Chapter 14

CLASSIFICATION AND COMPARISON OF CRITICAL INFRASTRUCTURE PROTECTION TOOLS

George Stergiopoulos, Efstratios Vasilellis, Georgia Lykou, Panayiotis Kotzanikolaou and Dimitris Gritzalis

Abstract  Modeling and analysis of critical infrastructure interdependencies is a research area that has attracted considerable interest. Interdependency and risk analyses can be computationally intensive, but can also yield useful results that enhance risk assessments and offer risk mitigation alternatives. Unfortunately, many tools and methodologies are left unsupported and are forgotten soon after the projects that developed them terminate.

This chapter attempts to identify and classify many existing tools and frameworks to create a common baseline for threat identification and risk assessment. It also compares their attributes and technologies in creating a taxonomy. Conceptual and qualitative studies about infrastructure interdependencies along with modeling and simulation approaches are examined. The comparison is based on two aspects: the purpose that each tool serves and its technical modeling approach. This work attempts to aid the industrial control system security community by acting as a single point of reference and drawing attention to possible modeling combinations to enable researchers to identify and construct complex combined solutions that yield better results. The analysis suggests that future research should address risk mitigation through qualitative rather than quantitative analyses. The contributions can be maximized by developing holistic meta-tools or focusing entirely on specific problems.

Keywords: Critical infrastructure protection tools, taxonomy, classification

1. Introduction

Critical infrastructures are defined by the U.S. Department of Homeland Security [10] as “assets, systems and networks, whether physical or virtual, so
vital that their incapacitation or destruction would have a debilitating effect on security, national economy security, national public health or safety, or any combination thereof.” Critical infrastructure protection methodologies, models and simulations are used to understand infrastructure systems, their interdependencies, vulnerabilities, impacts of potential failures and their propagation across interdependent infrastructure systems, based on risk assessments of all the involved critical infrastructures. They may also be used to support performance measurement, conceptual design, impact evaluation, response planning, vulnerability analyses and economic impact assessments. This chapter seeks to capture knowledge about critical infrastructure protection tools (and methodologies) and classify them to create a common baseline for threat identification and risk assessment.

2. Tool Classification and Comparison

The classification and comparison of critical infrastructure protection tools are based on two aspects: (i) purpose (i.e., functionality) of each tool [10, 20]; and (ii) technical modeling approach [13]. The categories used for each classification are:

- **Purpose Based Classification:** (i) risk identification; (ii) risk assessment; (iii) risk prioritization; (iv) risk mitigation planning; and (v) effectiveness evaluation.

- **Technical Approach Based Classification:** (i) empirical approaches; (ii) system dynamics approaches; (iii) agent based approaches; (iv) network based approaches; and (v) other approaches.

This research has identified, classified and compared 67 critical infrastructure protection tools, most of which were developed in the United States [14].

2.1 Purpose Based Classification

The National Infrastructure Protection Plan (NIPP) [20] classifies tools, frameworks and methodologies according to the purpose they serve. Specifically, the stage or stages of the risk management framework that they support. After setting the security goals, the following goals should be achieved (in serial order):

- **Goal 1: Risk Identification (RI):** Asset identification, vulnerabilities and events with relationships.

- **Goal 2: Risk Impact Assessment (RIA):** Assessment of probabilities and consequences of risk events. May include cost, schedule, performance impact and functionality impacts.

- **Goal 3: Risk Prioritization (RP):** Aggregation and analysis of risk assessment results, establishment of priorities that provide the greatest