Protection Issues in SCADA Systems

Samira Moazami Pour[1], Seyed Vahab Al-Din Makki[2]
1- Department of Electrical Engineering, Islamic Azad University Kermanshah Branch, Kermanshah, Iran
Email: moazami_291@yahoo.com
2- Department of Electrical Engineering, Razi University, Kermanshah, Iran
Email: v.makki@razi.ac.ir

Received: May 11, 2013 Revised: Oct. 5, 2013 Accepted: Sep. 15, 2013

ABSTRACT:
Supervisory Control and Data Acquisition (SCADA) is a term used to refer to systems and networks that monitor, manage and control automation, production and distribution of considred system. In this paper, we describe an overview of SCADA system and its supetibilities and commendations for implementing security and protection in this system.

KEYWORDS: SCADA, Supetibilities, Protection, Distribution .

1. INTRODUCTION

Supervisory Control And Data Acquisition (SCADA) system generally refers to the control system of the industry, where a computer system that controls and monitors a process.

SCADA is used by process industries including petro. micals, fertilizers, cement, paper and pulp, steel industries, aluminum plants and infrastructure as well. It is also used for monitoring and controlling physical processes like distribution of water, traffic lights, electricity transmissions, gas transportation and oil pipelines and other systems used in the modern society [1], [2].

SCADA protocols consist of conitel, profibus, modbus RTU and RP-570. Its Standard protocols are mainly IEC 61850, DNP3 and IEC 60870-5-101 or 104. These protocols of communication can be recognized, standardized and most of them contain extensions for operating over the TCP/IP. A SCADA system consists of a number of Remote Terminal Units (RTUs) collecting field data and sending data back to a master station via a communications system. The master station displays the scquired data and also allows the operator to perform remote control tasks. The accurate and timely data allows for optimisation of the plant operation and process. A further benefit is more efficient, reliable and most importantly, safer operation [3]. An RTU is a stand-alone data acquisition and control unit, generally microprocessor based, that monitors and controls equipment at a remote location. Its primary task is to control and acuire data from process equipment at the remote location and to transfer this data back to a central station. It generally also has the facility for having its configuration and control programs dynamically downloaded from some central station [3].

SCADA software can be divided into two types, properietary or open. Companies developed proprietary software to communicate to their hardware. These systems are sold as “turn key” solutions. Open software systems have gained popularity because of the interoperability they bring to the system. Interoperability in this case is the ability to mix different manufacturers‟ equipment on the same system [3].

Communications in a SCADA system will generally have a structure where some stations may be identified as master stations, and others as slave stations, sub-master stations, or outstations. In a hierarchical structure, there may be some devices that can act both as slave stations and master stations [3].

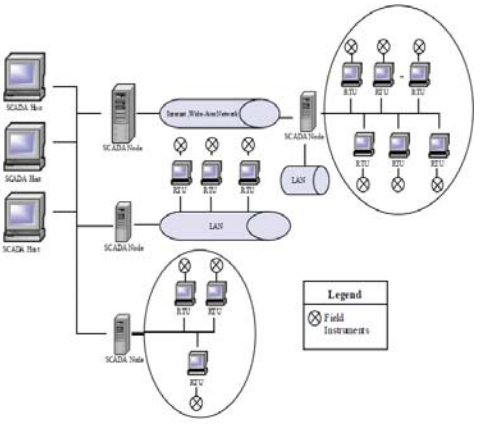

Fig. 1. SCADA system

One of the important SCADA features of DNP3 is that it provides time-stamping of events. Time stamping DNP3 provides resolution of events to one-millisecond. For events to match up correctly across the system, it is essential that clocks at all out-stations are synchronized with the master station clock [3].

2. SUSCEPTIBILITY OF SCADA SYSTEMS

In the past, when SCADA systems were independent and vendor-controlled systems with no connections to other systems and when the network protocol was proprietary, only a few people, such as developers and hackers, knew of the existence of SCADA installations. However, the present SCADA systems are widely distributed and networked. Since the systems are dependent on open protocols for the internet, they are vulnerable to external remote cyber threats as discussed in [4]. SCADA systems are different from general information systems in terms of security management. In the risk and security management of general information systems, after analyzing the assets, threats, and vulnerabilities of information systems and calculating the degrees of a risk, security measures are prioritized for calculating the remaining risk. In contrast, for SCADA systems, the analysis of the assets is performed not from the viewpoint of systems but from the viewpoint of target facilities managed and operated.

There are two distinct threats that can affect modern SCADA systems. The first one is the threat of unauthorized access to the control software, whether it is human access or changes made deliberately or unintentionally by virus infections and other software threats existing on the control host machine. The second is the threat of packet access to the network segments hosting SCADA devices. In particular, security researchers are concerned about security and authentication in the design, deployment, and operation of some existing SCADA networks. Moreover, they need to also take into consideration whether the SCADA networks are secured just because they are physically disconnected from the internet. In addition, security researchers are also concerned about the existing security and authentication protocols in the design, deployment, and operation of SCADA networks, with the belief that SCADA systems have the benefit of security through obscurity through the use of specialized protocols and proprietary interfaces.

The following list suggests ways to help protect the SCADA network in conjunction with the corporate network as discussed in [5]. Security measures of SCADA systems in terms of technology can be presented as follows: (a) strict limitations and authority control are needed for external connections, (b) reinforced security for the systems in demilitarized zones (DMZs) as well as for the internal network is recommended, (c) enhancing security using virtual private networks (VPNs) in addition to integrity tools of servers, (d) Minimization of access paths to the internal network and enhanced concentration of monitoring, (e) encryption of emails and locking of files and directories, (f) regular and thorough inspection of security and vulnerability, and (g) developing control and monitoring methods to cope with any contingencies in the SCADA equipment.

