317

SECURITY FOR INFORMATION SYSTEMS AND INTRANETS IN ELECTRIC POWER SYSTEMS

Joint Working Group
D2/B3/C2.01

April 2007

SECURITY FOR INFORMATION SYSTEMS AND INTRANETS IN ELECTRIC POWER SYSTEMS

Joint Working Group D2/B3/C2.01

JWG Members:

Convenor: **Åge H Torkilseng (Norway, D2)**
Editor: **Göran Ericsson (Sweden, D2)**

WG-members: **Åge H Torkilseng (Norway, D2), Giovanna Dondossola (Italy, D2), Göran Ericsson (Sweden, D2), Ton Jansen (The Netherlands, B3), Peter Roche (Ireland, C2), Jim Smith (Ireland, D2), Dennis K. Holstein (USA, B3), Andreï Vidrascu (France, D2), Joe Weiss (USA, C2)**

Observer members: **Tor Aalborg (Norway, D2), Werner Meier (Switzerland, D2), Lars-Ola Österlund (Sweden, C2)**

n° ISBN : 978-2-85873-003-2

SUMMARY

This Technical Brochure (TB) deals with the increasingly important issue of proper handling of information security for electric power utilities. The efforts described herein have been carried out within the Cigré Joint Working Group (JWG) D2/B3/C2-01 on "Security for Information Systems and Intranets in Electric Power System" between 2003 and 2006. As intermediate results, the JWG has produced the following five papers which are included as appendices:

1. G. ERICSSON: **"Managing Information Security in an Electric Utility"**
2. P. ROCHE: "**Cyber Security Considerations in Power System Operation**"
3. G. DONDOSSOLA, O. LAMQUET: **"Cyber Risk Assessment in the Electric Power Industry"**
4. Å. TORKILSENG, G. ERICSSON**: "Some Guidelines for Developing a Framework for Managing Cyber Security for an Electric Power Utility"**
5. T. JANSEN: "**Technical considerations for building secure Substation Automation systems**."

The purpose of this TB is to raise the awareness of information/cyber security in Electric Power Systems, and give some guidance on how to solve the security problem by focusing on security domain modelling, risk assessment methodology and security framework building.

As the computer networks and systems for administrative issues and power system control systems become more interconnected, a hardware-oriented approach is not appropriate for handling of those networks/systems. Therefore, this TB describes the "domain concept" for managing information security, where different domains and interactions are treated. This concept is also treated in the standards of ISO/IEC, which here must be adopted in the power control system environment.

The focus of the TB is more on the management issues, rather than on technical details. However, a part of the TB is devoted to technical issues, in the context of substation automation and risk assessment. Actually, to estimate the cyber risk is a delicate task, since experiences of cyber risk assessment in industrial control systems are still limited. A risk assessment methodology in this field is needed, in order to trace the logical links between system vulnerabilities -> threats -> attack processes.

It is concluded that a common information security terminology that can be shared and widely used must be agreed upon. Also, there is a need for a comprehensive Information and Control Systems Security Framework for electric utilities. Furthermore, the wheel shall not be "re-invented." Rather, an electric power utility (EPU) is recommended to use existing works from the general IT and SCADA/Control Systems areas to obtain a common approach.

Last but not least, Management of Information Security is an essential and natural part of daily operations of various tasks in an EPU. Therefore, it should be included and integrated within the work-flow and processes of the EPU, where the security framework must be aligned with many other frameworks.

KEYWORDS

Information Security, Cyber Security, IT Security, Risk Assessment, Substation Automation, ISO/IEC 17799, ISO/IEC 10181.

Contents

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 on office computers.

Over time these systems have been implemented 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 intentional cyber attacks or unintentional cyber events and to protect data from improper use. Implementation is reliant on an adequate and a cost-effective solution for:

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

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." In other words, "how much security is enough"?

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 [11]. 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 has been 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 are addressed, as they impact power utility information systems.

Within the JWG of Cigré, the standards of [1][2][3][4] have been used to define the fundamental principles of proper handling of information security for an electric utility. These principles define the parameters for the preservation, integrity, availability, and confidentiality of information. A PDCA model (Plan-Do-Check-Act) to establish and maintain an effective Information Security Management System (ISMS) is described in BS 7799-2 [4]. 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. The ISMS is to be adopted to fit into the power control system environment.

The work of the JWG began in 2003. The JWG will deliver results by the 2006 Paris Session. A part of the work has been to author five/six papers on the subject of information security in electric utilities. Also, prior to the first meeting of the JWG, a paper on the subject of information security was published in Electra, February 2003 [12]. That paper was on behalf of the Cigré WGD2.13 and some parts from that paper are found and further developed here by the JWG, especially the issues of different security domains.

1.2 Purpose

The purpose of this Technical Brochure (TB) is to raise the awareness of cyber security in Electric Power Systems, and give some guidance on how to solve the security problem by focusing on security domain modelling, risk assessment methodology and security framework building.

1.3 Outline

The Technical Brochure is outlined as follows. In Section 2, principal distinguishing features of modern power systems are described, making treatment of information security important. Thereafter in Section 3, it is further stressed why information security is important for the electric power industry. Here, we would like to raise the awareness of this issue. In Section 4, it is described how data computer networks and systems are evolving. Section 5 introduces the “domain concept” for managing information security. In Section 6, some actions are proposed to be taken while comprehensive measures are being developed. Sections 7 and 8 deal with cyber risk assessment. Section 7 studies the standards and industry practices, whereas Section 8 gives an overview of a methodology. In Section 9, some guidance is given and standards and best practices are studied, towards the goal of developing a framework for managing cyber security for an electric power utility. Section 10 deals with technical considerations, where the focus is on substation automation. In Section 11, some conclusions are drawn, and in Section 12, further works and research activities are proposed. Finally in Section 12, an extensive list of references is give. Also, some on-going works are studied. Last, a short, not complete, glossary is given. Papers 1-5 produced by the JWG are included as appendices.

2 Principal Distinguishing Features of Modern Power Systems

Only a generation ago the Vertically Integrated Utility (VIU) was the most usual form of organisation in the power supply industry. The adoption of a business model designed to encourage competition and to force the separation of generation, transmission, and distribution and supply businesses has dramatically altered the structure of the power supply industry. In

parallel with these structural changes the potential of computer systems to support change has lead to the installation of a multitude of IT systems, many of which depend on inter-operability to achieve their objectives.

The current power sector is characterised by a large and expanding number of participants, each of whom has a requirement to communicate with almost any other participant in the sector. The main participants in the sector and the principal reason for communicating with others are the following:

- Transmission Company (Transco) or Transmission System Operator (TSO) or Independent System Operator (ISO)
- Distribution Company (DISCO)
- Generation Company (GENCO)
- Independent Power Producer (IPP)
- Market Operator
- Consumers of all types
- Industrial Control System Vendors: SCADA/EMS (Supervisory Control & Data Acquisition/Energy Management System), RTUs, Relays, Power Plant Distributed Control Systems (DCSs), and Programmable Logic Controllers (PLCs)
- Plant/Substation equipment suppliers
- Equipment diagnostic providers
- Cyber security solution providers.

Tremendous productivity improvements have been achieved in most sectors, very often based on extensive deployment of computers. Computers underpin all aspects of the industry, from customer accounting and billing systems, to Geographical Information System (GIS) and trouble call logging systems. Especially significant are the large number of operational systems which depend on computers – e.g. SCADA, automatic metering systems, digital substation control systems, digital relaying systems etc. In many respects it could be said that the technological fabric of today's power industry is supported by information technology.

The different participants in the power industry each develop their own IT systems, often with different hardware and software, with various network architectures and with different network management tools, systems and philosophies. Each participant has the expectation that any entity (human or machine) can communicate with other participants, normally using industry standard methods. In some situations communication may take place through industry specific protocols (e.g., UCA/ICCP), but more usually the Internet, often with private subnets, is becoming the vehicle of choice for communications.

Managers of IT systems have limited control of the IT security aspects of communications across the Internet, using techniques and equipment such as encryption, access control, firewalls, etc. However an IT manager can never assume that those other organisations with whom his organisation communicates have taken adequate precautions to remove or minimize risk of electronic security threats or attacks.

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 with cyber 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 appropriate 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 or inappropriate 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.

3.1 Reported Cyber Security Incidents

Various cyber security intrusion studies by the U.S. Department of Energy (DOE) [32] and by commercial security consultants have demonstrated the cyber vulnerabilities of control systems to unauthorized access. There have been more than seventy real-world cases where control systems have been impacted by electronic means [41]. These events have occurred in electric power control systems for transmission, distribution, generation, 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 litres of sewage, opening breaker switches, tampering with boiler control settings causing thermal cycling damage to large steam turbines, shutdown of combustion turbine power plants, and shutdown of industrial facilities.

Very few of the reported incidents have been publicly described. To show how multi-faceted the problem is, a sample of incidents is given below.

- *Large Generating Plant Output Reduced to Zero*: The control system of a large generating plant operating at a number of 100 MW was infected by a virus and its output was reduced to virtually zero in a few seconds. Infection came from connected corporate IT network. The solution was to rigorously separate the real-time and corporate networks.
- *Distribution SCADA System Partly Disabled*: A virus infected lap-top was used by a maintenance technician to modify a telecoms router. The virus affected all telecom nodes, including some used by a SCADA system. The SCADA system was made partly inoperable for a number of days. A part solution required better management of virus protection on lap-tops.
- *Unauthorised Access to EMS Applications*: A utility gave remote access rights to an EMS supplier. It was observed that application patches had been applied without agreement. No problems arose, but the situation revealed that continuous, non-verified access had remained open to an external Internet port, with serious risk potential.

3.2 Attackers have a range of capabilities and motives

Threat agents can arise from many groups of people:

- Hackers
- Employees
- Insiders, contractors, competitors
- Traders
- Foreign governments
- Organized crime
- Extremist groups
- Terrorists
- Alliances of above groups

These potential attackers will also have a wide range of capabilities, resources, organizational support, and motivations. Paper 1 [13] from the JWG includes the list of potential attackers (as above), their capabilities and resources, and their motivation to initiate an attack.

In addition to intentional threats, unintentional incidents, which in many cases can be the most probable event, may occur. Here, a utility must also take such case into account.

4 Evolution of data computer networks and systems

This section describes 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 refer to the following definitions adopted from American Gas Association (AGA) [31], 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 they have been found to provide adequate support for covering the issues.

4.1 Separated situation

About 20 years ago, data and computer networks and systems were designed and built for their separate purposes, respectively. See Fig. 1. 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.

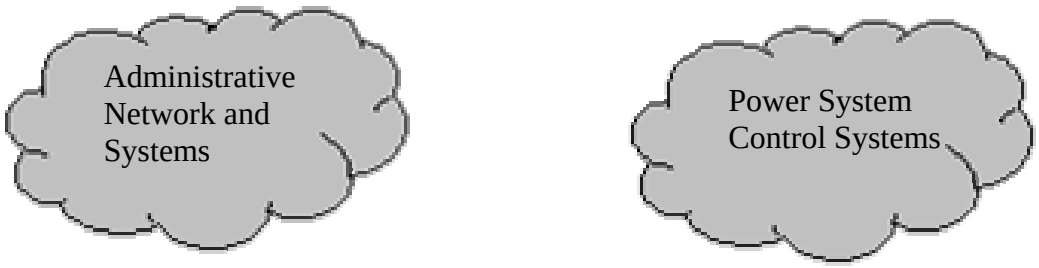


Fig. 1 Separate Administrative and Power System Control Networks.

4.2 Interconnected situation

The separated situation was followed by an interconnected situation. In the early 1980's, some vendors began to offer EMS solutions that were running on computers dedicated for EMS-functions sited in the administrative part of the network. The need for data transfer between SCADA and back-office computers was a fact. An example of a solution that supported this kind of interconnection was the ELCOM-83 communication protocol developed in 1983. This protocol together with others, like FTP (File Transport Protocol), were used to support simple data transfer from one data store to another. Data transfer characterised the interconnected situation.

In this interconnected situation, both administrative and power control networks are typically interconnected via external connection(s), which may be based on dedicated or leased lines or dial-up connections, see Fig. 2. 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.

Today, the administrative and power control networks are more tightly coupled. 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.

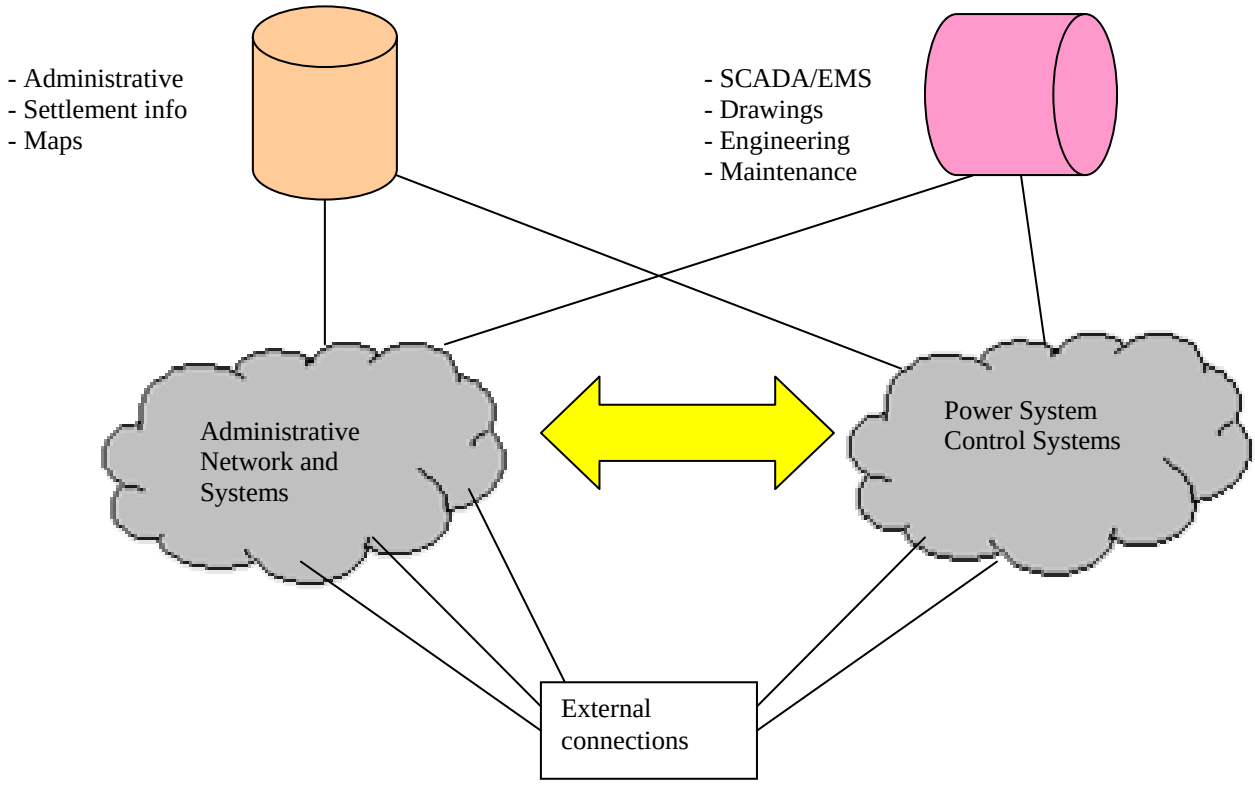


Fig. 2 The Administrative and Power System Control Networks are interconnected.

4.3 Integrated situation

Today, and in the future, SCADA system vendors are taking advantage of standardised system software that make integration possible, which are far more sophisticated than simple data transfer between data stores. The IP protocol stack, client server based man-machine-interfaces, client-server based database management systems, web technologies, etc., are supporting architectures to build integrated solutions. Hence, the networks are getting merged into one integrated administrative and power system control network, see Fig. 3.

In fact, there are utilities that are currently employing this architecture. Common data are then 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 is 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.

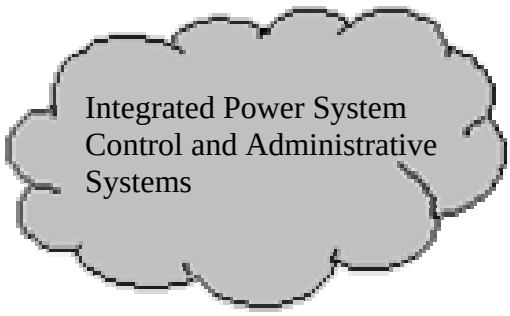


Fig. 3 New system architectures make the integration of the Administrative and Power System Control Networks possible.

4.4 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/Cyber 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/Cyber 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, new technology and various technical features and "gizmos" are often 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 adequately address all the security needs. A few are available, but more are emerging from standards making organisations.

5 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 [11][12], and it is further developed and described.

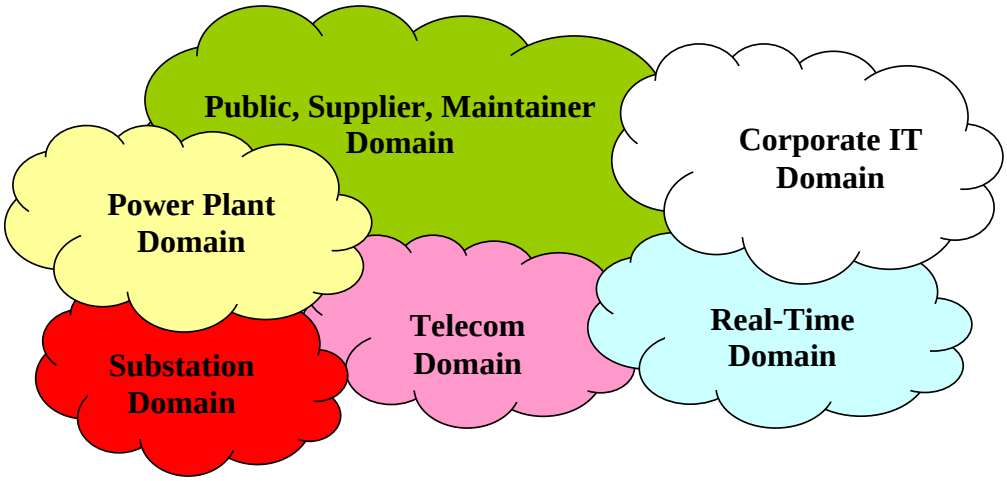


Fig. 4 Different Security Domains

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. 4:

- Public, Supplier, Maintainer Domain
- Power Plant Domain
- Substation Domain
- Telecommunication Domain
- Real-Time Operation Domain
- Corporate IT 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. Within, one security domain we shall rely on only one security policy and only one authority responsible for the security policy inside the domain. The authority should guarantee a minimum security level for the systems in the domain. The security level of the individual systems must be classified and may actually vary.

When communicating across power utilities, organisations, and other companies, etc., using communication networks, the security domains should be recognised. 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 in-

cluding the terms “security,” “critical asset,” etc. Also, there are no common control system security policies or procedures, although groups such as IEC TC57 WG 15 [35], IEC TC65 WG 10 [36], ISA [6][7], and NIST [33], 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. This is particularly true when the utility provides electric as well as gas, or water products and services. This becomes more of an issue when utilities share equipments, such as RTUs.

5.1 Interaction between Domains

In an unbundled and competitive market a large number of domains exist. In addition, each main domain will have a number of sub-domains. A sub-domain is a specific area, wherein particular activities/business operations are being undertaken and where a common set of IT applications are executed. There are some points of note:

- A sub-domain may be quite small in extent e.g. an IT system which monitors and records information on substation assets may be confined to a small number of locations,
- Some sub-domains may be geographically very extensive e.g. a SCADA system which extends through the entire territory of the business,
- A business unit such as a TSO may have many sub-domains – SCADA system, metering and billing system, asset monitoring system, digital substation control systems, business planning system, finance and accounting system, etc.
- There is no certainty that an explicit set of security policies is in force either across the entire domain or even in every sub-domain. Some businesses are more aware of the need for security policies than others.

It is frequently the case that different sections of a business develop computer systems in isolation and at different points in time. Certainly they will usually be interconnected, but their origins will be evident from the different hardware and software, various network architectures and from the different network management tools, systems and philosophies that are employed. Crucially different security practices may exist in each domain.

Where the extent of unbundling is limited, or where limited competition exists then the number of sub-domains may reduce – in this case a single business entity may, in effect, own a number of the domains outlined above.

Returning to the central theme of security of information systems in the power system operations field, it is evident that an incident or event that takes place in one domain could, if not properly managed and contained, spill-over to impact the domains to which it is connected Such a spill-over is most likely in situations where different cyber security practices apply in different domain – as will inevitably be the case. Obviously as the number of interacting domains increases, the source of threats and risks to the integrity of the IT networks of other participants increases – as is implied from the multiple boundaries shown in the schematic Fig. 4.

5.1.1 Security inter/intra domain considerations

There is a strong need for interchange of data between participants in the Electric Power Industry. This is well documented in our papers [13][14][15]. We have a situation where two or more security domains, each with a security authority and different security levels, have to be interconnected. In a security domain model the approach would be to define an inter- or intra-domain with all the domain characteristics like authority, domain perimeter and policy that could serve like a bridge between the interconnected domains. See Fig. 5.

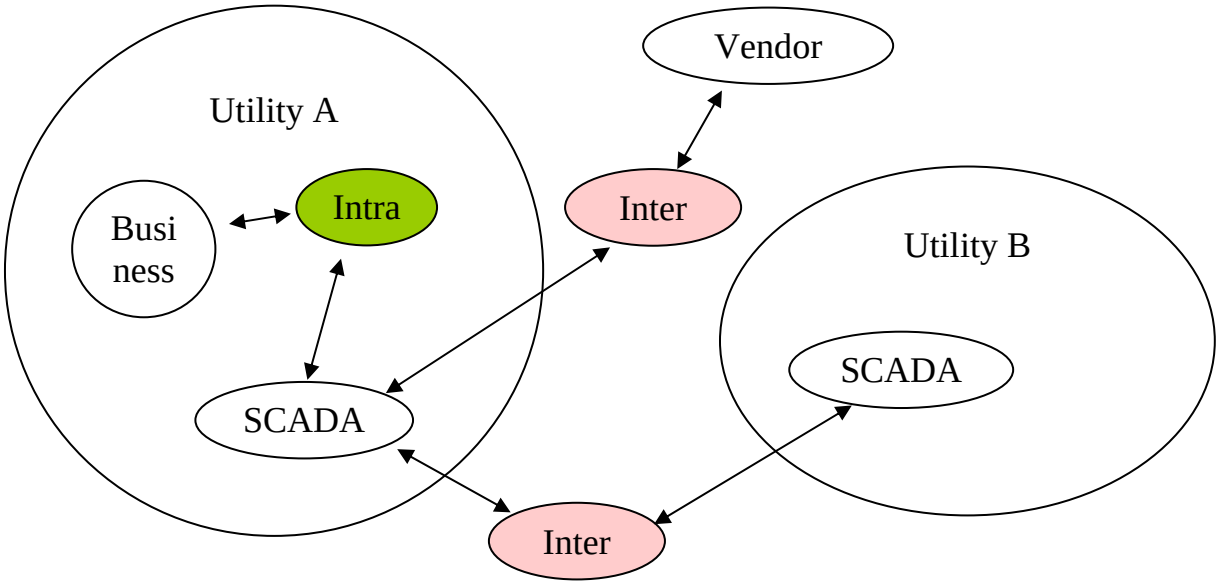


Fig. 5 Example of a Multi-Domain Security Model

Fig. 5 shows an example of a Multi-Domain Security Model. The model could be set up by using the following steps: 1) Define corporate domain perimeter, 2) identify corporate sub-domains and define their perimeters, 3) identify external domains to interchange data with, 4) reduce the number of sub-domains and domains by negotiation [13], and 5) define inter- and intra domains.

First of all, a security authority has to be established for each inter- or intra domain. A typical example is a vendor (see Fig. 5) that needs to access the SCADA system to make upgrade of system software. If the Service Level Agreement (SLA) tells nothing about security but only deals with functionality, there exists no security authority and probably no security for the interconnection. If the communication partners would be aware of the situation and use a domain model, they could establish a security authority by designating responsible persons. Then the inter-domain perimeter should be defined. On the SCADA side the vendor should only have access to those parts of the SCADA network that is necessary to do the update or upgrade work. On the vendor side the perimeter between the inter-domain and the vendor's internal domain should be carefully defined. E.g., if the upgrade includes testing and transfer of operational data to the vendor side, the data should be protected in a secured area. The inter-domain policy should define the security level of the interconnection itself, but also authorization and access rights of the data at rest on both sides. E.g., if operational data is transferred to the vendor domain, the policy could declare that the data should be deleted after use. In this example, the definition of the inter-domain could be a part of the SLA between the partners.

5.2 Multiple Users within Power System Operations Domains

One of the most significant differences between the challenges facing the management of real-time schemes, in contrast with non-real-time schemes, is that there may be very many groups of users who interact with real-time computer systems. For instance operators, system maintenance personnel, vendor support personnel or others may all have genuine reasons to access the same sub-domain. In paper 2 [14], a more detailed list of the owners of the domains, the primary users, the secondary users of the computer systems within the domains and the reasons why there are multiple users is summarised.

Most users of the computer systems will be employees of the owner of the sub-domain; however many users may report to other sections in the owning entity and other may belong to external organisations. This diversity of responsibility and reporting lines presents serious challenges for the secure management of the real-time computer systems.

6 Suggested Actions to be Taken While Comprehensive Measures are Developed

Fig. 6 shows a schematic representation of the IT systems which are used in real-time operations. The diagram represents the manner in which many real-time systems interact and exhibit vulnerabilities. The diagram depicts the following:

- How a central SCADA system collects data from RTUs in substations, indicating the connection points where a support engineer may gain access to the central system or to an RTU.
- How support may be provided for digital Substation Control Systems, where local access, or even remote access, may be obtained to enable local reconfiguration of devices or even remote support from a vendor's office.
- The points where a telecommunications engineer may access a node for maintenance or support purposes.

