SECURITY CONSIDERATIONS FOR ENERGY AUTOMATION NETWORKS

Albert Treytl[1], Peter Palensky[1], Thilo Sauter[1,2]

[1]Vienna University of Technology Institute of Computer Technology
Gußhausstraße 27-29/E384, A-1040 Vienna, Austria
{treytl, palensky}@ict.tuwien.ac.at
[2]Austrian Academy of Sciences Research Unit for Integrated Sensor Systems
Viktor Kaplan Strasse 2, A-2700 Wiener Neustadt, Austria
thilo.sauter@oeaw.ac.at

Abstract: Modern society relies on a reliable energy distribution network. Recent incidents such as the infiltration of a U.S. nuclear power plant together with the impacts of big power outages call for security measures to guarantee supply with energy. This article will deal with security goals, attacks, and protection mechanisms for energy automation systems. Nevertheless many of the discussed issues and solutions also apply to other large scale automation systems.

Keywords: security, power distribution and automation, security threats, access control, security requirements.

1. INTRODUCTION

Power outages during the last years clearly show that modern society depends on a reliable electric energy distribution network. Although most of these disasters stem from natural sources such as ice storms or dropped-out network components such systems are also vulnerable to malicious intentional attacks.

Many research activities deal with the problem of reliably distributing energy, preventing under and over voltage as well as failure of components. Solutions to the manifold threats result in automatic generation control (AGC), energy management systems (EMS), or special protection and remedial action systems (SPS/RAS) (Tomsovic, 2005)). All these systems increasingly rely on communication networks that allow collecting data and sending appropriate commands. In general there exist two parallel trends in energy automation (Bertsch, 2005):

1. centralization by moving network control to regional or even nationwide control centers,
2. decentralization by deploying "intelligent" components and "decision authority" locally.

Both trends demand for communication networks to allow for transport of the necessary information. At the moment there is still little awareness of security in these communication networks – i.e., measures that ensure a state of inviolability from hostile acts or influences –although risks are known, e.g., (U.S. Nuclear Regulatory Commission, 2003). At the moment many systems rely on the principle of security by obscurity by simply keeping information about the network undisclosed.

The integration of energy automation networks into public networks such as the Internet (e.g. tunneling of SCADA (Supervisory, Control and Data Acquisition) messages) and the increasingly distributed nature of network equipment increases the aspect of security. The authors are currently leading a project in this area called REMPLI (Remote Energy Management over Power Lines and Internet[1]), which connects automatic meters at the customers' premises via the medium and low voltage power lines with regional control centers (Sauter, et. al., 2005). A special issue of this project is the integration of security issues right from the beginning on.

This article will analyze the situation of security in energy automation systems ranging from security on low-level automation networks to the security of

[1] The REMPLI project is supported by the European Commission NNE5-2001-00825; (www.rempli.org)

Fig. 1 The Austrian high voltage 380kV grid, (Fischer-Drapela, 2003)

energy trading networks. Although the focus is on energy automation most issues also apply to classical (vertically integrated) automation systems. Section 2 will describe threats and risks and the resulting security goals. Section 3 will show common attacks. Finally section 4 will indicate possible solution to the mentioned problems.

2. SECURITY GOALS

Electric power systems rely on a highly distributed and pretty complex infrastructure. This includes the distribution lines, power plants, protection systems, SCADA systems, but also financial mechanisms like trading agreements, schedules or balance groups (Werner, 2002). Traditionally, all these systems were isolated, with no or no common security concept behind. Recent developments like the liberalization of the energy market, increased competition, and the need for cutting costs lead to two trends that both increase the need for sophisticated security measures.

First, in order to stay competitive, infrastructural investments were minimized. Unlike in former times the European power grid is no longer an over-engineered "copper plate" the utilities and transmission and distribution network providers are operating their equipment on the edge. Situations that were unthinkable before are now normal, like exceeding the thermal load limits of transmission lines multiple times per year (Fischer-Drapela, 2003). Such a system is weak and fault-prone. The increase of formerly unknown blackouts shows this very clearly.

