SCADA SYSTEMS SECURITY IN ENERGY MANAGEMENT SYSTEMS

J. Car[1], Pupin Institute, Belgrade, Serbia and Montenegro
G. Jakupović, Pupin Institute, Belgrade, Serbia and Montenegro

INTRODUCTION

Supervisory Control and Data Acquisition Systems (SCADA) developed in order to fulfill control needs of Power Utility of Serbia both at transmission and distribution level has almost all features which satisfy the needs of a modern power system. In the circumstances of establishing a deregulated power market, the advantages of the use of one such supervisory and control system become increasingly significant [10]. Process control and SCADA systems, with their reliance on proprietary networks and hardware, have long been considered immune to the network attacks that have wreaked so much havoc on corporate information systems. Unfortunately, new research indicates this complacency is misplaced – the move to open standards such as Ethernet, TCP/IP and web technologies is letting hackers take advantage of the control industry's ignorance. The hacking community is becoming increasingly aware of SCADA and process systems and is beginning to focus their attention on them and to develop both the interest and the technical expertise to deliberately attack control systems. Currently most devices appear to be highly vulnerable to even minor attacks and have no authentication/authorization mechanisms to prevent rogue control. That is the reason why SCADA & control protocols should be improved to include security features. This paper will present some possible solutions for SCADA system security improvement.

SECURITY OF THE CONTROL SYSTEMS

Security, as a term that describes electric stability in the high voltage network, is so well established among electric engineers, that it is reasonable to remind that other disciplines use the same term in other meanings. The term cyber security in information technology is used to describe the protection of computers and data communication from intentional and unintentional electronic events and malicious attacks. Cyber vulnerabilities describe the risks that arise when analog control systems are upgraded to digital, including Supervisory Control and Data Acquisition (SCADA), Plant Distributed Control Systems (DCSs), intelligent field devices such as Remote Terminal Units (RTUs), Programmable Logic Controllers (PLCs), and Intelligent Electronic Devices (IEDs). [1] The term cyber security is used

[1] *Jelena Car, Pupin Institute, Volgina 15,Belgrade, Serbia and Montenegro*
jelena.car@automatika.imp.bg.ac.yu

to differentiate the area from other security issues in control systems, like fire, earthquakes, and physical security such as gates and key readers. [2] The evolution of technology has given power utilities the capability of building open, integrated systems with possibility of using standardized components, breaking down security barriers created by earlier proprietary solutions.

There are three major misconceptions, important for SCADA system security commonly held by utility managers:

1. *The SCADA system is on a physically separate, standalone network.*

Most SCADA systems were originally built before and often separate from other corporate networks, and IT managers typically believe that these systems cannot be accessed through corporate networks or from remote access points. In reality, SCADA networks and corporate IT systems are often connected as a result of two key changes in information management practices. First, the demand for remote access computing that enable SCADA engineers to monitor and control the system from points on the corporate network. Second, connections between corporate networks and SCADA networks were added in order to allow corporate decision makers to obtain instant access to critical data about the status of their operational systems. Often, these connections are implemented without a full understanding of the corresponding security risks: the fact that access to these systems might allow unauthorized access and control of SCADA systems.

2. *Connections between SCADA systems and other corporate networks are protected by strong access controls.*

Many of the interconnections between corporate networks and SCADA systems require the integration of systems with different communications standards. Due to the complexity of integrating disparate systems, network engineers often fail to address the added burden of accounting for security risks. As a result, access controls designed to protect SCADA systems from unauthorized access through corporate networks are usually minimal. Although the strategic use of internal firewalls and intrusion detection systems (IDS), coupled with strong password policies, is highly recommended, few utilities protect all entry points to the SCADA system in this manner.