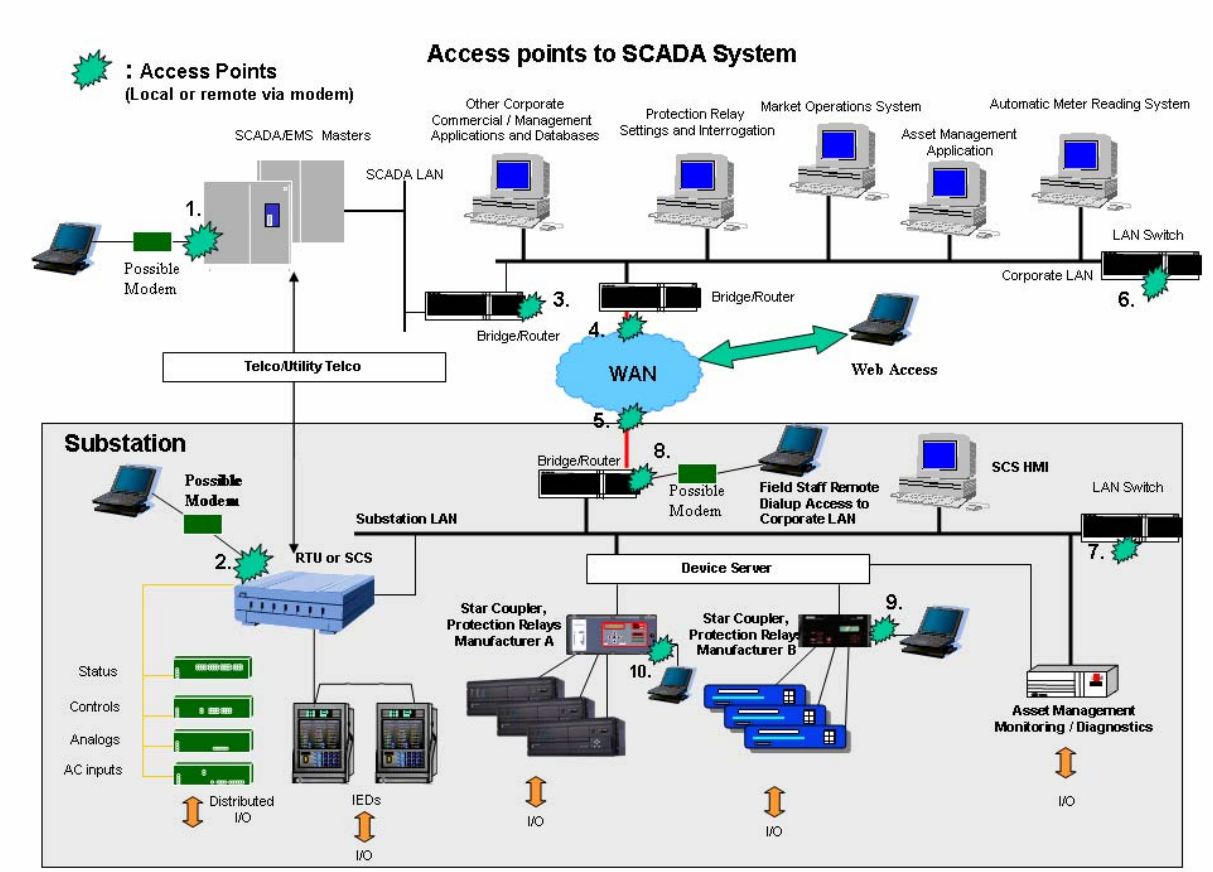


Fig. 6 Schematic Diagram of Main Real-time Sub-Domains

A brief examination of the diagram reveals that there are multiple points of access to the various IT systems. The systems are continuously transferring data and interacting with each other. There is a definite risk that an event in one system, such as the activation of a virus within the Operating System of a digital Substation Control System, could cause it to transmit spurious data into the shared telecommunications network, with the risk of affecting other IT systems. Note also that all points of connection of PCs, or equipments with embedded PCs, or even printers are potential access points to the integrity of the network.

The telecommunications system usually used by a SCADA system may share a physical infrastructure with other business users, e.g. fibre optic or microwave radio links shared with general IT applications. Traditionally, however, the SCADA system utilises non-shared and independent bandwidth e.g. its own fibres or channels. This separation may eliminate many spill-over effects from disturbances originating from other users/applications on the shared medium. Nonetheless within the SCADA system itself, the presence of many fixed PCs, of other maintenance terminals / lap-tops temporarily connected for maintenance purposes and possible direct connection to substation SCS systems, provides many points of weaknesses, through which IT security threats can enter the SCADA system.

6.1.1 Frequent Alterations in Network Configuration

A unique feature, almost unknown in the non-real time situation, is that the basic hardware configuration of real-time IT systems is subject to frequent change. The number of RTUs in a SCADA system is increasing; the number of Bay Control Units connected to digital Substa-

tion Control Systems is always increasing; the number of asset monitoring devices in substations increases and so on. The newly connected devices may be similar to those already on the network, often they may have been produced by a different manufacturer and only match existing systems in that they use a standard protocol. Thus the configuration of sub-domains frequently changes, without any guarantee that the new device entirely complies with existing IT security policy – where an explicit policy is actually in place. Here, the work of IEC TC57 WG 15 [35] should be mentioned.

However, one of the most threatening practices in real-time IT systems is the connection of maintenance terminals – often lap-tops – to nodes in the network, i.e. where a maintenance technician connects his lap-top / maintenance terminal to an RTU, protection relay, digital Control System etc. for a variety of purposes. This same lap-top represents one of the greatest source of risk to the integrity of IT security, as there is rarely a means of checking that the lap-top has not been infected with a virus, worm, Trojan horse etc.

6.1.2 Alterations/Modifications to Basic Device Parameters

Another unique feature, almost unknown in the non-real time situation, is that users may frequently access points in a sub-domain to make fundamental alterations to the parameters of embedded devices. For example a protection engineer may access a relay to reconfigure it, or to modify its characteristics. Or a support engineer may access a digital Substation Control System to reconfigure the software or hardware to add a new bay or signals to the existing system. In all cases the resultant alteration in the device software may introduce unexpected and unwanted effects.

To propose a comprehensive policy as to how to establish and maintain a high level of cyber security protection is a delicate task and such tool/support need to be further dealt with. As an interim measure, some key actions to be taken are summarized as follows.

1. Define the responsibilities and authorities of those charged with cyber security.
2. Document the network architecture and identify all real-time systems.
3. Perform security audits of all real-time networks and interconnected systems.
4. Identify all connections to real-time systems.
5. Carefully disconnect unnecessary connections and applications from real-time systems.
6. Strengthen the access controls for any remaining connections.
7. Install appropriate security facilities provided by vendors.
8. Establish strict control over non-routine access mechanisms.
9. Prepare a comprehensive, continuous risk management process.
10. Implement firewalls and Intrusion Detection Systems/Intrusion Prevention Systems, as appropriate.
11. Assess the integrity of physical security to real-time systems.
12. Establish a clear organisational cyber security philosophy.
13. Establish a system backup procedure and disaster recovery plans.

Furthermore, cyber security must be based on a general methodological approach, which includes the following:

1. Identify critical computing resources for the power control systems and the various constraints and requirements in connection with them.
2. Evaluate the level of potential or actual vulnerability of the information system or the associated infrastructures.

3. Estimate the threats, which can be of human and fortuitous origin (error), of human and voluntary origin (ill will), or related to an uncontrolled or unexpected event (accident, breakdown).
4. Determine the acceptable level of risk and select the risks on which it will be necessary to act and control.
5. Choose the appropriate protection measures and define an organization suited to reach the necessary level of security and to implement these controls.
6. Detect and treat any incident or anomaly relating to security.
7. Take care to maintain the level of security required by measurements of control, audit and experience feedback and improvement.

This approach has been the subject of a series of publications and tutorials [29][16] by the working group Cigré JWG D2/B3/C2-01 - Security for Information Systems and Intranets in Electric Power Systems "Managing Information Security in an Electric Utility" in Electra.

7 Cyber Risk Assessment in the Electric Power Industry – State of standards and industry practices

The cyber risk assessment in the Electric Power Industry is a continuous activity within the security process. It is aimed at identifying control system cyber risks within utilities. Risks are ranked and prioritised for actionable recommendations. According to the elements composing the definition of risk shown in Fig. 7, the identification of risks requires the analysis of asset vulnerabilities and threats, where the concept of threat is described in terms of the agent who performs a certain malicious or accidental action. In the malicious situation, the threat agent will take advantage of a system vulnerability by attempting an attack with the objective of damaging an asset and provoking a certain loss. In the case of accidental events, the violation of a system is due to human, environmental or physical causes provoking an erroneous situation that affects an asset. The multiple links between assets, vulnerabilities and threats form a many-to-many mesh that is difficult to disentangle.

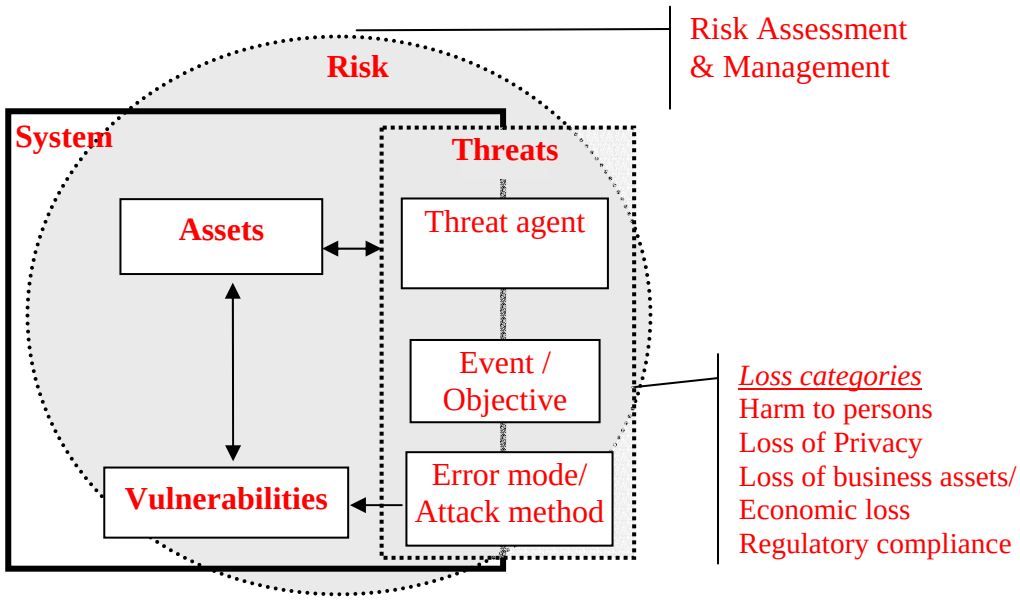


Fig. 7 The elements of risk.

7.1 Standards

Any standard for ICT security management requires performing security risk assessment. Standards relevant to our application domain are spread out into three different domain areas [27a]: 1) general IT-standards and best practice (BS [4][5], ISO/IEC [2]); 2) general guidelines to protect SCADA/Control Systems (ISA [7], AGA [31], DoE [32], NIST [33]) and 3) guidelines to protect SCADA/Control Systems in the Electric Industry (ISA [6][7], NERC [34]).

In US 1998, the Department of Energy (DoE) assigned to NERC (North American Reliability Council) the role of co-ordinator of the critical infrastructure protection activities for the electric power sector. It created the CIPC (Critical Infrastructure Protection Committee) to respond to security threats and incidents, and supports the production of standards and guidelines. NERC's Cyber Security Urgent Action was developed with the purpose to reduce the risks of cyber compromise of the Control Centre (NERC 1200). A new version of this standard [34] has passed industry ballot and will be up for NERC Board approval in early May, 2006. Its importance resides more in its specification of basic requirements and measures, and the definition of compliance monitoring processes, levels on non-compliance and sanctions. This is a language easily understandable by industry and demonstrates a commitment. This type of approach, although its results will always be far from comprehensive, gives an important indication to all players in industry and regulatory bodies: the recommendation we can derive is that the problem is serious, basic solutions are urgently needed and compliance and enforcement are a must.

In parallel NERC manages the ES-ISAC (Electricity Sector Information Sharing and Analysis Center), for the exchange of information on critical risks in the electric power sector. In particular two indexes have been developed for the threat levels indicating the possibilities of physical and cyber attacks. These instruments are very helpful for creating awareness of the situation, but have not been very successful for control system cyber events.
In June 2002, NERC issued the "Security Guidelines for the Electricity Sector" including a vulnerability and risk assessment methodology specific for cyber security in the electricity sector. The approaches and practices recommended are generic, and no indications of particular methodologies are given. In any case, the guidelines are useful for disseminating common requirements and could act as a basis for further developments.

In Europe the power industry practice for electric security assessment has been to use the deterministic approach, referred to as the N-1 criterion, which consists of examining the behaviour of an N-component grid following the loss of any one of its major components. Load flow analysis (steady-state), and occasionally transient stability analysis, is then applied to evaluate the resulting grid conditions. Here, it should be noted that the N-1 criterion was not developed for and it is not suitable to deal with the increasing number of changes happening during the power system operation, both related to cyber events and generation/load variations.

Recently developed probability-based techniques for risk assessment [25] are emerging in the electric power community. Probabilistic approaches to security assessment allow balancing the cost of security measures against the value in terms of avoided outage costs. They require estimates of the probabilities of unwanted events and the value of their consequences. The assignment of these estimates is definitely a non-trivial task for control system cyber events.

Such innovative assessment methodologies adopt conceptual frameworks dealing with deficiencies in the electrical supply, build and/or event trees linking causes and dependencies for power system blackouts, and classify consequences and durations for blackout situations. However they do not cover the evaluation of automation system failures and a comprehensive risk assessment methodology is far from becoming a standard practice.

7.2 Industrial experiences on cyber risk assessment

In recent experiences, risk assessment is performed by combining a top-down and bottom-up approach in which suggested baseline practices are driven by a top-down review of systems enriched by a bottom-up examination of events associated to risks in the business. From a methodological point of view, the top/bottom approach is supported by filling out a risk matrix, mapping subjective threats to their causes, consequences, risks and countermeasures. Exposure levels to threats are sometimes used to prioritise system vulnerabilities, which are obtained by the product of the estimated threat probability and its impact indexes on availability, integrity and confidentiality. Metrics need to be established to identify what constitutes an adequate risk assessment.

In summary the state of the art of cyber security analysis in industrial control is weak: conceptual frameworks are needed and methodologies specific for the power sector have to be developed.

8 Overview of a cyber risk assessment methodology

As described in the previous papers of this JWG, the security weaknesses of a system can be numerous and even commonplace failures of single components can have significant consequences on the electric power service. This highlights the need and importance to make an accurate analysis of security problems on every single subsystem and component.

A security analysis applied to a particular system aims at defining possible failures of the system: these hypotheses of security breaches are then used as inputs to evaluate proper security requirements. However the means to reach such an objective can be multiple and the use of an ICT security expert is not always possible. For this reason the security manager needs to use a methodological support to assist with the security analysis.

A methodology should give a framework of the relevant security concepts the security manager needs to examine to carry out a correct security analysis. But above all, a methodology should trace step-by-step a logical route through these concepts in order to obtain an exhaustive and consistent analysis. Another important aspect of a risk assessment methodology is its openness, since the ICT technologies are in constant evolution, and the same can be said for the system vulnerabilities and threats. Periodically, or after relevant system modifications, the security manager of a system may repeat the security analysis, taking into account all new security elements that have appeared since the last analysis, in order to verify that these new aspects have not modified the security profile of the system or with the aim of improving it.

8.1 The EPCSA methodology

Fig. 8 shows a functional overview of the EPCSA (Electric Power Cyber Security Assessment) methodology and its main relationships with the corporate security process. Data sources of information are essential inputs both for setting up the knowledge base supporting the assessment, and for supporting the severity and likelihood estimations of vulnerabilities, threats, attacks and failures. The control system security policy established by the corporate

management and the related (either designed or implemented) system architecture, including security technical countermeasures, composes the Target of Evaluation.

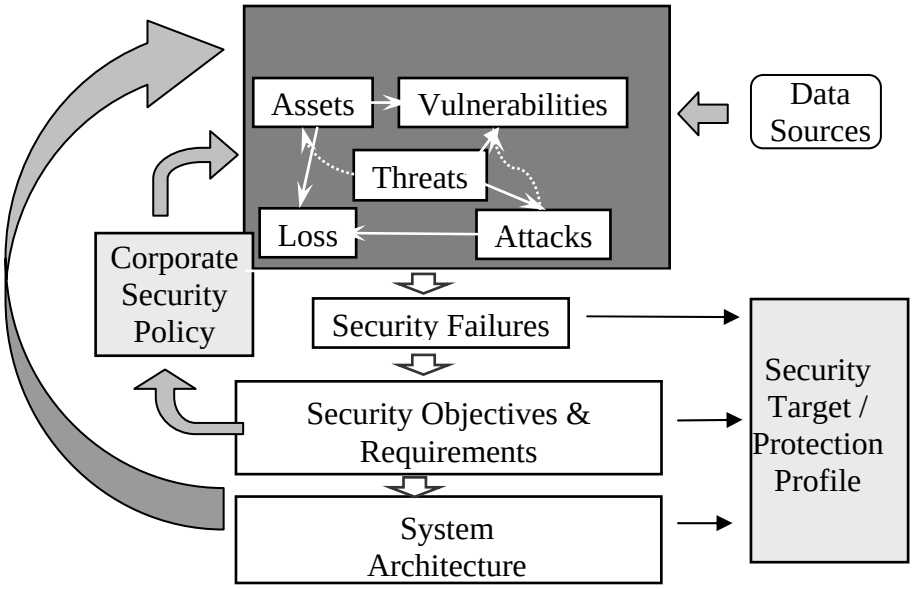


Fig. 8: The EPCSA methodology within the security management process.

8.2 Concept Correlation and assessment phases

The EPCSA methodology provides a conceptual framework correlating a set of core concepts, i.e. **asset, vulnerability, threat** and **attack**. Procedurally the assessment activity is structured into a sequence of phases, where each phase in turns formulates a set of hypotheses by means of pre-defined checklists, evaluates the hypotheses by estimating their severity and likelihood, and computes synthesised views in relation to phase-specific indexes.

The methodology provides the means to classify each system asset, vulnerability or threat according to predefined categories, and to characterise each of them according to a set of pre-defined attributes. The knowledge base underlying the methodology may be refined with application specific knowledge and needs to be updated whenever new kinds of problems are discovered by external sources of information.

8.3 Pre-assessment

Before undertaking a security analysis, it is important to go through a pre-assessment phase in which the analyst could become familiar with the system and could get a clear vision of it and of the boundaries of his analysis. A good knowledge of the system is a primordial step for a pertinent analysis. First of all, knowledge means to be aware of the context the system is inserted into; for this purpose, the analyst should be able to answer typical questions such as:

- Is there any security policy stated for the system or the corporate that provides a framework of the security context the system is inserted in?
- What are the consequences' categories that will be taken into account for this assessment? These categories deal with the negative effects that can be provoked by violations to the security policy. To make it easy, the analyst should be asked to select inside a typical list of categories those that, according to the security policy, are relevant to the system.

- An in-depth analysis will also require the development of a criticality table in which, for each category of consequences, the assessment team should define the different occurrences of consequences and their level of criticality (for instance High, Medium, and Low) for the electric power system. Relevant information could be to associate at each consequence occurrence its impact in monetary terms. The given value can just be an indication of the order of magnitude of the potential event. This estimation will turn particularly useful in the final evaluation of the risks incurred with each security failure deemed realistic for the system.

A step forward would be to clarify what is the internal architecture of the system. A classical but comprehensive description could be its decomposition into subsystems and components. By subsystems it should be understood those parts of the system that carry out fundamental tasks, i.e. those parts whose failures will be unacceptable because they might cause one of the relevant consequences' categories. Moreover, for each subsystem, it could be appreciable to enlarge its description with its functionality inside the system. That means with the characterisation of the services the subsystem delivers to the system; any failure of one of these services will cause a subsystem disservice. It also may be possible and useful to introduce external subsystem to characterise systems that do not belong to the system under study but directly interact with it. The analyst should be quite free to choose the granularity used to decompose the system in subsystems since the level of detail should be a mix between the complexity of the system and the sensitiveness of the analyst with the undertaking security issues.

However, subsystems are not sufficient to represent the architecture of the system as the topological description of relationships between subsystems is missing. Description of topology is an important and necessary step since they represent possible path for the propagation of failures. For this scope, not only physical links but also logical and communications links are relevant and should be accurately taken into account.

As vulnerabilities can be weaknesses in the architecture design/implementation of an application or a service, in a security analysis the approach of decomposing into subsystems are not adequate to cope with the indispensable step of vulnerability assessment. It is necessary to have a more detailed level of description of the system, which is consistent with vulnerability assessment. The granularity of assets, with reference to categories such as information assets (e.g., control commands, configuration parameters, alarms, measures, web pages, user authorisations, authentication, log files), software (e.g., operating systems, database management systems, web servers and applications, SCADA applications, VPN, firewalls), ICT hardware (e.g. workstations, gateways, firewalls, switches, and IEDs), or electro-mechanical equipment (e.g. transformers, breakers, disconnectors), may be adequate for such a purpose.

A particular attention should be put on the description of information assets. Since the use of digital data is getting more intensive in industrial systems, these assets are probably one of the most relevant features that security assessments should take into consideration. Due to the central role of digital data, information is by default a critical asset and its traditional security attributes like integrity, availability and confidentiality are always more directly related to system failures. A well stated classification of information assets may support the assessment in the identification of the failure consequences and the need of protection.

Moreover, information assets have some very particular characteristics that make them problematic. One is that they flow through the system, even out of its protected zones, and different instances of the same asset can at the same time be present in more than one point of the

system. This feature underlines the necessity to add, to information assets, a description of the paths over which they propagate. Paths will involve several topological links mentioned before.

To complete the framework of security analysis, the analyst should work out the disservice chains: these chains represent possible path that, starting from a disservice of a subsystem, can lead to a consequence event. The disservice graph links the disservices and connects the system disservices with the consequences that the system is intended to avoid.

Once completed the pre-assessment, the analyst may have all the preliminary information necessary to undertake a pertinent security analysis of the system.

8.4 Assessment phases and computation of indexes

The outputs of a risk assessment methodology are hypotheses on the possible security breaches the system may have to face. But there is a need to go further and organise these hypotheses with references to their relevancy or priority. It means that the risk assessment should not only define the security failures but it should also evaluate an estimate of the impact these failures could have on the system. The resulting index value is directly linked to the weight given to the consequence an event can have on the overall system. Then, the idea of index can be enlarged: not only security failures but all the security concepts discussed above, that means vulnerabilities, threats, attack/error processes and failures, can be characterised by the computation of a security index and organised with references to this index.
In the EPCSA methodology it is possible to compute the following indexes:

- **weakness index**, a function of all the weighted vulnerabilities of a particular asset or of a group of assets;
- **exposure index**, a function of all the weighted threats that can compromise a subsystem;
- **exploitability index**, a function of all the weighted attack processes that can compromise the system
- **security failure index**, a function integrating the previous indexes.

Either a worst case or a cumulative approach may be used for the computation of the above indexes. The worst case indexes may be useful when the assessment is meant for checking the violation of given thresholds, whereas the cumulative case may be used for selecting the most critical components.

Through the EPSCA methodology, the analyst has a method that makes him able to progressively highlight the relevant security aspects of the system under study; at each step, he will be asked to gather only the information which is strictly necessary to clarify on the system the security aspects the step is referred to. From a practical point of view, the methodology provides the framework to maintain a continuous risk assessment process. Its application to power control infrastructures produces:

- the documentation about the ICT network architecture, the real-time systems, their internal and external types of connections
- the System Security Profile, including detailed and synthetic views about the system security failures, scored according to the computed indexes.

The methodology has been applied to an experimental test platform of a substation control and management system available at a research laboratory at CESI, Italy. The application of the methodology has been conducted in parallel to the definition of a penetration testing plan,

which attack scenarios have been simulated in the laboratory. Some evaluations driven by that experience are reported in [27].

9 Some Guidelines for Developing a Framework for Managing Cyber Security for an Electric Power Utility

This section gives examples and an overview of existing standards, technical reports, "best practices", and guidelines, relevant to management of Information- and Control Systems security, and see how they might be used in a cyber security domain model. The purpose is to provide some guidelines when a framework for managing cyber security for an Electric Power Utility (EPU) is to be developed. The section emphasizes critical elements of a Cyber Security Management System (CSMS), and outlines a cyber security management framework for an Electric Power Utility. The list of sources referred is not complete, but the JWG consider the list to be representative and describes to some extent the state of the art in this area.

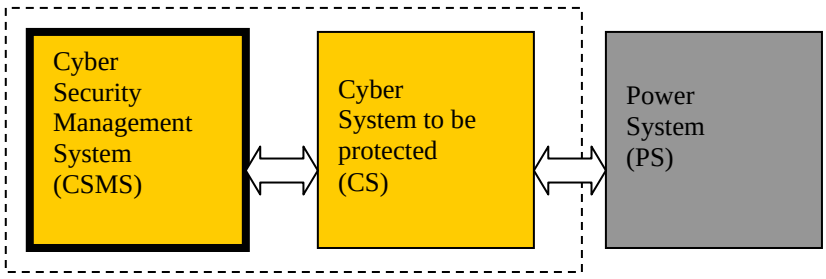


Fig. 9 Different infrastructures.

Fig. 9 shows the correlation between different infrastructures of the Power System (PS) and the Cyber System (CS). The functioning of the Power System relies very much on the proper functioning of Information- and Control systems. Therefore the Electric Power Utility needs to develop a Cyber Security Management System (CSMS) to protect its Cyber System. All infrastructures have their own lifecycle and a high degree of dependency exists.

When standards are considered, it will become quite obvious that several efforts already have been done within other sectors than the electric power industry. Here, it should be stressed that it is the authors' belief that major parts of already existing standards can be adopted for the purpose of developing a framework for managing information security for an electric power utility. In the following some standards are briefly reviewed, ordered as follows:

- General IT-standards, technical reports, and best practice
- General standards, technical reports, and guidelines to protect SCADA /Control Systems
- Guidelines to protect SCADA/Control Systems in an Electricity Utility

9.1 General IT-standards and best practice

In this group we have BS7799:2002 [4] and ISO/IEC 17799:2000 [2]. These standards constitute a consistent framework to support any organisation to develop an Information Security Management System (ISMS). A PDCA model (Plan-Do-Check-Act) to establish and maintain effective ISMS is described in [4]. Control objectives to consider are described in [2] and all

control objectives selected and the reason for their selection or exclusion must be documented in a “Statement of Applicability” to prove compliance with the standard.

In a security domain model these standards would belong to a general or main type of domain.

9.2 General standards, technical reports, and guidelines to protect SCADA /Control Systems

In this group of documents we have ISA-TR99.00.02-2004 [7] and AGA Report No 12 [31]. The ISA-TR99.00.02-2004 document is the second in a series of ISA Technical Reports whereas the first, ISA-TR99.00.01-2004 [6] provides an overview of relevant security technologies that a security program implementation must rely on. ISA-TR99.00.02-2004 provides guidance to personnel on how to plan, develop, implement and operate an electronic security program. The cyber system to be protected includes Manufacturing and Control Systems in all industries. The document describes important operational differences between general IT and Manufacturing and Control Systems. Similarities are also recognized, and many references are made to ISO/IEC 17799:2000 [2], instead of reinventing the wheel and retype similar security policies. However a series of new ISA standards on Manufacturing and Control Systems Security are now being developed and the first two of them are already drafted.

