchanged between the networks.

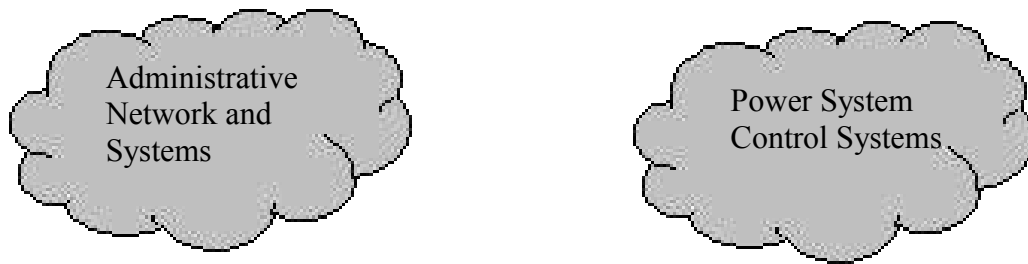


Fig. 2 Yesterday – Separate Administrative and Power System Control Networks.

### 2.3 Today's situation

Today, the administrative and process control networks are more tightly coupled. See Fig. 3. They are still to be considered as separate networks, designed for separate purposes. But the borderlines of the two systems are not as distinct as in the previous case. The administrative system interchange data with the process control database. The power system control network interchanges data with the administrative database. Also, both networks are interconnected via external connection(s), which may be based on Internet or dial-up connections. The same kind of data can be used for different purposes, in both networks, within the company. Also, it is common practice that the Administrative Systems and Power System Control Systems share the telecommunication network within a utility.

