# Classification and Comparison of Critical Infrastructure Protection Tools

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



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

mitigation of risk. Assessment of the criticality of risk using decision-analytic rules and ranking of risk events from the most critical to the least critical.

- **Goal 4: Risk Mitigation Planning and Implementation (RMP):** Selection of sector-appropriate protective actions and/or countermeasures to reduce or manage the identified risk.
- **Goal 5: Effectiveness Evaluation (EE):** Evaluation of countermeasures and strategies. Reassessment of risk.

Tables 1 and 2 present the tool taxonomy according to the risk management purpose served. Note that the majority of the tools start with the risk identification (RI) stage and proceed to the subsequent analysis steps (RIA, RP, RMP and EE). Tools that are lower in the classification tree support additional, multiple risk analysis purposes. A few tools skip the first two stages, while very few tools support all the stages of the risk management framework.

## 2.2 Modeling Approach Based Classification

Critical infrastructure modeling approaches refer to techniques used in developing critical infrastructure protection tools. The approaches are often chosen based on the intended purposes of the tools. Ouyang [13] has categorized critical infrastructure protection methodologies and tools using five main types of modeling and simulation approaches:

- **Empirical Approaches:** These approaches analyze interdependencies based on historical events, disaster data and expert knowledge. They can identify failure patterns, quantify interdependency strength metrics to aid in decision making, perform empirical risk analyses and provide alternatives for minimizing risk.
- **System Dynamics Approaches:** These approaches utilize a top-down method to manage and analyze complex adaptive systems with interdependencies. Feedback, stock and flow are the basic concepts in such approaches. Loops indicate connections and the directions of effects between critical infrastructure components.
- **Agent Based Approaches:** These approaches are commonly used by tools. Critical infrastructures are complex adaptive systems and their components can be modeled as agents. Agent based approaches adopt a bottom-up method and assume that complex behavior or phenomena emerge from many individual and relatively simple interactions of autonomous agents. Agents interact with each other and their environment based on a set of rules that mimic the way real infrastructure components would react.
- **Network Based Approaches:** These approaches model critical infrastructures as networks whose nodes represent critical infrastructure components and links represent physical and relational connections between

*Table 1.* Tool classification according to risk management purpose.

| **Tools** | **RI** | **RIA** | **RP** | **RMP** | **EE** |
|---|---|---|---|---|---|
| MIN | T | F | F | F | F |
| TRAGIS | T | F | F | F | F |
| MITS | T | F | F | F | F |
| L2SIM | T | F | F | F | F |
| RTDS | T | F | F | F | F |
| ActivitySim | T | F | F | F | F |
| SessionSim | T | F | F | F | F |
| PC Tides | T | F | F | F | F |
| UPMoST | T | F | F | F | F |
| CIMS | F | T | T | T | T |
| DECRIS | F | T | T | T | T |
| CAPRA | F | T | T | T | F |
| EPRAM | F | T | T | F | F |
| Multi-Graph | F | T | T | F | F |
| AIMSUN | F | T | F | T | F |
| Athena | F | T | F | F | F |
| Nexus Fusion | F | T | F | F | F |
| HCSim | F | T | F | F | F |
| HYDRA | F | T | F | F | F |
| NEMO | F | F | T | T | T |
| CISIA Pro | F | F | T | T | F |
| IntePoint VU | F | F | T | F | F |
| CIPMA | F | F | F | T | T |
| CI3 | F | F | T | F | T |
| Restore | F | F | F | T | F |
| TRANSIMS | F | F | F | F | T |
| CARVER-2 | T | F | T | F | F |
| MUNICIPAL | T | F | T | F | F |
| IEISS | T | F | T | T | F |
| IIM | T | F | T | T | F |
| CIP/DSS | T | F | T | T | T |
| CIPDSS-DM | T | F | T | T | T |
| N-ABLE | T | F | T | T | T |
| IRRIIS | T | T | T | T | T |

critical infrastructure components. A network provides an intuitive representation of a critical infrastructure along with descriptions of topologies and flow patterns. The performance response of a critical infrastructure to hazards can also be analyzed by modeling component failures due to hazards and then simulating cascading failures within and across the critical infrastructure at the system level.

