SECURITY ASPECTS OF INFORMATION EXCHANGE IN IT/AT NETWORKS INTERCONNECTIONS OF ELECTRICAL TRANSMISSION AND DISTRIBUTION FACILITIES

Paulo S. MOTTA PIRES
DCA/UFRN – Brazil
pmotta@dca.ufrn.br

Manoel F. MEDEIROS JR.
DCA/UFRN – Brazil
firmino@dca.ufrn.br

ABSTRACT

SCADA (Supervisory Control and Data Acquisition) networks of electric power transmission and distribution control centers that were isolated are now connecting to corporate networks, to vendors networks, and even with the Internet in order to increase productivity in a global and open electricity market. This model, Automation Technology (AT) networks connected with Information Technology (IT) networks introduces new security threats and vulnerabilities. This paper presents some considerations about the security aspects of this computer network configuration.

INTRODUCTION

Critical infrastructures are "*organisations and facilities that are of vital importance for public welfare and whose failure or disruption would result in long-lasting supply bottlenecks or substantial disturbance of public order and/or could have other dramatic consequences*" [1]. Facilities like oil refineries, chemical plants, and electrical transmission and distribution grids are components of strategic or critical infrastructure of nations. When a critical infrastructure disrupts the socioeconomic impact is devastating [2].

SCADA (Supervisory Control and Data Acquisition) systems are essential operational tools to strategic or critical infrastructure sectors. Human operators working at physically protected control centers use these systems for monitoring and control parameters with purposes to ensure proper and safe operation of these important industries. Basically, SCADA systems have three main components: a Central Processing Station unit called Master Terminal Unit (MTU), one or several Remote Station units that can be Remote Terminal Units (RTUs), Intelligent Electronic Devices (IEDs) or Programmable Logic Controllers (PLCs), and communication media used to exchange data. The term Central Processing Unit refers to the servers and software responsible for communicating with the field equipment, and then to the HMI (Human-Machine Interface) software running on workstations in the control room, or elsewhere. In smaller SCADA systems, the Central Processing Station may be composed of a single workstation. In larger SCADA systems, the Central Processing Station can be very complex and may include multiple servers, distributed software applications, and disaster recovery files. Communications between devices are done typically through wires (for shorter distances), wireless (microwaves or spread spectrum radio) and optical fibers.

SCADA systems are indispensable tools to provide Power Utilities with valuable knowledge and capabilities to manage power delivery in a reliable and safe manner. The design goals of former SCADA system networks components were driven by functionality and usability. Security was not a primary design consideration. These networks were isolated both physically and logically.

The challenging issues for SCADA systems today are not the same as ten years ago. Nowadays, there are more requests on integration, using new communication and network technologies, to make the information of the distributed database of SCADA systems accessible by more users, and for more purposes. Automation Technology (AT) networks, in particular SCADA networks are connecting to Information Technology (IT) networks, and to the Internet. This practice makes possible the joint treatment of acquired operational data from the plant, with many others available in the corporate network in decision routines in order to increase productivity and efficiency. Also, it is a common practice to connect the SCADA network of the facility to vendors networks through of networks backdoors entries to permit maintenance and diagnostic works. This network model introduces threats and vulnerabilities. The first public SCADA related vulnerability disclosure was released last year at US-CERT (United States Computer Emergency Readiness Team) homepage [3].

Our paper presents some security aspects of this new computer network configuration. The paper is organized as follows. In the next section, we present some relevant aspects about the operational characteristics of transmission and distribution facilities. Next, we present a brief overview of the threats and vulnerabilities in IT/AT networks interconnections of electrical transmission and distribution facilities. Finally, some considerations are drawn at the conclusions section.

TRANSMISSION AND DISTRIBUTION FACILITIES

The first control centers of power generation and transmission systems were designed to manage the whole system from information given by operators of substations and generating stations, which were transmitted sequentially via radio and/or telephone. Real-time operational functions couldn't be implemented, because of time-delay among various acquired data. This way, just quasi-static states could be supervised and controlled. The only one simulation tool to help control centers' operators was a load flow program running on a stand-alone computer, whose input data were manually prepared when available. Some control actions like voltage control were carried out locally, based in predefined rules. Later, more advanced decision-making

actions like optimal active and reactive power dispatches were implemented, but with local actuation to modify the scheduling. At this time, centralized control decisions were limited to generation and transmission systems.
Nowadays, most substations of some distribution facilities have no more operators, and reactive power dispatch, e.g., is assured through remote actuation. Other more critical tasks like adjustments of protection devices or switching in/off of transmission links - even not concerning to security control or system restoration - are frequently allowed to be done remotely from the control centre operators, after real time simulation. When major disturbances have been occurred and the *normal state* of energy supply has been affected, operational information has to be shared immediately with higher level decision's personnel.
DMS (Distributed Management Systems)/SCADA systems are used extensively in the electrical transmission and distribution sector. DMS/SCADA refers to a suite of application software that supports control and analysis of electric system operations. These software applications are often presented as options by DMS/SCADA vendors or by other software developers who specialize in providing some of these applications. Example applications include:

- Automatic Generation Control (AGC),
- Topology processor,
- On-line three-phase unbalanced distribution power flow and contingency analysis,
- Switch order management,
- Short-circuit analysis,
- Volt/var management,
- Loss analysis.

Recently, this last feature has been implemented through a state estimator, which is depicted to permit an assessment of energy losses in real-time [4].
All these applications provide operations staff and engineering personnel additional information and tools to help accomplish their objectives.