AGA Report No 12 [31] is a basic document in a series of recommending practices to protect SCADA Communications. The document focuses on technology but includes also a clause that describes steps to define security goals and an annex describing security practice fundamentals. The document highlights the importance of defining security goals starting with operation- and corporate business requirements including business partners, contractors and vendors. The document gives awareness of security assurance and gives recommendations for staffing security teams, for writing security policies and for performing assessment and analysis.

The US president’s Critical Infrastructure Protection Board and US Department of Energy has stated the “21 Steps to Improve Cyber Security of SCADA Networks” [32]. Steps 12-21 describe actions to establish an effective cyber security program.

In a security domain model these standards and guidelines would belong to a generic SCADA/Control type of domain.

9.3 Guidelines to protect SCADA/Control Systems in an Electricity Utility

In June 2002 NERC issued the “Security Guidelines for the Electricity Sector” [34], and the “NERC Urgent Actions standard 1200” [34] was developed with the purpose to reduce the risk of compromise of the Control Centre (August 2003). A short description of the document is done in one of our previous paper [15] and a new version of the document is also referred to.

In a security domain model these guidelines would belong to an Electric Power Utility SCADA/Control type of domain.

9.4 Similarities and differences

Here in this section, a comparison is made between the standards mentioned above, see Fig. 10.

	BS 7799	ISO/IEC 17799	ISA TR99.00.02	AGA12	21 steps	NERC 1200
Security definition	Ref. ISO 17799	Own	Own	Own	Cyber	Cyber
Confidentiality		Yes	Yes	Yes	Yes	Yes
Integrity		Yes	Yes	Yes	Partly	Partly
Availability		Yes	Yes	Yes	Partly	Partly
Scope						
Type of organisation	Any	Any	Any owning control systems	Gas distribution, Electric transmission and distribution, Water and Wastewater, and Pipeline systems	SCADA	Power entity
Type of system to protect	General IT	General IT	All control systems	SCADA Communications and dial-up access to maintenance ports of field devices.	SCADA, only	Critical cyber systems
Risk Assessment	Important	Important	Important	Important	Important	Important
Methodology guidance	No	No	Some	Some	No	No
Security policies						
Guidelines	No	Yes	Yes	Yes	No	No
Examples	No	Yes	Yes	Yes	No	No
Security Management System guidance	Yes	No	Yes	Yes	No	No

Fig. 10 Similarities and differences of some security standards and guidelines.

If we compare some elements of the standards and guidelines mentioned we can see that the security definitions used are different. All the referred sources claim that risk assessment and risk management are important but only a few of them say anything about methodology.

It is difficult to find cyber security guidelines and standards written for the Electricity Industry. The JWG has only found one document in this category on the list [34]. Fig. 10 shows that this document provides no guidance for establishing a Security Management System or making Risk Assessment. The conclusion is that so far, no comprehensive security guidelines or standards have been developed that address cyber systems used in the Electricity Industry. Therefore, an Electric Power Utility must rely on generic types of SCADA/Control – or general IT guidelines and standards when developing its own comprehensive security management framework

Furthermore, US Federal Information Processing Standards (FIPS) Publication 200 *Minimum Security Requirements for Federal Information and Information Systems* delegates specifications of cyber security controls, or countermeasures, to SP 800-53. These specifications are binding on non-national security information and information systems belonging to, or operated for, Federal government agencies. The results are expected to influence a wider circle, including regulatory agencies, some national security systems, and the private sector. SP 800-53 provides a comprehensive catalogue of security controls for information and information systems. Security controls are the management, operational, and technical safeguards or countermeasures used to protect the confidentiality, integrity, and availability of the system and its information. The challenge for organizations is to select the appropriate set of security countermeasures to meet the specific, and sometimes unique, security requirements of that organization thereby demonstrating the organization's commitment to security and due diligence. Here, SP 800-53 provides sets of baseline controls to assist organizations in making the appropriate selection of countermeasures.

The objective of NIST Special Publication 800-53 is to provide a sufficiently rich set of security countermeasures that satisfy the breadth and depth of security requirements levied on information systems and that are consistent with, and complementary to, other established security standards. The catalogue of security countermeasures can be effectively used to demonstrate compliance with a variety of governmental, organizational, or institutional security requirements.

Also, a new project has been initiated to analyze how well Special Publication (SP) 800-53-1 *Recommended Security Controls for Federal Information Systems* (revision 1) addresses cyber security in Industrial Control Systems (ICS)-, with particular focus on electric energy control systems that are part of the US critical infrastructure. The project focuses on comparing the NERC Cyber Security Standards (CIP 002-009) with SP 800-53.

9.5 Some critical Elements of an CSMS

In this section we discuss some critical elements of a CSMS with the view to give some hints or guidance for the readers of existing security standards- and guidelines but also to give some recommendations to the developers of new standards.

9.5.1 Definitions

As already mentioned the reader should be aware of that the definition of similar terms is not the same in different documents. The lack of a common or global glossary is obvious. However, a common vocabulary and interpretation of terms being used simplifies the security management work. Also, it unifies the understanding on a wide scale when information security issues are introduced and adopted. Therefore, it is here stressed that common definitions,

or at least common context for terms that are common across the electric power industry, are needed, such as security, control systems, SCADA, etc. Also to be mentioned here is that work is on-going to develop such “common, unified terminology”.

9.5.2 Risk Assessments

Risk Assessment and Risk Management are said to be important elements in any security program. As already concluded in our previous paper 3 [15], the state of the art of security analysis is weak; conceptual frameworks are needed and methodologies for the electric power Industry have to be developed.

9.5.3 Security policies

Security policies must be developed on different levels. When using the same phrase “security policy” this might be confusing. On the management levels we have corporate level, domain level, sub-domain level and inter/intra-domain level. Security policies on the management levels say much about scope, security objectives, responsibility, resources, organisation, training etc. and that means what to do. Then it is necessary to implement policies that give answers, that means how to. These policies are very often related to technological solutions like security architecture, about network, systems, applications, data, etc. It is important that security policies are defined and structured in a way that is easy to read, understand and apply to the relevant equipment to be secured.

9.5.4 Organisation

To actually organise the work on information security handling within an Electric Power Utility is a delicate task. It is depending on a variety of issues, such as:

- Different cultures, both within the company’s different departments, and as compared with other EPUs. Also, this varies between the countries.
- The size of the EPU, in terms of number of employers.
- Different roles and responsibilities within the company.

Here in this section, it is stressed that the treatment of Information Security must be a natural part of daily operation within the EPU, such as daily operation of SCADA/EMS and daily use of IT systems in general, including procurement, introduction, and deployment of IT systems. This means that security policies and procedures shall be adopted on a wide scale, within the entire organisation, not just within a “security group” at the IT department.

In practice, this means that every employer is depending on and part of the handling of Information Security within the EPU, including protection of data, handling of back-up and work PC, etc.

Hence, the organisation around information security “boils down” to establish and include information security treatment as a natural part of the other work processes within the EPU, such as the processes for managing the operation, maintenance, planning, refurbishment, etc. of the electric power system.

To support this work, comprehensive knowledge by Information Security experts is needed to provide guidance for the EPU. For a rather small utility, these experts may possibly be 1-2 persons as part of the IT department function within the company. For a large utility, one

may find a specific Information Security department. There is not one single model applying to both small and large utilities. But still in practice, the Information Security must be a necessity deployed at the entire organisation for an EPU, where daily internal support in information security issues are given by persons dedicated to deal with these issues.

Based on the arguments above, we here propose that Information Security is part of the work processes of daily operation. Furthermore, and not to re-invent the wheel, we propose that existing frameworks for managing information in general should be used to align security management processes and other related processes. To mention just a few general frameworks developed for the administrative IT environment – the list is certainly not complete – ITIL [8], COBIT [9], and BS 15000 [10], can be studied. In paper 4 [16], ITIL (Information Technology Infrastructure Library) [8] is further elaborated on.

9.5.5 Use existing experience from IT and/or Control System and adopt it for the electric power utility (EPU), in terms of Information Security Standards – do not re-invent the wheel

Based on the description above, it can be concluded that there is no "silver bullet". "The security framework" cannot be found. However here, we would like to provide some guidance when a security framework is to be developed.

An Electric Power Utility (EPU) should establish its cyber security frameworks based on the following facts and recommendations:

1. The EPU should use the appropriate IT and SCADA/Control system guidelines and standards as basis for developing a framework for Information Security Management, since no comprehensive security guidelines or standards are developed that exclusively address cyber systems used in the Electricity Industry.
2. Security Management in an integrated and complex network with different authorities and security requirements is a demanding and overwhelming task. The EPU is recommended to use a security domain concept as a methodology to analyse and split up the task in manageable areas.
3. Business, ownership, personnel, organisation, technology, threats, vulnerabilities etc. are all different issues that are rapidly changing. The EPU must establish a Cyber Security Management System that based upon an endless loop of "Plan", "Do", "Check" and "Act" activities are able to face an ever-changing environment and to support the on-going process of Security Management.
4. The SCADA/Control system domains include organisation, culture, technology, security risks, etc., which are different compared with general IT-domains. The EPU must be aware of this and define, adapt or adopt CSMS elements that support different type of domains. SCADA/Control system security policies should therefore be made by examining guidelines and best practices that are written to support SCADA/Control system domains.
5. Management of Information Security is an essential and natural part of daily operations of various tasks in an EPU. Therefore, it should be included and integrated within the work flow and processes of the EPU. The security framework must be aligned with any other frameworks the EPU uses for Information and SCADA/Control system management in general.

10 Technical Considerations – Focus on Substation Automation (SA)

This section focuses on the technical issues. Especially, based on the works of paper 5 [17] and paper [18], the mostly unmanned substations and the links between the substations and the control stations are studied. The reason for this focus is that substations are considered a very critical part of the power grid, and substation automation may introduce vulnerabilities.

The paper [17] gives a technical overview of the vulnerable objects and the counter measurements available to secure Substation Automation (SA) systems. It gives a brief analysis of:

- the security objectives
- how currently used objects meet security standards,
- how effective are counter measurements, and what (unwanted) side effects are generated.

The contents of this have a close resemblance to paper 3. Paper 3 is however focused on a methodology on risk assessment. Paper 5 approaches security from a list of typical vulnerable devices and points out (possible future) standards addressing the issue. If such a standard is not found, some best practices that can be applied are discussed. This section summarizes parts of findings from paper 5.

10.1 The Security objectives

A secure information system is very important for electric power industry. This is even truer for the SCADA, monitoring and substation control parts because of its hard real time requirements. We need uninterrupted control to guarantee normal grid operation. A more office-oriented information system can discontinue its service during a cyber attack. In SCADA environments a service interruption also blocks operators, leaving the grid in an uncontrolled state. That is why we need a different approach for SCADA. A secure SA information system is characterized by the following definitions:

10.1.1 Availability

It is essential to have availability of control in order to maintain the normal function of the power grid. For example this allows operators to restore power in case of outages (either by accident or by terrorist intent).

10.1.2 Integrity

But availability in itself is not enough. A hacker might take control of a substation and let the station pass wrong switchgear state data to the operator to trick him to do the remote control. By using this trick a hacker can still perform the actions that were not granted to him directly by the SCADA system.

10.1.3 Confidentiality

Confidentiality means in this context that nobody has access to data that he is not entitled to. We think this is especially important in a trading market model to prevent unfair trading or even fraud. But to keep the power grid operational availability and integrity are far more important.

The reader shall note that, compared with the standard ISO/IEC17799, the order of availability, integrity and confidentiality is reversed. This standard is not created for SCADA applications, but is a very useful guideline, provided we keep in mind the differences between for example bank transaction communication and power system SCADA communication needs.

10.2 Objects under attack

Not more than a decade ago electric power systems where operated in a SCADA style. These systems were very specialized and using equipment normally not available to many people. That made them an unknown system for malicious attackers. Following the general acceptance of personal computers and the Internet, utilities started to ask for more open systems, to give more employees access to the asset information systems. The benefits of open systems are obvious, the better the information is handled, the more efficient electric power systems can be controlled, maintained and expanded. The backside of this openness is the vulnerability that is added. If we are careless everyone can access the critical control systems with general-purpose personal computers.

What are the weak points from a technical security point of view? The older and current SCADA systems are unfortunately often not designed to be secure. In the SCADA design it was assumed that the building(s) or areas holding the primary and secondary SA equipment are trespasser-free by the use of mechanisms like fences, locks and intruder alarms. But a physical fence is no defence against a cyber attack.

The first level of weak spots is the communication system connecting the substation to the central control room. In practice a lot more links exist, for example service lines for IEDs (Intelligent Electronic Devices), connections for metering and service and so on. Especially the communication lines, which are not daily used like IED remote maintenance links, are popular attack points.

When the substation is connected by a network type connection (for example TCP/IP based), many new vulnerabilities may be introduced. New functions, such as DNS (Domain Name Server), authentication, and encryption key servers, are required. If failing, they can disrupt all communications on the network. Even if they are secure, they can be made useless by a DoS (Denial of Service) attack. Generally during a DoS attack, a device is overloaded by too many messages, such that normal messages can no longer get through. In general, this leads to loss of supervision and control of the process. More importantly, these vulnerabilities may lead to unauthorized access to equipment, which in turn may lead to significant hardware damage. Here, we are confronted with a fundamental paradigm. On one side, these routing type networks improve the functionality for a lower cost of the network. But on the other side, they weaken the communication on the security view point. The difference, compared to a serial link type communication, is that then only the connected device can be harmed if hacked. In an IP network, all devices in a substation may be harmed if hacked.

Since the dramatic drop in price of computers we find lots of people walking into substations and control rooms with a computer (notebook). They probably need this computer to do their job, but when these computers are connected to the secondary system and are equipped with a mobile Internet connection a security breach is created. To enter a critical building visitors are normally checked for name and reason for the visit, but the computer is not checked for viruses and other threats on carried notebooks. And this is only one of the many ways to create

a back door connection to the information system. There have been numerous cases where SCADA, substation and other control systems have been impacted by this type of vulnerability.

In the following three subsections, typical communication and control intelligent devices found in substation information and control systems are listed. Each device is classified for Availability, Integrity and Confidentiality, indicating the weakness and severity from a security point of view. Special remarks for each device are added.

10.3 Point to Point Communication systems

For each of the communication systems, the issues of Availability, Integrity, and Confidentiality are investigated. The description in coarse, where the level of security ("Low", "Medium", and "High") is indicated for each system and assuming that the individual systems are interconnected to build SA functions.

Systems	**Availability**	**Integrity**	**Confidentiality**
Leased lines	High	Low	Low
Dialup lines	Normally High, but low in busy periods like New Year's Eve or during a disaster	Average	Low, see leased lines.
Power Line Carrier (PLC)	High	Very Good.	Very Good
Radio link	Low	Low	Mostly poor
Radio Network Communication systems	Low	Low	Low
Privately operated IP network	High	High	High
Public operated IP network, such as ADSL, SDSL, GPRS, UMTS	High	Low	Low
Linux or Windows based Substation Controller	Low	Low	Low
Real Time Operating System based Substation Controller	High	Low	Low
Bay controllers and Intelligent Electrical Devices (IEDs)	High	High	Low, normally not addressing security
Station Bus in a Substation Control System	High	Low, protected by building	Low, protected by building

Fig. 11 Availability, Integrity, and Confidentiality for different Communication systems

The level of security of the older and most current SCADA systems is not enough for the current cyber situation. Also, the new IEC-61850 standard has no provisions for security yet. Because of its open network type communication, it is also opening the system for cyber attacks.

By using encryption on the dialup/leased lines and network links the level of security can be increased. But the key and name servers need to be protected.

The problem of unintended bridging of the power information system to the Internet is still open for future improvements (for example Mobile Internet on a notebook used for service). A promising approach is the end-to-end encryption of data-at-rest and when communicated. However, the technology does not yet commercially exist for the field devices. This eliminates the threat of bridging between the Internet and the local area network were the SCADA functions communicate. This bridging can still be there without being any threat anymore.

The second unresolved problem is the DoS attack. This attack can however be defeated by using multiple communication links. Mostly these multiple links are already required for the N-1 criterion. One must be aware of not placing the multiple links in the same cable duct or network switch!

Security has become an accepted topic for information systems, but we must be aware of that the standards for SCADA and control system applications are not yet available. Equipment built according to these future standards will not be available for some time.

10.4 Digital substation automation, architecture and integration with the information system

The introduction of digital substation automation offers news functionalities remotely available but their use raises technical, operational and security issues.

Modern digital substation automation use more and more largely spread commercial off-the-shelf (COTS) technologies like the operating systems Windows, UNIX, and LINUX operating systems, local and wide area networks, and TCP/IP protocols. Those technologies offer new opportunities for the owners like remote access to the supervision and configuration functions, to the electro-technical transient analysis data etc, but they also carry new risks, the "cyber-risks", which have to be taken into account.

Some of these remote accesses already existed, but modern systems offer broader possibilities for the operation (remote parameter setting) and maintenance (remote diagnosis) as seen in this power quality monitoring example:
The benefits of remote access are site intervention optimization and better response time for activities such as:

- Analysis of electro-technical incidents (power quality and sequence of events recorders, fault locator, component state logs, settings for protections and automata)
- Maintenance/Administration, (monitoring, consultation, diagnosis system, safeguards, repatriation of files, detection of anomalies and alarms...)
- Data Base Configuration (review, update, activate...).

Thus, two access modes are identified for these functions: “not intrusive" (monitoring, data browsing and retrieval) and "intrusive" (modification of data or active control). According to the access mode, different approaches from a security point of view must be considered.

Those benefits must be put in balance with the new “cyber-risks” they are related to, in order to safeguard the overall integrity and availability of the substation and the ability to control it.

10.5 Risk analysis for remote access to the digital substation automation

10.5.1 User needs

Digital substation automation makes it possible to ensure the operation, the supervision and the configuration of the control and protection of high voltage devices on a site made up of several substations. On each site, the digital substation automation consists of an Ethernet local area network that connects various equipment, such as, bay controllers, protections, IEDs, etc., but also the necessary general purpose computers that provide human interface to local control, to database configuration, fault analysis, logging and also office automation PC and printers. Substation automation local area networks from each site are also connected to the network of real time Telecontrol (RTU function), in order to allow control and supervision from the control centres. This real time network is dedicated to Telecontrol and it cannot be used for remote maintenance. In this context, a specific solution providing secure remote access must be designed for all substations equipped with recent digital substation automation.

10.5.2 The selected threats

A significant threat scenario would consist in using the remote access infrastructure, used for remote maintenance, to take control of the substation with the aim of acting directly or indirectly on the electric devices and of being able to connect to the Telecontrol network. The threats taken into account are:

- Loss of control of one or numerous substations
- Unauthorized access to the resources of a Substation and generally any unauthorized IT access
- Loss of integrity
- Loss confidentiality of remote access data

These last two risks can be considered less critical than the first two.

10.5.3 Security requirements and controls

The main computer security requirements are to prevent any unauthorized action on a grid component and to preserve substation observability and controllability.

Computer security aims to prevent:

- The unauthorized disclosure of data,
- Unauthorized data alteration,
- The unauthorized use of resources network or data processing in a general way. The system vendors must imbed and provide information security protections in their new systems and particularly an authentication scheme for any subsystem and integrity checks for data.

The computer security aims at guaranteeing the integrity the authenticity and the confidentiality of the data by means of the following functions:

- Identification and authentication,
- Access control,
- Data protection,
- Accountability and logging
- Specific protection of the remote access functions.

The possible mechanisms to guarantee the respect of these goals are:

- Strong user authentication for remote access: The users allowed to remotely access the substation are internal users or authorized contractors using some form of multi-factor authentication. In addition contractors using remote accesses must use workstations not connected to other networks.
- Simple "id/password" user authentication at local application level, but giving only specific rights
- Control of flows: Conformity with the security requirements of flows circulating between the sites of RTE, Substation and partners will be controlled by firewalls.
- Encryption of flows: Where possible, flows circulating between the sites, Substation and the contractors will be encrypted according to the VPN IPSEC method.

The main threats to be taken into account related to remote access to substation automation are gathered in Fig. 12, with, and in addition, the possible controls, the residual risks and possible reinforcements.

Risk Assessment

Risk	Controls	Residual Risks	Possible reinforcement
Unauthorised connection from an unauthorized site / user	Appropriate policies and procedures Strong Authentication Secured modem IP address filtering Firewalling	Authorised users malice or unintentional operation Configuration error	Audit and control Database locking for remote Clear access procedures
Denial of service for remote access	Appropriate policies and procedures. Cannot be avoided but generally not critical	None	Audit and control Use private telecommunications
Unauthorised access from an authorised site	Appropriate policies and procedures Inactivity Time out Prevent using the remote workstation as a gateway	Authorised users malice or unintentional operation Configuration error	Audit and control Database locking for remote Clear access procedures
Abuse of privilege	Appropriate policies and procedures Clear distinction between read-only rights and full rights	None	Audit and control Extend strong authentication at application level
Unauthorised access to IP resources on substation LAN	Appropriate policies and procedures Firewalling, appropriate routing policy	Exploit system known vulnerabilities	Regular security updates, audit, secure LAN. No shell or Terminal Server system access

Unauthorised access to other networks or sites	Appropriate policies and procedures Protocol discontinuity IP filtering, firewalling	None	Audit and control No shell or Terminal Server for remote system access
Exploit OS or infrastructure security hole	Appropriate policies and procedures Install Anti-virus and IDS (Intrusion Detection System) equipment, security corrective software patch management	None	Audit and control

Fig. 12 Risk assessment for substation automation.

11 Concluding Remarks

Experienced incidents have demonstrated that severe faults and catastrophic situations can be caused by malfunctions that can be related to threat agents that imply problems related to information and cyber security. Consequently, the awareness about the criticality and relevance of cyber risks in the power industry needs to be increased. This has been stressed in the work of Cigré JWG D2/B3/C2-01 addressed in this Technical Brochure. Also, several other efforts around the globe are addressing the issue of information security, e.g., IEC, NERC, ISA, AGA, NIST, and IEEE.

One of the steps forward, is to achieve an agreement on a security terminology that can be shared and used on a wide basis within the electric community. Here in this work, we have addressed that Information Security needs to be treated by identifying different information system domains and by managing their inter- and intra-domain interactions. Also, some suggested actions, to be taken while comprehensive measures are developed, are given.

Furthermore, there is a need for a comprehensive Information and Control Systems Security Framework for electric utilities. Here, some guidelines are given. Also, existing standards and industry practice of general IT and SCADA/Control Systems are studied. The security management is based on a multi-domain model. It is stressed that the wheel shall not be “re-invented.” Rather, an electric power utility (EPU) is recommended to use existing works from the general IT and SCADA/Control Systems areas to obtain a common approach. Also, the Management of Information Security is an essential and natural part of daily operations of various tasks in an EPU. Therefore, it should be included and integrated within the work flow and processes of the EPU, where the security framework must be aligned with any other frameworks.

To estimate the cyber risk is a delicate task, since experiences of cyber risk assessment in process control systems are still limited. A complete methodology supporting the security analysis of power control systems is needed, where a risk assessment methodology has to make explicit system services and consequences of their failures and the methodology has to trace the logical links between system vulnerabilities -> threats -> attack processes.

Last but not least, the technical considerations of treating information security are vast. Here, the focus has been on Substation Automation, since these are unmanned and they are considered the most complex and critical IT systems of the power grid.

12 Further works, Research

Having this TB as a basis, the JWG can see several efforts that need to be made. Here, some are given. The reader should here be aware of that the aim of the list is not to give a complete view, but rather provide some examples.

- More detailed work on frameworks for power utilities on how to manage information security, especially in the context of SCADA/Control systems. Here, the wheel does not need to be re-invented. Rather, the approach would be to adopt existing standards/best practice from other areas into the context of electric power utilities.
- Security policies for integrated administrative and industrial systems need to be developed, since both these systems types get increasingly tightly coupled.
- Support to operational security
    - Security technologies for industrial systems
    - Security of industrial systems including real time control networks
- Risk assessment: Common models and methods for treating vulnerabilities, threats and attacks are needed. This would facilitate the exchange of information across industry and with regulators/authorities, and it could imply consistent application of standards.
- The support to certification and third party verification of infrastructural systems, to assure cases for certification and mutual demonstration of security statements, and support to trust networks among stakeholders.
- Treatment of information security issues in the context of new data flows, dependencies, and new functions, in relation to market liberalization.
- How to recover cost for cyber security deployment.
- Investigations of resilient information- and communication technology architectures, in the perspective of dependable electric power systems.

13 Information Security Work in Progress – References, Bibliography, On-going works

This section briefly presents the committee works (not given in a particular order) that deal with information security. 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 authors and the JWG have found the following committee works very important to study.

13.1 International Standards – Published

[1] ISO/IEC 10181:1996 Information technology -- Open Systems Interconnection – Security frameworks for open systems

ISO/IEC 17799 and BS 7799 standards:

[2] ISO IEC 17799:2000 Information Technology – Code of practice for information security management.

[3] British Standard, BS 7799, Information security management. Part 2: Specification for management systems, 1999.

[4] BS 7799-2:2002, Information security management systems – Specifications with guidance for use.

[5] British Standards Institution, *Guide to BS 7799 - Risk assessment*, BSI, PD 3002:2002, www.bsi-global.com/index.xalter.

13.2 National Standards and/or Technical Reports – Published

Instrumentation, Systems and Automation Society (ISA) SP99: http://www.isa.org
ISA works consists of:

[6] ISA-TR99.00.01-2004: “Security Technologies for Manufacturing and Control System,” Instrumentation, Systems and Automation Society (ISA), USA.

[7] ISA-TR99.00.02-2004: “Integrating Security into the Manufacturing and Control Systems Environment,” Instrumentation, Systems and Automation Society (ISA), USA.

[8] ITIL – The Infrastructure Library, series of publications. Office of Governments Commerce (OGC) http://www.ogc.gov.uk, http://www.itil.co.uk/publications.htm

[9] COBIT – Control Objectives for Information and Related Technology. IT Governance Institute (ITGI). http://www.itgi.org/, http://www.isaca.org/

[10] IT Service Management. BS 15000-1:2002 Part1: Specification for service management. BS 15000-2:2003 Part2: Code of practice for service management. British Standards Institution (BSI) http://www.bs15000.org.uk/

13.3 Published Papers and Reports

[11] 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.

[12] A. Torkilseng: “Management of Information Security in Power Utilities,” Cigré, Electra, No. 206, February 2003.

[13] G. Ericsson: “Managing Information Security in an Electric Utility”, Electra No. 216, October 2004, pp. 20-27, http://www.cigre.org/gb/electra/electra.asp.

[14] Peter Roche: “Cyber Security Considerations in Power System Operations", Electra No. 218, February 2005, pp. 15-22, http://www.cigre.org/gb/electra/electra.asp.

[15] G. Dondossola, O. Lamquet: “Cyber Risk Assessment in the Electric Power Industry”, Electra No. 224, pp. 36-43, http://www.cigre.org/gb/electra/electra.asp.

