Chapter 5
ENISA Study:
Challenges in Securing
Industrial Control Systems

Rafal Leszczyna
ENISA, European Union & Gdansk University of Technology, Poland

Elyoenai Egozcue
S21sec, Spain

ABSTRACT
In 2011, the European Network and Information Security Agency (ENISA) conducted a study in the domain of Industrial Control Systems (ICS). Its objective was to obtain the current view on the ICS protection primarily in Europe but also in the international context. The ‘portrait’ included threats, risks, and challenges in the area of ICS protection as well as national, pan European, and international initiatives on ICS security. The study was performed through desktop research, survey and interviews, and a meeting with all involved stakeholders. This chapter highlights the most relevant parts of the final report of the study. It focuses on the challenges to securing ICS identified during the research, but also presents the context and the methodology of the study. In response to the challenges, the seven recommendations of ENISA for protecting ICS are proposed.

INTRODUCTION
Industrial Control Systems (ICS) are command and control networks and systems designed to support industrial processes (Igure, Laughter, & Williams, 2006). These systems are responsible for monitoring and controlling a variety of processes and operations such as gas and electricity distribution, water treatment, oil refining or railway transportation. The largest subgroup of ICS is SCADA (Supervisory Control and Data Acquisition) systems. Industrial control systems constitute a strategic asset of critical infrastructures.

Since the potential for catastrophic terrorist attacks that affect critical infrastructures is increasing (Commission of the European Communities,
ENISA Study

In 2004, a series of actions were launched to address this issue. These activities were driven by the European Commission, the Council and the Justice and Home Affairs Council and resulted in the adoption of the conclusions of a European Programme for Critical Infrastructure Protection (EPCIP) (Commission of the European Communities, 2006) by the Council of the European Union, in April 2007. The key element of EPCIP is the Directive on the Identification and Designation of European Critical Infrastructures (Commission of the European Communities, 2008). In parallel, the information security issues for vital infrastructures in Europe are addressed by The Digital Agenda for Europe (DAE) (Commission of the European Communities, 2010) and the CIIP action plan (Commission of the European Communities, 2009).

Recognising the importance of assuring the security of industrial control systems in the protection of critical infrastructures, in 2011 the European Network and Information Security Agency (ENISA) launched a series of activities, which aimed at bringing together the relevant stakeholders and engaging them into an open discussion on ICS protection. The principal goal of the open dialogue was to identify the main concerns regarding the security of ICSs as well as to recognize and support national, pan European and international initiatives on ICS security. The involved stakeholders included ICS security tools and services providers, ICS software/hardware manufacturers and integrators, infrastructure operators, public bodies, standardisation bodies and academia, R&D.

Furthermore, in order to help the stakeholders get a deeper insight on the issue, ENISA decided to further explore this problem by delivering a research and survey-based study on this topic. The objective of the study was to obtain the current perspective of ICS protection primarily in Europe, but also in the international context. This view includes threats, risks and challenges in the area of ICS protection as well as national, pan European and international initiatives on ICS security.

The outcomes of the study were gathered into the report “Protecting Industrial Control Systems: ENISA Recommendations” (ENISA, 2011), which is divided into the main part (the main report) and 5 annexes. The main report summarises the results of the study, while the annexes contain the detailed information on the results. Annex I presents the main results coming from a desktop research phase. It provides a comprehensive overview of the current panorama of ICS security. Annex II provides a detailed analysis of the data gathered from the interviews and the survey in which ICS security experts participated. Annex III is a compilation of current security guidelines and standards for ICS.

Annex IV includes a complete list of initiatives related with ICS security. Annex V provides detailed descriptions of the Key Findings which make up the knowledge base on which recommendations are built upon. Annex VI includes the minutes of the Workshop. The distribution of content among the appendices is illustrated in Figure 1.

This chapter highlights the most relevant parts of the report to present the study of ENISA and its core results. It starts with an overview of Industrial Control Systems and continues with the description of the study and the research approach applied to it. After that the selected results of the study are demonstrated, which includes the interesting outcomes of the literature study and the survey and the interviews of the experts. Based on the findings the seven recommendations of ENISA for the protection of Industrial Control Systems were derived. The recommendations call for:

1. Developing national and pan-European ICS security strategies
2. Creating a good Practices Guide for ICS Security
3. Developing ICS security plan templates
4. Raising awareness and training
5. Creating a common test bed or ICS security certification framework
Related Content

Cybercafé Physical and Electronic Security Issues
www.igi-global.com/chapter/cybercafe-physical-electronic-security-issues/28531?camid=4v1a

A Survey: Intrusion Detection Techniques for Internet of Things
www.igi-global.com/article/a-survey/218848?camid=4v1a

Cyber-Crimes against Adolescents: Bridges between a Psychological and a Design Approach
www.igi-global.com/chapter/cyber-crimes-against-adolescents/167235?camid=4v1a

Web Service Security: Authentication and Authorization Technologies
www.igi-global.com/chapter/web-service-security/105805?camid=4v1a