Second, IT is changing the energy business in every aspect. Electronic bills, remote administration of equipment, automated meter reading and other IT disciplines are used to be faster and more efficient than competitors. The link of all these IT systems to globally available communication infrastructure like telephone networks or the Internet lead to a new situation in which intruders do not need to be physically present: they can attack remotely. These two ingredients ultimately yield a weaker system with more points of attack than before.

Each subsystem of the energy business might take measures for securing their processes, but the "big picture" is sometimes not considered. Obviously non-critical events can be composed to a catastrophe with the right coordination applied: Let us assume the following – intentionally incomplete – example: A large city – the subject of our attack - is supplied via two non-redundant lines, each with its own transformer station. The IT equipment of the local utility is infiltrated by a sleeping computer virus that can be activated remotely. Via this virus, it was possible to get information from the utility's file servers such as telephone numbers of insecure AMR and SCADA equipment, trading partners and load plans, passwords, etc. Using this information, it is possible to estimate when the system is on its limits. Combined with faked trading and scheduling requests, attacks to the SCADA equipment and a collapsing IT department (computers, telephone, etc.), the utility would neither be able to avoid a provoked overload nor to react to it in the appropriate manner. Automatic, and non-networked, protection mechanisms would deterministically switch off parts of the distribution network. If the attacker would plan and coordinate this very carefully, this could lead to an arbitrary chain reaction, as it sometimes happens coincidentally.

This example naturally requires the application of multiple types and steps of attacks, but is not unrealistic. The U.S.-Canada power system outage in August 2003, although not initiated by an active attack, is a vivid example for the consequences of multiple failures inside the power grid. Sometimes there is even no need to find out weak points of the energy grid via hacking the servers of a utility. Instead it is possible to find out potential points of attack via journals (Brauner, 2004). Fig. 1 shows for instance the well-known weak points of the Austrian high voltage grid.

It is important to note, that the entire attack affecting widely distributed components is done by means of information technology. There is no need to recruit and coordinate a large amount of persons to cause all these disturbances that finally lead to the desired collapse.

To protect the automation systems and IT infrastructure of (energy) automation networks in general the following security goals can be identified:

- Confidentiality (privacy or secrecy) prevent unauthorized disclosure or traffic flow from analysis by unauthorized entities
- Integrity: no unauthorized entity (including accidental alterations) must be able to change data without the change being detected
- Availability: data is at hand when needed
- Authentication: origin of data is proofed
- Authorization and access control: determines what an entity allowed to do once you are authenticated and allowed access
- Non-repudiation: allows to legally prove that a certain event or action was done by a certain entity.

Following the first three most important goals often the abbreviation CIA is used.

Table 1 Threats and risks to powerline based energy automation system REMPLI

direct manipulations of input and output values	high	high
manipulation or replacement of equipment	medium	medium
manipulation and insertion of data into the Private Network	medium/ high	medium/ high
manipulation and insertion of data into the PLC network	low/ medium	low/ medium
denial of service	high	high

It is important that all threats to a system security can use the energy network as well as the superposed communication network. Although there are a lot of publications dealing with the energy aspect, there is only little awareness for the security of the communication system. Table 1 exemplarily lists the threats and risks to the above mentioned security goals for the REMPLI project that uses a medium and low voltage power line based communication system as well as a private IP-based network to access electricity meters at the customers' premises on a broad scale. The risks analysis of the REMPLI project (Treytl and Sauter, 2005) indicates the following important issues:

1. the most relevant goals for today's communication networks are integrity and authorization preventing the active misuse of the infrastructure
2. Attackers will choose the easiest point. E.g., in REMPLI an attacker would rather disconnect the meter from the communication system than hacking the communication system.

Confidentiality and non-repudiation are not important goals since the systems are usually only used by one company, but will gain importance in the future when communication infrastructure are shared between multiple companies. Similar research projects such as (Selma consortium, 2005) obtain similar results.