[16] A. Torkilseng, G. Ericsson: “Some Guidelines for Developing a Framework for Managing Cyber Security for an Electric Power Utility”, to be published in Electra 2006.

[17] T. Jansen: “Technical Considerations for building secure Substation Automation systems” to be published in Electra 2006.

[18] A. VIDRASCU et. al.: “Cyber Security in Substation Automation: Design and Supervision”, Cigré 2006 Paris Session.

[19] R. Carlson, Sandia SCADA Program High-Security SCADA LDRD Final Report, Sandia Report SAND2002-0729, 2002.

[20] P. Oman, E. Schweitzer, & J. Roberts, Safeguarding IEDs, Substations, and SCADA Systems Against Electronic Intrusions, Paper #1, Western Power Delivery Automation Conference, Spokane, (WA), 2001.

[21] J. Falco, K. Stouffer, A. Wavering, F. Proctor "IT Security for Industrial Control Systems" Intelligent Systems Division, National Institute of Standards and Technology (NIST) Gaithersburg, MD, in coordination with the Process Control Security Requirements Forum (PCSRF) http://www.isd.mel.nist.gov/projects/processcontrol/.

[22] A. Risley, J. Roberts, P. LaDow, Electronic security of real-time protection and SCADA communications, Schweitzer Engineering Laboratories, SEL 2003 Inc. Pullman WA USA.

[23] Paul W. Oman, Allen D. Risley, Jeff Roberts, and Edmund O. Schweitzer, ATTACK AND DEFEND TOOLS FOR REMOTELY ACCESSIBLE CONTROL AND PROTECTION EQUIPMENT IN ELECTRIC POWER SYSTEMS, Schweitzer Engineering Laboratories 2002, Inc. Pullman, WA USA.

[24] A. Wenger, V. Mauer, M. Dunn, I. Wigert (edited by) International CIIP Handbook 2006, Vol. I and Vol. II, Center for Security Studies, ETH Zurich, the Swiss Federal Institute of Technology, 2006. (A “reference manual” which provides an updated picture at international level in the context of CIIP (Critical Information Infrastructure Protection)).

[25] N. Flatabø, *Methods to assess power system vulnerabilities, risks and potential impact of blackout***,** Key note speech by Senior Advisor at SINTEF Energy Research (Norway) in the Workshop on « The future of ICT

for power systems: emerging security challenges » jointly organised by the DG INFSO, DG RTD and JRC, in Brussels on 3-4 February 2005, https://rami.jrc.it/workshop_05/Agenda.

[26] G. Dondossola, J. Szanto, M. Masera, I. Nai Fovino, "Evaluation of the effects of intentional threats to power substation control systems", International Workshop on Complex Network and Infrastructure Protection, CNIP 2006 March 28-29 Rome, Italy

[27] G. Dondossola, O. Lamquet, A. Torkilseng "Key issues and related methodologies in the security risk analysis and evaluation of electric power control systems" Cigré 2006 Paris Session.

[28] T. Kropp: "System Threats and Vulnerabilities", *IEEE power and energy magazine*, Vol. 4, No. 2, March/April 2006, pp. 46-50.

13.4 Committee Works – International, Regional, National

[29] **Cigré JWG D2/B3/C2-01 Security for Information Systems and Intranets in Electric Power Systems.** The JWG described herein. Work progress has been reported on http://www.cigre-d2.org/, and papers have been submitted for publication in Cigré Electra.

a. Tutorial "**MANAGING INFORMATION SECURITY FOR ELECTRIC POWER UTILITIES"**, presented at Cigré SC D2, International Colloquium on telecommunications and informatics for the Power Industry, Cuernavaca, Morelos, Mexico, June 8-10, 2005

[30] **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/

[31] **American Gas Association (AGA)**: Series of AGA12 reports. http://www.aga.org/

[32] "**21 Steps to Improve Cyber Security of SCADA Networks**," Department of Energy (DOE), USA, http://www.esisac.com/publicdocs/21StepsBooklet.pdf (NERC comments to DOE with respect to modifying the document)

[33] 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.

a. National Infrastructure Assurance Partnership (NIST and NSA), USA: http://niap.nist.gov/

b. NIST SP-800-53 "Recommended Security Controls for Federal Information Systems"

[34] **North American Electric Reliability Council (NERC)**: http://www.nerc.com
Critical Infrastructure Protection Committee (CIPC) of NERC
(http://www.nerc.com/~filez/cipfiles.html)

[35] **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/

[36] **IEC TC 65C WG10**: Technical Committee of IEC TC 65: "INDUSTRIAL-PROCESS MEASUREMENT AND CONTROL," Working Group 10 addressing cyber security for manufacturing and control systems.

[37] **Common Criteria and Best Practice**: http://www.commoncriteriaportal.org/
The Common Criteria ISO/IEC 15408—The Insight, Some Thoughts, Questions, and Issues (http://www.niser.org.my/resources/common_criteria.pdf)
SWEDAC, the Swedish Board for Accreditation and Conformity Assessment, http://www.swedac.se

[38] FMV (Swedish Defence Materiel Administration) Certification Body for IT Security Evaluation, http://www.csec.se

[39] **CERT/CC (Computer Emergency Response Team Coordination Center)** "Meet the CERT/CC" at: http://www.cert.org/meet_cert/meetcertcc.html

[40] **IECSA – Integrated Energy and Communications Systems Architecture**, http://www.iecsa.org

[41] **"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

[42] Delson, Martin and Weiss, Joseph, Chapter 17 ”Cyber Security of Substation Control and Diagnostic Systems”, **Electric Power Substations Engineering**, CRC Press, June 2003.

[43] Institutional work on the electronic security of SCADA systems promoted by **NISCC** (http://www.niscc.gov.uk/).

[44] CRUTIAL “Critical Utility Infrastructural Resilience”; Specific Targeted Research Project, EU Sixth Framework Programme, IST Project n. 27513, (http://crutial.cesiricerca.it).

[45] GRID “A Coordination Action on ICT vulnerabilities of power systems and the relevant defence methodologies; Co-ordination Action, EU Sixth Framework Programme, IST Project n. 26923, (http://grid.jrc.it).

[46] IRRIS “Integrated Risk Reduction of Information-based Infrastructure Systems”; Integrated Project, EU Sixth Framework Programme, IST Project n. 27560, (http://www.irriis.org/).

[47] The future of ICT for power systems: emerging security challenges » Workshop jointly organised by the DG INFSO, DG RTD and JRC, in Brussels on 3-4 February 2005, (https://rami.jrc.it/workshop_05)

13.4.1 Cigré JWG D2/B3/C2-01 Security for Information Systems and Intranets in Electric Power Systems

Within Cigré (www.cigre.org), the Joint Working Group “JWG D2/B3/C2-01 Security for Information Systems and Intranets in Electric Power Systems” has been formed. It is a joint work between the study committees of:

D2 – Information Systems and Telecommunication for Power Systems
B3 – Substations
C2 – Systems Operation and Control

The JWG was formed in 2002/2003, and it had its first meeting in July 2003. The JWG will produce a Technical Brochure (TB) on the Information Security, and the work should be finished in mid 2006. As intermediate deliveries, approximately five papers are published in Electra (Journal of Cigré) in 2004, 2005, and 2006.

The scope of the joint working group is to identify and define information security domains 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, such as secure Internet connections. The works will address the following issues, partly relying on the standard ISO/IEC 17799.

- Why is IT security important for the Power Industry?
- Threats/Vulnerabilities
- Definitions
- Management of IT Security
- Selection of controls
- Security mechanisms
- On-going works in Europe and North America, including standards bodies and Web references.

13.4.2 IEEE PSCC – New WG Information Security Risk Assessment

Within IEEE Power Engineering Society Power System Communications Committee (PSCC), a new Working Group has been formed, entitled “Information Security Risk Assessment.” The WG has the following scope: “Development of Recommended Practices, educational material, and other information related to the assessment of information security risks in power system operations.” The work will cover methodologies for determining what the security risks might be not only in substations but also in other power system operations, since

they are often interrelated. The expectation is that the main output will be a guideline "Recommended Practices for Information Security Risk Assessment."

PSCC recognizes and wishes to complement (not compete with) other efforts in the area of communications and data security, which are underway in the electric utility industry. The WG will therefore welcome any members and/or liaisons from other groups to provide the expertise needed, and will review carefully any material provided.

13.4.3 Instrumentation, Systems and Automation Society (ISA) SP99

ISA (http://www.isa.org) has formed the Standards and Practices Committee SP 99 with the express intent of developing guidance to provide secure Manufacturing and Control Systems that are not vulnerable to electronic or network based intrusion and failures. ISA committee membership is encouraged to provide representative expertise from the user, supplier, and academic communities.

ISA-TR99.00.01-2004, "Security Technologies for Manufacturing and Control System," provides an overview of the types of electronic security technologies currently available to the Manufacturing and Control Systems environment; the pros, cons, and specific details of how each technology fits the environment; and an idea of where security technology is headed in the future. A significant part of ISA-TR99.00.02-2004, "Integrating Security into the Manufacturing and Control Systems Environment," is technology-independent, but there are parts that rely on technology. The reader is referred to ISA-TR99.00.01-2004 for more comprehensive information on the alternatives available to implement security technologies.

The documents provide guidance, which is general in nature, for attaining adequate electronic security. They should be used to help identify and address vulnerabilities and reduce the risk of undesired intrusions that could compromise confidential information or cause disruption or failure of manufacturing or control systems. A Security Lifecycle Model has been developed and it is used in ISA-TR99.00.01-2004 and ISA-TR99.00.02-2004. These ISA Technical Reports provide a framework for developing an electronic security program and provide a recommended organization and structure for the security plan.

ISA SP-99 Working Group 3 is in the process of writing "SP-99 Part I: Models & Terminology." The document will provide a framework for understanding security in a control system environment by defining common terminology (i.e. security, threat, vulnerability, etc.) and providing a set of models that capture security relevant attributes of control systems.

ISA SP-99 Working Group 7 is working on coordination and liaison with other standards groups working on control system cyber security.

13.4.4 IEC TC 57 WG 15

Technical Committee of IEC TC 57 "POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE" (www.iec.ch) works with the scope to prepare international standards for power systems control equipment and systems including EMS (Energy Management Systems), SCADA (Supervisory Control And Data Acquisition), distribution automation, teleprotection, and associated information exchange for real-time and non-real-time information, used in the planning, operation and maintenance of power systems.

Within TC57, the Working Group WG 15 is chartered with developing security standards, which encompass all the work of TC57. At the time of 2004, this work divided based on five (5) New Work Item Proposals (NWIPs):

- Use of TLS (Transport Layer Security) as security for TASE.2.
- Security for MMS ISO 9506 within the context of TC57.
- Security for five (5) profiles in IEC 61850.
- Security for IEC 60870-5, Parts 101 and 104, and 60870-5 Derivatives.
- Management Information Base (MIB) Requirements for End-to-End Network Management based on IEC 61850 constructs and objects as appropriate.

13.4.5 IEC TC 65C

The IEC TECHNICAL COMMITTEE 65: INDUSTRIAL-PROCESS MEASUREMENT AND CONTROL (TC65) (www.iec.ch) prepares international standards for systems and elements used for industrial-process measurement and control concerning continuous and batch processes. The work of standardization is to be carried out in the international fields for equipment and systems operating with electrical, pneumatic, hydraulic, mechanical or other systems of measurement and/or control.

The IEC TC65C prepares standards on digital data communications sub-systems for industrial-process measurement and control as well as on instrumentation systems used for research, development and testing purposes. Within 65C, the working group WG10 addresses cyber security for manufacturing and control systems.

13.4.6 IECSA – Integrated Energy and Communications Systems Architecture

The IECSA (Integrated Energy and Communications Systems Architecture) Project is sponsored by Electricity Innovation Institute (E2I), which is an affiliate of the Electric Power Research Institute (EPRI). This project is part of the Consortium for Electric Infrastructure to Support a Digital Society (CEIDS), a collaborative research initiative of E2I.

The purpose is to develop a roadmap/architecture for the power system of today and in the future, consisting of automated transmission and distribution systems that support efficient and reliable supply and delivery of power. The goal is to create a "self healing" power system capable of handling emergency and disaster situations while able to accommodate current and future utility business environments, market requirements, and customer needs.

The IECSA project will develop open standards-based systems architecture for the data communications and distributed computing infrastructure that will enable the integration of a wide variety of intelligent electric power system components. This infrastructure will build upon prior industry infrastructure work.

The two main deliverables are:

- Description of Existing and Future Functions related to Power System Operations
- Reference Architecture for Power System Operations

A part of these works relate to handling of information security for an electric utility. Deliverables of the project and more information can be found at http://www.iecsa.org.

13.5 Organisations dealing with Information Security – International, Regional, National

13.5.1 NERC

The mission of North American Electric Reliability Council (NERC) (www.nerc.com) is to ensure that the bulk electric system in North America is reliable, adequate and secure. Since its formation in 1968, NERC has operated successfully as a voluntary organization, relying on reciprocity, peer pressure and the mutual self-interest of all those involved.

NERC provides several industry information sharing services and programs for the Electric Utility Industry. Concerning information security, a major effort is undertaken within the Critical infrastructure Protection Committee (CIPC) (http://www.nerc.com/~filez/cipfiles.html). CIPC develops and provides minimum-security standards that have been referenced by FERC (Federal Regulatory Commission in the USA). NERC CIPC has also issued two guidelines: "Securing Remote Access to Electronic Control and Protection Systems" and "Time Stamping of Operational Data Logs."

13.5.2 US Department of Energy (DOE)

DOE has issued "21 Steps to Improve Cyber Security of SCADA Networks". The NERC CIPC is providing comments to DOE for potential revision of the document.

13.5.3 AGA – American Gas Association

The purpose of the series of AGA12 reports is to recommend a comprehensive system designed specifically to protect SCADA communications. Although the work originates in the gas industry in the USA, the AGA 12 Task Group aims to develop a set of practices that protect gas, electric, water, wastewater, and pipeline control systems.

The AGA 12 Reports focus on the background needed to understand the threats to SCADA communications, an approach to developing security policies that include protection on SCADA communications, system level requirements, and a plan for testing equipment. Forthcoming AGA reports will address recommended practices including retrofitting existing SCADA systems, networked systems, and cryptographic protection embedded in SCADA system components. Key management, protection of data, and security policies are expected to be addressed in future addendums of AGA 12.

13.5.4 Common Criteria and Best Practice

Common Criteria (IEC/ISO 15408) is a standard for IT security evaluation of IT products and systems. The purpose of the standard is to evaluate the security at an adequate level with respect to addressed requirements and in relation to the products' use in a certain IT environment.

The evaluation is based on a Protection Profile (PP), which is developed for the product, supporting description of security requirements. The Common Criteria method provides support for a variety of personnel an industry overall (such as the electric power industry): users, procurement experts, developers and suppliers, test laboratories, companies and authorities. The Common Criteria approach was developed for IT systems. NIST's Process Control Security

Requirements Forum is working to develop a similar methodology that can be applied to control systems.

More information on Common Criteria can be found at http://www.commoncriteriaportal.org/, http://www.niser.org.my/resources/common_criteria.pdf, and at www.swedac.se where it is possible to select language.

13.5.5 National Institute of Standards and Technology (NIST)

The Process Control Security Requirements Forum (PCSRF) was developed by NIST in the USA, with the goal of sharing information in this area and developing standards that can be used to provide secure manufacturing and control systems.

NIST is developing several test beds to study performance measures and tests for manufacturing and control system security products to determine if particular time-sensitive requirements can be met. The test beds include emulations of water distribution and bottling plants so that the testing includes as much of the intended physical environment as possible.

NIST also has developed a test bed to measure the timing parameters of encryption modules intended to secure Supervisory Control and Data Acquisition (SCADA) System control loops. The newly developed NIST test bed provides techniques to measure the latency and jitter of encryption modules designed for both TCP/IP and RS 232 communications channels. The test bed has been designed to provide the information required by the proposed American Gas Association test method AGA-12-1. The test bed was developed in cooperation with representatives from the gas and electric power industries.

More information can be found at the Computer Security Resource Center (http://csrc.nist.gov/) and the National Infrastructure Assurance Partnership (NIST and NSA) (http://niap.nist.gov/).

13.5.6 CERT/CC

The CERT/CC (Computer Emergency Response Team Coordination Center) is a major reporting centre for Internet security problems. Staff members provide technical advice and coordinate responses to security compromises in the USA, to identify solutions to security problems, and disseminate information to the broad community. The CERT/CC also analyses product vulnerabilities, publishes technical documents, and presents training courses.

Established in 1988, the CERT® Coordination Center (CERT/CC) is a centre of Internet security expertise, located at the Software Engineering Institute, a federally funded research and development centre operated by Carnegie Mellon University. The CERT/CC is managed by the Networked Systems Survivability Program. The CERT/CC is funded primarily by the U.S. Department of Defence and the Department of Homeland Security of the USA, along with a number of other federal civil agencies. Other funding comes from the private sector. For more detailed information about the CERT/CC, refer to http://www.cert.org/meet_cert/meetcertcc.html.

13.5.7 Euro-SCSIE (NISCC)

NISCC (National Infrastructure Security Co-ordination Centre) is helping the CNI (Critical National Infrastructure) to understand and mitigate electronic attack risks to SCADA systems. It has developed a globally-recognised expertise on SCADA security. The NISCC SCADA program (http://www.niscc.gov.uk/niscc/scada-en.html) includes:

- The annual SCADA Conference. In 2005, more than 150 SCADA, network and security managers from UK CNI companies benefited from presentations on cutting-edge international research and industry experience;
- NISCC-funded vulnerability and protection research;
- SCADA and Control Systems Information Exchange (SCSIE), a confidential industry-NISCC forum that meets regularly to exchange information on SCADA threats, incidents and mitigation;
- A close working relationship to the SCADA programs being developed in USA, Canada, Australia, New Zealand and Europe.

The SCSIE is aimed for the companies in the CNI that are dependent upon SCADA systems or other process control or telemetry systems. It was formed in October 2003 to share confidentially mutually beneficial information regarding electronic security threats, vulnerabilities, incidents and solutions in the SCADA and Process Control environment.

The SCSIE includes members from UK-based Energy, Transport and Water companies and NISCC. The SCSIE is also able to influence the NISCC-funded research program into SCADA security, as well as the content of the SCADA Conference in May 2004.

13.5.8 Process Control Center Vulnerability Reduction Center

The Idaho National Engineering and Environmental Laboratory (INEEL) has been designated by the Department of Homeland Security as the “Process Control Vulnerability Reduction Center” in identifying and reducing PCS-related vulnerabilities critical to the United States domestic security. The Center will utilize the various test bed that exist at the INEEL and across the country. The Center will facilitate the timely and adequate determination of the actual vulnerabilities of the various control systems available in the market and develop appropriate mitigation measures. Most vulnerability assessments and intrusion testing of control systems in actual operation stop short of actually attempting to gain unauthorized access to the control systems. This is because the risk of interfering with the processes these systems control is too great. The Center will provide external capabilities needed to address SCADA vulnerability concerns, that include firewalls, intrusion detection systems (IDS), identification of HMI backdoors, and assisting industry in address security concerns related to control processing units (Remote Terminal Units (RTUs), Programmable Logic Controllers (PLCs), and other programmable control devices), intelligent electronic devices (IEDs), control system computer processing equipment and application software, encryption systems, routers, and data communication system protocols and network topologies over land and wireless systems. The goal is to focuses on assisting industry in identifying areas which will result in immediate improvements in reducing process control system vulnerabilities and developing prevention, detection, mitigation, and recovery technologies that result in more secure systems and components. These efforts will address improved systems standards and certification, by increasing industry awareness and understanding of vulnerabilities.

13.6 Conferences, Workshops

- **Conference on Critical Infrastructures**, http://www.cris2004.com
- **ISA Expo 2005**, October 25-27, 2005, Chicago, IL, www.isa.org/isaexpo2005
- **6th KEMA Workshop on Control System Cyber Security**, Aug. 6-9, 2006, Portland, Oregon, USA.

Abbreviations

Glossary

DISCO	Distribution Company	EMS	Energy Management System
GENCO	Generation Company	GIS	Geographical Information System
ICCP	Inter Control Centre Protocol	IPP	Independent Power Producer
ISO	Independent System Operator	IT	Information Technology
NMS	Network Management System	PEX	Power exchange
RTU	Remote Terminal Unit	SCADA	Supervisory Control & Data Acquisition
TELCO	Public Telecom Company	TRANSCO	Transmission Company
TSO	Transmission System Operator	UCA	Utility Communication Architecture
UTELCO	Utility owned TELCO		

Glossary

Confidentiality (courtesy to ISO/IEC 17799 [2]): Ensuring that information and associated services are accessible only to those authorised to have access.

Integrity (courtesy to ISO/IEC 17799 [2]): Safeguarding the accuracy and completeness of information and processing methods.

Availability (courtesy to ISO/IEC 17799 [2]): Ensuring that authorised users have access to information and associated services when required.

Threat (courtesy to American Gas Association (AGA) [31]): 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 (courtesy to American Gas Association (AGA) [31]): 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.

Attack (courtesy to T. Kropp [28]): Actual realisation of a threat.

Risk (courtesy to T. Kropp [28]): Measure of a probability of a successful and the consequences of a successful attack.

Countermeasures (courtesy to T. Kropp [28]): Actions which can be taken to avoid or minimize the risk of attack(s).

Authentication (courtesy to www.webopedia.com): The process of identifying an individual usually based on a username and password. In security systems, authentication is distinct from *authorisation*, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

Authorisation (courtesy to www.webopedia.com): See *Authentication*.

IT (courtesy to www.webopedia.com): Short for *Information Technology*, and pronounced as separate letters, the broad subject concerned with all aspects of managing and processing information, especially within a large organization or company. Because computers are central to information management, computer departments within companies and universities are often called *IT departments*

Information: The term here is used to not only to include data that can be viewed by humans, but also to data that is used as input to applications and outputs from applications, some of which can control other applications.

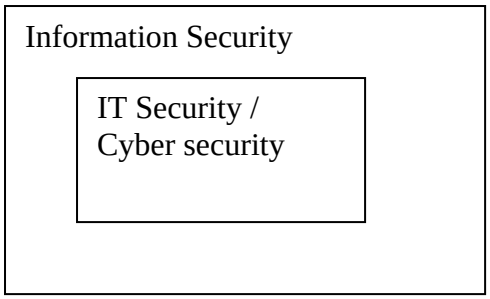
Security system (courtesy to www.webopedia.com): In the computer industry, the term refers to techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization. Most security measures involve data encryption and passwords. Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism. A password is a secret word or phrase that gives a user access to a particular program or system. The reader should here note that the JWG also would like to include systems (and/or parts of systems) which serve the purpose of "securing" the availability. E.g., this may be realised by means of a back-up system, a system for distributed storage, etc.

Information Security: The term refers to the security of information, where "information" is defined above. The reader should note that ISO/IEC 17779 give the definition of "Preservation of confidentiality, integrity and availability of information" regarding this term.

IT Security: The term refers to the computer-based systems and other physical and software-based systems that are implemented and used for information security purposes.

Cyber Security: This term and IT Security are used interchangeably.

Control systems security: The term refers to information security/IT security/cyber security in the context of control systems.



The following definitions refer to ISO/IEC 10181-1:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems [1]: Overview

- Security domain
  - ”A set of elements, a security policy, a security authority and a set of security relevant activities in which the set of elements are subject to the security policy for the specific activities, and the security policy is administered by the security authority for the security domain.”
- Security authority
  - ”An entity that is responsible for the definition, implementation or enforcement of security policy.”
- Security domain authority
  - ”A security authority that is responsible for the implementation of a security policy for a security domain.”
- Security domain A is said to be a security sub-domain B if, and only if:
  - The set of elements of A is a subset of, or is the same as, the set of elements of B
  - The set of activities of A is a subset of, or is the same as, the set of activities of B
  - Jurisdiction for A delegated from the security authority of B to the security authority of A; and
  - The security policy of A does not conflict with the security policy of B. A may introduce additional security policy if required, and if permitted by the security policy of B
- Security domain A is said to be a security superdomain of another security domain B if and only if B is a security subdomain of A

Appendix 1

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 bi-annual SCD2 meeting in September 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.

Furthernore, 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.

Attacker/threat agent	**Special capabilities/resources**	**Motivation**
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.

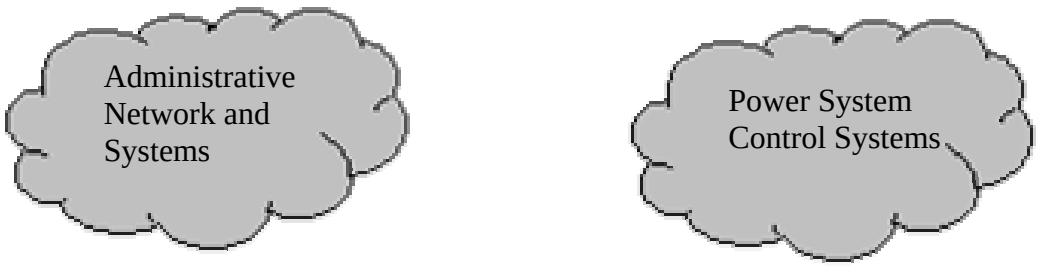


Fig. 2 Yesterday – Separate Administrative and Power System Control Networks.

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.

