NAPS 2003, 35th North American Power Symposium, University of Missouri-Rolla in Rolla, Missouri, October 20-21, 2003. pp. 559-566.

Security & Vulnerability in Electric Power Systems

David Watts

***Abstract*— Security of supply has been always a key factor in the development of the electric industry. Adequacy, quality of supply, stability, reliability and voltage collapse along with costs have been always carefully considered when planning the future of the electric power system. Since 1982, when world's deregulation process started, the introduction of competition at generation level brought new challenges, while the proper operation of the electric power system still require physical coordination between non cooperative agents. The increasing development of SCADA/EMS systems, the growing number of market participants, and the development of more complex market schemes have been more and more relying on Information Technologies, making the physical system more vulnerable to cyber security risks. Now cyber security risks look bigger than the physical ones. We developed a review of some of the vulnerability risks that actual electric power systems face, showing some implementation issues of it. We also comment some the steps that NERC is leading to ensure a secure energy sourcing to the U.S. Economy.**

***Index Terms*-- Vulnerability, Reliability, Information Technologies, Cyber attack .**

I. Introduction

Since the first electric deregulation process took place in Chile, in 1982, the deregulation process has been evolving through the time and many countries have introduced competition in their market looking for efficiency and lower energy prices. New markets has been developed relying every day in more modern and aggressive models, requiring complex interaction between an increasingly number of agents who face each other continuously in different markets (energy, capacity, ancillary services, transmission rights, etc.) and in multiple time frames (futures, day ahead, real time, etc.). Since the electric power system is only one and it requires real time coordination to work properly, new challenges has been arising [1].

The decentralization of the property and also the decentralization of the decision making process rely every day in more complex and evolving Information Technologies IT. In parallel to the increase of the number of market participants, we have faced an increase in the number of SCADA/EMS systems operating in the electric industry, raising the interdependency between the operation of the whole electric grid (including generation, transmission, distribution) and the operation of the wholesale electric market. The electric market and the electric power system are every day more closely tight. The operation of one depends on the continuous and reliable operation of the other [18].

Now the vulnerability of the power system is not mainly a matter of bulk power electric system or physical system, is every day more a matter of cyber security. A market participant unable to see accurately the market or a SCADA/EMS unable to control properly some facilities could be as disastrous as a terrorist attack to some key power plants or transmission lines.

Since September 11, 2001 the threat of terrorist attack has raised as a big threat to many areas of the US economy. Almost every economic and social function is based in some way on the sourcing of energy, telecommunication services, transportation, etc. An attack to these infrastructures would bring devastating effects on the economy and in the people's life [2][3][4].

As Massoud Amin explains in [5], from the power systems we can reflect on mainly three kinds of threats over society:

a) Attacks upon the power system.

Here the target is the electric infrastructure. For example, terrorists could attack simultaneously two substations or key transmission towers in order to cause a black out in a big area of the grid. Other example could be an attack to the electric market.

b) Attacks by the power system.

Terrorists could use some installations of the power system to attack the population, for example, using power plant cooling towers to disperse chemical or biological agents.

c) Attacks through the power system.

Terrorists could use some installations of the power system to attack civil infrastructure, for example, terrorists could couple an electromagnetic pulse through the grid to damage computer or telecommunications infrastructure.

We will focus our analysis in the first kind of threat, attacks on the electric power system itself. To contribute in this assessment, herein we develop an analysis of the existing material about vulnerability focusing in the interaction of the power systems with communication technologies.

Nowadays the power grid is not only vulnerable to the traditional terrorism (sabotage, bombing, etc.), but also vulnerable to the new terrorism that could produce multiple outages in the communication system or could attack the

D. Watts is with Department of Electrical Engineering, Universidad Católica de Chile, Casilla 306, Correo 22, Santiago, Chile (e-mail dwatts@ing.puc.cl) and is temporally with University of Wisconsin Madison (dwatts@wisc.edu) as a Graduate Student.

power system itself through the communication system. In order to face this new dimension we will revise cyber security as well. [10]

We also will briefly review the approach of the Critical Infrastructure Protection Advisory Group CIPAG to the vulnerability of the electric industry.