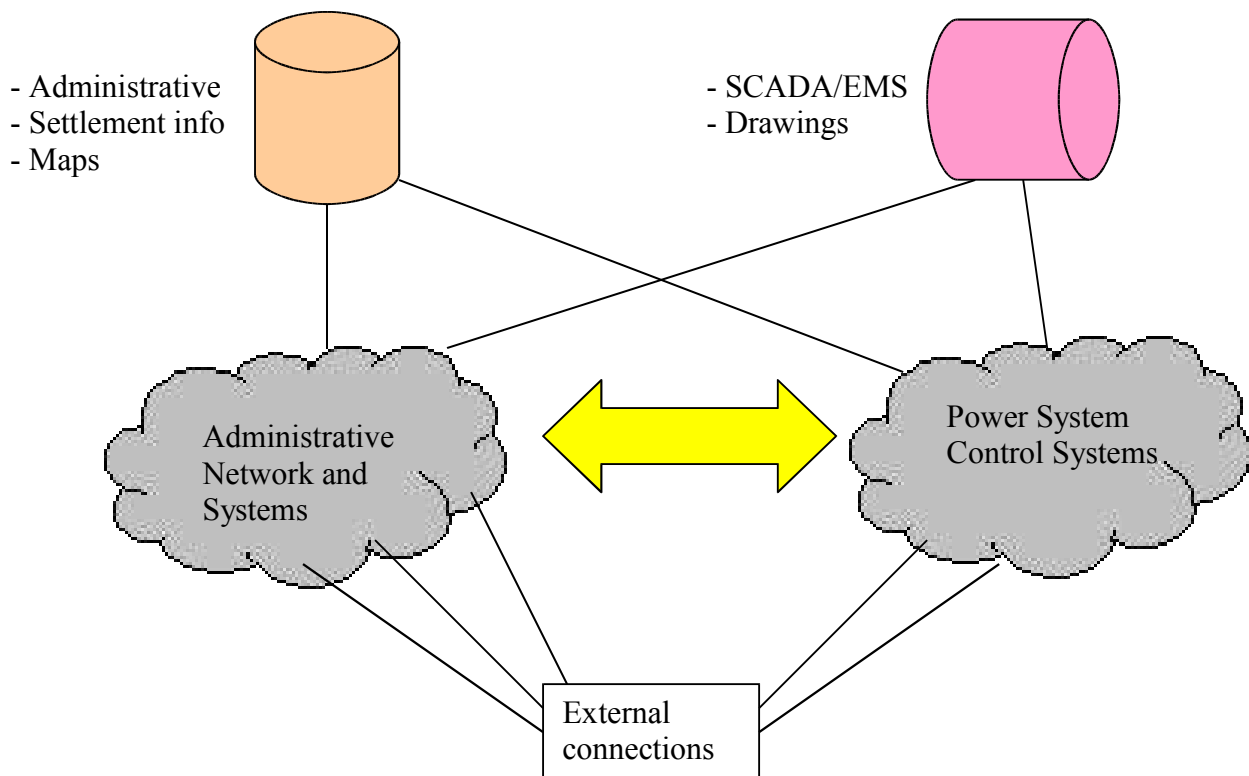


Fig. 3 Today – The Administrative and Power System Control Networks are interconnected.

## 2.4 Tomorrow's situation

Within the near future, the networks will be merged into one integrated administrative and power system control network, see Fig. 4. In fact, there are utilities that are currently employing this architecture. Common data will be possible to access from different parts of the company, and for different purposes. Access through Internet and other networking technologies require new ways of handling security issues and vital applications.

Also, it becomes more and more common that certain customers and entrepreneurs/service providers have some kind of connection to/from the network shown in Fig. 3. This implies connections with the customer's and the service provider's network.

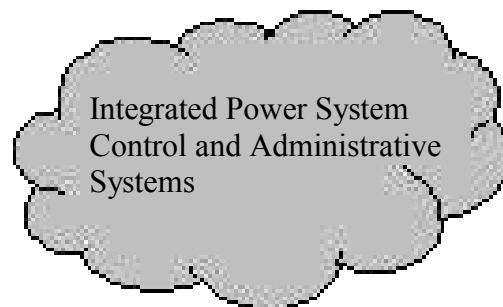


Fig. 4 Tomorrow – The Administrative and Power System Control Networks are integrated.

## 2.5 Threats

Based on the description above (today's and tomorrow's situations), the following threats may be evident:

- **Physical intrusion:** An intruder may physically damage, not only one part, but also several parts of the network, since the various parts are integrated/interconnected. By breaking into one part of the computer system, the intruder may be able to affect another part.
- **Logical intrusion:** This is the most difficult kind of intrusion to protect against. It is not visible for the human eye as the physical intrusion is, and there are more issues to consider and deal with.

Logical intrusion can be of different kinds:

- External intrusion – by unauthorized access or by customers and entrepreneurs who do more than they are allowed to do. Also, an intruder may interfere with the user system, such that the user cannot access and use the services of the system as expected (Denial of Service).
- Internal intrusion – by users within the own company. It could be with or without the intention to do harm.

Furthermore, the power industry is a technology driven industry. New technology and various technical features and “gizmos” are adopted and brought into use *before* they are tested and approved by the power company. Of course, this is a work process and managerial problem, but it is a fact that ambitious engineers tend to find new technical features and play with them, no matter what is allowed or prohibited. Also, it is common that, at the procurement stage, the

power company does not include security requirements to a great extent in the purchasing contract for power control systems, since standardised requirements specifications do not currently exist. This has stimulated work in several committees and industrial organisations, see Section 5.

### 3 The Domain Concept for managing Information Security

A traditional way of describing and analysing a computer network is from a hardware perspective, i.e., in terms of servers, bridges, routers, etc. But since the various systems, such as the power system control and the administrative systems, are getting more and more interconnected/integrated, another approach is needed to address and support analysis of the integrated system as a whole. Therefore, the concept of *security domain* is used here. It was first introduced in [1, 2], and it is further developed and described.

