Chapter 26
Cyber Security in Liquid Petroleum Pipelines

Morgan Henrie
MH Consulting, Inc., USA

ABSTRACT

The world's critical infrastructure includes entities such as the water, waste water, electrical utilities, and the oil and gas industry. In many cases, these rely on pipelines that are controlled by supervisory control and data acquisition (SCADA) systems. SCADA systems have evolved to highly networked, common platform systems. This evolutionary process creates expanding and changing cyber security risks. The need to address this risk profile is mandated from the highest government level. This chapter discusses the various processes, standards, and industry based best practices that are directed towards minimizing these risks.

INTRODUCTION

This chapter provides practitioners, researchers and those interested in critical infrastructure cyber security concerns a sound foundation on cyber security for crude oil transportation critical infrastructure SCADA systems. Understanding how evolutionary processes have changed this infrastructure control system landscape and how industry is responding to ever increasing cyber security threats is essential for anyone who interacts with these systems at any level.

This chapter's objective is to provide the SCADA system practitioner, manager, engineer, researcher and interested parties an overview of today's SCADA cyber security systems how they came to be, the challenges facing the owner/operator, a review of current industry standards and regulatory landscape as well as examples of how some entities are securing their SCADA networks. This information source provides all interested parties sufficient information to allow them to take the next steps in enhancing their system's cyber security posture.

DOI: 10.4018/978-1-4666-4707-7.ch026

To this end, the chapter is organized in a progressive manner with each section building on the next in following the following sequence.

- Critical infrastructure, what is it? A discussion on critical infrastructure and its background
- SCADA Systems; a review of how SCADA systems have evolved to the current cyber risk state
- A review of the SCADA Cyber security standards
- Resiliency of SCADA systems are secure SCADA Systems
- Defense in depth Cyber security concepts and applications
- SCADA Cyber Security Environmental Uniqueness
- The management structure required to support the system

CRITICAL INFRASTRUCTURE: WHAT IS IT?

Oil and gas transportation systems are identified as national level critical infrastructures. These infrastructures are essential to every nation's safety, defense, private industry commerce, business operations, and normal life. At some level, every nation's electrical grid, commercial enterprises, military facilities, businesses and homes are dependent on the safe, highly available, and reliable delivery of oil and gas liquids. Historical evidence, such as the recent earthquakes and hurricane events, clearly show that if the oil and gas infrastructures are no longer available, the ability to provide essential services is severely constrained or even prevented.

Transporting liquids from point A to point B has a rich historical background. Using pipelines to move liquid is traced back to at least the tenth century B.C. Around 691 B.C., the first water aqueduct was built in Assyria (BookRags, 2010) while later "The first aqueduct built to supply Rome … was constructed about 312 B. C. and had a length of about 11 miles" (Turneaure et al. 1916). Since these early water transportation efforts, utilization of pipeline systems to move water and other liquid and slurry commodities continues to increase. As an example, the United States (US) Department of Transportation (DOT), Pipeline and Hazardous Materials Safety Administration (PHMSA) Office of Pipeline Safety website identifies that within the United States, 168,900 miles of onshore and offshore hazardous crude oil liquid pipelines are in service. Overall, the "…energy transportation network of the United States consists of over 2.5 million miles of pipelines. That's enough to circle the earth about 100 times" (PHMSA, 2010).

These 168,900 miles of hazardous crude oil liquid pipelines are monitored and controlled by supervisory control and data acquisition (SCADA) systems. Crude oil SCADA systems provide critical status, alarm and process information back to the central operator stations while transferring controls commands and setpoint changes from the central operator station to the remote location. SCADA systems provide the ability to monitor and control thousands of miles of pipeline safely, efficiently and effectively as the infrastructure transports this hazardous material through major cities, environmentally sensitive terrain, under major water ways, and through your local neighborhood day-in and day-out. Without modern SCADA systems it is nearly impossible to safely operate and control these critical infrastructures.

To achieve this capability safely, the hazardous liquid pipeline SCADA system is dependent on telecommunication systems, remote terminal devices, computers, servers, routers, etc. to link field devices, such as a relay status, to the control room operator human machine interface (HMI). The remoteness associated with these systems, numerous physical connections, and ever expanding interconnectivity to other systems is raising crude oil SCADA cyber security vulnerability.