II. Initiatives of the Industry

After September 11, 2001, many efforts have been developed to protect the secure and reliable operation of electricity, gas, telecommunications, transportation, and financial infrastructure. The strong interdependence of these infrastructures can produce a cascading effect when one network is affected by a disturbance. [3]

A. Organizations

The Complex Interactive Network / Systems Initiative (CIN/SI), a joint program of the Electric Power Research Institute (EPRI) and the Department of Defense (DOD), is addressing the cascading effect based on the strong interdependence of the above mentioned infrastructures, trying to developed new tools and techniques that allow US infrastructures to self-heal in responds to threats, failures and other kinds of perturbations.

In the electric industry, the Standard Market Design (SMD) prepared by the Federal Energy Regulatory Commission (FERC) is including the Security Standards for the electric sector proposed by the North American Reliability Council (NERC).

The Critical Infrastructure Protection Advisory Group (CIPAG) coordinates the security activities of NERC, focusing in cyber, physical and operational security. They also interact with other organisms such as US Department of Energy (DOE), National Infrastructure Protection Center (NIPC), etc. [7]

B. NERC-CIPAG & Security

NERC has been in charge of the reliability (including safety and security) of the interconnected grid since 1968. It has developed many initiatives such as the followings:

Establishment of an Information Sharing and Analysis Center for the Electric Sector (ES-ISAC).

Development of a Public Key Infrastructure (PKI).

Development of spare equipment database.

Development of security guidelines for the electric sector.

1) Information Sharing and Analysis Center for the Electric Center

Due to interdependences between the different sectors of the economy, coordination between the private parties and the government is required to face the terrorist threat. The ISACs (Information Sharing and Analysis Centers) were created in the different industries to build a cooperative security planning and analysis, these ISACs are the communication channel within industry and government.

NERC hosts the ISAC [25] of the Electric System (ISAC-ES), it was working on September 11 and facilitated the necessary communication to secure key electric industry assets. [7] [21]

2) Public Key Infrastructure (PKI).

As Gent and Constantini explained in [7], PKI is a systematic approach to information security that connects policy and technology to establish a trusted environment to electronic businesses. It is based on public key cryptography and public key certificates, PKI provides privacy, authentification, integrity, and non-repudiation[1] in the digital market place. [21]

3) Spare equipment database.

In order to help electric companies to recover after a terrorist attack [7] one decade ago NERC created a spare equipment database. It helps to locate spare equipment for loan under emergencies, ensuring a rapid recovery. [21]

C. Security Guidelines

The *Security Guidelines* [26] [27] are mainly a compendium of practices, commonly accepted as best practices [23], to protect the critical facilities and functions, where each company define its own critical facilities[2] [7]. The Guidelines should be adapted to each company by themselves and should evolve through the time (as technology, organization of the market, power system and threat do). Also people in the company should be trained to success in protecting the company from the different threats. The main focus of the guidelines is Physical and Cyber Security [21]

The main components of the security guidelines are the followings:

a. Vulnerability and Risk Assessment
b. Threat Response Capability
c. Emergency Management
d. Continuity of Business Processes
e. Communications
f. Physical Security
g. Information Technology / Cyber Security
h. Employment Screening
i. Protecting Potentially Sensitive Information

We will briefly describe each of these guidelines:

[1] It means that a party cannot deny having engaged in an electronic transaction or having sent an electronic message. [7]

[2] Facilities if damaged have a significant impact on the ability to serve large quantities of clients for an extended period of time, have a detrimental impact on the reliability or operability of the energy grid, cause significant risk to public health and security.

a) Vulnerability and Risk Assessment

An initial step to identify critical assets to protect (Physical and Cyber assets), their vulnerabilities, risks, and countermeasures. [28] [37]

b) Threat Response Capability

A plan to help the company to develop actions and plans in response to threat advisories. The threat respond guideline is based on Threat Alert System of NERC. [29]

The ***Threat Alert System*** suggests specific actions that may be appropriate at each of the five levels of threat alert (Low-Green, Guarded-Blue, Elevated-Yellow, High-Orange, Severe-Red). They goes from following normal security standards (under low alert or green) to continuous monitor and inspections in substations or having medical emergency personal on site (under severe alert or red). [19] [20]

c) Emergency Management

Companies should be prepared to act under threat, people must be trained in how to follow the plans, respond plans must be coordinated with law enforcement officials. [30]

d) Continuity of Business Processes

Plans for relocating physical operations, allowing the company and its facilities to reduce the likelihood of prolonged interruptions. [31]

e) Communications

Ensures the effectiveness of threat response, emergency management and business continuity plans. Good and fast communications plans will ensure a fast and proper response of the workers and law enforcement officials. [32]

f) Physical Security

Mitigates the threat from inside or outside of the organization through deterrence, prevention, detection, communication, response, and corrective actions.