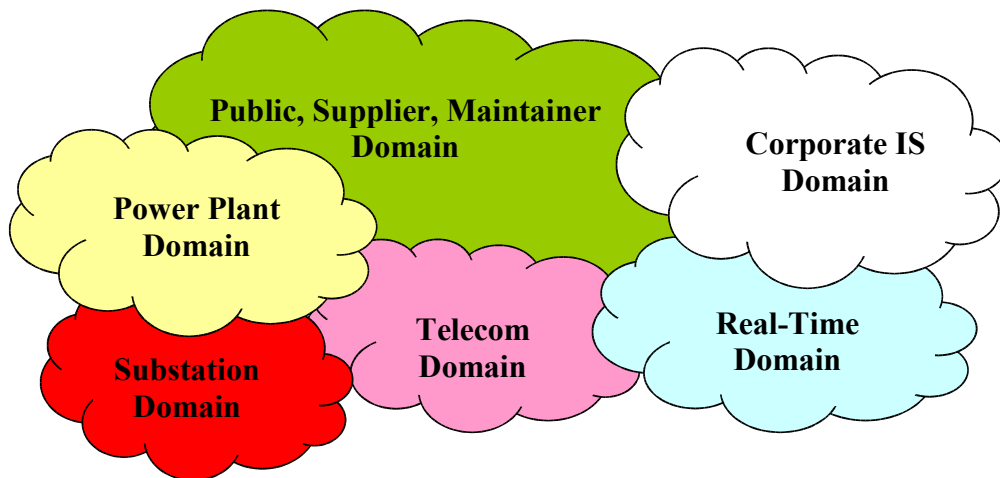


Fig. 5 Different Security Domains

A domain is a specific area, wherein specific activities/business operations are going on and they can be grouped together. Here, the following security domains are introduced, see Fig. 5:

- Public, Supplier, Maintainer Domain
- Power Plant Domain
- Substation Domain
- Telecommunication Domain
- Real-Time Operation Domain
- Corporate IS (Information System) Domain

The purpose of the domain concept is to emphasize for everyone involved within a specific area the importance and handling of information security issues. Also, one domain X may be using hardware equipment and/or communications that are also used by domain Y. Therefore, the domains are typically interrelated. The domains described above may be different from one electric utility to another, depending on the utility's operation and tasks. The proposed domains in this paper are found to be chosen in a natural way. It is of course up to each utility to choose and implement its domains. The ideas presented here are general and applicable to another set of security domains and their interdependencies.

Different interests, and compliance with legislative and contractual requirements could make it necessary to define a security policy structure using different security domains inside the power utility. One security domain shall have only one security policy and only one authority

responsible for the security policy inside the domain. The authority should guarantee a minimum IT-security level for the systems in the domain. The security level of the individual systems must be classified and may actually vary.

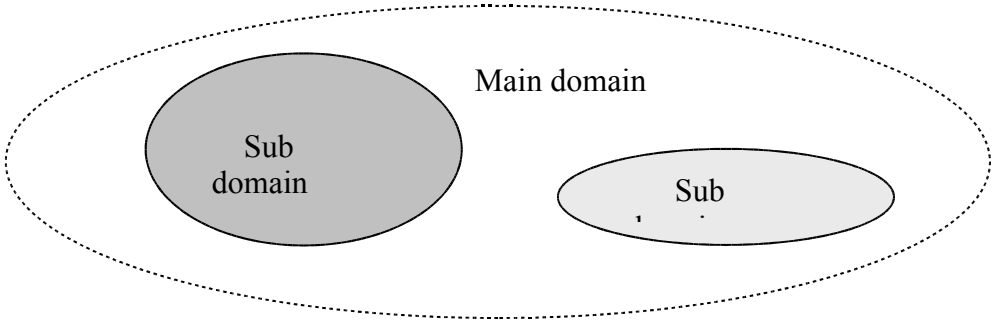


Fig. 6 A main security domain with its sub domains

Fig. 6 shows a security domain with two sub domains. The security policy in each sub domains could be set up by using some parts of the policy of the main domain, changing some parts of it and then making additions. Also, security policies may be different between the security domains.

When communicating across power utilities, organisations, and other companies, etc., using communication networks, the security domains should be recognised. Fig. 7 shows information exchange between different security domains.