3. *SCADA systems require specialized knowledge, making them difficult for network intruders to access and control.*

For example, at March 2002, an article in CIO Magazine entitled “Debunking the Threat to Water Utilities” stated there was no risk to SCADA systems from a network-based attack: *“Most public utilities rely on a highly customized SCADA system. No two are the same, so hacking them requires specific knowledge.” [7]*

The above misconception assumes that all attackers of a SCADA system lack the ability to access information about their design and implementation. Due to the fact that utility companies represent a key component of one of the nation’s critical infrastructures, these companies are likely targets of coordinated attacks by “cyber-terrorists”, as opposed to disorganized “hackers.” Such attackers are highly motivated, well-funded, and may very well have “insider” knowledge. Furthering this risk is the increasing availability of information describing the operations of SCADA systems: several standards for the interconnection of SCADA systems and remote terminal units (RTUs) have been published (standards for communication between control centers, acceptance of alarms, issuance of controls, and polling of data objects). Further, SCADA providers publish the design and maintenance documents for their products and sell toolkits to help develop software that implements the various standards used in SCADA environments. Websites often provide data useful to network intruders about company structure, employee names, e-mail addresses, and even corporate network system names. Domain name service (DNS) servers permit “zone transfers” providing IP addresses, server names, and e-mail information

SCADA SYSTEM AS A PART OF IT NETWORK

SCADA system security is often only as strong as the security of the utility’s corporate network. While the RTUs on a network may be difficult to access outside of the dedicated serial lines, it is only moderately difficult to penetrate the control panel for the SCADA manager through the corporate network and quickly ‘learn’ commands by watching actions that are carried out on the screen. Attacks on highly complex systems become much easier when attackers first penetrate the workstations of SCADA operators. [3]

The network architecture design is critical in offering the appropriate amount of segmentation between the Internet, the company’s corporate network, and the SCADA network. Network architecture weaknesses can increase the risk that a compromise from the Internet could ultimately result in compromise of the SCADA system. Some common architectural weaknesses include the following:

- Configuration of file transfer protocol (FTP), web, and e-mail servers sometimes inadvertently and unnecessarily provides internal corporate network access;

- Network connections with corporate partners are not secured by firewall, IDS, or virtual private network (VPN) systems consistent with other networks;
- Dial-up modem access is authorized unnecessarily and maintenance dial-ups often fail to implement corporate dial access policies;
- Firewalls and other network access control mechanisms are not implemented internally, leaving little to no separation between different network segments.

The details of safety related incidents have been recorded for over a century, while cyber security incidents have less than two decades of occurrence, never mind record keeping. Furthermore, most organizations are highly reluctant to report security incidents as they are viewed as potential embarrassments. In fact, many organizations have denied that there even is a risk to industrial systems from cyber attack. Figure 1 shows the trend of events between 1995 and 2003. It appears that there is a sharp increase in events occurring around 2001 (indication of an actual increase in attacks or the result of the increased efforts to collect data).

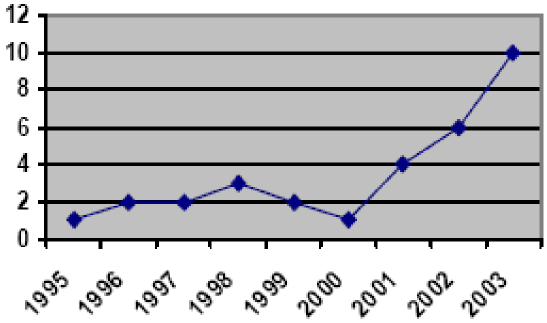

Figure 1: Security Incidents between 1995 and 2003 [7]

Figure 2 shows the result of collecting of 13 incidents between the years 1982 and 2000. Incidents were split between accidental, internal and external sources, with only 31% of the events being generated from outside the company. Accidents, inappropriate employee activity and disgruntled employees accounted for most of the problems.