*Table 2.* Tool classification according to risk management purpose (continued).

| **Tools** | **RI** | **RIA** | **RP** | **RMP** | **EE** |
|---|---|---|---|---|---|
| AIMS | T | T | F | F | F |
| FINSIM | T | T | F | F | F |
| PFNAM | T | T | F | F | F |
| FAIT | T | T | F | F | F |
| BIRR | T | T | F | F | F |
| QualNet | T | T | F | F | F |
| CASCADE | T | T | F | F | F |
| LS-DYNA | T | T | F | F | F |
| VISAC | T | T | F | F | F |
| FEPVA | T | T | F | F | F |
| Net-Centric | T | T | F | F | F |
| EpiSimS | T | T | F | F | T |
| Comm-Aspen | T | T | F | F | T |
| (AMTI) Loki | T | T | F | F | T |
| NG Analysis | T | T | F | F | T |
| PipelineNet | T | T | F | T | F |
| WISE | T | T | F | T | T |
| ATOM | T | T | F | T | T |
| CIMSuite | T | T | F | T | T |
| R-NAS | T | T | F | T | T |
| SIERRA | T | T | F | T | T |
| EMCAS | T | T | T | F | F |
| MBRA | T | T | T | F | F |
| FastTrans | T | T | T | F | F |
| AT/FP | T | T | T | F | F |
| TEVA | T | T | T | F | F |
| EURACOM | T | T | T | F | F |
| MSM | T | T | T | F | F |
| RAMCAP | T | T | T | F | F |
| CIPRSIM | T | T | T | F | T |
| LogiSims | T | T | T | T | F |
| NSRAM | T | T | T | T | T |
| Counteract | T | T | T | T | T |
| CIDA | F | F | T | T | T |

- **Other Approaches:** Other major approaches that model and analyze interdependent critical infrastructures are: (i) economic theory based approaches; (ii) cellular automata based approaches; (iii) mathematical equation based approaches; and (iv) real-time simulation based approaches.

Critical infrastructure modeling appears to be associated with simulation techniques and mathematical models. The following simulation techniques and

*Table 3.* Critical infrastructure sectors and their abbreviation prefixes.

| Sector | Prefix | Sector | Prefix |
|---|---|---|---|
| Chemical | CH | Financial Services | FS |
| Commercial Facilities | CF | Food and Agriculture | FA |
| Communications | C | Government Facilities | GF |
| Critical Manufacturing | CM | Healthcare and Public Health | HPH |
| Dams | D | Information Technology | IT |
| Defense Industrial Base | DIB | Nuclear Reactor Materials/Waste | NRMW |
| Emergency Services | ES | Transportation Systems | TS |
| Energy | E | Water/Wastewater Systems | W |

mathematical models were identified in this research: (i) continuous time-step simulation; (ii) discrete time-step simulation; (iii) Monte Carlo simulation; (iv) decision trees; (v) geographical information systems; and (vi) risk management.

The classification model of Ouyang [13] is used to categorize the critical infrastructure tools. Each tool is assigned to one category. Hybrid methodologies and tools (i.e., those engaging more than one approach) are categorized based on their dominant approach and are further classified based on the additional approaches used. Tools are also categorized according to supplementary techniques (e.g., continuous/discrete time-step simulation, geographical information system). In general, the most dominant approaches are agent and network based approaches.

## 2.3 Classification Summary

Table 3 shows the sixteen infrastructure sectors that are designated as critical by the U.S. Department of Homeland Security [12]; the table also shows the sector abbreviation prefixes that are used in the discussion below.

*Table 4.* Classification abbreviation prefixes.

| Purpose Functionality | Prefix | Modeling Technique | Prefix |
|---|---|---|---|
| Risk Identification | RI | Continuous Time-Step | CS |
| Risk Impact Assessment | RIA | Decision Tree | DT |
| Risk Prioritization | RP | Discrete Time-Step | DS |
| Risk Mitigation Planning | RMP | Geographical Information System | GIS |
| Effectiveness Evaluation | EE | Monte Carlo Simulation | MC |

Table 4 shows the risk purpose and modeling techniques along with their abbreviation prefixes.

Figure 1 summarizes the comparison aspects for the two dimensions of tool classification (i.e., purpose and technical approach). Tables 5 through 9 present the detailed taxonomy of the critical infrastructute tools examined in this study.