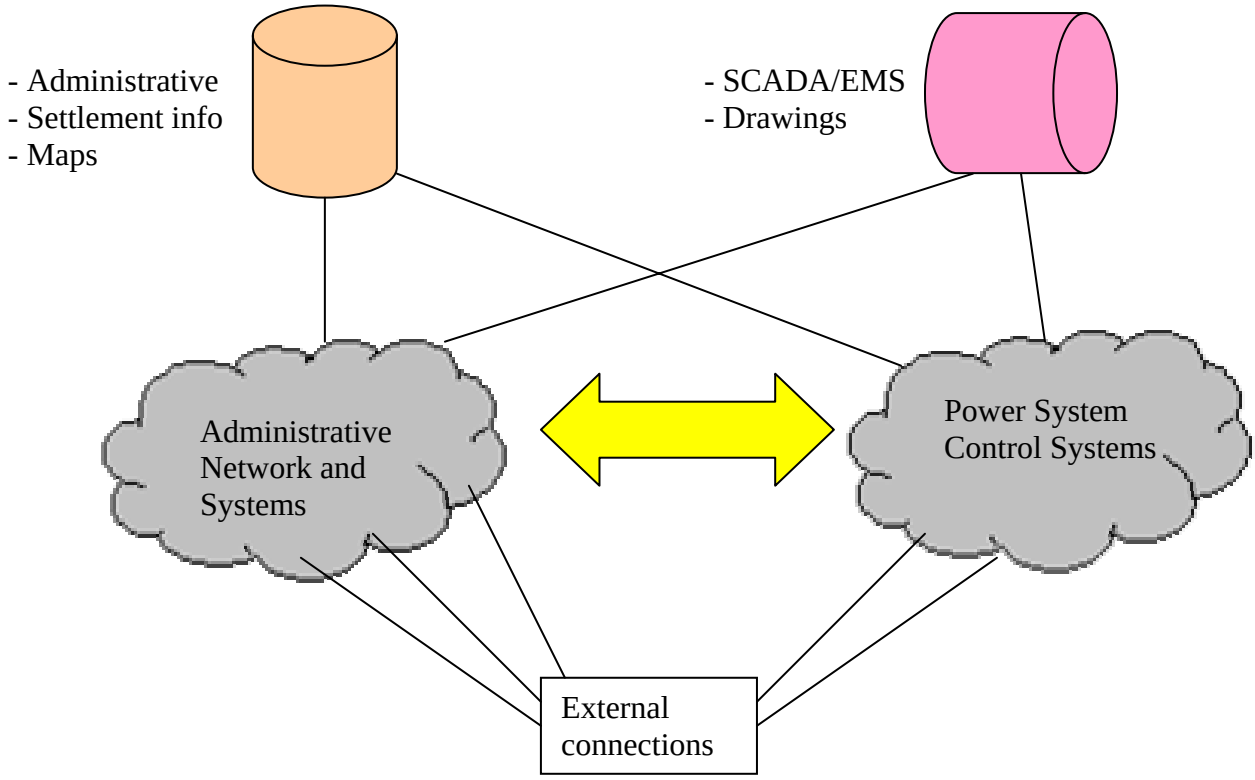


Fig. 3 Today – The Administrative and Power System Control Networks are interconnected.

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.

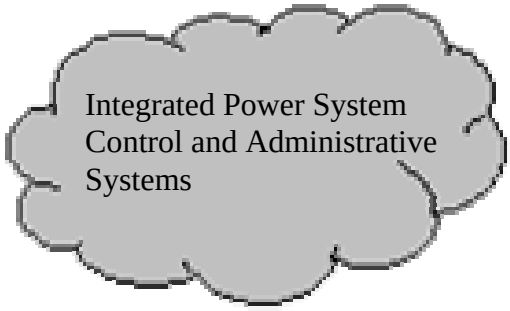


Fig. 4 Tomorrow – The Administrative and Power System Control Networks are integrated.

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.

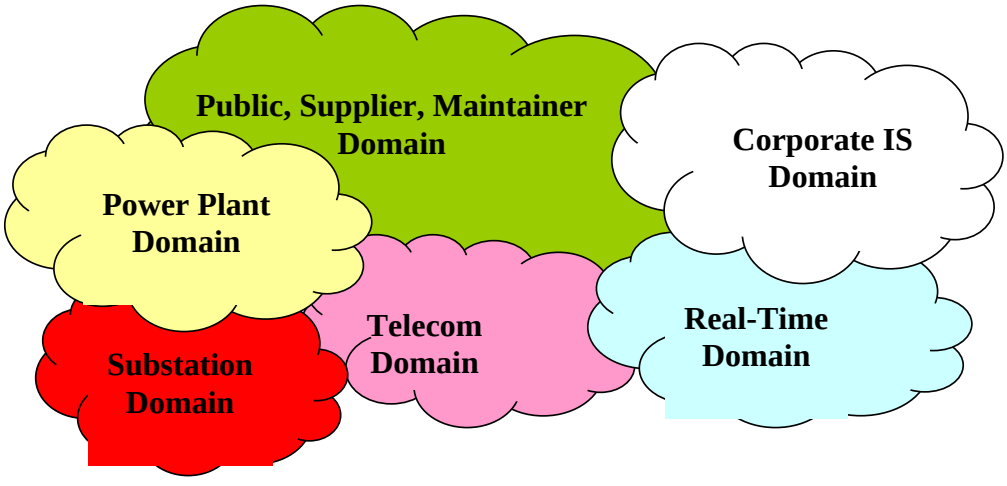


Fig. 5 Different Security Domains

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.

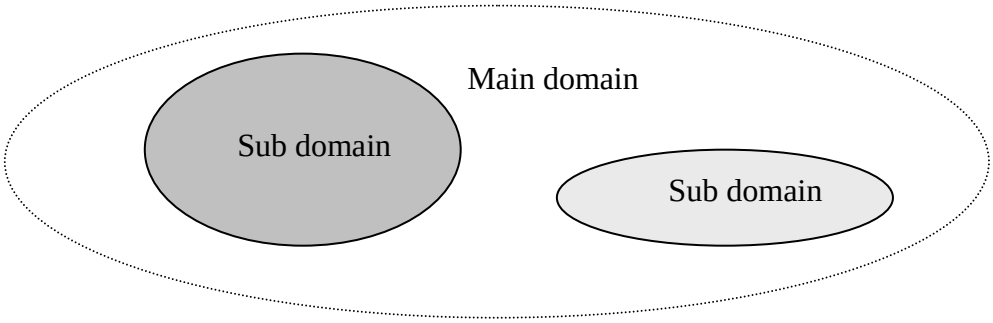


Fig. 6 A main security domain with its sub domains

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.

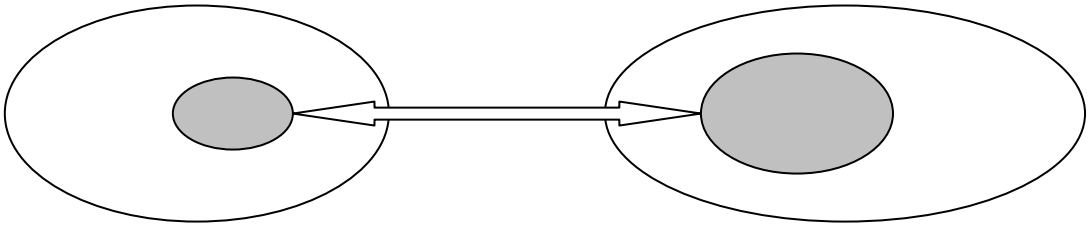


Fig. 7 Data exchange between domains

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.

	Companies / security authorities		
(Sub) domains	**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)

	Companies / security authorities		
(Sub) domains	**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/ and papers will be published 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)
  [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
- [22] **IECSA – Integrated Energy and Communications Systems Architecture**, http://www.iecsa.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-link to be added>
- [24] **Workshop on Cyber Security**, Aug 16-18, 2004. http://www.kemaseminars.com/

Appendix 2

CYBER SECURITY CONSIDERATIONS IN POWER SYSTEM OPERATIONS

Peter Roche, ESB International

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

Summary

This paper is the second in a series prepared through the efforts of the CIGRÉ Joint Working Group (JWG) D2/B3/C2-01 “Security for Information Systems and Intranets in Electric Power Systems.” The paper describes the distinguishing features of IT systems in the power industry, with emphasis on the operations area. The concept of an IT Security domain, as a means of analysing the interactions of IT systems is presented. The main domains in the power system operations area are discussed, the range of possible users is considered and the points of weakness are identified. The paper summarises a few known cyber security incidents to illustrate how real and extensive the risks are. Finally – as an interim measure - a list of immediate actions items to establish a high level IT security policy are presented.

1 Introduction

Today’s power industry makes extensive use of the capabilities of Information Technology. The benefits of such use have been enormous, in the efficiencies that have been achieved, in the extent of automation that has been introduced and in the depth and breadth of information that is available both inside and outside the organisation. A very high degree of dependency on the proper functioning of IT systems has developed. The converse is equally true – that the organisations are quite vulnerable to mal-operation of IT systems.

An earlier paper entitled “Managing Information Security in an Electric Utility”, published in Electra in October 2004, provided general background on:

- why information security is important for the electric power industry,
- where the threats and vulnerabilities arise,
- how the evolution of the architecture of IT systems has made modern systems more vulnerable and
- general information on the work of various groups which have examined IT Security issues.

The main purposes of this paper are to:

- describe the forces which have influenced the development of multiple, interconnected IT networks within the power industry,
- examine the special features of operational systems which make them vulnerable to IT threats,
- describe some reported cyber security incidents and experiences from case studies,
- suggest some immediate measures that can be taken to protect the integrity of key IT systems.

2 Principal Distinguishing Features of Modern Power Systems

Only a generation ago the Vertically Integrated Utility (VIU) was the most usual form of organisation in the power supply industry. The adoption of a business model designed to encourage competition and to force the separation of generation, transmission, distribution and supply businesses has dramatically altered the structure of the power supply industry. In parallel with these structural changes the potential of computer systems to support change has lead to the installation of a multitude of IT systems, many of which depend on inter-operability to achieve their objectives.

The current power sector is characterised by a large and expanding number of participants, each of whom has a requirement to communicate with almost any other participant in the sector. The main participants in the sector and the principal reason for communicating with others is shown below in Table 1:

Participant	Business Activity	Main Business Partner
Transco or TSO or ISO	Energy Transmission	DISCO, GENCO
SCADA / EMS Vendor	Remote Support for SCADA / EMS	DISCO, TRANSCO
Market Operator	Operate energy market	All market participants
GENCO	Power Generation	DISCOs, TRANSCO, Major consumer
IPPs	Power Generation	Major consumer, DISCOs
DISCO	Energy Distribution	TRANSCO, GENCO
RTU Vendor	Remote support of RTU	DISCO, TRANSCO
Relay Vendor	Remote support of protection relays	DISCO, TRANSCO
Consumers of all types	Cost minimisation, value	DISCO, TRANSCO, Market operator

Table 1: Main Participants in Power Industry

Tremendous productivity improvements have been achieved in most sectors, very often based on extensive deployment of computers. Computers underpin all aspects of the industry, from customer accounting and billing systems, to GIS and trouble call logging systems. Especially significant are the large number of operational systems which depend on computers – e.g. SCADA, automatic metering systems, digital substation control systems, digital relaying systems etc. In many respects it could be said that the technological fabric of today's power industry is supported by information technology.

The different participants in the power industry each develop their own IT systems, often with different hardware and software, with various network architectures and with different network management tools, systems and philosophies. Each participant has the expectation that he can communicate with other participants, normally using industry standard methods. In some situations communication may take place through industry specific protocols (e.g. UCA / ICCP), but more usually the internet, often with private subnets, is the vehicle of choice for communications.

Managers of IT systems have limited control of the IT security aspects of communications across the internet, using techniques and equipment such as encryption, access control, firewalls, etc. However an IT manager can never assume that those other organisations with whom his organisation communicates have taken adequate precautions to remove any risk of IT security threats or attacks.

3 Main Information System Domains in Power System

3.1 Concept of Information System Domain

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.

The safe, secure, responsive and confidential nature of the communications between networks and participants is at the core of the issue of IT Security.

The concept of Information System Domain is a powerful tool in the description and analysis of the interactions between the participants.

3.2 Interaction between Domains

In an unbundled and competitive market a large number of domains exist - often as many as the number of participants shown in Table 1. In addition each main domain will have a number of sub-domains. A sub-domain is a specific area, wherein particular activities/business operations are being undertaken and where a common set of IT applications are executed. There are some points of note:

- A sub-domain may be quite small in extent e.g. an IT system which monitors and records information on substation assets may be confined to a small number of locations,
- Some sub-domains may be geographically very extensive e.g. a SCADA system which extends through the entire territory of the business,
- A business unit such as a TSO may have many sub-domains – SCADA system, metering and billing system, asset monitoring system, digital substation control systems, business planning system, finance and accounting system, etc.
- There is no certainty that an explicit set of security policies is in force either across the entire domain or even in every sub-domain. Some businesses are more aware of the need for security policies than others.

It is frequently the case that different sections of a business develop IT systems in isolation and at different points in time. Certainly they will usually be interconnected, but their origins will be evident from the different hardware and software, various network architectures and from the different network management tools, systems and philosophies that are employed. Crucially different IT security practices may exist in each domain.

Where the extent of unbundling is limited, or where limited competition exists then the number of sub-domains may reduce – in this case a single business entity may, in effect, own a number of the domains outlined above.

Returning to the central theme of security of information systems in the power system operations field, it is evident that an incident or event that takes place in one domain could, if not properly managed and contained, spill-over to impact the domains to which it is connected Such a spill-over is most likely in situations where different cyber security practices apply in different domain – as will inevitably be the case. Obviously as the number of interacting domains increases the source of threats and risks to the integrity of the IT networks of other participants increases – as is implied from the multiple boundaries shown in the schematic diagram below.

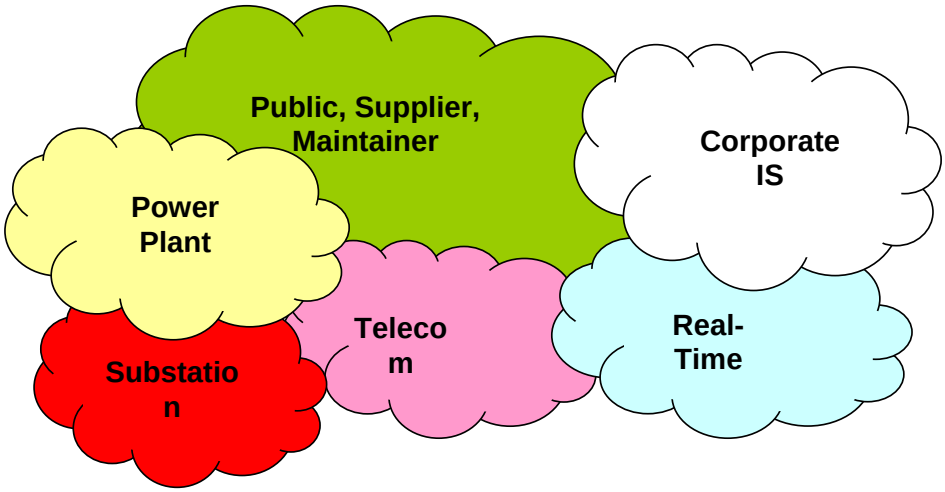


Figure 1 Concept of Overlapping IT Domains

3.3 Multiple Users within Power System Operations Domains

One of the most significant differences between the challenges facing the management of real-time schemes, in contrast with non-real-time schemes, is that there may be very many groups of users who interact with real-time IT systems. For instance operators, system maintenance personnel, vendor support personnel or others may all have genuine reasons to access the same sub-domain. In Figure 2, at the end of the paper, a more detailed list of the owners of the domains, the primary users, the secondary users of the IT systems within the domains and the reasons why there are multiple users is summarised.

Most users of the IT systems will be employees of the owner of the sub-domain; however many users may report to other sections in the owning entity and other may belong to external organisations. This diversity of responsibility and reporting lines presents serious challenges for the secure management of the real-time IT systems.

4 Points of Access / Weakness in Real-Time Systems

Figure 3 shows a schematic representation of the IT systems which are used in real-time operations. The diagram represents the manner in which many real-time systems interact and exhibit vulnerabilities. The diagram depicts the following:

- how a central SCADA system collects data from RTUs in substations, indicating the connection points where a support engineer may gain access to the central system or to an RTU.
- how support may be provided for digital Substation Control Systems, where local access, or even remote access, may be obtained to enable local reconfiguration of devices or even remote support from a vendor's office.
- the points where a telecommunications engineer may access a node for maintenance or support purposes.

A brief examination of the diagram reveals that there are multiple points of access to the various IT systems. The systems are continuously transferring data and interacting with each other. There is a definite risk that an event in one system, say the activation of a virus within the Operating System of a digital Substation Control System, could cause it to transmit spurious data into the shared telecommunications network, with the risk of effecting other IT systems. Note also that all points of connection of PCs, or equipments with embedded PCs, or even printers are potential access points to the integrity of the network.

The telecommunications system usually used by a SCADA system may share a physical infrastructure with other business users, e.g. fibre optic or microwave radio links shared with general IT applications. Traditionally, however, the SCADA system utilises non-shared and independent bandwidth e.g. its own fibres or channels. This separation may eliminate many spill-over effects from disturbances originating from other users / applications on the shared medium. Nonetheless within the SCADA system itself, the presence of many fixed PCs, of other maintenance terminals / lap-tops temporarily connected for maintenance purposes and possible direct connection to substation SCS systems, provides many points of weaknesses, through which IT security threats can enter the SCADA system.

4.1 Frequent Alterations in Network Configuration

A unique feature, almost unknown in the non-real time situation, is that the basic hardware configuration of real-time IT systems is subject to frequent change. Not alone may the number of RTUs in a SCADA system grow; the number of Bay Control Units connected to digital Substation Control Systems is always increasing; the number of asset monitoring devices in substations increases and so on. The newly connected devices may be similar to those already on the network, often they may have been produced by a different manufacturer and only match existing systems in that they use a standard protocol. Thus the configuration of sub-domains frequently changes, without any guarantee that the new device entirely complies with existing IT security policy – where an explicit policy is actually in place.

However the most threatening practice in real-time IT systems is the connection of maintenance terminals – often lap-tops – to nodes in the network, i.e. where a maintenance technician connects his lap-top / maintenance terminal to an RTU, protection relay, digital Control System etc. for a variety of purposes. This same lap-top represents one of the greatest source of risk to the integrity of IT security, as there is rarely a means of checking that the lap-top has not been infected with a virus, worm, Trojan horse etc.

4.2 Alterations / Modifications to Basic Device Parameters

Another unique feature, almost unknown in the non-real time situation, is that users may frequently access points in a sub-domain to make fundamental alterations to the parameters of embedded devices. For example a protection engineer may access a relay to reconfigure it, or to modify its characteristics. Or a support engineer may access a digital Substation Control System to reconfigure the software or hardware to add a new bay or signals to the existing system. In all cases the resultant alteration in the device software may introduce unexpected and unwanted effects.

5 Some Reported Cyber Security Incidents

A significant number of cyber security incidents have taken place; only some have been described or admitted to. To show how multi-faceted the problem is, a sample of incidents is given below.

Large Generating Plant Output Reduced to Zero

The control system of a large generating plant operating at a number of 100 MW was infected by a virus and its output was reduced to virtually zero in a few seconds. Infection came from connected corporate IT network. The solution was to rigorously separate the real-time and corporate networks.

Distribution SCADA System Partly Disabled

A virus infected lap-top was used by a maintenance technician to modify a telecoms router. The virus effected all telecom nodes, including some used by a SCADA system. The SCADA system was made partly inoperable for a number of days. A part solution required better management of virus protection on lap-tops.

Unauthorised Access to EMS Applications
A utility gave remote access rights to an EMS supplier. It was observed that application patches had been applied without agreement. No problems arose, but the situation revealed that continuous, non verified access had remained open to an external internet port, with serious risk potential.

6 Suggested Actions to be Taken While Comprehensive Measures are Developed

In a later Electra paper the Joint Working Group intend to propose a comprehensive policy as to how to establish and maintain a high level of cyber security protection. As an interim measure some key actions to be taken are suggested below.

1. Define the Responsibilities and Authorities of those Charged with Cyber Security
   Establish a cyber security organisational structure that defines roles and responsibilities and clearly identifies how cyber security issues are escalated and who is notified in an emergency. Those who design, operate, maintain real-time systems should be fully aware of the range of cyber security risks and their specific responsibilities to minimise the incidence and effects of cyber events.

2. Document the Network Architecture and Identify All Real-Time Systems
   Ensure that critical real-time systems are properly documented and that their telecommunications and IT links are accurately recorded. Ensure that documentation is kept up-to-date. During system design and extension, the designer must be fully aware of the risks and threats posed by Cyber security events. Maintain copies of all software off-site and record all changes to software and hardware.

3. Perform Security Audits of all Real-time Networks and interconnected Systems
   Technical audits of all real-time systems and networks are critical to ongoing security integrity. Establish the organisational importance of each system. Analyse the vulnerability of each system and place a risk assessment on the issue. Identify the software versions and extent of patches applied so as to be aware of the levels of protection / vulnerabilities that exist. Establish an action-plan to address the more significant weaknesses.

4. Identify all connections to Real-time Systems
   Identify and assess the risks posed by intra-company and external types of connections, including LANs, Intranets, Internet, leased or dial-up links, dedicated links, radio access systems etc.

5. Disconnect unnecessary Connections and Applications from Real-Time Systems
   To ensure the highest degree of security of real-time system, isolate the real-time sub-domains from any other network connections as far as possible.

   Disable or remove unnecessary applications or services, so only essential processing takes place on the system. Internet connections or infrequently run applications should be deleted.

6. Strengthen the Access Controls for any Remaining Connections
   Where essential connections to external sub-domains are required, implement access control systems at every point of connection, e.g. with firewalls, intrusion detection systems, password protected and dial-back type modems and other appropriate security measures. Where infrequent connections are required, consider installation of access devices which can be temporarily enabled.

7. Install Appropriate Security Facilities provided by Manufacturers.
   Analyse each real-time system to determine whether security features are present. offered by the manufacturers should be assessed. Install all appropriate security features and settings, with high threshold levels of security.

Note that reliance on proprietary protocols will not necessarily protect systems, unless suitable security measures are incorporated into the devices.

8. Establish Strict Control over non-Routine Access Mechanisms
   Identify clearly those providers of services who must be given access to real-time systems. Where, for instance, external vendor connections must be provided for support purposes, strong authentication must be implemented to ensure secure communications. Wireless access is least desirable as its presence may be very hard to detect. Access should only be permitted through a temporarily enabled access route, which should be automatically disconnected after a set period of time.

9. Maintain a Comprehensive, Continuous Risk Management Process.
   Due to rapidly changing technology and the emergence of new threats on a daily basis, a continuing and comprehensive risk assessment process is needed so that routine changes can be made to the protection strategy to ensure it remains effective. Fundamental to risk management is the identification of residual risk with a system protection strategy in place and acceptance of that risk by management.

10. Implement Intrusion Detection Systems
    To be able to effectively respond to cyber attacks, it is necessary to be aware of cyber events on the real-time systems. Where possible an intrusion detection system should be installed. Regular monitoring and active follow-up is an essential feature of an effective cyber security protection scheme.

11. Assess the Integrity of Physical Security to Real-time Systems.
    At every location where a node to a real-time system is installed (e.g. substations, telecommunications masts / towers, pole-top units etc.) conduct a physical security survey and list access points that could provide entry to a real-time sub-domains.

12. Establish a Clear Organisational Cyber Security Philosophy
    Organisations and companies need structured security programs with documented requirements to establish standards and to enable personnel to be held accountable. A formal cyber security policy is essential for establishing a consistent, standards based approach to cyber security. Policies and procedures also inform employees of their specific cyber security responsibilities and the consequences of failing to meet those responsibilities.

    The need for staff to comply with confidentiality practices and to avoid disclosure of sensitive information is a key requirement.

13. Establish a System Backup Procedure and Disaster Recovery Plans.
    Establish a disaster recovery plan that allows for rapid recovery from any emergency (including a cyber attack). System backups are an essential part of any plan and allow rapid reconstruction of the network. Routinely exercise disaster recovery plans to ensure that they work and that personnel are familiar with them. Make appropriate changes to disaster recovery plans based on lessons learned from the exercises.

7 Conclusions

Modern power system operations are heavily dependent on IT systems, many of which operate in real-time. The introduction of competition and unbundling has brought many new organisations into the power sector. Much of the interaction between the participants in the power sector is carried out through IT systems. There are a wide variety of mechanisms though which cyber threats - viruses, worms, etc.- to the integrity of IT systems can propagate. It is important that every organisational entity in the power sector becomes aware of the cyber security threats. The paper presented a brief overview of the threats posed to real-time systems. A number of immediate steps that can be taken to ameliorate

the risks have been outlined. The JWG will discuss further aspects of IT security in further papers in this series.