It is very important to protect employees, critical facilities and information from undesired parties. [33]

g) Information Technology / Cyber Security

Mitigates the threat from inside or outside of the organization with special consideration of computer network monitoring, intrusion detection, with particular care of SCADA/EMS systems, firewalls, and security protocols. [34]

h) Employment Screening

Provides guidelines to mitigate the threat of insiders, including contractors and vendors. (Ex: Hiring standards, pre-employment history checks) [35]

i) Protecting Potentially Sensitive Information

Reduces the likelihood that information could be used by people trying to damage critical facilities or interrupt the operations. It takes care of production, storage, transportation and disposal of physical and electronic information. [36]

III. Cyber Security Risks

A. Dependency on technology and SCADA systems

Industry has been becoming every day more dependant of computers and electronic communications, an interference on these technologies has become a more serious and likely matter. This fact requires collective attention to security, disaster recovery, and planning, in order to ensure continuity of service [6].

Some examples of disruptions of Supervisory Control And Data Acquisition SCADA has been faced on other industries; A dissatisfied former employee of a chemical company was detected while trying to disable some controls of the plants; A gas processing plant from a US petroleum company was hacked by a plant's supplier sabotaging the plant, shooting the services to homes and businesses in a Western European country, producing huge problems, losses and 6 month of investigations [6].

Different groups are developing standards, guidelines and procedures for mitigating cyber security risks, publishing specific actions to prevent unwanted break-ins [6].

There is no experience of hackers braking in the US power grid, but the experience in other industries raise the question if the power grid, natural gas pipelines, nuclear plants, water systems, refineries and industrial facilities that run similar control systems (sometimes based on internet) are vulnerable to cyber attack? [8]

Can a terrorist, a disgruntled employee, or a teenager cause lethal accidents and millionaire damages? [8]

These industrial control systems used to monitor and operate utilities and factories were developed without taking in count security issues. Their own nature makes them hard to secure, sometimes linked to WebPages [9].

Some security companies have found important bugs in the security of some electric utilities, for example article [8] explains how driving close to a electric substation, just using a wireless LAN card and a notebook, they connected to the system in five minutes because the system was not using a password [8]. After some minutes they mapped every piece of equipment in the control network and some minutes after they were able to talk to the business network going into several business reports.[8]

Article [6] explain that many workstations, servers and routers bring security protection mechanisms (themselves or through internet) but users or their organizations have no time or resources to configure the security settings of the piece of equipments. Even big companies with important IT Teams and resources have these problems [6]. Moreover, more than a 90% of the successful cyber attacks take advantage of known vulnerabilities and misconfigured operating systems, servers, and network devices. [6]

B. Wireless Intrusion

Wireless systems are especially vulnerable to attacks. Some people use these systems in their networks and feel secure because they think firewall would protect them from unauthorized access, and therefore some people don't use security features of the wireless equipment.

In fact, if you are close to a wireless system and you have a directional antenna such as *Pringles Antenna* (look at Google to know how to build an antenna with a can of Pringles), you can go into the network without need to overcome the firewall. [8] Wireless security standards are easily defeated, wireless transmitters use IEEE 802.11b and it has serious security flaws. Simply using free software, such as AirSnort and NetStumbler, a hacker can have enough tools to crack wireless codes within 15 minutes [8].

After they get the wireless encryptation key, they can use a freebie protocol analyzer like Ethereal or Sniffit to spy on the network [8].

