Chapter 8

DIVISION OF CYBER SAFETY AND SECURITY RESPONSIBILITIES BETWEEN CONTROL SYSTEM OWNERS AND SUPPLIERS

Ruth Skotnes

Abstract  The chapter discusses the important issue of responsibility for information and communications technology (ICT) – or cyber – safety and security for industrial control systems and the challenges involved in dividing the responsibility between industrial control system owners and suppliers in the Norwegian electric power supply industry. Industrial control system owners are increasingly adopting information and communications technologies to enhance business system connectivity and remote access. This integration offers new capabilities, but it reduces the isolation of industrial control systems from the outside world, creating greater security needs. The results of observation studies indicate that Norwegian power network companies and industrial control system suppliers have contributed to the creation of a culture that does not focus on information and communications systems safety and security. The increased use of standards and guidelines can help improve cooperation between industrial control system owners and suppliers. Norwegian industrial control system owners should also implement a culture change in their organizations and should attempt to influence the safety and security culture of their suppliers. Power network companies need to place information and communications systems safety and security on par with operational priorities and they need to become more vocal in demanding secure products from their suppliers.

Keywords: Power networks, Norway, industrial control systems, owners, suppliers

1. Introduction

Industrial control systems (ICSs) are vital to the operation of critical infrastructure assets that are increasingly interconnected and mutually depen-
dent. Industrial control systems include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCSs) and other systems such as programmable logic controllers (PLCs) and human-machine interfaces (HMIs) [14]. Industrial control systems are deployed worldwide and are traditionally used by utilities and industries in areas such as electric power supply, oil and natural gas, railroads, water and wastewater. These systems support many aspects of modern life and are vital to societal wellbeing and the functioning of the economy [16].

Historically, industrial control systems have had little resemblance to traditional information and communications technology (ICT) – or cyber – systems in that they were isolated systems running proprietary control protocols using specialized hardware and software. However, according to Leith and Piper [14], industrial control systems are increasingly adopting information and communications technologies to support corporate system connectivity and remote access. Manufacturers, vendors and suppliers of industrial control systems (collectively referred to as “suppliers” in this work) are designing and implementing industrial control systems using commodity hardware, software, network devices and protocols; hence, they increasingly resemble traditional information and communications systems. This integration supports new business and operational capabilities, but it reduces the isolation of industrial control systems from the outside world, creating a greater need for security.

According to the U.S. Industrial Control Systems Emergency Response Team (ICS-CERT), infrastructure assets that use industrial control systems have become high-profile targets and are recording increasing numbers of cyber vulnerabilities and incidents [22]. Byres [4] has stated that shifts in technology have greatly increased the complexity and interconnectedness of control systems. As a result, industrial control systems now have many of the same vulnerabilities that have long plagued enterprise networks. In addition, devices in industrial control networks are being subjected to new threats that they were not designed to handle. All these conditions have led to significant increases in the numbers of industrial plant disruptions and shutdowns due to cyber security problems.

This chapter focuses on the Norwegian electric power supply sector. Electric power supply is the basic infrastructure for all kinds of production and services and is highly dependent on computers and communications [15]. Since the early 1990s, the energy sectors in European countries have undergone considerable institutional restructuring, where large state-owned monopolies have been transformed to multiple, smaller independent entities [3]. Emerging control systems that make intensive use of information and communications technologies have greatly assisted in dealing with the multiple independent entities, open access and progressive integration of electricity markets, and the intensification of cross-border trade. However, the full application of these technologies demands a new approach to system design and operation, and their integration in existing control infrastructures and practices has been very challenging [26].