Glossary

DISCO	Distribution Company	EMS	Energy Management System
GENCO	Generation Company	GIS	Geographical Information System
ICCP	Inter Control Centre Protocol	IPP	Independent Power Producer
ISO	Independent System Operator	IT	Information Technology
NMS	Network Management System	PEX	Power exchange
RTU	Remote Terminal Unit	SCADA	Supervisory Control & Data Acquisition
TELCO	Public Telecom Company	TRANSCO	Transmission Company
TSO	Transmission System Operator	UCA	Utility Control Architecture
UTELCO	Utility owned TELCO		

Domain Owner	Primary User Group	Secondary User Group	Purpose of Access
Transmission system company – Transco	Operations & Maintenance staff	• Hardware asset vendors and their support staff • ISO • Utelco • Telco	• Protection equipment support and settings, etc. • Disturbance data retrieval • Vendor Support for Digital Control Schemes • SCADA via RTUs, • On call engineers with remote access rights • Public web access to open data • Provision of voice & data links
Distribution company – Disco	Operations & Maintenance staff	• Hardware asset vendors and their support staff • ISO • Utelco • Telco	• Protection equipment support & settings, etc. • Disturbance data retrieval • Vendor Support for Digital Control Schemes • SCADA via RTUs, • On call engineers with remote access rights • Public web access to open data • Provision of voice & data links
Independent System Operator – ISO or ISA	System Dispatch staff	• Asset Vendors and their support staff • Market participants • Telco	• SCADA system vendor support • On call engineers with remote access rights • Market system operators • Transco and Disco operators • Public web access to open data
Market Operator	Market Operations staff	• Asset Vendors and their support staff • Market participants	• Vendor system support • ISO interactions • Transco and Disco operators • On call engineers with remote access rights • Public web access to open data
Utility Telecommunications Company – Utelco	Network Management staff	• Asset Vendors and their support staff • Various clients using services • Telco	• NMS support, • In house staff supporting remote device configuration • On call engineers with remote access rights • Support from asset Vendors
Independent Power Producers – IPPs	Operations & Maintenance staff	• Asset Vendors and their support staff • Market operator • Transco operator • Telco	• Protection equipment support & settings, etc. • Vendor Support for Digital Control Schemes • ISO interactions • Public web access to open data • SCADA via RTUs • Provision of voice & data links
Power Exchange - PEX		• Asset Vendors and their support staff • Market participants	• Asset Vendors • ISO operator • Interactions with Market Operator

		• Utelco • Telco	
Public Telecommunications Company – Telco		• Asset Vendors • Multiple other users both within and outside power sector	• In house NMS support • Support from asset Vendors • On call engineers with remote access rights

Figure 3 Owners and Users of IT Domains

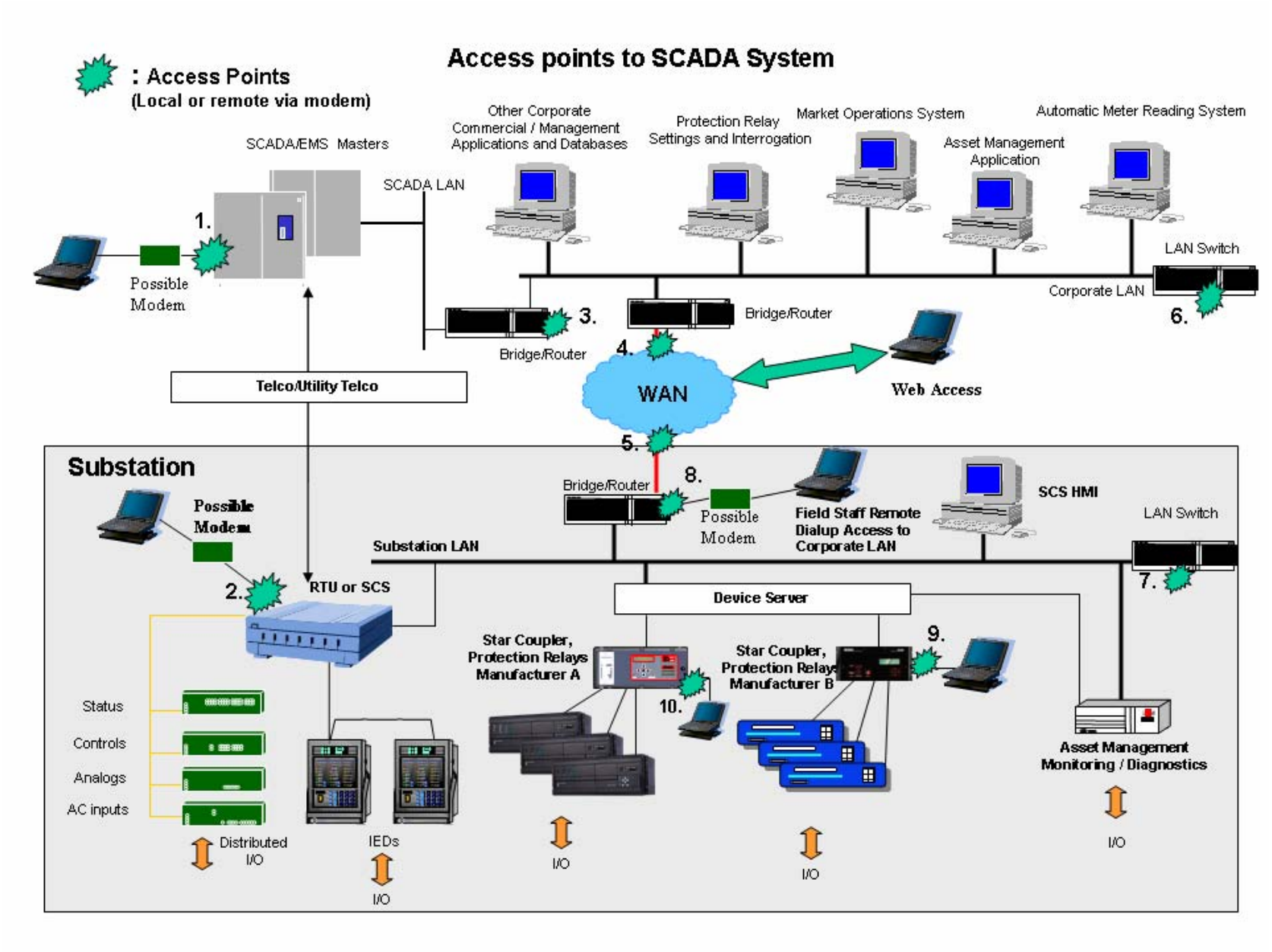


Figure 4: Schematic Diagram of Main Real-time Sub-Domains

Appendix 3

Cyber Risk Assessment in the Electric Power Industry

Giovanna Dondossola, Olivier Lamquet
CESI

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

Summary

This paper is the third in a series prepared through the efforts of the CIGRÉ Joint Working Group (JWG) D2/B3/C2-01 “Security for Information Systems and Intranets in Electric Power Systems”. The paper introduces the key aspects that a methodology for the security analysis of power utility information systems should cover. The elements that need to be identified in the preliminary system assessment are described. Then the paper discusses one method that can be used to correlate asset vulnerabilities, potential threats and the possibility of attacks; the definition of indexes to compute a qualitative estimate of the relevant properties of the system; the exploitation of correlation and indexes for scoring security failures and building the System Security Profile. The findings of the methodology support the system hardening activity and the verification of the adequacy of the adopted countermeasures.

1 Introduction

In the era of pervasive usage of information and communication technologies in everyday life, there is a great drive in utilities (which are invariably managing critical infrastructures) towards the use of Information and Communication Technology (ICT) for monitoring and controlling their technical, service and market processes. The migration of isolated Power Utility Information Systems towards inter and intra connected ICT systems has been underlined in the first paper published by this JWG [1]. Open ICT architectures and shared infrastructures have been adopted for information and maintenance purposes by technologically advanced power utilities. They are becoming a reality in the future ICT applications supporting the remote control of a power infrastructure composed of bulk and dispersed power generation, and associated power grids.

Power control systems are complex interacting infrastructures involving process knowledge, advanced control and information and communication technologies. Interconnected control and monitoring systems, coupled to enterprise networks and occasionally Internet servers increase the threats. Modern control systems are increasingly based on standard components such as operating systems and data communication protocols, creating an open infrastructure.

The purpose of this paper is to describe the main functions of a methodology for the Electric Power Cyber Security Assessment currently under development, called EPCSA in the following, supporting the security risk assessment of ICT applications for the Electric Power System. The methodology could be further extended by covering the analysis and ranking of electric power contingencies. Its functionality is presented in relation to the security domain concept[1] and the cyber security considerations in power system operations [2] described in the previous papers of this JWG. It provides support to several of the actions for establishing and maintaining a high level of cyber security protection as suggested in the second paper.

The EPCSA methodology is mainly addressed to technical security managers as an off-line analysis tool supporting the power system design and planning phases. The methodology may be also used by the security operators as a tool supporting security audits and intrusion monitoring activities during the system operation phase, thus contributing to preventing and counteracting the risk of control system degradation or block.

The paper is structured into five sections: 1) summary of the state of standards which are relevant to cyber security for the electric power industry, 2) overview of a cyber risk assessment methodology currently under development, 3) pre-assessment phase of the methodology, 4) assessment steps, computation of security indexes, generation of Profiles 5) concluding remarks.

2 State of standards and industry practices

The Cyber Risk Assessment in the Electric Power Industry is a continuous activity within the security process. It is aimed at identifying control system cyber risks within utilities. Risks are ranked and prioritised for actionable recommendations.
According to the elements composing the definition of risk shown in Figure 1, the identification of risks requires the analysis of asset vulnerabilities and threats, where the concept of threat is described in terms of the agent who performs a certain malicious or accidental action. In the malicious situation, the threat agent will take advantage of a system vulnerability by attempting an attack with the objective of damaging an asset and provoking a certain loss. In the case of accidental events, the violation of a system is due to human, environmental or physical causes provoking an erroneous situation that affects an asset. The multiple links between assets, vulnerabilities and threats form a many-to-many mesh that is difficult to disentangle.

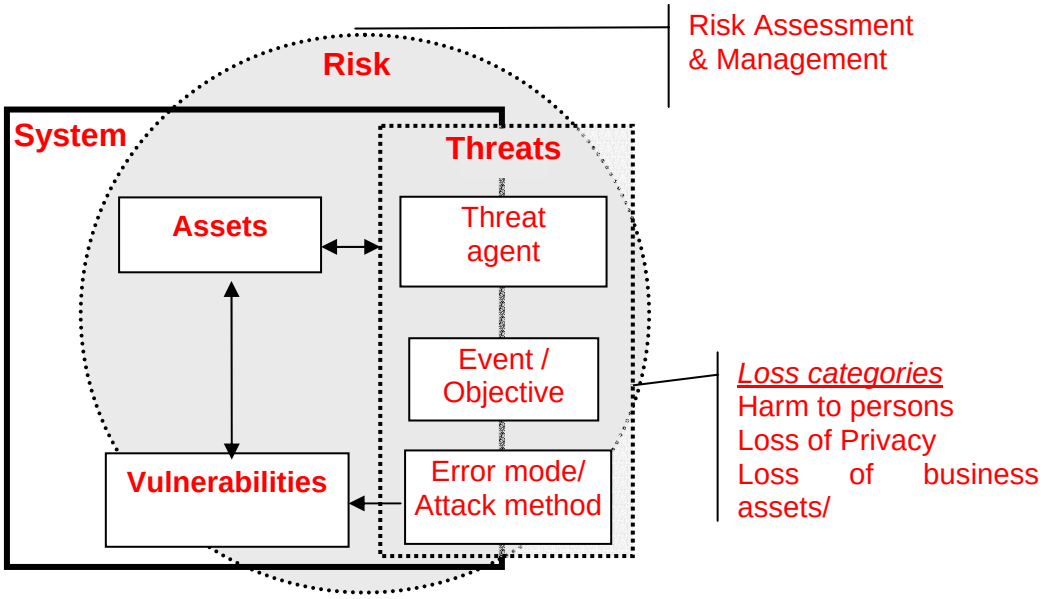


Figure 1: the elements of risk.

2.1 Standards

Any standard for ICT security management requires performing security risk assessment. Standards relevant to our application domain are spread out into three different domain area [3]: 1) general IT-standards and best practice (BS [4], [5], ISO/IEC [6]); 2) general guidelines to protect Scada/Control Systems (ISA [7], AGA [8], DoE [9]) and 3) guidelines to protect SCADA/Control Systems in the Electric Industry (NERC [10]).
In US 1998, the Department of Energy (DoE) assigned to NERC (North American Reliability Council) the role of co-ordinator of the critical infrastructure protection activities for the electric power sector. It created the CIPC (Critical Infrastructure Protection Committee) to respond to security threats and incidents, and supports the production of standards and guidelines. NERC's Cyber Security Urgent Action was developed with the purpose to reduce the risks of cyber compromise of the Control Centre (NERC 1200). A new version of this standard [11] is currently under review by the drafting team and expected to be finished by mid 2005. This standard presents detailed metrics. Its importance resides

more in its specification of basic requirements and measures, and the definition of compliance monitoring processes, levels on non-compliance and sanctions. This is a language easily understandable by industry and demonstrates a significant commitment. This type of approach, although its results will always be far from comprehensive, gives an important indication to all players in industry and regulatory bodies: the recommendation we can derive is that the problem is serious, basic solutions are urgently needed and compliance and enforcement are a must.
In parallel NERC manages the ES-ISAC (**Electricity Sector Information Sharing and Analysis Center**), for the exchange of information on critical risks in the electric power sector. In particular two indexes have been developed for the threat levels indicating the possibilities of physical and cyber attacks. These instruments are very helpful for creating awareness of the situation, but have not been very successful for control system cyber events.
In June 2002, NERC issued the "Security Guidelines for the Electricity Sector" including a vulnerability and risk assessment methodology specific for cyber security in the electricity sector (Figure 2). The approaches and practices recommended are generic, and no indications of particular methodologies are given. In any case, the guidelines are useful for disseminating common requirements and could act as a basis for further developments.

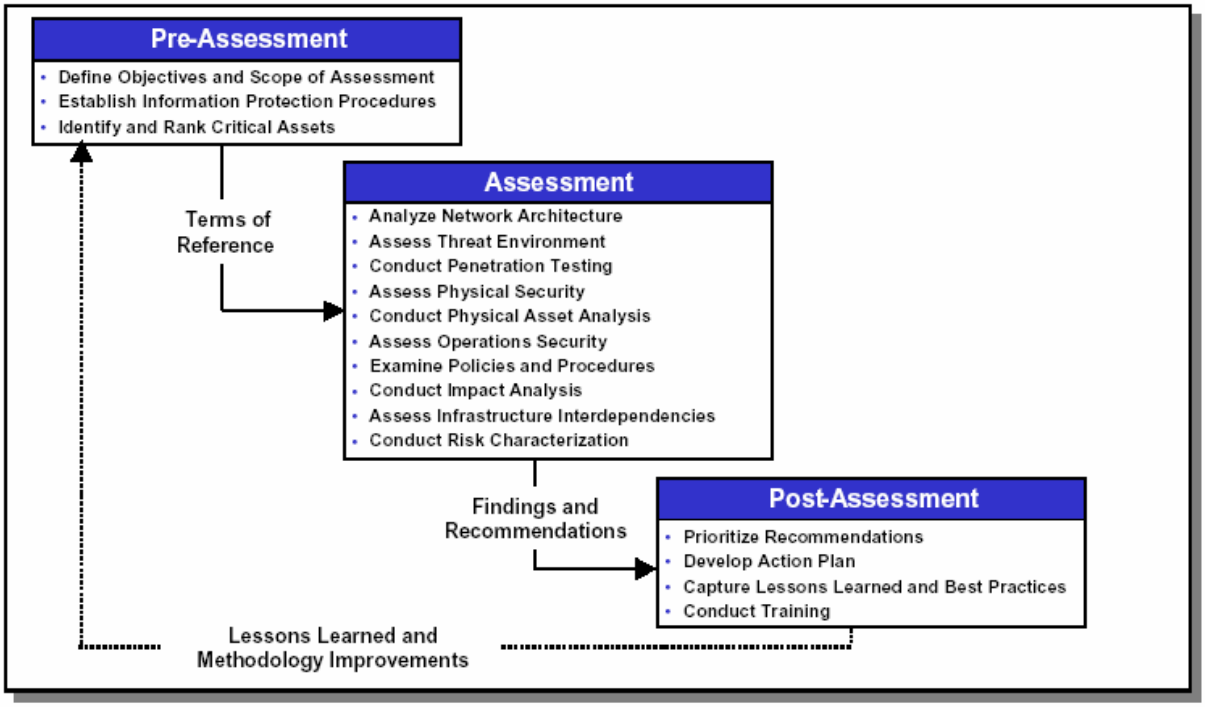


Figure 2: Phases of the NERC vulnerability assessment methodology.

In Europe the power industry practice for electric security assessment has been to use the deterministic approach, referred to as the N-1 criterion, which consists of examining the behaviour of an N-component grid following the loss of any one of its major components. Load flow analysis (steady-state), and occasionally transient stability analysis, is then applied to evaluate the resulting grid conditions.
Recently developed probability based techniques for risk assessment [12] are emerging in the electric power community. Probabilistic approaches to security assessment allow balancing the cost of security measures against the value in terms of avoided outage costs. They require estimates of the probabilities of unwanted events and the value of their consequences. The assignment of these estimates is definitely a non-trivial task for control system cyber events.
Such innovative assessment methodologies adopt conceptual frameworks dealing with deficiencies in the electrical supply, build and/or event trees linking causes and dependencies for power system blackouts, and classify consequences and durations for blackout situations. However they do not cover

the evaluation of automation system failures and a comprehensive risk assessment methodology is far from becoming a standard practice.

2.2 Industrial experiences on cyber risk assessment

In recent experiences risk assessment is performed by combining a top-down and bottom-up approach in which suggested baseline practices are driven by a top-down review of systems enriched by a bottom-up examination of events associated to risks in the business. From a methodological point of view, the top/bottom approach is supported by filling out a risk matrix, mapping subjective threats to their causes, consequences, risks and countermeasures. Exposure levels to threats are sometimes used to prioritise system vulnerabilities, which are obtained by the product of the estimated threat probability and its impact indexes on availability, integrity and confidentiality. Consultants providing risk assessment service are expected to be well experienced in risk numbers and threat areas.
In summary the state of the art of cyber security analysis in industrial control is weak: conceptual frameworks are needed and methodologies specific for the power sector have to be developed.

3 Overview of a cyber risk assessment methodology

As described in the previous papers of this JWG, the security weaknesses of a system can be numerous and even commonplace failures of single components can have huge consequences on the electric power service. This highlights the need and importance to make an accurate analysis of security problems on every single subsystem and component.
A security analysis applied to a particular system aims at defining possible failures of the system: these hypotheses of security breaches are then used as inputs to evaluate proper security requirements. However the means to reach such an objective can be multiple and the use of an ICT security expert is not always possible. For this reason the security manager needs to use a methodological support to assist with the security analysis.
A methodology should give a framework of the relevant security concepts the security manager needs to examine to carry out a correct security analysis. But above all, a methodology should trace step by step a logical route through these concepts in order to obtain an exhaustive and consistent analysis. Another important aspect of a risk assessment methodology is its openness, since the ICT technologies are in constant evolution, and the same can be said for the system vulnerabilities and threats. Periodically or after relevant system modifications, the security manager of a system may repeat the security analysis, taking into account all new security elements that have appeared since the last analysis, in order to verify that these new aspects have not modified the security profile of the system or with the aim of improving it.

3.1 The EPCSA methodology

Figure 3 shows a functional overview of the EPCSA methodology and its main relationships with the corporate security process. Data sources of information are essential inputs both for setting up the knowledge base supporting the assessment, and for supporting the severity and likelihood estimations of vulnerabilities, threats, attacks and failures. The Security Policy established by the corporate management and the related (either designed or implemented) System Architecture, including security technical countermeasures, composes the Target of Evaluation.

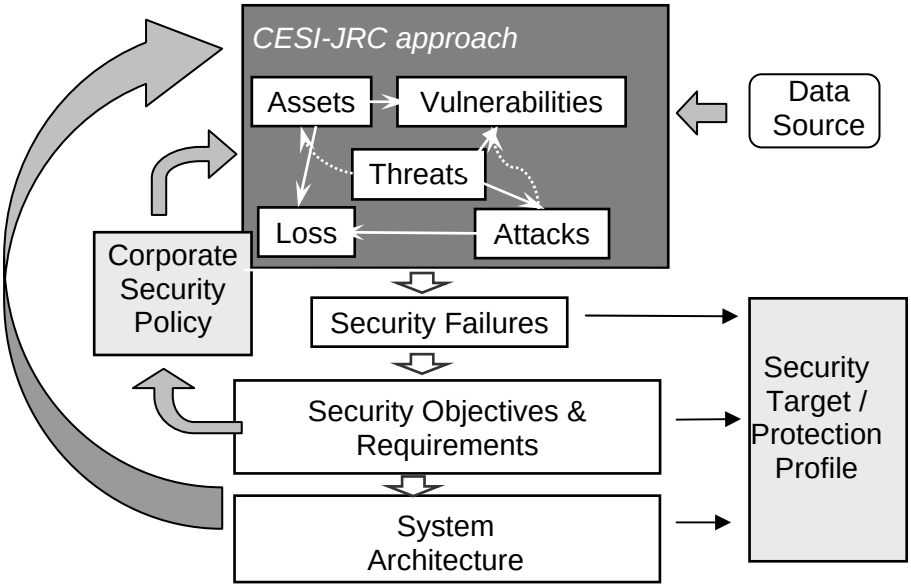


Figure 3: EPCSA methodology within the security management process.

For the tuning of the methodology we are using the architecture of a Substation Management System shown in Figure 4. It consists of functionally separated networking applications which require different levels of isolation. The **real time sub-domain** is the most isolated area, dedicated to controlling the substation, whose functions are performed by a distributed, highly reliable application optimally distributed over station-level and bay-level IEDs (Intelligent Electronic Devices). With the aim of supporting the supervision of substation data, the substation site provides a **data historian** and a **web server** for the remote monitoring of the substation behaviour by different categories of authorised users (maintainers, power engineers, ICT engineers, substation clients). An **administration** network, devoted to the monitoring and management of the substation networks, is also present. Communications between the substation and the remote **Control Centre** is through a secured open infrastructure.

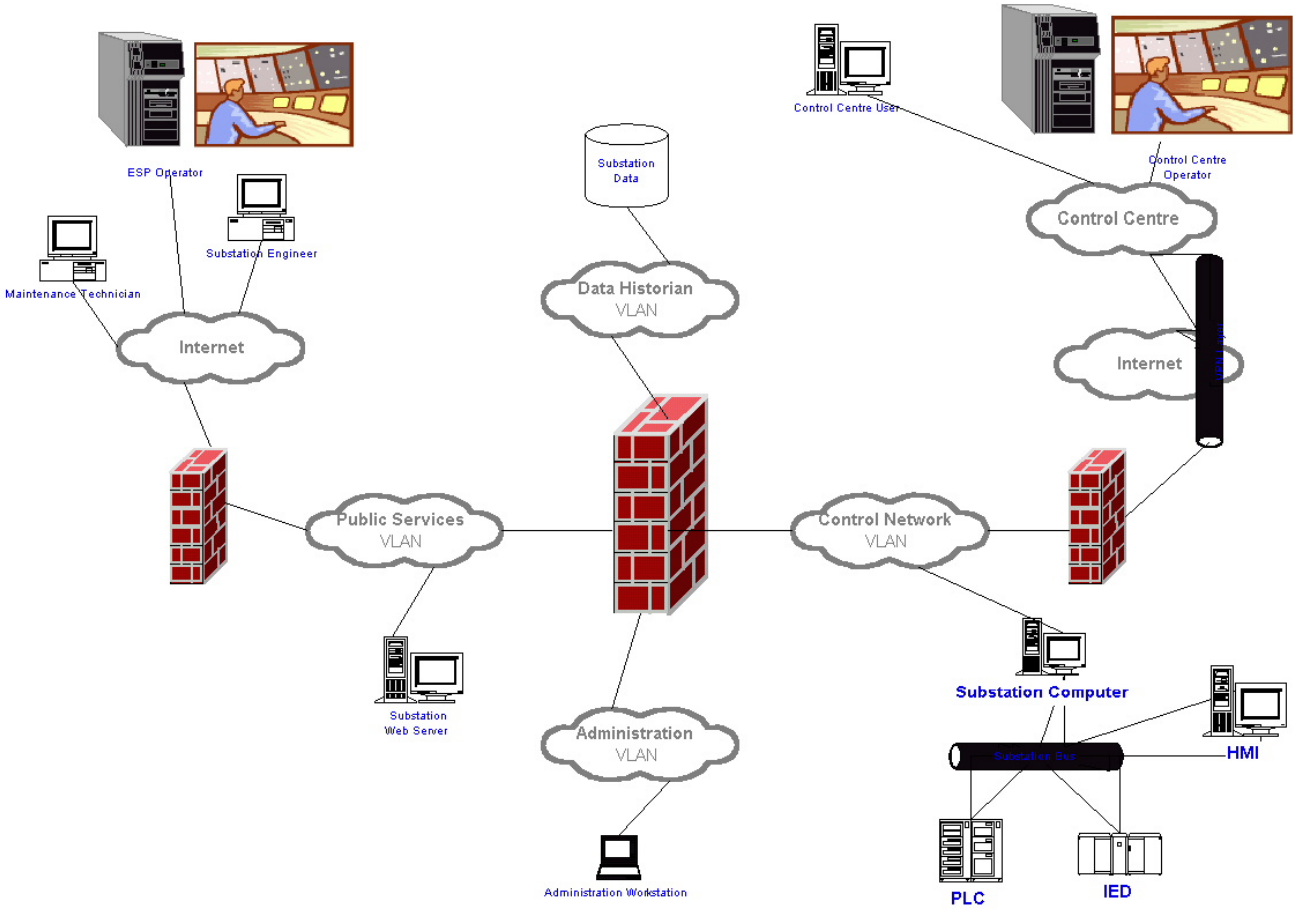


Figure 4: Substation Management System architecture.

3.2 Concept Correlation and assessment phases

The EPCSA methodology provides a conceptual framework correlating a set of core concepts, i.e. **asset, vulnerability, threat** and **attack**. Procedurally the assessment activity is structured into a sequence of phases, where each phase in turns formulates a set of hypotheses by means of pre-defined checklists, evaluates the hypotheses by estimating their severity and likelihood, and computes synthesised views in relation to phase-specific indexes.
The methodology provides the means to classify each system asset, vulnerability or threat according to predefined categories which are specific to the electric power industry, and to characterise each of them according to a set of predefined attributes. The knowledge base underlying the methodology may be refined with application specific knowledge and needs to be updated whenever new kinds of problems are discovered by external sources of information.

The assessment activity proposed by the EPCSA methodology proceeds through the phases visualised in Figure 5.

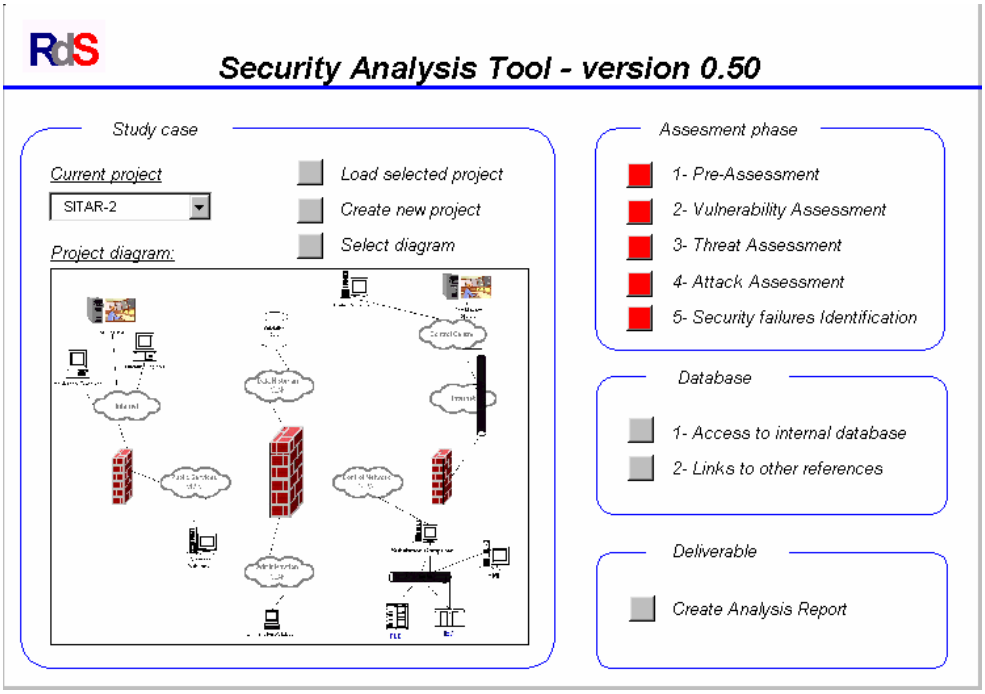


Figure 5: Assessment phases.

An accurate analysis of the characteristics of a system (Pre-Assessment) in terms of a description of its components, information flows, services and consequences supports the identification of the system weaknesses, i.e. its vulnerabilities (Vulnerability Assessment). Then considering these vulnerabilities and analysing the consequences they can have on the overall system (where the overall system refers not only to the information/control system, but also to the operational/business processes), it is possible to list the threats the system could be subjected to (Threat Assessment). Finally, starting from a particular threat related to a specific vulnerability, and making some hypothesis of the processes that can lead to the realisation of that threat, it is possible to describe an attack (Attack assessment). The results of the previous assessment phases are presented for the final evaluation (Security failures Identification).

4 Pre-assessment

Pre-assessment is aimed at producing a risk-oriented description of the system to be used by the next assessment steps.

The description of the system as a whole provides, together with minor information, a list of its **services** and of the main **consequences** provoked by a system failure. Technical, service and market oriented processes performed by the system are also part of this description. Finally links to the **security policy** documents are established.