At this point, they can see people login into different equipments (for example Programmable Logic Controllers PLC), and since people tend to repeat passwords, they probably could log into other PLCs and networks. The Institute of Electrical and Electronics Engineers IEEE is currently revising its standards and some software has been developed to overcome IEEE 802.11b security flaws. [8]

Dr. Douglas Maughan (from Darta ATO) resumes it saying: *more and more wireless equal more and more vulnerability*. [11]

C. Network Security & Encryption: SCADA, Modem, PLC

Application of conventional network security measures work well in IT environment, but it is not always possible to implement in industrial control systems. These systems assume that devices are competent to answer a password and identify itself, but most PLCs can't answer passwords. The problem is that PLCs, and SCADA systems were designed without security in mind. Designers implicitly assumed that these systems would be isolated, no connected to other systems, and also assumed that only authorized people would have access to the system, and it is not a good assumption today. [8]

The fact is that every day more and more employees have been replaced by automated controls at substations, pipelines, etc., and now thousands of these facilities are being controlled by SCADA systems linked to networks [8].

Nowadays, many SCADA systems carry some data through Internet in order to avoid more expensive private lines. In addition to this, almost all RTU's (Remote Terminal Units that coordinate a facility's automated field devices) or control systems are Web or Network enabled and often times we use these features. Also some breakers, switchgears and pumps have its own connections and can be managed through telephone lines. Many power plants and substations have many modems, being another easy target to hackers. They represent an alternative way to go into a network (like a backdoor). Hackers find these modems dialing phone numbers sequentially and once they are connected they can map the system and spy for passwords [8]. More secure systems use dial back modems (they respond to a password by dialing a confidential phone number for confirmation) this system are hacked by trying sequentially different passwords, when they enter the password they also send a hang up tone, in this way the hacker remain in the line and the modem's attempt to dial back has no effect.

Nowadays many field devices, designed to do specific tasks are still based on low cost micro processor such as Intel 8088 and they can't run encrypted authentication schemes fast. Article [8] explain that these systems can be easily hacked by using an protocol analyzer software, intercepting the control messages from the communication site, and taking control of the network by injecting their own signals. [8]

A direct reapplication of traditional IT policies is not the solution in these systems, for example you can't look down a console in a power system because the operator made three mistakes while entering his password. Because of that many organisms in the industry are developing procedures and standards to improve control systems security (Institute of electrical and electronics engineering IEEE, Instrumentation Society of America, International Electrotechnical Commission).

In the short term some people is working in better uses of encryption. Encryption techniques applied to SCADA would help to avoid the effect of hackers watching their data and also would keep energy traders from gaining inside information to face the market with advantages or influencing a company's operation. Since utilities have already installed many SCADA systems without this technology, it would take 10 to 15 years to have all their SCADA systems operating with these new standards. [8]

The communication era presents SCADA's security flaws as the main vulnerable point from remote point through Internet. The new standard would be install dedicated encryption devices between the SCADA RTU and the modem that link it to the Internet, in this way you could authenticate the sender and the hacker only could see encrypted data. [8]

Encryption would help to prevent remote attack on data but hackers can still attack corporate networks an through these networks attach key facilities (often times the corporate networks is connected to the SCADA system). With regard to corporate networks (usually based on Windows or Unix), you can secure your computer network by avoiding use wireless systems (because their security flaws) in strategic networks, you should use a rigorous network security, use a role based security (give different privileges to different people) making difficult an attack of an insider, use secure modems, implement better password policies, hire well-trained people with practice in response and recovery procedures. [8]

Security in IT systems require protect critical core servers, following this strategy most of SCADA Operation centers in transmission and distribution companies has been

protected to physical attacks, they usually can face fire, bombs, etc, without major complications. All the critical equipment here (computers, communication equipment, etc) is replicated inside the protected area.

On the other hand, the "real" real time management of the facilities in a generation u other industrial plant for example, is made by PLCs that control the process of the plants (is not being made by the SCADA). But usually these PLCs are easier to access than SCADA systems. This fact shows the need of re-think a different architecture scheme to apply to the electric system, because the before mentioned strategy is not protecting enough the core of the process. [8]

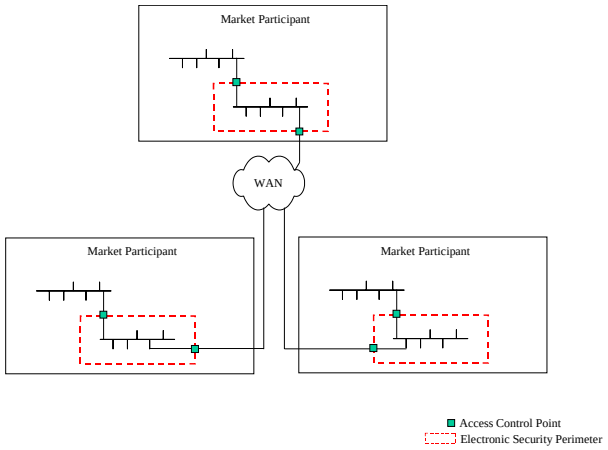

Fig. 1. Market Model (Source: NERC-CIPAG) [39]