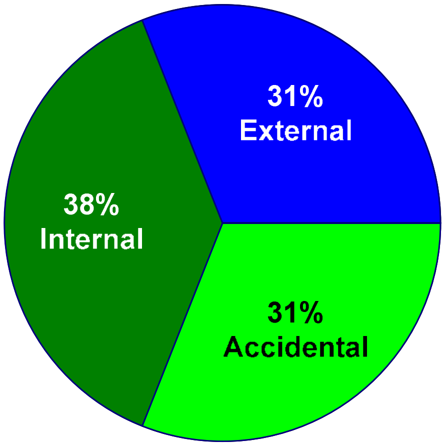

Figure2: Security Incidents by type 1982 and 2000 [7]

The same graph for the period 2001 to 2003, is shown in Figure 3 where externally generated incidents are 70% of all events, indicating a significant change in threat source. There are a few reasons because the threat source change so significantly in such a short period of time:

- First the emergence of automated worm attacks starting with Code Red1 in July 19, 2001 shows that many of the intrusions have become non-directed and automated. The control system has become just a target of opportunity rather than a target of choice.
- Second, common operating systems (e.g. Windows 2000 or Linux) and applications (e.g. SQL Server) now dominate the Human Machine Interface (HMI), engineering workstation and data historian systems. These often come configured more appropriately to business requirements and are vulnerable to a wide variety of common IT attacks and viruses. Issues with applying patches to these critical systems exacerbate the problem.
- Finally the increasing interconnection of critical systems has created interdependencies we haven't been aware of in the past. As the Slammer Worm incident documented by the North American Electric Reliability Council illustrates, Internet incidents can indirectly impact a system that doesn't use the Internet at all. In this case the power utility used frame relay for its SCADA network, believing it to be secure. Unfortunately the frame relay provider utilized a common Asynchronous Transfer Mode (ATM) system throughout its network backbone for a variety of its services, including commercial Internet traffic and the SCADA frame relay traffic. The ATM bandwidth became overwhelmed by the worm, blocking SCADA traffic to substations [7].

Default network services in commercial or open-source operating systems on which SCADA system are based, may be used in attack. Because of that, it is necessary to remove or disable unused services and network daemons, to the greatest degree possible (examples of services to remove from SCADA networks include automated meter reading/remote billing systems, email services, and internet access. An example of a feature to disable is remote maintenance). Different SCADA systems use different protocols for communications between field devices and servers. Although, some of them are unique, proprietary protocols, secrecy of these protocols or factory default configuration settings could not protect SCADA system. It is important to demand that vendors disclose any backdoors or vendor interfaces to SCADA systems, and to provide secure system. Security features must be enabled after installation (they are often disabled to ensure easier installation), or they must be added in the form of product patches or upgrades. Factory default security settings (such as in computer network firewalls) are often set to provide maximum usability, but minimal security, and they must be set to provide the maximum level of security. System administrators may use some of commercial and open-source security tools to identify system vulnerabilities. Then, after identification vulnerabilities and determination their significance, it will be taken corrective actions as appropriate. Finally, retest systems after corrective actions have been taken to ensure that vulnerabilities were actually eliminated.

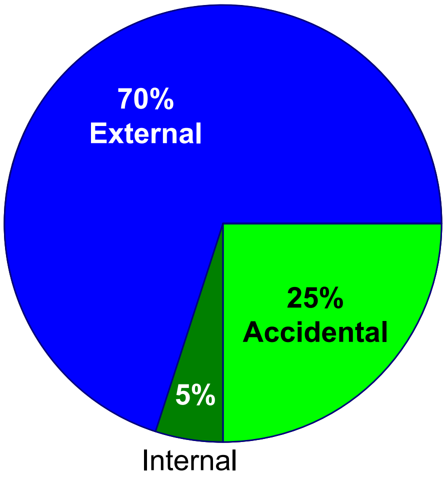

Figure3: Security Incidents by type 2001 and 2003

The predominant security effort in most SCADA facilities tends focus on attacks via the Internet or through the business network. This leaves open attacks from other intrusion points such as remote field stations, the SCADA transmission infrastructure, trusted 3rd parties or wireless control network connections. Once an attacker has access to the SCADA system, any moderately skilled hacker would be able to carry out the majority of the attacks. [4]

“EXTERNAL” AND “INTERNAL” SECURITY THREATS

It is very important to identify all contacts to SCADA networks: internal LAN, WAN, business networks, the internet, wireless network devices, satellite uplinks, modem or dial-up connections, all connections to business partners, vendors or regulatory agencies. Any location that has a connection to the SCADA network is a target, especially unmanned or unguarded remote sites, remote telephone/computer network/fiber optic cables that could be tapped; radio and microwave links that are exploitable; computer terminals that could be accessed; and wireless local area network access points. Hardware and software configurations of system need to be carefully designed, well-tested and documented on security base and unchangeable due to the security purposes. Changes to hardware or software can easily introduce vulnerabilities that undermine network security.