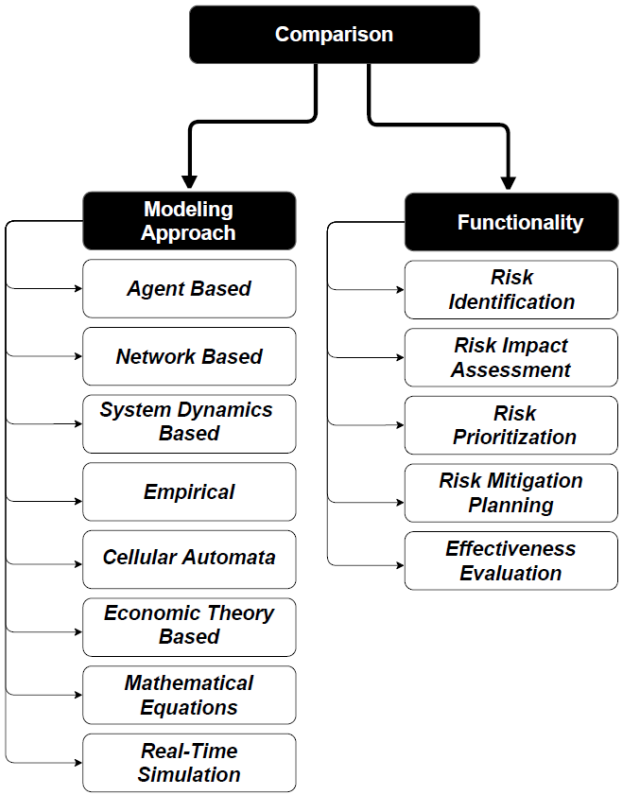


*Figure 1.* Comparison aspects for tool classification.

## 3. Modeling Tool Comparison

It should be stated that most tools considered in this study were for in-house use only. As a result, it was not possible to have hands-on access to all the tools for evaluation purposes. Most of the information used in the following classification and comparison was obtained from technical reports and published articles.

### 3.1 Purpose Based Comparison

Comparing critical infrastructure tools based on the risk management stages in which they are used provides valuable insights. In all, 76% of the tools deal with risk identification (RI), 67% deal with risk impact assessment (RIA), 42% provide some sort of risk prioritization (RP), 41% are used for risk mitigation planning (RMP) and just 35% evaluate the effectiveness of countermeasures (EE).

Due to the complex data analysis requirements, it is difficult to create a single tool that supports all the risk management stages. Less than 5% of the

*Table 5.* Tool classification based on purpose and technical approach.

| Tool | Developer | Modeling | Purpose | Sector |
|---|---|---|---|---|
| ActivitySim | Los Alamos National Laboratory | Agent Based, DS | RI | CF |
| AIMS | University of New Brunswick | Agent Based, CS | RI, RIA | E, C, WWS, IT |
| AIMSUN | Transport Simulation Systems | System Dynamics Based | RIA, RMP | TS |
| AMTI | Sandia National Laboratories | Network Based | RIA, EE | E, TS, FS |
| AT/FP | Naval Postgraduate School | Agent Based, GIS | RI, RIA, RP | DIB, ES, HPH, TS |
| Athena | California Institute of Technology | Network Based, DT | RIA | C, CF, CM, DIB, E, FS, IT, NRMW, WWS, TS |
| ATOM | Sandia/Los Alamos National Laboratories | Network Based | RI, RIA, RMP, EE | TS |
| BIRR | U.S. Dept. of Homeland Security | Methodology | RI, RIA | All Sectors |
| CAPRA | World Bank/ United Nations Project | System Dynamics Based | RIA, RP, RMP | WWS, HPH, TS, FS |
| CARVER-2 | National Infrastructure Institute | Empirical | RI, RP | HPH |
| CASCADE | Det Norske Veritas | Empirical | RI, RIA | All Sectors |
| CI3 | Argonne National Laboratory | Network Based, MC | RP, EE | C, CM, E, NRMW, WWS |
| CIDA | Athens University of Economics and Business | Empirical, Network Based | RP, RMP, EE | All Sectors |
| CIMS | Idaho National Laboratory | Agent Based, MC | RIA, RP, RMP, EE | C, CF, E, TS, HPH |

*Table 6.* Tool classification based on purpose and technical approach (continued).