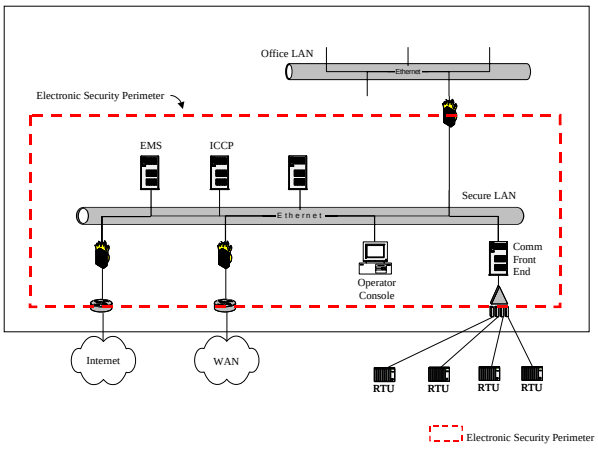

Fig. 2. Electronic Security Perimeter (Source: NERC-CIPAG) [39]

IV. Cyber Security Standards for the Wholesale Market

NERC's (CIPAG) security standards are mainly focused on Cyber Security [24], including also the Physical Security of the Cyber Assets[3].

The interdependency and mutual vulnerability of the wholesale electric grid and the wholesale electric market requires to ensure that market participants understand their role in maintain market stability. They have to identify their critical cyber assets related to the market and place an appropriate Security Program that must cover governance, planning, prevention, operations, incident response, and business continuity. [18]

As shown in figures 1 and 2, market participants must define their electronic security perimeters and identify their boundaries and defenses. They must identify also the entry an exit points and the requirements for access control. [18]

Here the *Electronic Security Perimeter* is defined as the border surrounding the secure network where the critical cyber systems are connected. All computer connected to the secure network is considered within the electronic border even if they are not defined as critical systems per this standard. Only authorized data traffic is allowed and therefore Data communication in and out of the secure network are passed though electronic access points (eg firewalls, routers) [18].

The standard also requires access control to the physical security perimeter, only authorized personal (trained in cyber security) could go into this perimeter. [18]

Each market participant must submit self-certification of the compliance of these cyber-security standards to FERC in order to keep being part of the market. [18]

A. Actions

From security standards for electric market participants and cyber security standards [18] we obtained the procedures implemented to protect critical cyber assets in the security perimeter. They must consider [22]:

1) The use of effective password routines that periodically require changing of passwords, including the replacement of default passwords on newly installed equipment;

2) Authorization and periodic review of computer accounts and physical access rights;

3) Disabling of unauthorized (invalidated, expired) or unused computer accounts and physical access rights;

4) Disabling of unused network services and ports;

5) Secure dial-up modem connections;

6) Firewall software;

7) Intrusion detection processes;

8) Security patch management;

9) Installation and update of anti-virus software checkers;

10) Assurance that telecommunications assets and channels connecting critical cyber assets between electronic security perimeters or with other market participants are secure. (Example: telemetry that is exchanged directly between market operations systems and power plants and substations.)

11) Operator logs, application logs, and intrusion detection logs shall be maintained as appropriate for the purpose of checking system anomalies and for evidence of suspected unauthorized activity.

B. Implementation Issues

[3] Computers, software, and communication network that support, operate or interact with the wholesale market operations. [18]

The first issue with the implementation of these standards is the higher cost. To increase the security standards in the system brings higher operational costs and also requires important investments. To start a new program of considerable investment in a company that operates in the market requires many months, semesters or a year, in order to include this program in the investment budget of the next year (more equipment, software, personnel, etc., usually require share holder approval). [38]

The second issue is the implementation of a transition period, where companies that are currently not accomplishing the standards are allowed to keep operating in the market without penalty in order to give them a reasonable time to improve their security standards. Once this period is finished the companies that are not accomplishing the standards should not be allowed to keep working in the electric market because they represent a risk for the whole power system. A proper transition time is very critical, a mistake could cause companies going out of the market. Maybe you can accept a couple of inefficient generators going out of the market, but can you have transmission companies not allowed to participate in the market because of their low security standards?. What would happen with the generators connected to these lines?. Again, the electric power grid requires coordination to operate properly and one bad link of the chain can cause a disaster. A transmission company can not be easily replaced. What would happen with the supply contracts of a non-compliant wholesale market participant if immediately loose access to the wholesale market?.