Security is typically defined by three attributes: confidentiality, integrity, and availability of information (ISO/IEC 17799).

Confidentiality is defined as ensuring that information is accessible only to those authorized to have access.

Integrity is defined as safeguarding the accuracy and completeness of information and processing methods.

Availability is defined as ensuring that authorized users have access to information and associated assets when required. [5]

To be secure, assets (whether information or equipment) should only be accessible by authorized users, modifications should be prevented, and they should be there when you need them. These concepts hold true for both “external” and “internal” security threats and for both physical and cyber security. [6]

Important part of network protection strategy is defense-in-depth, and must be considered early in the design phase of the development process. Defense-in-depth means to mitigate threats from identified risks at all levels of the network and to layer cyber security defense to limit security incidents. Each layer must be protected against other systems at the same layer. For example, to protect against the insider threat, restrict users to access only those resources necessary to perform their job functions.

If we divide security threats into “external” and “internal”, we can find some interesting results in statistic data about their entry point, figures 4 and 5:

For example, database records show that the Slammer Worm had at least four different infiltration paths in the control systems it impacted:

- The Davis-Besse nuclear power plant process computer and safety parameter display systems via a contractor’s T1 line;
- A power SCADA system via a VPN;
- A petroleum control system via a laptop;
- A paper machine HMI via a dial-up modem. [7]

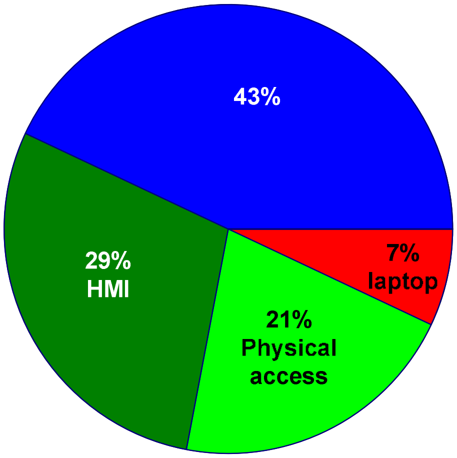

Figure 4: Internal Security Incidents by Entry Point

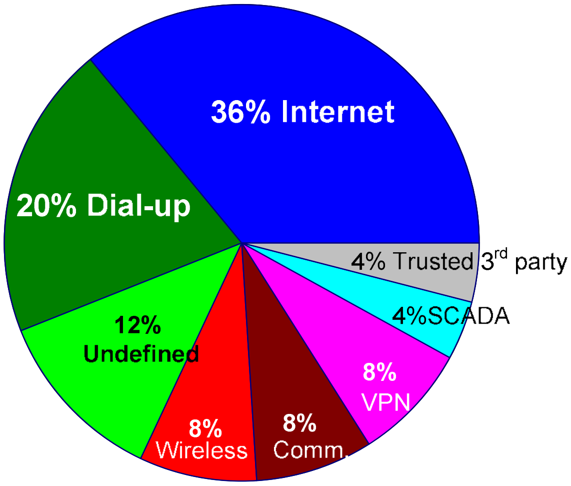

Figure 5: External Security Incidents by Entry Point

For the internal incident, the business network is the major source. Direct physical access to the equipment was also significant. For the external event, the Internet was a major source, but dial-up connections, VPNs, telco networks, wireless systems and 3rd party connections were all contributors. The obvious conclusion is that there are many routes into a system as complex as a modern SCADA or control system. Focusing on a single intrusion point with a single solution (such as the Internet firewall) is likely to miss many possible attack points.