Even if attacks by means of information technology are not yet as developed as they could be, they will certainly gain more and more relevance, since the costs of such attacks are very low compared to traditional physical attacks like blowing up selected transformer stations in a coordinated way. In general there is an increasing need to protect systems actively. The still very common attitude of security by obscurity – i.e., keeping essential information about a system confidential – is no longer an appropriate measure against serious attacks.

3. ATTACKS

Attacks to automation systems can be classified in various ways. One classification uses the origin of attacks which can be divided into internal and external sources as well as intentional and unintentional attacks. Another possibility of classification is the kind of harm done to the system. In this rating, attacks are in general associated with one of the following classes:

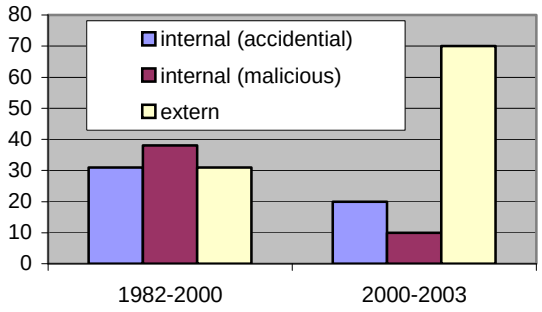

Fig. 2 Attack sources for automation systems [% of incidents] (British Columbia Institute of Technology, 2005)

1. eavesdropping of data,
2. modification of data,
3. fabrication of data, and
4. interruption of communication

Finally, attacks could also be classified by the technology used such as Viruses, Worms, Trojans etc. or by the impact such as in (Tomsovic, et. al. 2005), who classifies by attacks upon the power system, attacks by the power system or attacks through the power system. For this article the focus should be on the first two classes since these show technology independently the threats to automation systems.

3.1 Source of Attack

For classical office communication systems various sources concerning information on security exists, e.g., CERT Coordination Center (www.cert.org), and in general information about recent attacks becomes public quite fast. For automation systems the situation is different and information is hardly made public. The industrial security incident (ISI) database maintained by the British Columbia institute of technology (British Columbia Institute of Technology, 2005) and the reports of the U.S. nuclear regulatory commission are two of the rare yet restricted sources for information.

Owing to the fact that automation systems have been located in restricted areas and that knowledge about the systems was not made public, attacks from insiders have been a major source of threat. In the last years this situation changed and attacks from the outside are becoming more frequent.

Two trends caused this increase of external attacks: first, automation systems became interconnected with other automation networks (horizontal integration) as well as with management and administration networks (vertical integration) – automation networks are no longer island solutions. Second, standardized components are replacing proprietary solutions. Typical examples are operator stations which are based on common operating systems such as MS Windows or Linux.

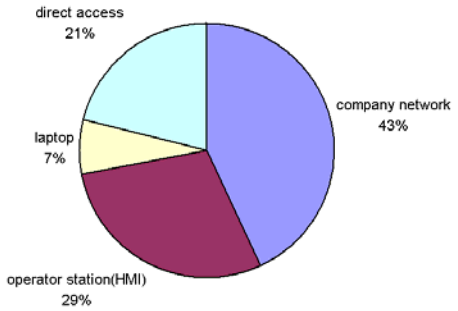

Fig. 3 Infiltration of automation networks listed by intrusion path

Both facts allow for electronic remote – no physical presence in a restricted area is necessary – and automated attacks such as worms or viruses. Nevertheless it must be clearly stated that standardized components are not less secure than proprietary ones. In general, standardized and wide spread components undergo a better security audit, but once a weakness is discovered it can be used more easily since it can be applied not only to one system but to multiple ones. As an example the misuse of the Maroochy Shire sewage system [14] – the attacker flooded parks and a river in an Australian town with sewage – was based on an exploit of a weakness of the WEP encryption algorithm of the IEEE 802.11b wireless LAN used in the system. For the intrusion a tool available from the Internet was used.

Another important issue is whether an attack was done intentionally or accidentally. Especially in view of remote maintenance this is a critical issue since the majority of systems, once access is granted, do not apply any further security measures such as restricting access to units that an engineer is responsible for. Fig. 2 shows clearly that the number of accidental attacks is already beyond the number of malicious insider attacks. Since the estimated number of not reported incidents is around 90% (for all kind of attacks) the share of accidental wrong operation will most likely be much higher.

