# IT Security for SCADA:
## A Position Paper

*Rahul Rastogi, Engineers India Limited, New Delhi, India and Nelson Mandela Metropolitan University, Port Elizabeth, South Africa*

*Rossouw von Solms, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa*

## ABSTRACT

*SCADA (Supervisory Control and Data Acquisition System) is a cyber-physical system, wherein IT (Information Technology) components work in conjunction with field devices to control a physical process. The security of these IT components becomes crucial in view of the damaging effects that any security breach of these IT components can have on the underlying physical process. In response to this critical issue, various governments across the world have recognized the issue of SCADA security and have initiated the creation of a regulatory framework for mandating SCADA security in their respective countries. This paper provides a brief overview of the cyber-security issues of SCADA and the implications of Stuxnet for SCADA security. The paper reviews the steps taken by the governments of India and South Africa; and it provides guidance to the owners of SCADA regarding SCADA security, as mandated by the Government of India.*

*Keywords: Cyber Security, India, Information Technology, SCADA, South Africa, Stuxnet*

## 1. INTRODUCTION

SCADA (Supervisory Control and Data Acquisition System) is a cyber-physical system, wherein IT (Information Technology) components work in conjunction with field devices to control a physical process. The security of these IT components becomes crucial in view of the damaging effects that any security breach of these IT components can have on the underlying physical process. A typical SCADA installation consists of an IT infrastructure, comprising servers, workstations, operating systems and applications that utilize databases and web-servers, and that communicate using LAN, WAN and/or Internet technologies.

In 2010, the Stuxnet worm spread across various countries and emerged as a potent IT security attack on SCADA systems. The Stuxnet worm made the world realize that attacks on SCADA security could have a devastating impact on the underlying physical process. The security of the IT components of SCADA has since become a crucial topic, and an emerging imperative for all countries. The new imperative requires entire countries, as well as individual organizations, to rethink their strategy for SCADA security. Many countries, e.g. India, have initiated regulatory

DOI: 10.4018/IJCWT.2015070102

action for mandating SCADA security. Such regulatory action renders SCADA security mandatory for organizations that operate SCADA. This also presents a business opportunity for security consultants, who may so far have worked only in the corporate or government sector, but have not yet focused their attention on the security of SCADA.

As an example of the impact of this new imperative, it is estimated that the market for critical infrastructure security and protection in the Middle East will grow from USD 5.74 billion in 2013 to USD 13.07 billion by 2018, at a CAGR (Compound Annual Growth Rate) of 17.9% (Middle East Critical Infrastructure Protection (CIP): Market Advancements, Business Models, Technology Roadmap, Market Forecasts & Analysis (2013 – 2018), 2013).

This paper is structured as follows. The next section provides an overview of SCADA, and its related-IT security issues. The subsequent sections discuss the Stuxnet worm and its implications for SCADA security. Finally, as an example of the strategy that various countries are implementing for SCADA security, the paper discusses the regulatory framework established by the Governments of India and South Africa. The paper concludes by presenting a suite of actions that individual organizations can initiate regarding SCADA security.

## 2. IT SECURITY FOR SCADA

SCADA consists of many IT components, viz. servers, networking systems, databases, webservers, SCADA software, operating systems etc. The SCADA system is also interfaced with Programmable Logic Controllers (PLCs) and Remote Terminal Units (RTUs). The PLCs and RTUs are, in turn, connected to sensors and actuators. PLCs and RTUs are also IT components, albeit as special-purpose computers with special-purpose software. SCADA systems depend upon networking for communicating the data to various components. LAN/WAN technologies are used to interconnect these components within a location, or across multiple locations. Webservers are often used to make SCADA accessible on the Internet.

For support and remote maintenance, remote access is also enabled.

The same security issues that affect IT systems in general also affect SCADA. Bugs are present in the SCADA system software; and new ones are being discovered on an ongoing basis. Since, the SCADA software runs on computers, the security issues of the underlying operating system and any other software on the computers also become relevant. The use of networking, together with its inherent weaknesses in the communication protocols, is also relevant for the security of SCADA. Since, SCADA systems are to be accessed by people, issues related to password security and access rights become important. In order to share and move information between systems, USB thumb-drives or other removable media may be used; however, these increase the chance of a virus infection.

Finally, the use of networking also means that all vulnerabilities can be exploited remotely, and local access to the SCADA system is not mandatory. The use of Internet connectivity means that potentially, any hacker in the world can attack the SCADA system. All the above factors combine to increase substantially the SCADA attack surface. Some of the attacks that a SCADA system can face include the following:

- Denial of service, which blocks the flow of information or access to a system;
- The use of weak passwords, or default passwords, may allow access to unauthorized personnel;
- Unauthorised changes to configurations, or commands, may affect the working of the SCADA system;

Aligning Two Specifications for Controlling Information Security
Riku Nykänen and Tommi Kärkkäinen (2014). *International Journal of Cyber Warfare and Terrorism (pp. 46-62).*
www.igi-global.com/article/aligning-two-specifications-for-controlling-information-security/123512?camid=4v1a

# In Internet's Way: Radical, Terrorist Islamists on the Free Highway

Raphael Cohen-Almagor (2012). *International Journal of Cyber Warfare and Terrorism (pp. 39-58).*
www.igi-global.com/article/in-internets-way/86075?camid=4v1a