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 microelectronics, and the introduction of microcontrollers and microprocessors revolutionised the field (Byres,

DOI: 10.4018/978-1-7998-2466-4.ch038

Copyright © 2020, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

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

What Does the Concept of Ambidexterity Mean in the Current Military Planning Process and Organization Construction?
Aki-Mauri Huhtinen (2012). *International Journal of Cyber Warfare and Terrorism (pp. 11-21).*
www.irma-international.org/article/what-does-the-concept-of-ambidexterity-mean-in-the-current-military-planning-process-and-organization-construction/81250

Media Development Trends as a Counter for Terrorism in Ukraine
Nadezhda Anatolievna Lebedeva (2022). *Media and Terrorism in the 21st Century (pp. 124-143).*
www.irma-international.org/chapter/media-development-trends-as-a-counter-for-terrorism-in-ukraine/301085

Intelligent Strategy and Security in Education: Big Data (Text Analytics)
Samson Oluwaseun Fadiya (2019). *Applying Methods of Scientific Inquiry Into Intelligence, Security, and Counterterrorism (pp. 87-110).*
www.irma-international.org/chapter/intelligent-strategy-and-security-in-education/228467

On the Behavior-Based Risk Communication Models in Crisis Management and Social Risks Minimization
Yuriy V. Kostyuchenko, Viktor Pushkar, Olga Malyshevaand Maxim Yuschenko (2020). *International Journal of Cyber Warfare and Terrorism (pp. 27-45).*
www.irma-international.org/article/on-the-behavior-based-risk-communication-models-in-crisis-management-and-social-risks-minimization/250904

Cyberinsecurity and Cyberwarfare: The Case for Social Science and Philosophical Approaches. Reflections from Asia.
Alan Chong (2015). *Cybersecurity Policies and Strategies for Cyberwarfare Prevention (pp. 383-396).*
www.irma-international.org/chapter/cyberinsecurity-and-cyberwarfare/133940