PROTECTIVE MECHANISMS

The implementation of protective mechanisms is to a large extent made difficult due to a geographic distribution of electric power systems and due to a presence in the system of a large number of devices with numerous input nodes that are vulnerable to hacker attacks. The additional difficulty is posed by the fact that the system is not interoperable, so that the different protocols that protective intelligent electronic devices use to communicate with PLCs, RTUs, PCs, and other SCADA systems limit the attempts to protect the communication between the center and substations. Besides the diversity of the devices used in the system, different communication media are often used between system parts (commercial and leased phone lines, wireless communication, optical fibers), thus posing additional demands when protective model of a system is defined. [8]

Although the first security protection step is isolation the SCADA network from other network connections to as great a degree as possible, additional security solutions must be perform. Any connection to another network introduces security risks and despite of efficiently and conveniently, insecure connections are simply not worth the risk. Since the SCADA network is only as secure as its weakest connecting point, it is necessary to develop a robust protection strategy for any remaining connections and any pathways to the SCADA network: implement firewalls, intrusion detection systems (IDSs), and other appropriate security measures at each point of entry. Strategically place IDSs at each entry point to alert security personnel of potential breaches of network security. Intrusion detection system monitoring is essential 24 hours a day, it is necessary to audit system logs daily to detect suspicious activities.

VIEW2 SCADA SYSTEM SEGMENTATION

After the first step, isolation the SCADA system from the rest of IT network (usually in the most implementations of VIEW2 SCADA systems), figure 6, it is recommended further segmentation of SCADA network. [9]

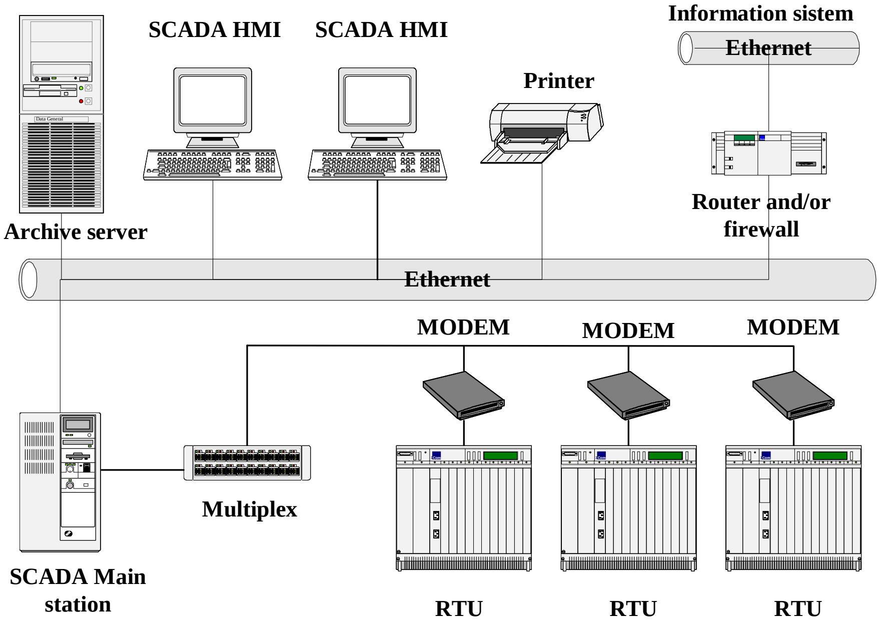

Figure 6: Isolate SCADA system from the rest of IT network

Segmenting the SCADA network into security zones is a recommended security method where devices like PLCs, RTUs, and IEDs that control physical equipment are in the same, first zone, communication media are in another, second security zone, HMI and SCADA servers are in the third zone, archive and web servers are in the fourth, and so one… (figure 7). Security zones are separate with a small distributed firewalls, managed from rack-mountable console somewhere in the system.