3.2 Attacks on Automation Level

Attacks on the automation level are manifold and it would go far beyond the scope of this article to list them all. Beside attacks which are tailored to a particular system – the range begins at knowing the telephone numbers of SCADA stations and ends at complex tasks like protocol re-engineering - a special focus should be set to automated attacks and exploitation of standardized protocols.

Automated attacks, which at the moment are not directly aiming at automation systems, use means of Trojan horses or Internet worms to intrude utility equipment. The Internet worm Slammer (2003) or Code Red (2001) are typical representatives of such automated attacks. It infiltrated control systems of the U.S. nuclear power plant Davis Besse and other industrial automation systems. The typical points of infiltration were Internet connections (36%), dial-up IP connections (12%), wireless systems (8%), plain telecom networks (8%), trusted connections (4%) or SCADA networks (4%) (Byres and Lowe 2005). Fig. 3 shows the paths of intrusion. Interesting are the high rates of intrusion via the company network but also the direct infiltration via operator control stations. The conclusions that can be draw are that companies as well as automation networks are no longer isolated networks and no special knowledge is necessary to initiate such attacks. With the availability of tools to create viruses and worms by click and drop and irrespective whether the malicious code is introduced by an unprotected laptop or directly via the Internet, the network, or relevant network segments must be protected.

Another sensitive area is the denial of service (DOS) attack which cuts off control stations from the network. In general three kinds of DOS attacks can be distinguished:

1. DOS by overloading the device
2. DOS by overloading the connecting network
3. DOS by congesting a “parallel” network

Whereas the first type of attack blocks a device by requesting the intended service of the machine too frequently, the other types block the network by congesting or interrupting the network. Especially type three is hard to account for: A particular incident of this type has been the loss of monitoring capability due to the side effects of an overload cause by the Slammer worm: although the utility company had a frame relay connection with guaranteed bandwidth, one segment which was tunneled over an ATM line broke down by the unlimited increase of a parallel Internet connection. The same might also happen to normal GSM or POTS systems when in emergency situation or during extraordinary traffic situations no free entrance points of the telephone system are available.

Additional to the total denial of service discussed before, heavily congested networks also introduce additional delays that might severely affect SCADA operations which sometimes require soft-real-time behavior. Concerning these delays the experience gathered by the authors in the REMPLI project showed that timing requirements are seldom clearly specified for remote access in energy management applications. Often the capacity of a 9600 kbit per second modem line is demanded although – seen from the application level – much higher delays would be acceptable. This fact is quite noticeable if security devices need to be integrated in low-cost devices like meters.

3.3 Attacks on Energy Management Level

Beside the on-line connectivity of distribution equipment, transformer stations and energy meters there are plenty of other processes in the energy business that more and more rely on global communication channels with questionable IT security.

Some utilities still use plain text e-mails with spreadsheet documents to exchange energy business data such as load charts or load estimations. Such e-mail based, non-secured communication can easily be intercepted, manipulated, or faked.

Business processes such as exchanging roadmaps will in future be more and more based on standards in order to achieve a higher level of interoperability and efficiency. The natural level of obscurity that today's proprietary intermediate solutions offer will then be lost. A top-level candidate for exchanging business data, especially for the energy business, is ebXML (van der Togt, 2003). ebXML uses XML as a means of transport and a means of interoperability for electronic business (Patil et al. 2003). It is clear, that there are entire teams working on making such an important business tool more secure.

(OASIS security team, 2001) names the Security Assertion Markup Language (SAML), XML encryption, WebTrust principles, XML Key Management Specification (XKMS) and various public key infrastructures (PKI) as necessary countermeasures to potential security risks of electronic business with XML-based data.

