Chapter 8
Cybersecurity Risks With Supervisory Control and Data Acquisition (SCADA) Systems is a Public Health and National Security Issue

Horace C. Mingo
https://orcid.org/0000-0002-2395-2990
Marymount University, USA

Darrell Norman Burrell
https://orcid.org/0000-0002-4675-9544
Marymount University, USA

ABSTRACT

Protecting networks that are part of industrial control systems (ICS), such as supervisory control and data acquisition (SCADA) systems, is a significant issue that affects public health as well as public safety and national security. Industrial control systems such as the SCADA systems that manage our electrical grids, oil pipelines, and water distribution systems remain vulnerable to cyber-attacks from different directions through various technologies in the U.S. It is essential to understand that the security of critical infrastructure goes far beyond the scope of cybersecurity. Qualitative interviews with subject matter experts were used to discover the best practices for protecting these systems.

DOI: 10.4018/978-1-6684-7207-1.ch008

INTRODUCTION

Security and Privacy of SCADA Technology

Supervisory Control and Data Acquisition (SCADA) systems are industrial control systems (ICS) networks that contain computers and applications that perform vital functions in providing essential services and commodities (e.g., electricity, natural gas, gasoline, water, waste treatment, transportation) to all Americans (Ginter, 2016; Coffey et al., 2018). As such, they are part of the critical infrastructure in the U.S. and require protection from various threats in cyberspace today (Ginter, 2016; Coffey et al., 2018). By allowing the collection and analysis of data and control of equipment such as pumps and valves from remote locations, SCADA networks provide significant efficiency and are widely used. However, they also present a security risk. SCADA networks were initially designed to maximize functionality, with little attention paid to security (Ginter, 2016; Coffey et al., 2018). As a result, the performance, reliability, flexibility, and safety of distributed control/SCADA systems are robust, while the security of these systems is often weak (Ginter, 2016; Coffey et al., 2018). This makes some SCADA networks potentially vulnerable to service disruption, process redirection, or manipulation of operational data that could result in public safety concerns and severe disruptions to the nation's critical infrastructure (Ginter, 2016; Coffey et al., 2018). Action is required by all organizations, government or commercial, to secure their SCADA networks to adequately protect the nation's critical infrastructure (Ginter, 2016; Coffey et al., 2018).

Protecting networks that are part of industrial control systems (ICS), such as supervisory control and data acquisition (SCADA) systems, is a significant issue affecting public health, safety, and national security. If access to clean water is cut off, it will have repercussions for many community residents and other public services, such as airports, hospitals, manufacturing plants, fire systems, and HVAC systems. In addition, specific components of utilities, such as generators, must be replaced after a certain amount of time has passed. If they were destroyed, it might take months to deliver and implement them, rendering the utility inoperable for an extended period of time. This would worsen the damage and cause people to be injured and harmed.

There has been a rise in the number of cyberattacks launched against infrastructure in the United States in the past three years, specifically against the systems that manage our electrical grids, oil pipelines, and water distribution systems (Cimpanu, 2021). As a result of the attacks, the threat actors encrypted files and, in one instance, even corrupted a computer used to control the SCADA industrial equipment installed inside the treatment plant (Cimpanu, 2021).

A hacker attempted to contaminate a water treatment plant in January 2021, which served several communities in the San Francisco Bay Area (Cimpanu, 2021).

A hacker attempted to change the chemical levels at the WWS facility in Oldsmar, Florida, in February of 2021. The breach was discovered immediately, and the hacker's changes were rolled back as soon as they were identified (Cimpanu, 2021).

A WWS [water and wastewater system] facility in California was attacked by malicious cyber actors using a variant of the ransomware known as Ghost in August 2021. When three supervisory control and data acquisition (SCADA) servers displayed a ransomware message, it was discovered that the ransomware variant had been in the system for approximately one month (Cimpanu, 2021).

In July of 2021, malicious cyber actors used remote access to install the ZuCaNo ransomware onto the wastewater SCADA computer of a WWS facility in Maine. In the interim, while the SCADA computer