Chapter 2
Methodology for Cyber Security Risk Mitigation in Next Generation SCADA Systems

Jasna D. Marković-Petrović
https://orcid.org/0000-0002-0373-8022
Public Enterprise "Electric Power Industry of Serbia", Serbia

ABSTRACT

The evolution of architecture of contemporary SCADA systems follows trends in industry sector. Today, SCADA systems imply the application of smart grid and artificial intelligence concepts, the use of IP-based technologies, new mobile devices, as well as the use of private and public cloud computing services. Security risk assessment of contemporary SCADA systems needs to include new security aspects. This chapter analyzes information security in contemporary SCADA systems. Focus is then directed to SCADA network architecture and recommended security mechanisms for mitigating the security risk that assumes the use of Defense in Depth concept. Special attention is paid to SCADA-specific intrusion detection and intrusion prevention technologies. A case study outlines recommendations for security risk mitigation of SCADA system in a hydropower plant.

INTRODUCTION

Supervisory Control and Data Acquisition (SCADA) systems are widely used in industrial sector, primarily in production, transmission and distribution of electrical energy, oil and gas refining, telecommunications, transportation, as well as water and wastewater control. These industrial sectors are a part of critical infrastructure. Therefore, SCADA systems are a target for cyber attacks, since the malfunction or failure of such systems can cause serious consequences, due to their strategic importance for critical infrastructure of every country. This problem rises with the introduction of new generation SCADA systems that are no longer isolated and are not using only proprietary protocols and software.

Next generation SCADA systems assume deployment of smart grids, artificial intelligence concept and remote control of complex systems, the use of the Internet Protocol (IP) technology, the rise in the

DOI: 10.4018/978-1-7998-2910-2.ch002

number of remote users, the use of public and private cloud and fog computing services, the emergence of new mobile devices and the Industrial Internet of Things (IIoT). From stand-alone, isolated systems, these systems have evolved into those connected with other SCADA and corporate IT systems. This has caused a rise in the number and type of connections to SCADA systems, and consequently, a rise in the number and variety of attacks to the telecommunication networks of industrial control systems. Several successfully performed attacks on the SCADA systems' infrastructure have been registered and reported worldwide, producing ill effects of varying degrees.

In order to reduce the security risk, it is necessary to take large-scale, comprehensive measures, which include adopting an appropriate security policy for information infrastructure, staff informing and training on the adopted policy, establishing the adopted policy and conducting continuous information security risk management.

This chapter starts from the premise that the application of conventional security mechanisms is not always a proper solution for telecommunication networks of SCADA systems. The reasons for this are the different requirements regarding availability and quality of service, as well as the applied information and communication technologies in comparison with the business information systems. Hence, the implementation of the specific security mechanisms designed for SCADA systems is of high importance for achieving the efficient protection. The rest of the chapter is structured as follows. The literature review is presented in the background section.

In the following section, performance requirements of SCADA networks are presented, considering the differences between general-purpose and industrial information systems. Further, security aspects of SCADA systems have been analyzed, including the cyber threats directed towards the infrastructure of the next generation SCADA systems and the infrastructure's vulnerability. The next section presents the evolution of the SCADA systems architecture, with the emphasis on next generation SCADA systems. The chapter continues with the consideration of secure SCADA network architecture in the future Internet environment. The basis for defining such an architecture is the functional and logical architecture describing the structure and basic functions of SCADA systems. The next section considers security mechanisms, namely the firewall and intrusion detection and prevention systems (IDPS), which are specific for the design and application in next generation SCADA systems. In the following section, based on the previous observations, a case study is presented, which proposes the network architecture and technology for reducing the information security risk of SCADA system in a hydropower plant. The chapter ends with emphasizing the future research directions and concluding remarks.

BACKGROUND

The strategic role of critical infrastructure and technological progress causes the need for contemporary information and communication systems. All systems have to provide high reliability, availability, and transmission of correct and timely information in order to plan production, efficient resource utilization, remote control of production facilities, reporting and successful operation of industrial system.

IP technology is widely adopted as a base for the integration of operational and business services in contemporary industrial telecommunication networks. Such networks have flaws and vulnerabilities known to malicious users. Particularly, potential migration of SCADA systems towards cloud computing environment needs to be considered. Such a realization contributes to cost reduction and business