Business applications that act as an Internet service platform like the JEVis system (Palensky, 2005) face an additional problem. Applications are typically hosted on an external server providing all databases, applications, and connectivity. When multiple users host their proprietary data on this server, they want to be assured that the other users – possible competitors – get no access whatsoever to their data, under no circumstance. Therefore, beside the proper user management, access rights and database design, the usage of virtual private databases within one database, as Oracle9i offers it, or even more sophisticated measures are necessary (Dwivedi et al., 2005) to achieve the need of privacy and protection of business critical data.

4. SYSTEM PROTECTION

This section will deal with the protection of (energy) automation systems. Since security measures must be adapted to each particular system only general recommendations for the planning of security and selected problems existing in many energy automation systems will be discussed.

4.1 Security Architecture

The most important first step to introduce security is to define the security architecture and policy. Security should be introduced top-down to prevent flaws due to unconsidered threats.

A security policy is a formal statement of rules through which people are given access to an organization's assets (information as well as hardware). It defines business and security goals and contains a description of the implemented security measures. The security policy is an organization's approach to risk. It is important to note that only 20% of security are technological aspects like username/password or cryptography. Hence most (80%) aspects of the security policy will be dealing with procedural, organizational, and cultural aspects of the system. These areas can be characterized by the "4 Ps" of security – people, policy, processes (description of the system), and procedures.

It is obvious that it will not be feasible to physically protect all components of an energy distribution center. Rather only key infrastructure will be protected in order to obtain the needed security level. Security is always a compromise between the costs caused by an attack and the costs of the countermeasures. The omnipresent dilemma of security is that it should make a system more secure without losing productivity. Being only economically feasible, i.e. providing reasonable protection is not enough. In order to prevent that a security architecture from being circumvented by the users it must be understandable, consistent, and most important should not interfere with normal operation.

Special issues for security in automation networks and in energy automation networks in particular are maintenance and the long life time of components.
For maintenance the wide spatial distribution and the human-less remote control is a limiting constraint.
Concerning the life time (up to 30 years) issues of technology migration, capital expenses and limited life time of cryptographical algorithms are boundary conditions that are not known to classical IT systems.

4.2 Securing remote access

A common measure to secure remote access are still username and passwords. Nevertheless this technology has its limitations. Besides improper transmission via plain text, passwords introduce heavy requirements on distribution and memory of the user if used for large systems. From the security point of view unique passwords with big length and a long character set are desirable. Yet such passwords cannot be remembered by the user and often will be replaced by simple mnemonics such as names or number passwords which are more vulnerable to lexical attacks.

To solve the problem of secure transmission in remote access virtual private networks (VPN), http authentication, SSL (Secure Socket Layer), and TLS (Transport Layer Security) are common measures that use cryptographic operations to secure communication and to authorize users (Sauter and Schwaiger, 2002). Also access portals such as the Multi-tier architecture or the virtual private infrastructure (VPI) (Sikora and Brügger, 2005) allow to handle administration in a efficient and secure way.

A still pending issue for most remote access systems is that once access is granted no further access restrictions exist. In particular during maintenance of bigger units a defense in depth that allows only access to a certain subgroup of components of the unit will increase the resistance against accidental failures as well as intentional attacks and therefore increase the robustness of the system.

4.3 Security in automation networks

Typical protocols for energy automation do not implement any security measures. The most used standards such as IEC 60870, IEC 62056 (also known as IEC 1107), or M-BUS offer no security at all. Also industrial fieldbus systems have no serious security measures built-in (Treytl, et. al., 2004) – they are mostly limited to simple UNIX-like access control and plaintext passwords. For the building automation networks BACnet and LonWorks the situation is a little bit better due to the usage of cryptographic measures, but also these systems have their vulnerabilities (Schwaiger and Treytl, 2003).

Ethernet-based solutions on the other hand base their security on network address and port numbers. Switched networks offer additional security against eavesdropping since traffic is separated. Nonetheless, with regard to a planned attack these measures are far too week, since it must be assumed that an attacker will have the computational resources common in the IT world and not the ones of limited embedded systems.

Today, calling line identification and plain text passwords are common measures for field level automation networks but also for remote administration and monitoring. Only in the case of IP-based networks and connection over the Internet (direct telephone connections still use the above mentioned simple measures) advanced measures such as SSL/TLS are used.