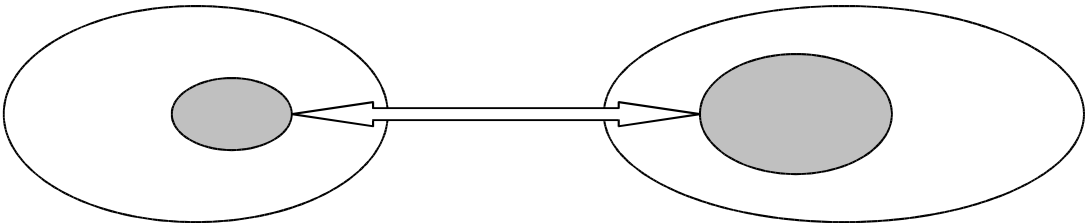


Fig. 7 Data exchange between domains

For example, a power utility could define a security domain and related policies and procedures for its telecontrol activity to assure compliance with legislative or regulatory requirements. If similar definitions, procedures, policies, etc. were developed by other power utilities, it would be easier to discuss and define common rules for the information exchange or the usage of common resources in a communication network. However today, there are no common definitions including the terms “security,” “critical asset,” etc. Also, there are no common control system security policies or procedures, although groups such as ISA [9, 10, 11], are working on generic policies and procedures.

A power utility should also discuss and define the policy structure depending on the topology and the importance of resources in the telecontrol network itself. A power utility on a regional level for example, must decide if all substations, all local control centres, and the

regional control centre should belong to the same security domain or be split into several domains.

### 3.1 Inter domain communication – Reduction of the number of sub domains

From the description of domains above, it is desirable to achieve an adequate overview of the domains and their relations from an information security perspective. A good starting point could be to list all domains and define the different security authorities within the company. See Fig. 8.

A first approach would be to “X” in each box in the matrix to indicate the responsibility and inter-domain relations. However, it becomes easily a great number of inter-dependencies. Here, fourteen (14) “X”, i.e., security authorities, are shown.

(Sub) domains	Companies / security authorities		
	C1	C2	C3
D1	X	X	X
D1.1	X	X	X
D1.2	X	X	X
D2	X		X
D3	X	X	X

Fig. 8 Number of (sub) domains before negotiation (14)

(Sub) domains	Companies / security authorities		
	C1	C2	C3
D1	X	X	X
D1.1	X	X	X
D1.2	X	X	X
D2	X		X
D3	X	X	X

Fig. 9 Number of (sub) domains after negotiation (8)

Instead, in order to reduce the number of dependencies and to coordinate the authorities, a way could be to let all security issues for a certain domain to be treated by only one authority. In Fig. 9, it is depicted how one authority of the D1.1 domain handles all security issues related to D1.1 issues, covering C1, C2, and C3. The same apply for the D1.2 and D3 domains. The number of security authorities has been reduced to eight (8).

After reducing the numbers of domains it remains to find a solution for the interchange of information between domains having different security policies. One way of handling this is to define and use inter-domains. The communication partners need to agree on the inter-domain security policy. Examples of subjects that need to be developed are:

- How to develop an inter-domain policy.
- How to establish the inter-domain authority.

- What elements could be included in the inter-domain.
- The relationship between internal policies and inter domain policy, etc.

Discussions of these subjects will be found in the forthcoming papers of the Cigré JWG.

## 4 Further works and Concluding Remarks

The JWG is working on the following issues that are to be treated in forthcoming papers:

- Intruders' aspects
- Business and operational aspects
- Technological aspects
- Security Management

The issues presented in this paper – evolution of power utility information systems, threats, security domains – are some issues along the way to raise the awareness of providing guidance for proper handling of information security within the electric power industry.

In order to further improve the “road-map” of dealing with information security, collaborations across the borders and between organisations are of great advantage. To build up contact networks and to share experiences are some one of the key issues.