Other issue emerges when different market participants merge in one, and they have very different cyber security systems and procedures and they may not be easily merged with the ones of the pre-existing company.

Finally, to provide a report to the authority with all the flaws that your security system have is another source of risk (it is a requirement to inform authority about security problems). Now not only your security manager and his team would know about these secret flaws, the authority and may be many employees could have access to this document and nobody can assure that the authority will take care of these documents as confidential as you do.

With regards to potentially sensitive information, workable competition in the market requires to eliminate all sources of asymmetric information, this fact and the cost economies that internet brings to the companies has driven a tendency to publish almost all data in web pages, even when part of these data could be used against the company.

After September 11, 2001 most of the critical data of the electric companies have been taken out of the WEB, an now is provided to market participants u other related agents in "a need to know" base [17]. The lack of transparency or a small delay in process a requirement of data can produce a problem of asymmetric information, since information is valuable not only for market participants but also for the whole market, this could bring some imperfect competition and in this way we could face some loose of market efficiency.

Every day the automated systems are moving toward more open architecture, potentially increasing security vulnerabilities [12]. The SCADA/EMS are every day more standard and you can access key information/documentation of theses systems through Internet with their vendors. The use of Window as a base to the SCADA/EMS systems has been also increasing, and it is not clear that these operating systems can achieve the reliability of other less commercial alternatives.

C. Some Practical Experience

Some South American countries have had some experience developing systems thinking in terrorism, but they where built expecting physical attacks, nowadays the threat has an additional dimension, Cyber attack. Some decades ago, various Latin American countries faces military dictatorial governments, their counterparts, in absence of the democracy and freedom of speech, started protesting by using bombs in transmission lines, substations, etc.

In Chile transmission and distribution companies reacts increasing the security measures mainly in the following ways:

Keeping mobile substations, power substations ready to connect to the system, mounted permanently over wheels accompanied by a contingency plan, coordinated with law enforcement officers to manage the movement of these huge units through the city. This option is available for very limited transmission voltages, but it is more useful for step down the voltage from transmission to distribution levels.

Establishment of some standardization of power transformers, mainly at low transmission voltage levels and for transmission / distribution voltage levels. It is only available for low power levels 10, 15, 25, 50MVA. Each class must use the same kind of base, similar shapes, etc.

Keep a stock of power transformers installable in a couple of days (very expensive, usually a couple of units only).

Use a double fence non-scalable scheme in the surroundings of the power substation, very tall and built with more resistant materials than the typical ones. They also use an additional interior fence as usual. Alarm systems were installed between fences to notify workers and law enforcement officers about intruders there. The main door gate is 4-5mts high, of steel and with non-scalable system.

Substations' access key used to be based on a proprietary system not available in the commerce but very expensive.

Transmission lines were almost not protected, only inside the city some small fences were located where a car could crash the towers and regular fences and "wires" were installed to avoid the approximation of people to the towers' bases.

After more than two decades of deregulation in Chile and in absence of terrorist attacks, some secure physical policies have been forgotten in order to reduce "unnecessary" costs. It looks like that is the actual trend, even in the US now (after 911) the physical security standards do not look very

high, the focus is Cyber security.

D. Multiple Contingency & Islanding

A few countries have developed some smart islanding scheme to face multiple contingency events. The Brazilian Defense Plan, developed by ELECTROBRAS, CEPEL and ONS, is one of the most revolutionary ones [13]. The main objective is to minimize the cascaded outages as a consequence of multiple contingencies in the Brazilian Interconnected Power System.