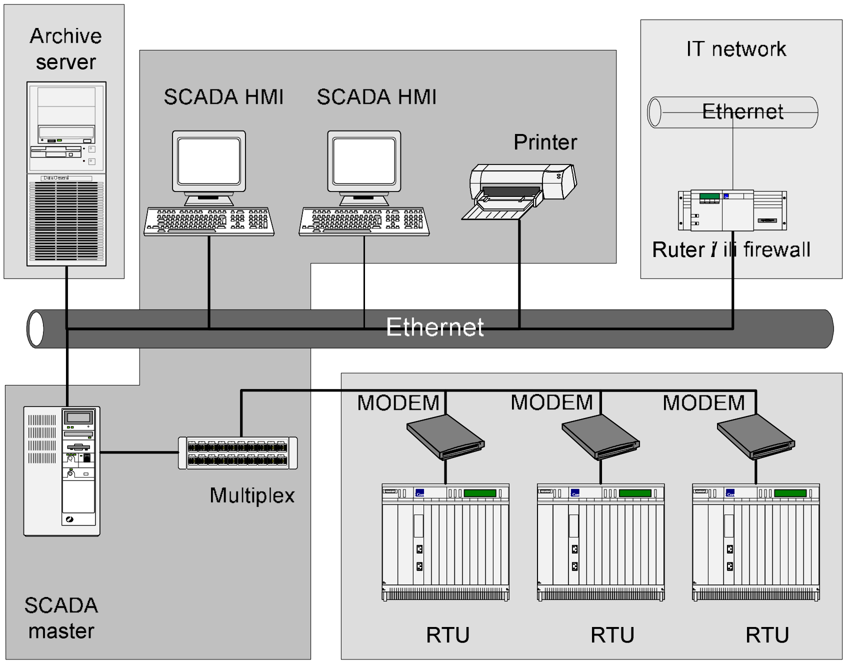

Figure 6: Segmented SCADA system

CONCLUSION

SCADA Systems, which used to be more predominantly proprietary in nature, have evolved in recent years to become based on more open standards like Visual Basic, ODBC connectivity, Ethernet communications and web-enabled screens. Most SCADA systems encapsulated their proprietary protocols in TCP/IP packets, and although open based standards are easier for the industry to integrate various diverse systems together, it is also increased the risks of unauthorized personnel gaining access to these industrial networks. This paper presents SCADA system segmentation as a possible mechanism of cyber security protection. The method is presented conceptually, without detailed description, because it is depend of implementation demands.

REFERENCES

[1] M. Matijević, G. Jakupović, J. Car, Računarski podržano merenje i upravljanje, Mašinski fakultet u Kragujevcu, Septembar 2005

[2] Sandstrom E, Weiss J., “Cyber Security”, 2th CIGRE/IEEE PES International Symposium, New Orleans, USA, October 5-7 2005

[3] Riptech Talking Points, "Understanding SCADA System Security Vulnerabilities", www.iwar.org.uk/cip/resources/

[4] E. J. Byres, D. Miller, "The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems", Available: www.bcit.ca/files/appliedresearch/ pdf/security/attacktrees.pdf

[5] A. Torkilseng, "Management of Information Security in Power Utilities", *ELECTRA*, No. 206, February 2003, pp 37-44

[6] M. Franz, D. Miller, "Industrial Ethernet Security: Threats & Countermeasures", Available: www.io.com/~mdfranz/papers/franz-miller-industrial-ethernet-sec-03.pdf

[7] E. J. Byres, J. Lowe, "The Myths and Facts behind Cyber Security Risks for Industrial Control Systems" www.tswg.gov/tswg/ip/The_Myths_and_Facts_behind_Cyber_Security_Risks.pdf

[8] F. Sheldon , T. Potok, A. Loebl, "Energy Infrastructure Survivability, Inherent Limitations, Obstacles and Mitigation Strategies", Available: www.csm.ornl.gov/~sheldon/public/ SheldonPwrCon03-434-801.pdf

[9] J. Pollet, "Is Your SCADA Network Environment Insecure by Design?" www.plantdata.com/Is_Your_SCADA_Network_Environment_Insecure_By_Design.pdf

[10] J.Trhulj, G.Jakupović, N. Čukalevski, M. Stojić, 2002, "Komparativna analiza postojećih nadzorno-upravljačkih sistema prenosnih i distributivnih EES", Odeljenje za upravljanje EES, IMP