A general approach to secure existing networks is tunneling. Comparable to secure web browsing, where the unprotected http protocol is encapsulated in SSL/TLS packets and therefore secured, tunneling can also be applied to automation networks. A general approach is the usage of specialized security modules as suggested in [NAE04, PP00], which allows to efficiently handle security functions that usually consume more computational power than is available in resource-limited devices such as meters or SCADA actuators. Such an approach was selected for the PROFInet security concept. Another approach, yet rarely applied, is to directly integrate the security measures in the communication protocol. This is commonly done only for more powerful services such as embedded web servers or web services, but still some systems such as the REMPLI system (REMPLI consortium, 2004) implement security measures from the beginning on all protocol layers.

4.4 Intrusion Detection and Access Control

The advantage of automation networks for intrusion detection systems lies in the static nature of the network, well defined communication and the limited group of users and devices. Based on these (semi-) static patterns it is easy to identify malicious activities. Systems can use well-known strategies such as network-based or host-based intrusion detection systems, but already simple plausibility checks increase the overall security, e.g., metering values that result in a negative increment are suspicious, the same happens if the input in a low-voltage segment differs from the sum of consumed energy. In the REMPLI system such measures are used to detect manipulation on the connected meters since the used M-Bus and IEC 62056 protocols do not offer any security measures.

Another advantage of (energy) automation networks is that they are monitored by control centers that are manned 24h a day and allow for fast reaction in case an intrusion is detected. On the other hand the rising personnel costs also result in a reduction of remote staff at remote sites make equipment installed in the field more vulnerable to physical attacks. In order not to jeopardize the overall security of the system it is important to store security-relevant information in special tamper-proof devices. Since it is not feasible to physically protect all components in the field, a layered approach should be selected: A physical housing that is a first barrier against vandalism and simple attacks; a second layer that prevents the remainder of security-relevant information in the memory of the device if the device is powered off; finally, a reliable security token such as a smart card known from banking or mobile communication applications that can retain the secret information even if the entire device is stolen.

As the deregulated market forces distribution network providers to deliver energy from various producers to the connected consumers, metering and information transport also become a multi-user problem. Previously, all infrastructure – energy as well as information technology – belonged to one single company. Now, it is more and more common that infrastructure must be shared: a further challenge to IT security, which has to guarantee fairness and confidentiality of transmitted data.

5. CONCLUSION

With respect to the serious damage that misuse of automation systems can cause the still widely applied policy of security by obscurity offers not enough protection against threats of the (near) future. Also the increasing interconnection of units, usage of standard components such as operating systems and the trend towards remote control higher security measures must be integrated. Such measures usually also increase the safety of the communication system (e.g. prevents accidental misuse by unauthorized maintenance personal).

Initiatives such as SELMA or REMPLI show ways to integrate security into automation systems, although it should be pointed out that security measures will introduce additional overhead. Hence, the overall security policy must define the balance between the risk and the overhead. Special attention must be drawn to integrate the system environment into the security policy to avoid indirect attacks such as the indirect DOS attack described in section 3.2.

The lesson learned from the Internet and also from incidents in energy automation networks is that well designed security measures must be applied for vital systems. The old scenario of an isolated and physically protected system is no longer true.

REFERENCES

Bertsch, J., et. al. (2005). Wide-Area Protection and Power System Utilization. *Proceedings of the IEEE*, **VOL. 93**, NO.5, pp. 997-1003.

Brauner, G. (2004). Simulation for congestion management to avoid blackouts. Elektrotechnik und infromationstechnik, Vol 11.2004, pp. 425-429.