| **Tool** | **Developer** | **Modeling** | **Purpose** | **Sector** |
|---|---|---|---|---|
| CIMSuite | Idaho National Laboratory | System Dynamics Based | RI, RIA, RMP, EE | All Sectors |
| CIP/DSS | Los Alamos/ Sandia/Argonne National Laboratories | System Dynamics Based | RI, RP, RMP EE | All Sectors |
| CIPDSS-DM | Los Alamos/ Sandia/Argonne National Laboratories | Empirical | RI, RP, RMP, EE | All Sectors |
| CIPMA | Government of Australia | System Dynamics Based | RMP, EE | C, E, IT, TS, FS |
| CISIA-Pro | University of Roma Tre | Agent Based, Relational Databases | RP, RMP | C, CM, E, WWS, C |
| Comm-Aspen | Sandia National Laboratories | Agent Based, MC | RI, RIA, EE | FS, C, E |
| Counteract | European Research Project | Methodology | RI, RIA, RP, RMP, EE | TS, E, HPH |
| DECRIS | SAMRISK Project | Methodology | RIA, RP, RMP, EE | E, WWS, TS, C, IT |
| EMCAS | Argonne National Laboratory/Adica Consulting | Agent Based, DS | RI, RIA, RP | E |
| EpiSimS | Los Alamos National Laboratory | Agent Based, GIS | RI, RIA, EE | HPH |
| EPRAM | NISAC | Cellular Automata | RIA, RP | E |
| EURACOM | EU/DG for Enterprise and Industry | Methodology | RI, RIA, RP | All Sectors |
| FAIT | Sandia National Laboratories | Network Based, GIS, Relational Databases | RI, RIA | E, ES, FS, TS, WWS |
| FastTrans | Los Alamos National Laboratory | Agent Based, DS | RI, RIA, RP | TS |
| FEPVA | Los Alamos National Laboratory | Network Based, GIS, Relational Databases | RI, RIA | E |

*Table 7.* Tool classification based on purpose and technical approach (continued).

| Tool | Developer | Modeling | Purpose | Sector |
|---|---|---|---|---|
| FINSIM | Los Alamos National Laboratory | Agent Based, CS | RI, RIA | FS, E, C |
| CBRSim (Fort Future) | U.S. Army Corps of Engineers | Agent Based, GIS | RI, RIA, RP, EE | C, CF, CM, E, ES, FS, HPH, IT, NRMW, TS, WWS |
| HCSim | Los Alamos National Laboratory | Agent Based, DS | RIA | D, HPH, NRMW |
| HYDRA | Los Alamos National Laboratory | Network Based, GIS, Relational Databases | RIA | HPH, FS |
| I2SIM | University of British Columbia | Agent Based, GIS | RI, RP, RMP | CF, TS, CM, HPH |
| IEISS | University of Virginia | Agent Based, GIS | RI, RP, RMP | E, TS, WWS |
| IIM | Sandia/Los Alamos National Laboratories | Economic Theory Based | RI, RP, RMP | FS, E, C, IT, TS, FS |
| IntePoint VU | IntePoint | Agent Based, GIS | RP | C, E, CF, TS |
| IRRIIS | IRRIIS Project | Network Based, DS | RI, RIA, RP, RMP, EE | All Sectors |
| Knowledge Management Visualization | Carnegie Mellon University | Network Based, Rating Matrices | RMP, EE | E, TS, WWS |
| LogiSims | Los Alamos National Laboratory | Empirical | RI, RIA, RP, RMP | HPH, E |
| LS-DYNA | Livermore Software Technology | System Dynamics Based | RI, RIA | CM, D, TS |
| MBRA | Naval Postgraduate School | Network Based, FT | RI, RIA, RP | FS, TS, E |
| MIITS | Los Alamos National Laboratory | Agent Based, DS | RI | C, IT |
| MIN | Purdue University | Agent Based, CS | RI | CF, TS |

*Table 8.* Tool classification based on purpose and technical approach (continued).