When doing contingency analysis we traditionally use N-1 or N-2 criteria [14] and we assume that 3, 4 or more outages are very unlikely to occur and we simply don't consider them. The problem is that these events are less likely to happen, but their impact is usually huge (a blackout for example), then the expected value of the losses due to these events is still big and must be carefully considered. We also know that, for example, often times a bus fault bring some line outages and with this, we could start a sequence of events that could collapse the system, the fact is that often times the failure in one installation is closely related to the failure of other installation. They are not fully independent as we assumed when we compute N-1 or N-2 contingency analysis. Some countries have even experienced N-30 and N-36 contingencies.

In order to minimize the effect of big disturbances the Brazilian system was divided in 7 areas, applying a hierarchy structure of its protection system. They added some intelligence inside each area by installing around 10 or 20 PLCs in the different substations of the area and one Master PLC. The communication topology connects all these substations with the master one, and the master of each zone is connected at least with the masters of all the neighbors' zones. The national supervisory system also communicates with all the master PLCs.

They developed the concept of a Network Security Matrix as a risk indicator associated to major disturbances in the electric system. They implemented a Special Protection Scheme to limit the impact of losing each installation, they also modified the substation layout and protection system to achieve a lower risk of outage in their installations.

The most interesting part of this implementation is the fact that since the PLC network is permanently monitoring the system, the PLC network detect the fault very fast and the Master PLC decide and order generation drop and load shedding obtaining a stable operation in a couple of seconds. This system is capable to take care of losing a complete substation, and this is a really extreme contingency.

A critic to this kind of systems could be that they don't provide a particular answer to all different possible contingencies, but we can design this scheme to deal with some scenarios and after that we can test it under other scenarios to make sure it is robust (William Mittelstadt). Luiz Pilotto (from CEPEL) also said that the model implemented in the PLCs should be evolving along the time. [15]

Massoud Amin from EPRI explained that EPRI would be starting a project called adaptive islanding (it is coming out from the complex interactive network and would be developed with Iowa state university and University of Washington) to face emergency control, looking for remedial action schemes in contingency analysis. This project would generate methods to minimize load drop, to minimize load shed, to help system self-heal, and to recover the system back. He pointed out the fact that you have to drop more load at earlier frequency as frequency is going on instead of waiting for it. Ram Adapa (from EPRI) pointed out that when studying adaptive islanding they learned that the rate of change in frequency and the frequency are good inputs to do adaptive islanding. [15]

V. Conclusion

The interconnection of old SCADA systems to internet, networks or telephone lines, and the every more intensive use of computer networks and wireless systems have risen the fact that potential terrorists, bored hackers, unhappy employees, and smart kids around the world, could access the controls of power systems and hurt countries in one of the key factors of their economies, producing billionaire losses in almost all the sectors of their economies.

We have presented the scale of this problem, some examples, and the main measures and practices that the electric industry must be taken in order to reduce these risks as much as is economically desirable.

Since some risk still remain, we need to reduce at a minimum the threat of a cascading failure of the electric power system and the electric market. It requires important changes in the way we have though the system [16], and its architecture, many research is being performed in modeling complex interactive networks, the future architecture of the system could switch towards a more robust and adaptive infrastructure [72], maybe in the future the infrastructure will be able to self-heal in response to threats, failures, and other perturbations as mention M. Amin [3] in *Towards Self-Healing Energy Infrastructure Systems*.

Some countries have started moving towards network schemes that provide some intelligence to the grid, isolating the failures before they destabilize the whole system, intelligent adaptive islanding looks like a good next step in electric power industry. And maybe the following step will be similar to the one mentioned by Wired magazine, S. Silberman, July 2001. He said: *The best minds of electricity R&D have a plan: Every node in the power network of the future will be awake, responsive, adaptive, price-smart, ecosensitive, real-time, flexible, humming-and interconnected with everything else.*

VI. REFERENCES

[1] Watts David, Atienza Paulo, Rudnick Hugh, Second Generation Reforms in Chile, Power Exchange Model. The Solution?, Second IASTED International Conference, Power and Energy Systems, EuroPES 2002, Crete, Greece, June 2002.

[2] Amin Massoud, Modeling and Control of Complex Interactive Networks. *IEEE Control Systems Magazine*, February 2002.

[3] Amin Massoud, Towards Self-Healing Energy Infrastructure Systems. *IEEE Computer Applications in Power*, January 2001.