British Columbia Institute of Technology (2005). *Industrial security incident knowledgebase* [online]. [available at] http://www.bcit.ca/ appliedresearch/security/services.shtml

Byres, E., Lowe J. (2005). Real World Cyber Security Risks For Industrial Control Systems. *The Online Industrial Ethernet Book*, **Response No. i22 35** [online]. [available at] http://ethernet.industrial-networking.com/ origarticles/i22cyber.asp

Dwivedi, S. Menezes, B. and. Singh (2005), A. Database Access Control for E-Business – A case study. *Proceedings of the International Conference on Management of Data*, Haritsa and Vijayaraman (Eds.), 6.-8.1.2005, Goa, India

Fischer-Drapela, B. (2003). Nadelöhr für Österreich und Europa?. *VEOE Journal*, **March 2003**, pp. 4-7 (in German)

OASIS security team (2001). Technical Architecture Risk Assessment V1.0, technical report, OASIS [online]. [available at] http://www.ebxml.org/ specs/secRISK_print.pdf

Palensky, P. (2005). The JEVis Service Platform - Distributed Energy Data Acquisition and Management. In: *The Industrial Information Technology Handbook*, Zurawski, R. (ed.), CRC Press, Boca Taton, Florida, pp. 111-117.

Patil, S. and Newcomer, E. (2003). ebXML and Web Services. *IEEE Internet Computing*, **Volume 7**, Issue 3, May-June 2003.

REMPLI consortium (2004): White Paper REMPLI Security Concept [online]. [available at] http://www.rempli.org

Sauter, T., Schwaiger, C. (2002). Achievement of secure Internet access to fieldbus systems. *Microprocessors and Microsystems*, **Vol. 26**, pp. 331–339.

Sauter, T., Pratl, G. Treytl, A., Bumiller, G. (2005). Secure and Reliable Wide-Area Power-Line Communication for Soft-Real-Time Applications within REMPLI. *Proceedings of 2005 International Symposium on Power Line Communications and Its Applications*", IEEE 05EX981, pp. 57 - 60.

Schwaiger, C., Treytl, A. (2003). Smart Card Based Security for Fieldbus Systems. *Proceedings of 2003 IEEE Conference on Emerging Technologies and Factory Automation*. pp. 398 - 406.

SELMA consortium(2005). SELMA - Sicherer ELektronischer Messdaten-Austausch (secure and reliable exchange of metering data) [online]. [available at] http://www.selma-project.de

Sikora, A., Brügger, P. (2005). Secure Architecture for Embedded Web Servers. *The Online Industrial Ethernet Book* [online]. **Response No. Issue 23:32**. [available at] http://ethernet. industrialnetworking.com/ieb/articledisplay.asp? id=39

Tomsovic, K., et. al. (2005). Designing the Next Generation of Real-Time Control, Communication, and Computations for Large Power Systems. *Proceedings of the IEEE*, **VOL. 93**, NO.5, pp. 965-979.

Treytl, A., Sauter, T., Schwaiger, C. (2004).Security Measures for Industrial Fieldbus System - State of the Art and Solutions for IP-based Approaches. *Proceedings of the 2004 IEEE International Workshop on Factory Communication System*. pp. 201 - 209.

Treytl, A., Sauter, T. (2005). Security Concept for a Wide-Area Low-Bandwidth Power-Line Communication System. Proceedings of 2005 International Symposium on Power Line Communications and Its Applications. IEEE 05EX981, pp. 66 - 70.

U.S. Nuclear Regulatory Commission (2003). NRC Issues Information Notice on Potential of Nuclear Power Plant Network to Worm Infection. *NRC News*, **No. 03-108**, 2. September 2003. [available at] http://www.nrc.gov/ reading-rm/doc-collections/gen-comm/info-notices/2003/

van der Togt, Ted (2003). Standardisation and security in message exchange. *Metering International, **Issue 3/2003**, pp. 44, 2003*

Werner, T. G. (2002). Load profiling in Germany. 1st Telemark Discussion Forum: Technology Evolution and Future European Electricity Markets, 2-4 September 2002, London, UK, http://www.telmark.org/

Check the following lit:

(The Strategic Power Infrastructure Defense (SPID) system. A conceptual Design IEEE Control System Magazine, vl 20, no.4

EPRI Infrastructure security initiative (ISI)
EPRI-ISI, infrastructure security issues, project status report, Electric Power Research Institute (EPRI), 2003

Section 4.3 check security of or DNP (distributed network protocol and add to protocols