3. IMPLEMENTATION OF PROTECTION IN SCADA

Based on the analysis of the past and current developments, we identified key requirements and features that can improve the security of control systems as follows:

3.1. Harden SCADA networks by eliminating or immobilizing unnecessary services

SCADA control servers built on commercial or open-source operating systems can be exposed to attack through default network services. To the greatest degree possible, remove or disable unused services and network daemons to reduce the risk of direct attack. This is particularly important when SCADA networks are interconnected with other networks. Do not permit a service or feature on a SCADA network unless a thorough risk assessment of the consequences of allowing the service/feature shows that the benefits of the service/feature far outweigh the potential for vulnerability exploitation. 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. Numerous secure configuration guidelines for both commercial and open source operating systems are in the public domain, such as the National Security Agency's series of security guides. Additionally, work closely with SCADA vendors to identify secure configurations and coordinate any and all changes to operational systems to ensure that removing or disabling services does not cause downtime, interruption of service, or loss of support[6].

3.2. Establishing a accurate, current risk management process

A thorough understanding of the risks to network computing resources from denial-of-service attacks and the vulnerability of sensitive information to compromise is essential to an effective cyber security program [7].

Risk assessments form the technical basis of this understanding and are critical to formulating effective strategies to mitigate vulnerabilities and preserve the integrity of computing resources. Initially, perform a baseline risk analysis based on a current threat

assessment to use for developing a network protection strategy. Due to rapidly changing technology and the emergence of new threats on a daily basis, an ongoing risk assessment process is also needed so that routine changes can be made to the protection strategy to ensure it remains effective. Fundamental to risk management is identification of residual risk with a network protection strategy in place and acceptance of that risk by management [8], [9].

3.3. Stronger protection policies and procedures

Solutions for preventing the attacks are becoming more important to enterprises and software vendors. The best first steps recommended for preventing attacks against control systems are increased awareness of potential vulnerabilities and solutions, as well as implementing stronger safety policies and procedures. It is essential that every enterprise is taking security seriously when developing software, or managing the control systems**.**

3.4. Conduct physical precautions surveys and evaluate all remote sites connected to the SCADA network to determine their protection

Any location that has a connection to the SCADA network is a target, especially unmanned or unguarded remote sites. Conduct a physical security survey and inventory access points at each facility that has a connection to the SCADA system. Identify and assess any source of information including 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. Identify and eliminate single points of failure. The security of the site must be adequate to detect or prevent unauthorized access. Do not allow "live" network access points at remote, unguarded sites simply for convenience [7].

3.5. Guarantee endorsement, confidentiality, reliability, accessibility, and non-repudiation

Security of SCADA control systems must ensure far more than the confidentiality of information in transit. It must also ensure that only authorized parties have access to such information, a task that will require abuse-resistant methods for identifying such parties. In the information security context, the SCADA control systems require features that support key security concepts such as authentication, authorization, confidentiality, integrity, availability, and non repudiation. Also, control protocols should be improved to include security features.

3.6. Evaluating risk as impact to security and safety

Effective risk analysis for SCADA systems requires a unified definition for mishap and identification of potential harm to safety. As computer systems are more integrated, the distinction between security and safety is beginning to disappear. In bridging the gap between these domains, we propose a unified risk framework which combines a new definition of mishap with an expanded definition of hazard to include the security event [10], [11].

4. ACKNOWLEDGMENT

I'd like to thank gas national organization of Esfehan city because of their encouragemnet and support during conducting this research**.**

REFERENCES

[1] SCADA information Available in, http://www.scadasystems.net

[2] A. Daneels, W. Salter, "**What is SCADA**?" *International Conference on Accelerator and Large Experimental Physics Control Systems*, Trieste, Italy, 1999.

[3] D. Reynders, G. Clarke and E. Wright, "**Practical Modern SCADA Protocols, 60870.5 and Related Systems**", *Newness and Elsevier Advance Technology Limited*, United Kingdom, 2004.

[4] D. H. Ryu, H. Kim, and K. Um, **"Reducing security vulnerabilities for critical infrastructure,"** *Journal of Loss Prevention in the Process Industries*, Vol. 22, pp. 1020-1024, Nov. 2009.

[5] C. Wilson, **"Botnets, cybercrime, and cyberterrorism: vulnerabilities and policy issues for congress"**, *CRS Report for Congress*, 2008.

[6] M. A. Young, **"SCADA Systems Security",** SANS Institute, 2004.

[7] R. Craft, G. Wyss, R. Vandewart & D. Funkhouser, "**21st National Information Systems Security Conference Proceedings"**, *An open framework for risk management*, 2007.

[8] W. Ozier, "**A framework for an automated risk assessment tool"**, The Institute of Internal Auditors, 2007.

[9] Hentea, Patel, Graham, **"A perspective on security risk management of SCADA control systems",** *Proceedings of 23rd International Conference on Computers and Their Applications*, 2008.

[10] D. Geer, "**Security of critical control systems sparks concern**," *IEEE Computer Journal*, Jan. 2006, p. 20-23.

[11] J. Byres, D. Hoffman, N. Kube,"**A study of security vulnerabilities incontrol protocols**", *5th American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human Machine Interface Technology*, American Nuclear Society, 2006.