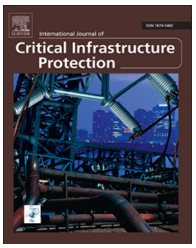
Available online at www.sciencedirect.com

ScienceDirect

www.elsevier.com/locate/ijcip



Critical infrastructure protection: Requirements and challenges for the 21st century

Cristina Alcaraz[a,*], *Sherali Zeadally*[b]

[a]*Computer Science Department, University of Malaga, Campus de Teatinos s/n, 29071 Malaga, Spain*
[b]*College of Communication and Information, University of Kentucky, Lexington, Kentucky 40506-0224, USA*

ARTICLE INFO

Article history:
Received 17 July 2014
Accepted 11 October 2014
Available online 11 December 2014

Keywords:
Critical infrastructure protection
SCADA systems
Risk
Security
Requirements
Challenges

ABSTRACT

Critical infrastructures play a vital role in supporting modern society. The reliability, performance, continuous operation, safety, maintenance and protection of critical infrastructures are national priorities for countries around the world. This paper explores the vulnerabilities and threats facing modern critical infrastructures with special emphasis on industrial control systems, and describes a number of protection measures. The paper also discusses some of the challenging areas related to critical infrastructure protection such as governance and security management, secure network architectures, self-healing, modeling and simulation, wide-area situational awareness, forensics and learning, and trust management and privacy.

1. Introduction

A critical infrastructure comprises systems and assets, whether physical or virtual, that are so essential to a nation that any disruption of their services could have a serious impact on national security, economic well-being, public health or safety, or any combination thereof [76]. The European Union (EU), through its European Programme for Critical Infrastructure Protection (EPCIP), also stresses the importance of critical infrastructure protection to all its member states and their citizens. To address critical infrastructure protection, the European Commission issued a communication [26] to establish a legislative framework for transparency with regard to critical infrastructure protection and to enable cooperation across national borders. According to EPCIP, critical infrastructures are classified as follows:

- *Energy:* Energy production sources, storage and distribution (oil, gas and electricity).
- *Information and communications technology:* Information system and network protection (e.g., Internet); provision of fixed telecommunications; provision of mobile telecommunications, radio communications and navigation, satellite communications and broadcasting.
- *Water:* Provision of water (e.g., dams), control of water quantity and quality.
- *Food and agriculture:* Food provision, safety and security.
- *Healthcare and public health:* Medical and hospital care; medicines, serums, vaccines and pharmaceuticals; biolaboratories and bio-agents.
- *Financial systems:* Banking, payment services and government financial assignments.
- *Civil administration:* Government facilities and functions, armed forces, civil administration services, emergency services, postal and courier services.
- *Public, legal order and safety:* Maintaining public and legal order, safety and security; administration of justice and detention.

*Corresponding author.
E-mail address: alcaraz@lcc.uma.es (C. Alcaraz).

http://dx.doi.org/10.1016/j.ijcip.2014.12.002
1874-5482/

- *Transportation systems:* Road transport, rail transport and air traffic; border surveillance; inland waterways transport; ocean and short-sea shipping.
- *Chemical industry:* Production and storage of dangerous substances, pipelines carrying dangerous goods.
- *Nuclear industry:* Production and storage of nuclear materials.
- *Space:* Communications and research.
- *Research facilities:* Operation of major research facilities.

The U.S. National Infrastructure Protection Plan (NIPP) [73] as defined by the Department of Homeland Security (DHS) considers the following additional critical sectors:

- *National monuments and icons:* Monuments, physical structures, objects or geographical places that represent national culture or have religious or historical importance.
- *Commercial facilities:* Commercial centers, office buildings, sports stadiums and other places that accommodate large numbers of people.
- *Critical manufacturing:* Transformation of materials into goods, including all the processes involved in manufacturing and transportation.
- *Defense industry base:* Facilities that produce military resources (e.g., weapons, aircraft and ships) and maintenance of essential national security services (e.g., communications).

The connections between critical infrastructure sectors produce special interdependence relationships. The relationships express the fact that one critical infrastructure could depend on products and services provided by another critical infrastructure, and the second critical infrastructure may also depend on the products and services provided by the first critical infrastructure. These interdependencies could trigger cascading effects in multiple critical infrastructures when one critical infrastructure is disrupted, damaged or destroyed [7]. Rinaldi et al. [63] have identified and analyzed four types of interdependencies: (i) physical; (ii) geographic; (iii) cyber; (iv) and logical. A physical interdependency exists when a critical infrastructure requires resources or raw materials from other infrastructures. A geographic interdependency exists when multiple infrastructures share a close spatial proximity, and a problem in one critical infrastructure can reach the other critical infrastructures. A cyber interdependency is the result of a dependency on information and communications systems. A logical interdependency exists when systems, actions or decisions connecting an agent in one infrastructure to an agent in another infrastructure are not physical, geographic or cyber in nature (e.g., bureaucratic or political decisions) [82].

Given the influence of information systems on the performance of other critical infrastructures, this paper focuses primarily on critical information infrastructures and their security issues. A critical information infrastructure consists of information processes supported by information and communications technologies that form critical infrastructures themselves or that are critical to the operation of other critical infrastructures [16]. The vast majority of, if not all, critical infrastructures are dependent on information systems. Thus, a disruption to a cyber infrastructure can lead to serious consequences that affect the performance, reliability, security and safety of the dependent infrastructures. The massive dependence on the cyber infrastructure has created the new research area known as critical information infrastructure protection (CIIP).

According to the European Commission [25], critical information infrastructure protection comprises programs and activities of infrastructure owners, manufacturers, users, operators, research and development institutions, governments and regulatory authorities that aim to maintain the performance of critical information infrastructures in the event of failures, attacks or accidents above a defined minimum level of service and to minimize damage and recovery time. Critical information infrastructure protection should, therefore, be viewed as a cross-sector activity instead of being limited to specific sectors. Critical information infrastructure protection should be closely coordinated with critical infrastructure protection under a holistic perspective [25]. The U.S. Government also emphasizes critical information infrastructure protection in Public Law 107-296 [77], which states that the "protection of critical information infrastructures is important to the national defense and economic security of the nation." This law deems critical information infrastructures to be critical infrastructures themselves because their information is not normally in the public domain and is related to the security of critical infrastructures and other vital systems. In fact, information and communications technologies, which underlie communications links, network topologies and interfaces that manage and transmit sensitive data in a reliable and timely manner, constitute the backbone of critical infrastructures.

One of the most important types of critical information infrastructures is industrial control systems (ICSs) that supervise and control processes in industrial infrastructures such as bulk energy generation systems, electrical distribution and transmission systems, water treatment systems, oil and gas pipelines, and chemical plants and refineries [12]. These systems incorporate communications architectures for connecting control centers to remote substations located at the infrastructures being controlled (Fig. 1). The substations incorporate automated systems called remote terminal units (RTUs) that house sensors for collecting and sending status data to the control center and actuators for performing control actions as directed by the control center.

Industrial control systems include supervisory control and data acquisition (SCADA) systems and distributed control systems (DCSs). A SCADA system is an event-driven centralized network with substations located over a large geographic area (Fig. 1). It incorporates three main components: the control center, substations and a corporate network. The control center is responsible for managing and supervising the overall system. The functionality is supported by SCADA servers and data historians that store process and system information. External access to these resources must be secured using firewalls, demilitarized zones (DMZs), intrusion detection systems (IDSs), intrusion prevention systems (IPSs) and anti-virus software. Access must also be provided to the corporate network, which supports business operations. In contrast, a distributed control system is a process-oriented