## 5 Committee works, References

This section briefly highlights the committee works (not given in a particular order) that deal with information security; a more complete presentation will be given in a forthcoming paper. The purpose is to list the most well known works within the field of information security in relation to the electric power industry, and to give corresponding references on the Internet and/or in journals. The author and the JWG have found the following committee works very important to study:

- **Published papers:**
  - [1] A. Vidrascu, G. Fahlén, J. Smith, A. Torkilseng: ”Information Security in Power Utilities,” Proposal/Position paper, TF on Information Security, Advisory Group D2.02, Cigré SCD2, October 2002.
  - [2] A. Torkilseng: “Management of Information Security in Power Utilities,” Cigré, Electra, No. 206, February 2003.
- **Cigré JWG D2/B3/C2-01 Security for Information Systems and Intranets in Electric Power Systems.** The JWG described in this paper. Work progress will be reported on <http://www.cigre.org/GB/SC/D2.htm>, and papers will be submitted for publication in Cigré Electra.
- **IEEE Power Engineering Society (PES) Power System Communications Committee (PSCC) – New WG Information Security Risk Assessment.** Work progress will be reported on <http://www.ieee.org/pes/>
- **International Standards:**
  - [3] ISO/IEC 10181:1996 Information technology -- Open Systems Interconnection – Security frameworks for open systems
  - ISO/IEC 17799 and BS 7799 standards:
  - [4] ISO IEC 17799:2000 Information Technology – Code of practice for information security management.

- [5] British Standard, BS 7799, Information security management. Part 2: Specification for management systems, 1999.
- [6] BS 7799-2:2002, Information security management systems – Specifications with guidance for use.
- [7] **American Gas Association (AGA)**: Series of AGA12 reports. <http://www.aga.org/>
  - [8] **“21 Steps to Improve Cyber Security of SCADA Networks,”** Department of Energy (DOE), USA, <http://www.esisac.com/publicdocs/21StepsBooklet.pdf>
  - [9] **Instrumentation, Systems and Automation Society (ISA) SP99**: <http://www.isa.org>  
ISA works consists of:
    - [10] ISA-TR99.00.01-2004: “Security Technologies for Manufacturing and Control System,” Instrumentation, Systems and Automation Society (ISA), USA.
    - [11] ISA-TR99.00.02-2004: “Integrating Security into the Manufacturing and Control Systems Environment,” Instrumentation, Systems and Automation Society (ISA), USA.
  - [12] Computer Security Resource Center, **National Institute of Standards and Technology (NIST)**, USA, <http://csrc.nist.gov/>, including the Process Control Security Requirements Forum (PCSRF) and test bed development.
    - [13] National Infrastructure Assurance Partnership (NIST and NSA), USA: <http://niap.nist.gov/>
  - [14] **North American Electric Reliability Council (NERC)**: <http://www.nerc.com>
    - [15] Critical Infrastructure Protection Committee (CIPC) of NERC (<http://www.nerc.com/~filez/cipfiles.html>)
  - [16] **IEC TC 57 WG 15**: Technical Committee of IEC TC 57 “POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE”, Working Group 15 developing security standards for TC57, <http://www.iec.ch>
  - [17] **IEC TC 65C WG13**: Technical Committee of IEC TC 65: “INDUSTRIAL-PROCESS MEASUREMENT AND CONTROL,” Working Group 13 addressing cyber security for fieldbus communications in process control applications.
  - [18] **Common Criteria and Best Practice**: <http://www.commoncriteria.org>
    - [19] The Common Criteria ISO/IEC 15408—The Insight, Some Thoughts, Questions, and Issues ([http://www.niser.org.my/resources/common\\_criteria.pdf](http://www.niser.org.my/resources/common_criteria.pdf))
    - [20] SWEDAC, the Swedish Board for Accreditation and Conformity Assessment, <http://www.swedac.se>
  - [21] **CERT/CC (Computer Emergency Response Team Coordination Center)** “Meet the CERT/CC” at: [http://www.cert.org/meet\\_cert/meetcertcc.html](http://www.cert.org/meet_cert/meetcertcc.html)
  - [22] **IECISA – Integrated Energy and Communications Systems Architecture**, <http://www.iecisa.org>
  - [23] **“Control Systems Cyber Security—Maintaining the Reliability of the Critical Infrastructure”**, Testimony of Joseph M. Weiss before the US House Government Reform Committee's Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, **U.S. House of Representatives**, March 30, 2004. <http://reform.house.gov/TIPRC/Hearings/EventSingle.aspx?EventID=900>
  - [24] **Workshop on Cyber Security**, Aug 16-18, 2004. <http://www.kemaseminars.com/>