The current issue and full text archive of this journal is available on Emerald Insight at:
www.emeraldinsight.com/2056-4961.htm

Security gaps assessment of smart grid based SCADA systems

AQ:au

Abdul Wahid Mir and Ramkumar Ketti Ramachandran
Department of Computer Science and Engineering, Chitkara University, Chandigarh, India

Received 28 December 2018
Revised 25 January 2019
6 March 2019
Accepted 6 March 2019

Abstract

Purpose – Supervisory control and data acquisition (SCADA) systems security is of paramount importance, and there should be a holistic approach to it, as any gap in the security will lead to critical national-level disaster. The purpose of this paper is to present the case study of security gaps assessment of SCADA systems of electricity utility company in the Sultanate of Oman against the regulatory standard and security baseline requirements published by the Authority for Electricity Regulation (AER), Government of Sultanate of Oman.

Design/methodology/approach – The security gaps assessment presented in this paper are based on the security baseline requirements that include core areas, controls for each core area and requirements for each control.

Findings – The paper provides the security gaps assessment summary of SCADA systems of electricity utility company.

Practical implications – The summary of threats and vulnerabilities presented will help stakeholders to be proactive rather than reactive in the event of any attack.

Originality/value – This case study discusses the various security challenges in smart grid based on SCADA systems and provides the summary of challenges and recommendations to overcome the same.

Keywords Government regulation, SCADA, Smart grid, Gap assessment, Security challenges, Industrial control systems (ICS)

Paper type Case study

1. Introduction

The smart grid is the futuristic way of managing the critical infrastructures that are used to operate various aspects of electricity services business. It consists of electricity generation stations, transmission overhead lines, power substations, transformers and additional infrastructure to provide electricity services to consumers. Supervisory control and data acquisition (SCADA) systems are used to manage, control and monitor operations in typical critical infrastructural deployments. The deployments can be any critical sectors of power utility, oil and gas, sewage management plants, nuclear energy, railways, water supply or desalination plants, etc. SCADA acts as the central component in smart grid decision-making.

The electricity services are backbone of the modern world without which survival will be a major challenge. The smart grid paradigm enables efficiency, reliability and availability for critical electrical infrastructural systems (Khurana *et al.*, 2010). The smart grid facilitates efficient transmission of electricity, quicker restoration of electricity in the event of any failures, reduced operations and maintenance costs, competitive consumer pricing, management of peak and off-peak power needs, and overall systems security (Delgado *et al.*, 2015). SCADA systems are at the core of the smart grid architecture. They are essential components of Sultanate of Oman's national critical infrastructures.

SCADA system is a control system primarily used to control and monitor the entire electricity generation process (Cherdantseva *et al.*, 2016). The various sensors and actuators

Information & Computer Security
© Emerald Publishing Limited
2056-4961
DOI 10.1108/ICS-12-2018-0146