Chapter 38
Cyber–Security for ICS/SCADA:
A South African Perspective

Barend Pretorius
Transnet and University of KwaZulu-Natal, Durban, South Africa

Brett van Niekerk
Transnet and University of KwaZulu-Natal, Durban, South Africa

ABSTRACT

Industrial control systems (ICS) or supervisory, control, and data acquisition (SCADA) systems drive many key components of the national infrastructure. It makes these control systems targets for cyber-attacks by terrorists and nation-states who wish to damage their target economically and socially, and cyber-criminals who blackmail the companies operating the infrastructure. Despite the high risk of leaving these systems exposed, providing adequate cyber-security is often challenging. The Stuxnet worm illustrated how vulnerable control systems potentially are when it bypassed a number of security mechanisms to cause physical damage to an Iranian nuclear facility. The article focuses on ICS/SCADA in South Africa discussing the unique challenges and legislation relate to securing control system in the South Africa. A governance and security framework for overcoming these challenges are proposed.

INTRODUCTION

Industrial control systems (ICS) and supervisory, control and data acquisition (SCADA) are terms that are used to describe all forms of control systems and automation in industrial and process controls. However, this is not entirely accurate. It has been become practice that ICS is used as the general term, and SCADA is a subset of this and generally refers to systems that span a large geographic area (Byres, 2012). These types of systems are often used in critical national infrastructure (Miller & Rowe, 2012) such as pipelines and electric power generation and distribution (Chileshe & van Heerden, 2012). These types of systems were being implemented using mechanical pneumatics prior to the advent of microelec-tronics, and the introduction of microcontrollers and microprocessors revolutionised the field (Byres,

2012). ICS/SCADA systems were originally separate from the corporate network and operated specialist communication protocols, however they slowly started implementing standardised protocols and were connected to the corporate networks and the Internet (Miller & Rowe, 2012; Brodsky & Radvanovsky, 2013). Control systems were originally limited to a specific plant or site, however with the evolution of computing and networks there was a drive towards real-time monitoring and control of geographically separate sites. As the ICS/SCADA developed to interconnected systems with standard protocols, they became more vulnerable to attack (Krutz 2006; Brodsky & Radvanovsky, 2013).

During the 1990s the concept of information warfare and cyber-attacks started becoming a concern. The RAND institute in the US conducted a number of studies which indicated that the Internet connectivity and remote access to control systems was originally assuming a trusted communications environment, however the Internet was becoming increasingly hostile and the concern was a rogue state and terrorist group would intentionally attack the SCADA systems over the Internet to create devastation (Molander, Riddile & Wilson, 1996; Molander, Wilson, Mussington & Mesic, 1998). This threat resulted in a series of Presidential Decision Directives and Executive Orders being issued between 1996 and 2003 with the objective of addressing the protection of US critical infrastructure (Krutz, 2006).

The structure of the paper is: a background to security in the ICS/SCADA environment is provided, followed by a discussion of the South African SCADA environment, and the challenges around cyber-security and governance for SCADA. A framework for ICS/SCADA security and governance in South Africa is proposed, then the paper is concluded.

CYBER-SECURITY AND GOVERNANCE OF ICS/SCADA ENVIRONMENTS

This section will discuss the differences between ICS/SCADA environments and traditional enterprise networks, cyber-security incidents involving industrial control and related systems, the vulnerabilities and threats related to ICS/SCADA, and the international frameworks for these environments.

Differences between ICS/SCADA and Corporate Networks and the Associated Challenges

There are a number of differences between ICS/SCADA networks and traditional organisational IT networks, which often result in challenges for managing the security of the ICS/SCADA networks. Neitzel and Huba (2014) describe some of these differences as:

1. **Different security objectives:** Ensuring availability is the primary objective of security in ICS/SCADA networks, whereas confidentiality is often the primary focus on many corporate IT networks;
2. **Network topology and segmentation:** ICS/SCADA systems are usually smaller with static configurations. The use of Dynamic Host Control Protocol (DHCP) and WiFi is discouraged. Ideally, ICS would not have access to internet or email access, and should be defended from internal network segments that have such access. Traditionally corporate networks are segmented into subnets;
3. **Functional partitioning:** The majority of corporate networks will be partitioned by administration function (e.g. HR, finance). ICS/SCADA is partitioned into three levels, namely the physical process, the intelligent devices and sensors, and the control systems which are described by the ANSI/ISA95 Purdue reference model (Control Global, 2008). ICS devices need to be mapped

16 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/cyber-security-for-icsscada/251453

Related Content

US Foreign Policy Challenges of Non-State Actors' Cyber Terrorism against Critical Infrastructure
Natalia Tereshchenko (2012). *International Journal of Cyber Warfare and Terrorism (pp. 28-48).*
www.irma-international.org/article/us-foreign-policy-challenges-of-non-state-actors-cyber-terrorism-against-critical-infrastructure/90839

Cyber Hygiene in Health Care Data Breaches
Jomin Georgeand Aroma Emmanuel (2020). *Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications (pp. 1309-1321).*
www.irma-international.org/chapter/cyber-hygiene-in-health-care-data-breaches/251494

Media Stereotypes of Terrorism
Georgios Terzis (2014). *Exchanging Terrorism Oxygen for Media Airwaves: The Age of Terroredia (pp. 96-108).*
www.irma-international.org/chapter/media-stereotypes-of-terrorism/106153

Strategic Communication for Supporting Cyber-Security
Tuija Kuusistoand Rauno Kuusisto (2013). *International Journal of Cyber Warfare and Terrorism (pp. 72-79).*
www.irma-international.org/article/strategic-communication-for-supporting-cyber-security/104524

A World without Islam
Maximiliano E. Korstanje (2012). *International Journal of Cyber Warfare and Terrorism (pp. 50-52).*
www.irma-international.org/article/world-without-islam/75765