The characterisation of the system distinguishes **internal** from **external subsystems** and their **interactions**, thus supporting the identification of the multiple users or **stakeholders**, where the internal subsystems identify different security sub-domains and the stakeholders are their external access points. Subsystem services, assets and information flows are characterised. Subsystem interactions together with their information flows form a basis which will be refined during the next assessment phases for deriving the tables of the potentially hazardous interdependencies and (vulnerability, hazard, attack) chains.

Two additional pieces of information are worth mentioning: the **consequence criticality table** and the **failure graph**. The first one defines the criticality levels of the consequences due to assets' loss or compromise. It is an agreed result of an activity performed by a cross-functional team involving

personnel from Process Control, Information Technology, Telecommunications, Operations and Production, Maintenance, Security, Management, Training, Human Resources, Finance.
The failure graph captures the links between asset failure and subsystem failure, between subsystem failure and system failure, finally connecting system failure to system consequences. The information about consequences and failures are then used in the following assessment phases, for the severity estimations of vulnerabilities, threats, attacks and failures.

During the life of the system, the pre-assessment phase should take into account all the possible alterations in the ICT and control network configuration responding to new operation requirements. For instance a protection engineer may require a local access to a relay for reconfiguring it or modifying its characteristics; a software/hardware engineer may need to remotely access a digital substation control system to reconfigure the application software or the automation network; an electrical engineer may require to remotely communicate with the substation control system to add a new bay or signal to the existing system.

5 Assessment phases and computation of indexes

The outputs of a risk assessment methodology are hypotheses on the possible security breaches the system may have to face. But there is a need to go further and organise these hypotheses with references to their relevancy or priority. It means that the risk assessment should not only define the security failures but it should also evaluate an estimate of the impact these failures could have on the system. The resulting index value is directly linked to the weight given to the consequence an event can have on the overall system. Then, the idea of index can be enlarged: not only security failures but all the security concepts discussed above, that means vulnerabilities, threats, attack/error processes and failures, can be characterised by the computation of a security index and organised with references to this index.
In the EPCSA methodology it is possible to compute the following indexes:

- **weakness index**, a function of all the weighted vulnerabilities of a particular asset or of a group of assets;
- **exposure index**, a function of all the weighted threats that can compromise a subsystem;
- **exploitability index**, a function of all the weighted attack processes that can compromise the system
- **security failure index**, a function integrating the previous indexes.

Either a worst case or a cumulative approach may be used for the computation of the above indexes. The worst case indexes may be useful when the assessment is meant for checking the violation of given thresholds, whereas the cumulative case may be used for selecting the most critical components.
Let us have a look at the results of the vulnerability assessment phase when applied to an instance of the Substation Management System in Figure 4. After having identified a set of plausible and relevant vulnerabilities associated with the subsystem assets, the Weakness Profiles may be observed with the aim of knowing if the vulnerabilities of the systems stay below a given threshold in the weakness range [0,1] (let us assume, for example, the threshold value is 0.5). By adopting the worst case approach, it is possible to visualise the System Weakness Profile by subsystem which is represented by the radar chart in Figure 6. From the picture it can be noticed that three subsystems have some assets whose weakness values are over the stated threshold: they are the Real Time subsystem (i.e. the Control Network), the Communication subsystem with the Control Centre and the Substation ICT Network. The System Weakness Profile by asset category may be visualised (Figure 7) also, in order to know which are the asset categories overcoming the threshold. The picture shows that information, software and hardware assets fall out of the acceptable weakness range.
Then the analyst may require a more indepth profile for the Real Time subsystem focusing on the weakness values of its assets. By observing the picture in Figure 8, it can be seen that specific software assets of the control network need a special attention. The findings summarised by the Weakness Profiles guide the identification of the threat hypothesis in the next assessment phase.

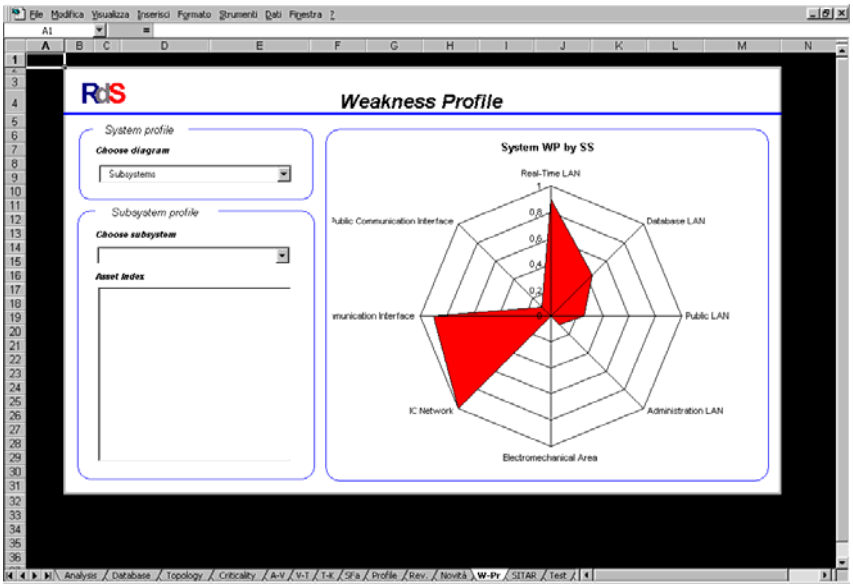


Figure 6: Weakness Profile of the Substation Management System by Subsystem.

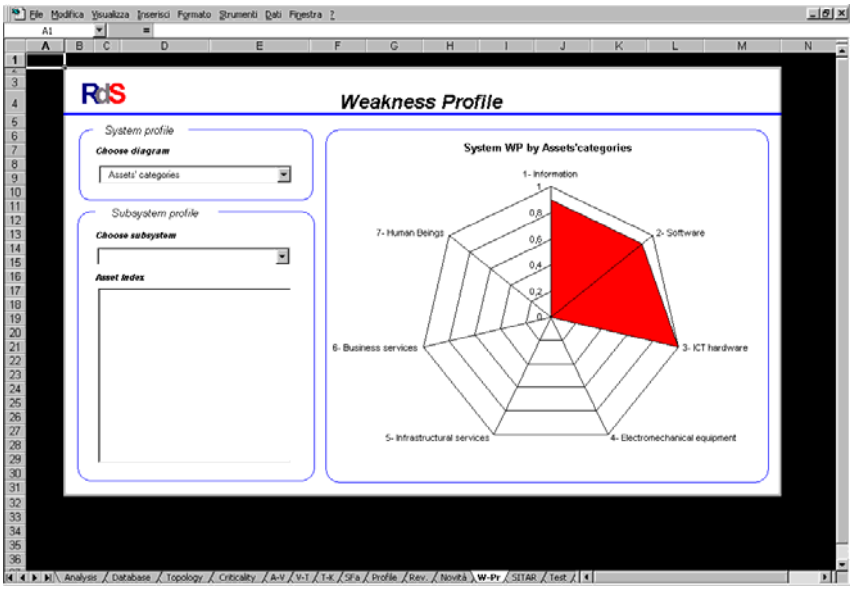


Figure 7: System Weakness Profile of the Substation Management System by asset category.

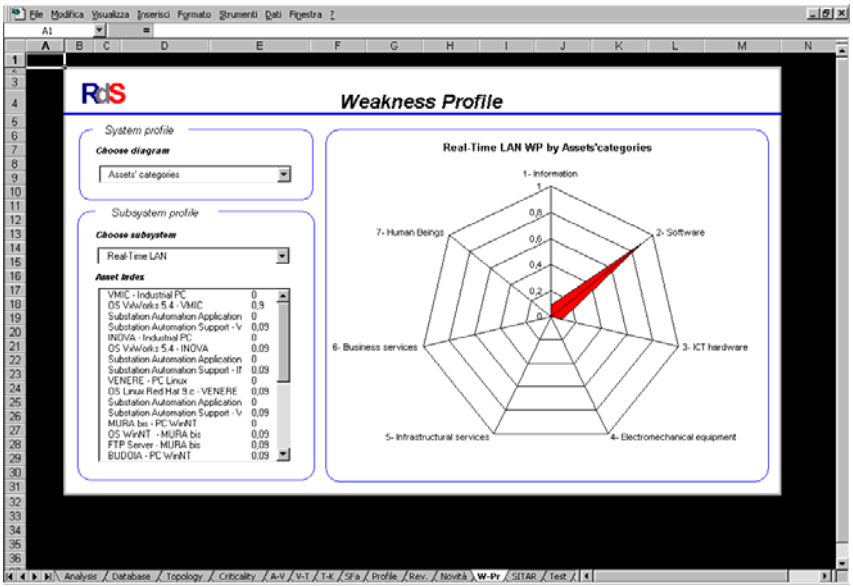


Figure 8: Weakness Profile of the Real Time Subsystem by category.

From the three assessment phases of the methodology a set of hypothetical security failures are derived, tracing the links among assets, vulnerabilities, threats, attacks, disservice and consequences. Failures hypotheses are evaluated and possible countermeasures considered. Finally selected failures are ranked according to the security failure index, and the System Risk Profile is generated.
After calculating the indexes and profiles of the existing Target of Evaluation, it should then be possible to change some of the input parameters with the view to study the effects of new countermeasures and architectural changes.

6 Conclusions

The EPCSA methodology presented in this paper provides the framework to maintain a continuous risk assessment process. More concretely its application to power system control infrastructures produces

- the documentation about the ICT network architecture, the real-time systems, their internal and external types of connections
- the System Security Profile, including detailed and synthesised views of (sub)system indexes together with a set of security failures, scored according to the computed indexes.

The findings of the methodology support the identification of non-routine accesses to the real-time sub-domains by external service providers, of their unnecessary connections, services and applications, to be addressed by the system hardening activity. Exposed accesses for essential connections to external sub-domains may be identified, indicating the need for strengthening the access control mechanisms. Finally the application of the methodology provides evidence for security audits of real-time networks and interconnected systems, allowing us to verify if any risk judged relevant by the analysis has been managed by adequate counter measures, or if some risks require to be investigated further for appropriate solutions. Then risk mitigation or avoidance plans may be compiled with the support of the methodology results, whose actions are aimed at implementing security measures for unacceptable residual failures.
In the case of the Substation Management System referred to in the paper the application of the EPCSA methodology has been conducted in parallel to the definition of a penetration testing plan, whose attack scenarios have been simulated in an experimental test platform at CESI Labs.

7 References

[1] G. Ericsson, *Managing information security in an electric utility,* Electra Magazine n. 216, October 2004, http://www.cigre.org/gb/electra/electra.asp.
[2] P. Roche, *Cyber security considerations in power system operations,* Electra Magazine n. 218, February 2005, http://www.cigre.org/gb/electra/electra.asp.

[3] A. Torkilseng, *Framework for Managing Information and Control Systems Security in an Electric Utility*, Part 2 of the Tutorial "Security for information systems and intranets in electric power systems" of the Cigré SC D2, International Colloquium on telecommunications and informatics for the Power Industry, Cuernavaca, Morelos, Mexico, June 8-10, 2005, http://www.cigre-sc35.org/.
[4] British Standards Institution, *Information security management systems – Specification with guidance for use, BS7799:2002.*
[5] British Standards Institution, *Guide to BS 7799 - Risk assessment*, BSI, PD 3002:2002, www.bsi-global.com/index.xalter.
[6] International Organisation for Standardisation, *Information security management - Code of practice for information security management*, ISO/IEC 17799:2000., www.iso.org.
[7] The Instrumentation, Systems and Automation Society, *Integrating Electronic Security into the Manufacturing and Control System Environment*, ISA-TR99.00.02-2004, www.isa.org.
[8] American Gas Association, *Cryptographic Protection of SCADA Communications*, Series of AGA12 reports, www.aga.org.
[9] US Department of Energy, *21 Steps to improve cyber security of SCADA networks,* The Presidents Critical Infrastructure Protection Board and US Department of Energy, http://www.energy.gov/engine/content.do.
[10] North American Electric Reliability Council, *Urgent Action Cyber Security Standard 1200*, August 2003, www.nerc.com.
[11] North American Electric Reliability Council, *CIP-002-1 through CIP-009-1* (formerly known as *Urgent Action Cyber Security Standard 1300*), www.nerc.com.
[12] N. Flatabø, *Methods to assess power system vulnerabilities, risks and potential impact of blackout***,** Key note speech by Senior Advisor at SINTEF Energy Research (Norway) in the Workshop on « The future of ICT for power systems: emerging security challenges » jointly organised by the DG INFSO, DG RTD and JRC, in Brussels on 3-4 February 2005, https://rami.jrc.it/workshop_05/Agenda.

Acknowledgements

The authors would like to thank Marcelo Masera (JRC-Joint Research Centre, Ispra, Italy) for his valuable contribution and collaboration to the EPCSA methodology development.

Appendix 4

Some Guidelines for Developing a Framework for Managing Cyber Security for an Electric Power Utility

Åge Torkilseng, Göran Ericsson

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

1 Summary

This paper is based on the efforts of Cigré JWG D2/B3/C2-01 “Security for Information Systems and Intranets in Electric Power Systems”. It provides guidance when a framework for managing cyber security for an Electric Power Utility is to be developed, with respect to: existing standards, “best practices”, and guidelines from other areas than the electric power industry. It is stressed that to not re-invent the wheel, but rather to adopt cyber security issues from general IT and/or control system areas. A comparison is made between BS 7799, ISO/IEC 17799, AGA12, “21 steps to improve cyber security of SCADA networks”, and NERC 1200. The work of this paper relies on the domain concept for managing information security. Also, it is emphasized that Information Security Management must be a natural part of daily operation for the Electric Power Utility, such that the operation, maintenance, planning, etc., of the electric power system.

2 Introduction

This paper is number 4 in a series of five (5) papers prepared through the efforts of the CIGRÉ Joint Working Group (JWG) D2/B3/C2-01 “Security for Information Systems and Intranets in Electric Power Systems” and published in Electra. This paper 4 gives examples and an overview of existing standards, “best practices”, and guidelines, relevant to management of Information- and Control Systems security, and see how they might be used in a cyber security domain model. The purpose is to provide some guidelines when a framework for managing cyber security for an Electric Power Utility (EPU) is to be developed. The paper emphasizes critical elements of a cyber security management system, and outlines a cyber security management framework for an Electric Power Utility.

The paper is based on efforts in the JWG, where a number of information security experts from the electric power industry participate, and it relies on some standards present in the general information technology (IT) area and in the SCADA/Control System area.

Paper 1, entitled “Managing Information Security in an Electric Utility” [1] provided general background on:

- Why information security is important for the electric power industry,
- Where the threats and vulnerabilities arise,
- How the evolution of the architecture of IT systems has made modern systems more vulnerable, and
- General information on the work of various groups which have examined IT Security issues.

Paper 2, entitled “Cyber Security Considerations in Power System Operations”[2]:

- Described the forces which have influenced the development of multiple, interconnected IT networks within the power industry,

- Examined the special features of operational systems which make them vulnerable to IT threats,
- Described some reported cyber security incidents and experiences from case studies,
- Suggested some immediate measures that can be taken to protect the integrity of key IT systems.

Paper 3, entitled “Cyber Risks Assessment in the Electric Power Industry”[3], described the main functions of a methodology for the Electric Power Cyber Security Assessment, supporting the security risk assessment of Information and Communication Technology (ICT) applications for the Electric Power System.

Regarding technical considerations, it is outside the scope of this paper 4 to discuss relevant technology and choice of technical solutions. Some technical issues will be dealt with in paper 5. However here, we would like to refer to the efforts done by IEC TC57 WG15 [4], which are developing security services for the most important protocols that are used in the Electric Power Industry.

3 Examples of Cyber Security standards, guidelines, and best practices

In this section we have a look on standards, guidelines and best practices that an EPU might take advantage of when establishing its own Cyber Security Management System (CSMS). The list of sources referred is not complete, but the JWG consider the list to be representative and describes to some extent the state of the art in this area.

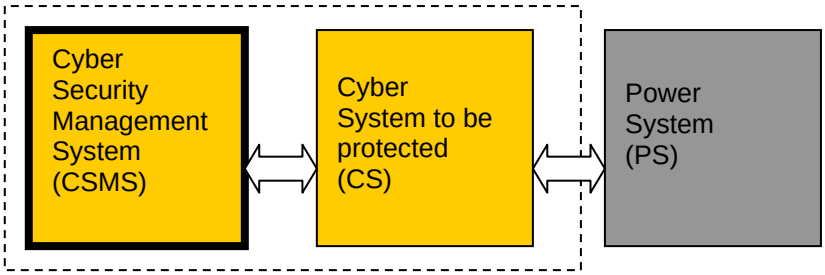


Fig. 1 Different infrastructures

Figure 1 shows the correlation between different infrastructures of the Power System (PS) and the Cyber System (CS). As discussed in previous papers the functioning of the Power System relies very much on the proper functioning of Information- and Control systems. Therefore the Electric Power Utility needs to develop a Cyber Security Management System (CSMS) to protect its Cyber System. All infrastructures have their own lifecycle and a high degree of dependency exists.

When standards are considered, it will become quite obvious that several efforts already have been done within other sectors than the electric power industry. Here, it should be stressed that it is the authors’ belief that major parts of already existing standards can be adopted for the purpose of developing a framework for managing information security for an electric power utility. In the following some standards are briefly reviewed, ordered as follows:

- General IT-standards and best practice (3.1)
- General standards and guidelines to protect SCADA /Control Systems (3.2)
- Guidelines to protect SCADA/Control Systems in an Electricity Utility (3.3)

3.1 General IT-standards and best practice

In this group we have BS7799:2002 [5] and ISO/IEC 17799:2000 [6]. These standards constitute a consistent framework to support any organisation to develop an Information Security Management System (ISMS). A PDCA model (Plan-Do-Check-Act) to establish and maintain effective ISMS is described in [5]. Control objectives to consider are described in [6] and all control objectives selected and the reason for their selection or exclusion must be documented in a “Statement of Applicability” to prove compliance with the standard.

In a security domain model these standards would belong to a general or main type of domain.

3.2 General standards and guidelines to protect SCADA /Control Systems

In this group of documents we have ISA-TR99.00.02-2004 [7] and AGA Report No 12 [9]. The ISA-TR99.00.02-2004 document is the second in a series of ISA Technical Reports whereas the first, ISA-TR99.00.01-2004 [8] provides an overview of relevant security technologies that a security program implementation must rely on. ISA-TR99.00.02-2004 provides guidance to personnel on how to plan, develop, implement and operate an electronic security program. The cyber system to be protected includes Manufacturing and Control Systems in all industries. The document describes important operational differences between general IT and Manufacturing and Control Systems. Similarities are also recognized, and many references are made to ISO/IEC 17799:2000 [6], instead of reinventing the wheel and retype similar security policies. However a series of new ISA standards on Manufacturing and Control Systems Security are now being developed and the first two of them are already drafted.

AGA Report No 12 [9] is the basic document in a series of recommending practices to protect SCADA Communications. The document focuses on technology but includes also a clause that describes steps to define security goals and an annex describing security practice fundamentals. The document highlights the importance of defining security goals starting with operation- and corporate business requirements including business partners, contractors and vendors. The document gives awareness of security assurance and gives recommendations for staffing security teams, for writing security policies and for performing assessment and analysis.

The US president’s Critical Infrastructure Protection Board and US Department of Energy has stated the “21 Steps to Improve Cyber Security of SCADA Networks” [10]. Steps 12-21 describe actions to establish an effective cyber security program.

In a security domain model these standards and guidelines would belong to a generic SCADA/Control type of domain.

3.3 Guidelines to protect SCADA/Control Systems in an Electricity Utility

In June 2002 NERC issued the “Security Guidelines for the Electricity Sector” [11], and the “NERC Urgent Actions standard 1200” [12] was developed with the purpose to reduce the risk of compromise of the Control Centre (August 2003). A short description of the document is done in one of our previous paper [3] and a new version of the document is also referred to.

In a security domain model these guidelines would belong to an Electric Power Utility SCADA/Control type of domain.

3.4 Similarities and differences

Here in this section, a comparison is made between the standards mentioned above, see Fig. 2.

	BS 7799	ISO/IEC 17799	ISA TR99.00.02	AGA12	21 steps	NERC 1200
Security definition	Ref. ISO 17799	Own	Own	Own?	Cyber	Cyber
Confidentiality		Yes	Yes	Yes	Yes	Yes
Integrity		Yes	Partly	Partly	Partly	Partly
Availaility		Yes	Partly	Partly	Partly	Partly
Scope						
Type of organisation	Any	Any	Any	Any	Any	Power entity
Type of system to protect	General IT	General IT	SCADA	SCADA Communications	SCADA	Critical cyber systems
Risk Assessment	Important	Important	Important	Important	Important	Important
Methodology guidance	No	No	Some	Some	No	No
Security policies						
Guidelines	No	Yes	Yes	Yes	No	No
Examples	No	Yes	Yes	Yes	No	No
Security Management System guidance	Yes	No	Yes	Yes	No	No

Fig. 2 Similarities and differences of some security standards and guidelines

If we compare some elements of the standards and guidelines mentioned we can see that the security definitions used are different. All the referred sources claim that risk assessment and risk management are important but only a few of them say anything about methodology. It is difficult to find cyber security guidelines and standards written for the Electricity Industry. The JWG has only found one document in this category on the list [12]. Fig. 2 shows that this document provides no guidance for establishing a Security Management System or making Risk Assessment. The conclusion is that so far, no comprehensive security guidelines or standards have been developed that address cyber systems used in the Electricity Industry. Therefore, an Electric Power Utility must rely on generic types of SCADA/Control – or general IT guidelines and standards when developing its own comprehensive security management framework

4 The Domain Concept for managing Information Security

The analysis and management of information security in an interconnected network is an overwhelming task. However, the task might be separated into independent areas and dependencies could be discussed and managed as a specific subject. The Domain Concept was introduced in [1] and many examples and considerations were given in [2]. A more detailed and distinct definition of security domains can also be found in [13].

4.1 The Domain Concept and existing standards and guidelines

The different security authorities will be free to select any analysis method, security program and security implementation for their own security domains or sub domains. The great number of domains might be reduced by negotiation as discussed in [1] but at the end there exist a number of domains that need to interact and exchange data. The question is then; how do existing security standards or guidelines support a security domain model? The works of [5] and [6] do not refer to security domains. The work of [7] has defined network segments like “Enterprise Network Segment”, Process Information Network Segment”, etc. that might be representations of domains but a domain concept in general is not used. The work of [9] encourages using domains when doing security analysis at the architectural level but provide no guidance. The JWG has not found any guidance that provide general support of the process of defining common policies for the exchange of data between domains and sub domains.

4.2 Steps to set up a Multi-Domain Model

To set up a Multi-Domain Model is not trivial task and require a lot of attention and efforts of all participants. The JWG is not in position to further develop the theoretical basis of the model but it would like to demonstrate and give some practical examples of the advantages of the Domain Concept.

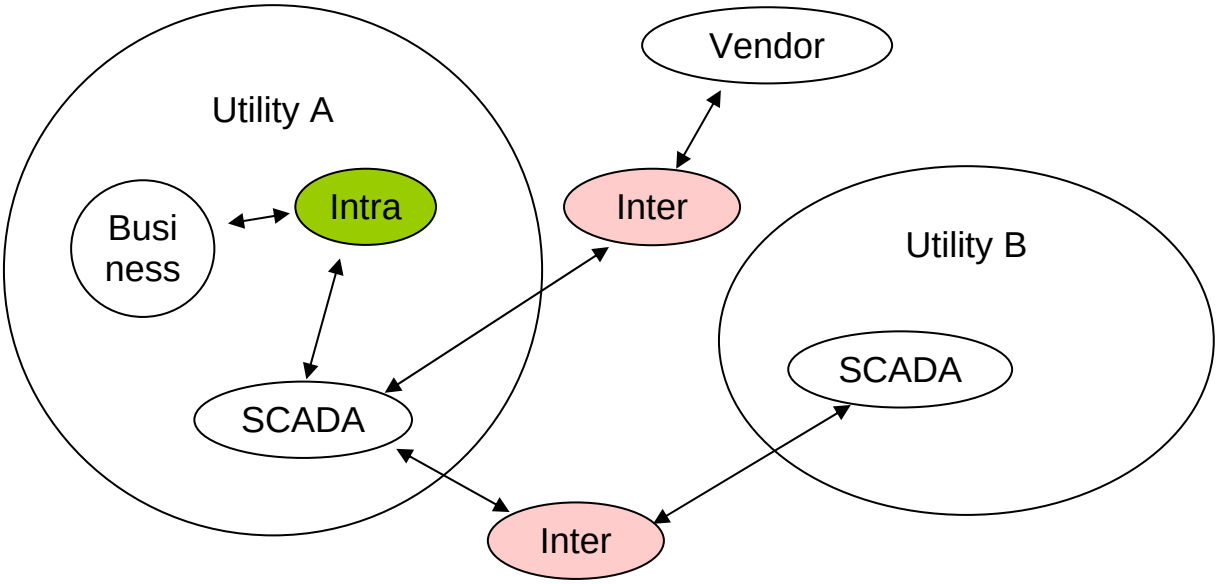


Fig. 3 Example of a Multi-Domain Security Model

Figure 3 shows an example of a Multi-Domain Security Model. The model could be set up by using the following steps: 1) Define corporate domain perimeter, 2) identify corporate sub-domains and define their perimeters, 3) identify external domains to interchange data with, 4) reduce the number of sub-domains and domains by negotiation [1], and 5) define inter- and intra domains.

4.3 Security inter/intra domain considerations

There is a strong need for interchange of data between participants in the Electric Power Industry. This is well documented in our previous paper [2]. We have a situation where two or more security domains, each with a security authority and different security levels, have to be interconnected. In a security domain model the approach would be to define an inter- or intra-domain with all the domain characteristics like authority, domain perimeter and policy that could serve like a bridge between the interconnected domains. See Fig. 3.

First of all, a security authority have to be established for each inter- or intra domain. A typical example is a vendor (see Fig. 3) that needs to access the SCADA system to make upgrade of system software. If the Service Level Agreement (SLA) tells nothing about security but only deals with functionality, there exists no security authority and probably no security at all for the interconnection. If the communication partners would be aware of the situation and use a domain model, they could establish a security authority by nominating responsible persons. Then the inter-domain perimeter should be defined. On the SCADA side the vendor should only have access to those parts of the SCADA network that is necessary to do the update or upgrade work. On the vendor side the perimeter between the inter-domain and the vendor's internal domain should be carefully defined. E.g., if the upgrade includes testing and transfer of operational data to the vendor side, the data should be protected in a secured area. The inter-domain policy should define the security level of the interconnection itself, but also authorization and access rights of the data at rest on both sides. E.g., if operational data is transferred to the vendor domain, the policy could declare

that the data should be deleted after use. In this example, the definition of the inter-domain could be a part of the SLA between the partners.