[4] Amin Massoud, National Infrastructure as Complex Interactive Networks. *Automation, Control, and Complexity: An Integrated Approach*, Samad & Weyrauch (Eds.), Jhon Wiley and Sons, pp 263-286, 2000.

[5] Amin Massoud, Security Challenges for the Electricity Infrastructure. *Supplement to computer, Security & Privacy 2002*.

[6] D'Amico Esther, Cybersecurity gains momentum, global and national groups introduce guidelines, Chemical week, August 21, 2002, vol. 164, issue 33.

[7] Gent Michael, Constantini Lynn, Reflections on Security, IEEE power & energy magazine, January/February 2003.

[8] Brown Alan, SCADA vs the hackers, can freebie and a can of Pringles bring down the U.S. power grid?, Mechanical engineering, New York, December , vol. 124, issue 12.

[9] Piazza Peter, SCADA on Thin ICE, *Tech Talk*, October 2002.

Documents from NSF-OSTP Technical Workshop:

NSF-OSTP Technical Workshop on Information Technology for Critical Infrastructure Protection, September 19-20, 2002 - National Conference Center, Lansdowne, VA. The following presentations of this workshop were cited in the present paper:

[10] Thomas Robert. *NSF/OSTP Workshop on Information Technology Research for Critical Infrastructure Protection (unnamed)*, September 2002.

[11] Maughan Doug, Information Assurance / Critical Infrastructure Protection, Hard Problems (and Research), DARPA ATO, September 2002.

Documents from NSF-EPRI Workshop:

NSF-EPRI Workshop on Urgent Opportunities for Transmission System Enhancement, October 12, 2001. The following presentations of this workshop were cited in the present paper:

[12] Amin Massoud, EPRI, Electricity Infrastructure Vulnerability, September 2002.

[13] Pilotto Luiz. *Brazilian Defense Plan Against Extreme Contingencies*, September 2002.

[14] Mittelstadt Bill, Power Infrastructure Vulnerability, September 2002.

[15] Workshop report, Moderator: Massoud Amin EPRI, Sesion 4: Power Infrastructure Vulnerability, September 2002.

[16] McCalley James, Thrusts for addressing Systems Vulnerability, September 2002.

Documents from NERC:

The following documents prepared by NERC were cited in the present paper:

[17] NERC's comments in response to the NOPR that the Commission issued on September 5, 2002 on the subject of protecting critical energy infrastructure information.

[18] Final CIPAG comments of Security Sections of FERC SMD NOPR

[19] Threat Alert System and Physical Response Guidelines for the Electricity Sector

[20] Threat Alert System and Cyber Response Guidelines for the Electricity Sector

[21] Electric Industry Initiatives Reducing Vulnerability to Terrorism Presentation by Michael Lynch at the NARUC meeting.

[22] Proposal for FERC Security Standards for SMD

[23] CIPAG Presentation on FERC Security Standards , FERC SMD Conference

[24] CIPAG Security Standards Self-Directed Work Team SCOPE Document

[25] Hearing Before the United States House of Representatives, Committee on Energy and Commerce, Subcommittee on Oversight and InvestigationsTestimony of Lynn P. Costantini, Director - Information Technology, NERC

[26] Security Guidelines for the Electricity Sector: Version 1.0. It includes 13 individual Security Guidelines:

[27] Guideline Overview

[28] Vulnerability and Risk Assessment

[29] Threat Response

[30] Emergency Plans

[31] Continuity of Business Practices

[32] Communications

[33] Physical Security

[34] Cyber Security

Cyber Security Risk Management

Cyber Security Access Controls

Cyber Security IT Firewalls

Cyber Security Intrusion Detection

[35] Employment Background Screening

[36] Protecting Potentially Sensitive Information

[37] Electricity Sector Response to the Critical Infrastructure Protection Challenge

[38] Addendum to Final CIPAG comments of Security Sections of FERC SMD NOPR

[39] Electronic Security Perimeter diagram included in Final CIPAG comments of Security Sections of FERC SMD NOPR

VII. BIOGRAPHIES

David Watts is a researcher in the Electrical Engineering Department at Catholic University of Chile. He obtained his B.Sc. and M.Sc. degrees in Electrical Engineering from Catholic University of Chile. His research and teaching activities focus on the economic operation, planning and regulation and tariffs of electric power systems. He has been a consultant with utilities and regulators of Bolivia and Chile.