THREATS AND VULNERABILITIES

Some procedures that have potential security risks were considered safe in former AT networks thanks to their logical isolation [5, 6, 7]. Procedures like:

- Multiple user access and authentication based on simple default password (or no password at all),
- Transmission of sensitive data in plaintext,
- Use of protocols that do not implement security,
- Use third-parties communication and control channels, and
- Use of unsafe operational systems

were common in these networks. The interconnection of AT networks and IT networks brought to the former security threats and vulnerabilities that were restrict to the corporate environment. With the connection of these networks, problems like:

- Propagation of malicious code (viruses, worms, Trojan Horses),
- Denial or Distributed Denial of Services,
- Vulnerability exploitation of operational systems and software applications, and
- Bad services configuration

are of fundamental importance. A slight security problem in AT environments can have serious consequences.
DMS applications such as on-line distribution power flow and state estimation [8] still require an electric system model including connectivity, impedance, equipment, load distribution, and most likely geographic coordinates for all components. Obtaining this data and allowing for regular updates requires access to data originated in sources such as GIS (Geographic Information Systems), AM/FM (Automated Mapping/Facilities Management), CIS (Customer Information Systems)/billing, and system study load flow packages. Moreover, most commercial SCADA systems for Power Systems Supervision and Control are developed according to the philosophy of open software. It means that users or external system developers can aggregate new self developed modules to DMS/SCADA software. This fact can lead to security vulnerabilities because the developed software should be linked to DMS/SCADA system.

CONCLUSIONS

Several propositions for security administration in industrial environment have been developed. In particular, there are works developed by The Institute of Electrical and Electronics Engineers, IEEE, [9], North American Electric Reliability Council, NERC, [10], and ISA [11]. Also, we can point out some security research areas to be considered:

- Analyze network architectures, firewalls, gateways, intrusion detection and prevention systems (IDS/IPS) and techniques for hardening operating systems,
- Develop assessment tools for security flaws of software used on Automation Technology components such as embedded software or software interfaces of PLCs or IEDs,
- Develop security software tools that are specific for Automation Technology systems,
- Analyze security aspects of the protocols used in Automation Technology components,
- Analyze security aspects of protocols, architectures and software used in Automation Technology wireless devices,
- Develop security policies models that consider the specificities of Automation Technology networks.

Security administration structures of electrical transmission and distribution facilities, in spite of their peculiar characteristic, can be helped too by experiences made in corporate environments [12].
Other relevant factor to be considered is the interpersonal relationship between personal with distinct formation and purpose: the Information Technology and Automation

Technology professionals. It is important to define the actuation of these professionals into the electrical transmission and distribution facilities in this network convergence scenario.

Acknowledgments

The authors would like to thank the Department of Computer Engineering and Automation (DCA), Federal University of Rio Grande do Norte (UFRN) for the support received during the development of this work. Paulo S. MOTTA PIRES also wishes to acknowledge REDIC (Instrumentation and Control Research Network) for the support he received during the development of this work.

REFERENCES

[1] D. Reinermann, J. Weber, "Analysis of Critical Infrastructures: The ACIS methodology", *Preprints of the First GI Workshop on Critical Infrastructure Protection (CIP) – Status and Perspectives*, Paper 4.4, Frankfurt a.M., 29-30 Sept. 2003.

[2] P. Pourbeik, P.S. Kundur, C.W. Taylor, "The Anatomy of a Power Grid Blackout", *IEEE Power & Energy Magazine*, September /October 2006, pp. 22-29.

[3] US-CERT, Vulnerability Note VU#190617, "LiveData ICCP Server heap buffer overflow vunerability", (on-line) available on Jan. 2007 at http://www.kb.cert.org/vuls/id/190617.

[4] M. Firmino de Medeiros Jr., M. A. D. de Almeida, D. B. F. Silveira, "Estimating Loads in Distribution Feeders Using a Estate Estimator Algorithm with Additional Adjustment of Transformers Loading Factors". *International Symposium on Circuits and Systems – ISCAS 2003/IEEE*, Bangkok, Thailand, May/2003.

[5] T. Kropp, "System Threats and Vulnerabilities – An EMS and SCADA Security System Overview", *IEEE Power & Energy Magazine*, March/April, 2006, pp. 46-50.

[6] P.S. Motta Pires, L.A.H. Guedes de Oliveira, "Security Aspects of SCADA and Corporate Network Interconnections: An Overview", *Proceedings of 1st International Conference on Dependability of Computer Systems DepCoS-RELCOMEX-2006*, Szklarska Poreba, Poland, pp. 127-134.

[7] D. Dzung, M. Nadele, T.P. Von Holf, M. Crevatin, "Security for Industrial Communication Systems", *Proc. IEEE*, vol. 93, N. 6, pp. 1152-1177, June, 2005.

[8] MONTICELLI, A. J., 1999, *State Estimation in Electric Power Systems*, Norwell, Massachusetts-USA: Kluwer Academic Publishers.

[9] IEEE, "1402-2000 Guide for Electric Power Substation Physical and Electronic Security", *The Institute of Electrical and Electronics Enginners, Inc.*, Jan. 2000.

[10] NERC, "Security Guidelines for the Electricity Sector", *North American Electric Reliability Council*, (on-line) available on Jan. 2007 at http://www.nerc.com.

[11] ANSI/ISA, "Security Tecnologies for Manufacturing and Control Systems", TR 99.00.01-2004, *The Instrumentation, Systems, and Automation Society*, ISA, 2004.

[12] P.S. Motta Pires, I. M. dos Anjos, "Improvements on Ethernet LAN Network Infrastructure for Automation: A Case Study", *Proceedings of the 11th IEEE International Conference on Emerging Technology and Factory Automation*, ETFA-2006, Sept. 20-22, 2006, Prague, Czech Republic, pp. 16-22.