5 Some critical Elements of an CSMS

In this section we discuss some critical elements of a CSMS with the view to give some hints or guidance for the readers of existing security standards- and guidelines but also to give some recommendations to the developers of new standards.

5.1 Definitions

As already mentioned the reader should be aware of that the definition of similar terms is not the same in different documents. The lack of a common or global glossary is obvious. However, a common vocabulary and interpretation of terms being used simplifies the security management work. Also, it unifies the understanding on a wide scale when information security issues are introduced and adopted. Therefore, it is here stressed that common definitions, or at least common context for terms that are common across the electric power industry, are needed, such as security, control systems, SCADA, etc. Also to be mentioned here is that work is on-going to develop such “common, unified terminology”.

5.2 Risk Assessments

Risk Assessment and Risk Management are said to be important elements in any security program. As already concluded in our previous paper [3], the state of the art of security analysis is weak; conceptual frameworks are needed and methodologies for the electric power Industry have to be developed.

5.3 Security policies

Security policies must be developed on different levels. When using the same phrase “security policy” this might be confusing. On the management levels we have corporate level, domain level, sub-domain level and inter/intra-domain level. Security policies on the management levels say much about scope, security objectives, responsibility, resources, organisation, training etc. and that means what to do. Then it is necessary to implement policies that give answers, that means how to. These policies are very often related to technological solutions like security architecture, about network, systems, applications, data, etc. It is important that security policies are defined and structured in a way that is easy to read and understand.

5.4 Organisation

To actually organise the work on information security handling within an Electric Power Utility is a delicate task. It is depending on a variety of issues, such as:

- Different cultures, both within the company’s different departments, and as compared with other EPUs. Also, this varies between the countries.
- The size of the EPU, in terms of number of employers.
- Different roles and responsibilities within the company.

Here in this section, it is stressed that the treatment of Information Security must be a natural part of daily operation within the EPU, such as daily operation of SCADA/EMS and daily use of IT systems in general, including procurement, introduction, and deployment of IT systems. This means that security policies and procedures shall be adopted on a wide scale, within the entire organisation, not just within a “security group” at the IT department.

In practice, this means that every employer is depending on and part of the handling of Information Security within the EPU, including protection of data, handling of back-up and work PC, etc.

Hence, the organisation around information security "boils down" to establish and include information security treatment as a natural part of the other work processes within the EPU, such as the processes for managing the operation, maintenance, planning, refurbishment, etc. of the electric power system.

To support this work, comprehensive knowledge by Information Security experts is needed to provide guidance for the EPU. For a rather small utility, these experts may possibly be 1-2 persons as part of the IT department function within the company. For a large utility, one may find a specific Information Security department. But still in practice, the Information Security must be a necessity deployed at the entire organisation for an EPU.

Based on the arguments above, we here propose that Information Security is part of the work processes of daily operation. Furthermore, and not to re-invent the wheel, we propose that existing frameworks for managing information in general should be used to align security management processes and other related processes. To mention just a few general frameworks developed for the administrative IT environment – the list is certainly not complete – ITIL [14], COBIT [15], and BS 15000 [16], can be studied. Here, parts of ITIL are further elaborated on.

ITIL (Information Technology Infrastructure Library) [14] is a customisable framework, which addresses the organisational structure for an IT organisation, by presenting a comprehensive set of management procedures, which are supplier independent and adopted in a wide range of organisations, including government, energy, public utilities, retail, finance, and manufacturing.

The ITIL framework is divided into eights "sets", see below, which in turn is divided into different "disciplines".

1. Services Delivery
2. Service Support
3. Planning to Implement Service Management
4. Security Management
5. ICT Infrastructure Management
6. The Business Perspective
7. Application Management
8. Software Asset Management

The authors have not found any contradiction in using this framework to provide guidance for Information Security handling within an EPU. Rather, we claim it is valuable for the organisation of the Information Security treatment.

6 Development of a Security framework for an Electric Power Utility: some guidance and concluding remarks

Based on the description above, it can be concluded that there is no "silver bullet". "The security framework" cannot be found. However here, we would like to provide some guidance when a security framework is to be developed.

An Electric Power Utility (EPU) should establish its cyber security frameworks based on the following facts and recommendations:

1. The EPU should use general IT and SCADA/Control guidelines and standards as basis for developing a framework for Information Security Management, since no comprehensive security guidelines or standards are developed that exclusively address cyber systems used in the Electricity Industry.
2. Security Management in an integrated and complex network with different authorities and security requirements is a demanding and overwhelming task. The EPU is recommended

to use a security domain concept as a methodology to analyse and split up the task in manageable areas.

3. Business, ownership, personnel, organisation, technology, threats, vulnerabilities etc. are all different issues that are rapidly changing. The EPU must establish a Cyber Security Management System that based upon an endless loop of “Plan”, “Do”, “Check” and “Act” activities are able to face an ever-changing environment and to support the on-going process of Security Management.
4. The SCADA/Control system domains include organisation, culture, technology, security risks, etc. that are different compared with general IT-domains. The EPU must be aware of this and define, adapt or adopt CSMS elements that support different type of domains. SCADA/Control system security policies should therefore be made by examining guidelines and best practices that are written to support SCADA/Control system domains.
5. Management of Information Security is an essential and natural part of daily operations of various tasks in an EPU. Therefore, it should be included and integrated within the work flow and processes of the EPU. The security framework must be aligned with any other frameworks the EPU uses for Information and SCADA/Control system management in general.

7 References

[1] “Managing Information Security in an Electric Utility”, Electra No 215, October 2004, pp. 20-27.

[2] “Cyber Security Considerations in Power System Operations”, Electra No 217, February 2005, pp. 15-22.

[3] “Cyber Risks Assessment in the Electric Power Industry”, Electra, February 2006. ____

[4] 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: 62351 “Data and Communications Security, http://www.iec.ch/

[5] BS 7799-2:2002, Information security management systems – Specifications with guidance for use.

[6] ISO/IEC 17799:2000 Information Technology – Code of practice for information security management.

[7] ISA-TR99.00.02-2004: “Integrating Security into the Manufacturing and Control Systems Environment,” Instrumentation, Systems and Automation Society (ISA), USA.

[8] ISA-TR99.00.01-2004: “Security Technologies for Manufacturing and Control System,” Instrumentation, Systems and Automation Society (ISA), USA

[9] American Gas Association (AGA): Series of AGA12 reports. http://www.aga.org/

[10] “21 Steps to Improve Cyber Security of SCADA Networks,” Department of Energy (DOE), USA, http://www.esisac.com/publicdocs/21StepsBooklet.pdf

[11] NERC 2002. “Security Guidelines for the Electricity Sector”, http://www.nerc.com/

[12] “NERC Urgent Actions standard 1200”, http://www.nerc.com/

[13] ISO/IEC 10181:1996 Information technology -- Open Systems Interconnection – Security frameworks for open systems

[14] ITIL – The Infrastructure Library, series of publications. Office of Governments Commerce (OGC) http://www.ogc.gov.uk, http://www.itil.co.uk/publications.htm

[15] COBIT – Control Objectives for Information and Related Technology. IT Governance Institute (ITGI). http://www.itgi.org/, http://www.isaca.org/

[16] – IT Service Management. BS 15000-1:2002 Part1: Specification for service management. BS 15000-2:2003 Part2: Code of practice for service management. British Standards Institution (BSI) http://www.bs15000.org.uk/

Appendix 5

Technical considerations for building secure Substation Automation systems

Ton Jansen

On behalf of JWG D2/B3/C2-01 "Security for information Systems and intranets in Electric Power Systems".

1 Summary

This paper is the number 5 in a series prepared through the efforts of the CIGRÉ Joint Working Group (JWG) D2/B3/C2-01 "Security for Information Systems and intranets in Electric Power Systems." The previous papers in this series covered security from an organizational point of view. This paper focuses on the technical problems, especially in the mostly unmanned substations and the links between the substations and the control stations.

2 Introduction

The first paper [1] provided general background on:

- Why information security is important for the electrical power industry.
- Where the threats and vulnerabilities arise.
- General information on the work of various Groups, which have examined IT security issues.

A second paper [2] described:

- The focus that have influenced the development of multiple, interconnected IT networks within the power industry, and what properties made them vulnerable to IT threats.
- Some reported cyber security incidents and experiences from case studies.
- Suggestions on some immediate measures that can be taken to protect the integrity of key IT systems.

A third paper [3] described the main functions of a methodology for the Electric Power Cyber Security Assessment, supporting the security risk assessment of ICT applications for the Power System.

A fourth paper [4] provided:

- Examples of existing cyber security standards, "best practices" and guidelines. See how these examples might be used in a cyber security domain model.
- Information that emphasize critical elements of a cyber security management system.
- An outline of a cyber security management framework for an Electric Utility.

This fifth paper gives a technical overview of the vulnerable objects and the counter measurements available to secure Substation Automation (SA) systems. The paper gives a brief analysis of:

- The security objectives.
- How currently used objects meet security standards,
- Effectiveness of counter measurements and what (unwanted) side effects are generated.

The contents of this paper have a close resemblance to paper [3]. This paper is however focused on a methodology on risk assessment, approaches security from a list of typical vulnerable devices and points out (possible future) standards addressing the issue. If such a standard is not found, we still reference some best practices that can be applied.

3 The Security objectives

A secure information system is very important for electric power industry. Because of its hard real time requirements, this is even more valid for the SCADA, monitoring and substation control parts. To guarantee normal grid operation, uninterrupted control is required. A more office-oriented information system can discontinue its service during a cyber attack. In SCADA environments a service interruption also blocks operators, leaving the grid in an uncontrolled state. That is why we need a different approach for SCADA. A secure SA information system is characterized by the following definitions:

Availability

It is essential to have availability of control in order to maintain the normal function of the power grid. For example this allows operators to restore power in case of outages (either by accident or by terrorist intends)

Integrity

But availability in itself is not enough. A hacker might take control of a substation and let the station pass wrong switchgear state data to the operator to trick him to do remote controlling. By using this trick, a hacker can still perform the actions that were not granted to him directly by the SCADA system.

Confidentiality

Confidentiality means in this context that nobody has access to data that he is not entitled to. We think this is especially important in a trading market model to prevent unfair trading or even fraud. However, to keep the power grid operational availability and integrity are far more important.

Note that compared to the standard ISO/IEC17799 the order of availability, integrity and confidentiality is reversed. This standard is not created for SCADA applications, but is a very useful guideline, provided we keep in mind the differences between for example bank transaction communication and power system SCADA communication needs.

4 Objects under attack

Not more than a decade ago Electric Power Systems where operated in a SCADA style. These systems were very specialized and used equipment normally not available to many people. That made them an unknown system for malicious attackers. Probably following the general acceptance of personal computers and of Internet, utilities started to ask for more open systems to give more employees access to the asset information systems. The benefits of open systems are obvious. The better information is handled, the more efficient Electric Power Systems can be controlled, maintained and expanded. Unfortunately this openness makes the systems also more vulnerable. If we are careless, everyone can access the critical control systems with general-purpose personal computers.
What are the weak points from a technical security point of view? The older and current SCADA systems are not designed to be secure. And, even worse, these systems cannot be modified to integrate security mechanisms into either the field devices or the SCADA master. A SCADA design assumed that the building(s) or areas holding the primary and secondary SA equipment are trespasser free by the use of simple mechanisms like fences, locks and intruder alarms. But a physical fence is no defense line against a cyber attack. Only a band-aid approach, called a retrofit solution, can be used to avoid unwanted modification of the existing hardware and software.

The first level of weak spots is the communication system connecting the substation to the central control room. Because intruders outside the fenced area of the utility often can physically access these lines, communication systems can never be secured enough. In practice a lot more links exist, such as service lines for IEDs, connections for metering and service. The communication lines that are not daily used, such as IED remote maintenance links, are easily forgotten in a risk assessment scan. Because of this, they are vulnerable attack points.

When the substation is connected by a network type connection (for example TCP/IP based), many new different vulnerabilities can be introduced. New functions such as DNS (Domain Name Server), authentication and encryption key servers are required, and if failing they can disrupt all communications on the network. Even if communication lines are secure, they can be made useless by a DoS (Denial of Service) attack. Generally during a DoS attack a device is overloaded by too many messages. So normal messages can no longer pass. [15]. This generally leads to loss of view and control of the process. More important, these vulnerabilities can lead to unauthorized access to equipment, resulting in significant hardware damage. We are confronted here with a fundamental paradigm: on one side these routing type networks improve the functionality for a lower cost of the network, but on the other side they weaken the communication on the security viewpoint. The difference between an IP network and a serial link type communication is the following:

- In an IP network all devices/substation can be harmed if hacked.
- In a serial link type communication only the connected device can be harmed if hacked.

Since the dramatic drop in price of computers lots of people are in substations and control rooms with a notebook. They probably need this computer to do their job. But a security breach can be created when these computers are connected to the secondary system. To enter a critical building visitors are normally checked for name and reason for the visit. But their notebooks are not checked for viruses and other threats. If for example this notebook has a mobile Internet connection, this can create a back-door connection from the Internet to the information system. Numerous cases show that this type of vulnerability has impacted SCADA, substation and other control systems.

5 Communication and Control systems

The following chapter lists a lot of typical intelligent devices found in substation information communication and control systems. Each device is classified for Availability, Integrity and Confidentiality. All these devices have typical weaknesses from a security point of view. The tables points out these weaknesses and their severity. The tables also give possible "Counter Measurements" actions to reduce these weaknesses.

> ***NOTE:***
> *The Counter Measurement actions are explained in Chapter 6. The numbers in the Counter Measurements column refer to the paragraph that addresses a suitable action in terms of authentication, firewalls, encryption, multiple connections, remote disable of communication links and logging, to indicate best practices. If possible, standards are referenced that handle security for the given device.*

5.1 Point to Point Communication systems

5.1.1 Leased lines

Availability	Integrity	Confidentiality	Counter Measurement
High	Low	Low	See section 6.1, 6.3 and 6.4

Normally the availability is good, but these lines are easily found (for example lines on poles) and damaged. The integrity is low. Simple protocols are used. A 'man in the middle' could easily change data to give an operator the wrong impression of the actual situation.

Confidentiality is as with integrity, these lines are not hard to get information from.

5.1.2 Dialup lines

Availability	Integrity	Confidentiality	Counter Measurement
Normally high, but low in busy periods like New Year or during a disaster	Average	Low, see leased lines	See section 6.1, 6.3 and 6.4

The integrity is normally average. Compared to the leased lines, because of the connect/disconnect type of service we have the opportunity to authenticate the caller and server, and to get a better integrity from it. This improvement can be achieved by using the popular PPP protocol for link control. Devices that do not support this link control protocol (as may be often the case) can be connected by a port switch that does support. Constructing a 'man in the middle' is also slightly more complicated than with leased lines.

5.1.3 PLC (Power Line Carrier)

Availability	Integrity	Confidentiality	Counter Measurement
High	Very good	Very good	See section 6.1 and 6.3

The availability is normally very good, but unfortunately bad during outages when we are especially in need of information. Because of dangerous high voltages the power cable makes it hard to hack.

NOTE:
This system is not very reliable and not fast. Don't forget that the high voltage cable carrying the signal is hard to sabotage. But every transformer blocks the signal, forcing the construction of a bypass that can easily be hacked. So the only advantage lies in the fact that the bypass is placed in a (possible secure) building, the ring main unit or the substation, compared to communication lines that are easy to access.

5.1.4 Radio link

Availability	Integrity	Confidentiality	Counter Measurement
Low	Low	Mostly poor	See section 6.1 and 6.3

A radio link can be selected from a wide range of products. When using a low frequency product a long distance can be reached, with low selectivity that allows easy cyber access to the link. On the other side of the radio selection range is a very high frequency end-to-end link by GHz (Gigahertz) technology and line of site disks. In the second case tampering will not be unnoticed, and therefore have proper integrity and confidentiality. Because of the broad range of radio links, a general opinion is not possible. The approach will therefore be: be very careful, but use the good exceptions.

NOTE:
A secured communication link gives a not justified feeling of a secure solution. If the next station is hacked, the secured communication might still be used. But we use communication with a data source/sink that is harming this station.

5.2 Network Communication systems

5.2.1 Radio Network

Availability	Integrity	Confidentiality	Counter Measurement
Low	Low	Low	See section 6.1, 6.2, 6.3 and 6.4

These links are easily blocked by electromagnetic interference. An acceptable exception is perhaps the spread spectrum type of radios using combined encryption. Only for the spread spectrum type of radios the integrity and confidentiality is perfect. However the availability is still low. Most other radio system shows low performance for all three criteria.

5.2.2 Privately operated IP network

Availability	Integrity	Confidentiality	Counter Measurement
High	High	High	See section 6.1, 6.2, 6.3 and 6.4

We wrongly assume that hackers form no threat for private operated networks. The majority of the past attacks have been performed by possible dissatisfied (former) employees. Therefore we still need all the protection tricks like encryption and authentication.

5.2.3 Public operated IP network, like ADSL, SDSL, GPRS, UMTS

Availability	Integrity	Confidentiality	Counter Measurement
High	Low	Low	See section 6.1, 6.2, 6.3 and 6.4

Encryption such as VPN, SSH or SSL can make public networks save to use. Because of the huge recent improvements they are often faster, cheaper and more available than privately operated networks. Funny problems can be found when multiple links prove to be routed trough one single network node, making the availability vulnerable. Non-repudiation is normally not addressed, but providers do logging to improve their level of service, which can be used to reach non-repudiation goals.

This type of network is the most likely to have DoS attacks. Because of this it is a poor choice for time critical communication. For less time critical applications (power quality or metering) it should be considered as an alternative.

5.3 Substation Control Systems

Normally Substation Controllers do alarm logging and login logging. However they do not log security intrusion. This does not help to reach the non-repudiation objective.

5.3.1 Linux or Windows based Substation Controller

Availability	Integrity	Confidentiality	Counter Measurement
Low	Low	Low	See section 6.1, 6.2, 6.3, 6.4, 6.5 and 6.6

Using Windows or UNIX operating systems for Substation Control functionality may lead to a low availability. Careful maintenance and constant upgrading all virus and spyware patches keeps optimal availability. The benefit of these computers comes from their ability to run databases and having at least access control. But popular operating systems are sensitive to cyber attacks.

5.3.2 Real Time Operating system based Substation Controller

Availability	Integrity	Confidentiality	Counter Measurement
High	Low	Low	See section 6.1, 6.2, 6.3, 6.4, 6.5 and 6.6

By using dedicated real-time operating systems the availability is mostly much better. The sensitivity to cyber attacks is low due to the propriety character. However the functionality is lower, for example it has no relational database.

5.3.3 Bay controllers and IEDs Intelligent Electrical Devices

Availability	Integrity	Confidentiality	Counter Measurement
High	High	Low, normally not addressing security	See section 6.5 and 6.6

Recent security standards try to move from "protecting the lines" to "creating application level end-to-end security protocols". This is necessary because network bridging is defeating the secured lines security solution.

5.3.4 Station Bus

Availability	Integrity	Confidentiality	Counter Measurement
High	Low, protected by building	Low, protected by building	See section 6.3 and 6.4

This communication system in a substation is the heart of the present and future secondary system and it should really be better protected.

6 Technical considerations of building counter measurements

Already the following standards should be studied on how to secure Electric Power Systems information systems. For general IT-topics BS7799:2002 [6] and ISO/IEC 17799:2000 [7]. More specialized for SCADA areas we can reference ISA-TR99.00.02-2004 [8] [9] and AGA Report No 12 [10] and the NERC documents "Security Guidelines for the Electricity Sector" [12], and the "NERC CIP 002-009 standard" [13], "21 Steps to Improve Cyber Security of SCADA Networks," [11] Department of Energy (DOE) and ISO/IEC 10181:1996 Information technology -- Open Systems Interconnection - Security frameworks for open systems [14].

In paper [4] these documents are compared to each other.

TC57 is currently creating the standard IEC 62351 Data and Communication Security [5]:

- Part 1: Introduction
- Part 2: Glossary of Terms
- Part 3: Profiles Including TCP/IP
- Part 4: Profiles Including MMS
- Part 5: Security for IEC 60870-5 and Derivatives These security standards cover IEC60870-5-101 and 104 and DNP3.
- Part 6: Security for IEC 61850 Profiles
- Part 7: Management Information Base (MIB) Requirements for End-to-End Network Management.

It may still take some time to finish this new and very much needed standard. But most installed equipment is produced before this standard was developed. Therefore we urge to use other solutions. The following section contains technical considerations of building counter measures based on best practice to mitigate the security weaknesses that are discussed above.

6.1 Authentication

Availability	OK
Integrity	Not addressed
Confidentiality	Not addressed

Network sniffers (free to download from Internet) easily hack plain username and password systems. Combined with encryption, simple username/password systems are secure and easy to use.

Without encryption username and password authentication must be secure, such as the Challenge/Response system as used in PPP. But beware that only the user is authenticated and not the actions he subsequently takes.

For critical situations it is better to use 'strong authentication'. Here authentication is done with a device that holds a secret (normally an encryption algorithm) that can be checked. The device has to be activated by for example a PIN number, preventing misuse after theft.

6.2 Firewalls

Availability	Low, during an attack the firewall blocks
Integrity	Not addressed
Confidentiality	Not addressed

In office type networks, firewalls are used to safely connect the company local area network to the Internet. The firewall makes the user nameless to the outside world (good for privacy) and protects against attacks coming from the outside world. Only messages initiated from inside the local network are copied from the outside world to the local area network.

This is not very useful for accessing a substation from a SCADA system. A possible solution is to let the substation take the initiative. But a modern substation can be accessed for example on its web server. And a web server does nothing until accessed by somebody. This leaves us to a not accessible substation. Placing the web server in a demilitarized zone allows access to the server at the expense of switching of the cyber attack filtering of the firewall. Specialized firewalls meeting the requirements are available and we urge to use them despite the higher cost.

A firewall is mandatory when older systems without security features are connected to a substation or control room local area network.

With specialized companies, more advanced firewalls are available that use strong authentication and communication encryption. These advanced firewalls are save to use for SCADA purposes.

6.3 Encryption

Availability	High, when using a proper key scheme
Integrity	Perfect
Confidentiality	Perfect

Using encryption adds complete confidentiality to a communication or data storage. This removes all risks of sniffing and illegal command acceptance.

Key management is a drawback of encryption. This must be setup carefully. Keys with a short live will increase security. But the keys with a short live can block accessing the whole network by a DoS attack on the key server. Because SCADA communications are designed for low speed links, they pass few data per second. This allows the use of keys for a longer period, to avoid the blocking by a DoS attack.

On slow links, encryption can clash with real-time requirements. Some protocols require for example 50 milliseconds response time. If the encryption is setup to encrypt blocks of 250 bytes and we use a high link speed of 34-kilo baud, we still get a response time of approximately 150 milliseconds. If decreasing the response time or

increasing the baud rate is not possible, we will have to replace the protocol (and possibly the connected equipment).

A lot of information on encryption can be found in the AGA [10] document.

6.4 Multiple connections

Availability	High
Integrity	Not addressed
Confidentiality	Not addressed

The only defense against DoS attacks is using multiple connections combined with firewalls. Especially by letting the redundant connection sleep during normal usage makes it a hard target for hackers. The network setup should be similar to the setup of the primary power lines. This gives a N-1 property at a low price.

6.5 Remote disable of communication links

Older systems use dial up lines for remote service. These devices are often not equipped with security mechanisms to make things worse. Blocking these lines in a telephone switch or by a special modem is needed. Activation can than done only after a request from an IED supplier. This procedure is simple and allows for checking the supplier and his equipment.

6.6 Logging

Availability	Not addressed
Integrity	Not addressed
Confidentiality	Not addressed

Logging does not protect against any attack. But to learn about an attacker it is necessary to record as many information as possible. This information is needed by a security officer investigating an attack to setup a defense plan.

7 Conclusions and future developments

The level of security of the older and most current SCADA systems is not enough for the present cyber situation. To make things worse the new IEC-61850 standard has no provisions for security yet. Because of its open network type communication, it also opens the system for cyber attacks. This new communication standard is really dangerous if used in a network with a poor security design. Because the protocol does no longer compartment the communication, it may loose control over the whole grid. All older communication standards do not address security as well.

Using encryption on the dialup/leased lines and network links can increase the level of security. But take care to protect the key and name servers.

The problem of unintended bridging of the power information system to the Internet is still open for future improvements, such as Mobile Internet on a notebook used for service. A promising approach is the end-to-end encryption of data at rest and when communicated. However, the technology does not yet commercially exist for the field devices. This end-to-end encryption eliminates the threat of bridging between the Internet and the local area network (were the SCADA functions communicate). The bridging can still be there without being any threat anymore.

The second still not resolved problem is the DoS attack. This attack can however be defeated by using multiple communication links. Mostly these multiple links are already required for the N-1 criterion. Just don't place the multiple links in the same cable duct or network switch!

Security has become an accepted topic for information systems. But beware: for SCADA applications the standards are not yet available, they are still in draft. Equipment build according to these future standards will not be available for some time.

8 References

[1] "Managing Information Security in an Electric Utility", Electra No 215, October 2004, pp. 20-27.

[2] "Cyber Security Considerations in Power System Operations", Electra No 217, February 2005, pp. 15-22.

[3] "Cyber Risks Assessment in the Electric Power Industry", Electra, February 2006.

[4] "Some Guidelines fro Developing a Framework for Managing Cyber Security for an Electric Power Utility", Electra

[5] 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: 62351 "Data and Communications Security, http://www.iec.ch/

[6] BS 7799-2:2002, Information security management systems - Specifications with guidance for use.

[7] ISO/IEC 17799:2000 Information Technology - Code of practice for information security management.

[8] ISA-TR99.00.02-2004: "Integrating Security into the Manufacturing and Control Systems Environment," Instrumentation, Systems and Automation Society (ISA), USA.

[9] ISA-TR99.00.01-2004: "Security Technologies for Manufacturing and Control System," Instrumentation, Systems and Automation Society (ISA), USA

[10] American Gas Association (AGA): Series of AGA12 reports. http://www.aga.org/

[11] "21 Steps to Improve Cyber Security of SCADA Networks," Department of Energy (DOE), USA, http://www.esisac.com/publicdocs/21StepsBooklet.pdf

[12] NERC 2002. "Security Guidelines for the Electricity Sector", http://www.nerc.com/

[13] "NERC Cyber Security Standards (CIP 002-009)", http://www.nerc.com/

[14] ISO/IEC 10181:1996 Information technology -- Open Systems Interconnection - Security frameworks for open systems

[15] G. Dondossola, J. Szanto, M. Masera, I. Nai Fovino, "Evaluation of the effects of intentional threats to power substation control systems", International Workshop on Complex Network and Infrastructure Protection, CNIP 206 March 28-29 Rome, Italy.