| **Tool** | **Developer** | **Modeling** | **Purpose** | **Sector** |
|---|---|---|---|---|
| MSM | Massachusetts Institute of Technology | Network Based, DT | RI, RIA, RP | E, WWS, HPH |
| Multi-Graph Vulnerability Analysis | Network Based, DS | RIA, RP | E, W, CH | All Sectors |
| MUNICIPAL | Rensselaer Polytechnic Institute | Network Based, GIS, Relational Databases | RI, RP | E, C, IT, TS |
| N-ABLE | Sandia/Los Alamos National Laboratories | Agent Based, DS | RI, RP, RMP, EE | E, FS, TS |
| NEMO | Sparta | Network Based, GIS, Relational Databases | RP, RMP, EE | C, E, WWS, TS, DIB |
| Network-Centric GIS | York University | Network Based, GIS, Relational Databases | RI, RIA | TS, WWS, ES |
| Nexus Fusion Framework | BT Pervasive ICT Research Centre | Agent Based, GIS | RIA | E, C, TS, DIB |
| NGAT | Argonne National Laboratory | Agent Based, Relational Databases | RI, RIA, EE | E |
| NSRAM | James Madison University | Agent Based, MC | RI, RIA, RP, RMP, EE | E, IT, C |
| PC Tides | Neptune Navigation Software | Mathematical Equations | RI | HPH, ES |
| PFNAM | Argonne National Laboratory | Network Based | RI, RIA | E, TS |
| PipelineNet | Federal Emergency Management Agency/ EPA/TSWG | Network Based, GIS, Relational Databases | RI, RIA, RMP | WWS, HPH |
| QualNet | Scalable Network Technologies | Network Based, DS | RI, RIA | C |
| RAMCAP-Plus | ASME Innovative Technologies Institute | Mathematical Equations | RI, RIA, RP | NRMW, CH, D, W |

*Table 9.* Tool classification based on purpose and technical approach (continued).

| Tool | Developer | Modeling | Purpose | Sector |
|---|---|---|---|---|
| Restore | Argonne National Laboratory | Empirical | RMP | CM, E |
| R-NAS | Sandia/Los Alamos National Laboratories | Network Based | RI, RIA, RMP, EE | FA, TS |
| RTDS | Idaho National Laboratory | Real-Time Simulation | RI | E |
| SessionSim | Los Alamos National Laboratory | Agent Based, DS | RI | C |
| SIERRA | Sandia/Los Alamos National Laboratories | Network Based | RI, RIA, RMP, EE | TS |
| TEVA | EPA National Homeland Security Research Center | Empirical | RI, RIA, RP | HPH, WWS |
| TRAGIS | Oak Ridge National Laboratory | Network Based, GIS, Relational Databases | RI | TS, WWS |
| TRANSIMS | Los Alamos National Laboratory | Agent Based, DS | EE | TS, CF |
| UPMoST | NISAC | Methodology | RI | CF |
| VISAC | Oak Ridge National Laboratory | System Dynamics Based | RI, RIA | CH, NRMW |
| WISE | Los Alamos National Laboratory | Agent Based, CS | RI, RIA, RMP, EE | CS, TS, WWS, HPH |

tools cover five stages and 17% cover four stages. Nearly 80% of the tools cover three or fewer stages.

Methodologies such as Counteract, IRRIIS, EURACOM and BIRR and sophisticated tools such as NSRAM cover all five stages of risk analysis. NSRAM is a complex network modeling and simulation tool, but it only covers three sectors (E, IT, C). A limited number of tools (5%) cover more than four risk analysis stages and more than ten sectors. Once again, most of them incorporate broad methodologies or are advanced tools developed in the United States such as CIP/DSS, CIPDSS-DM, CBRSin (Fort Future) and CIMSuite.

CIP/DSS [2], for example, is a complete risk assessment methodology that can be applied to all sectors. Developed under the National Infrastructure Protection Plan, the methodology uses system dynamics with continuous time-step simulation. Like CIP/DSS, the CIPDSS-DM tool is designed to help analysts and policy makers evaluate and select optimal risk mitigation strategies. CIP/DSS and CIPDSS-DM are a robust combination. As a matter of fact, the ability of CIPDSS-DM to facilitate the selection of the most effective mitigation strategies is helpful in restricting the impact of failures and reducing economic losses.

CBRSim (Fort Future) [17] was developed by the U.S. Army Corps of Engineers. It is an agent based tool with geographical information system support that runs multiple dynamic simulations to evaluate a set of alternative scenarios.

CIMSuite [4], CIDA (Critical Infrastructure Dependency Analysis tool) [19] and Athena [3, 14, 22] can depict cascading effects in all sectors and for all infrastructure relationships. CIMSuite is a system dynamics based tool that implements a variety of probabilistic simulations and covers four risk management stages (RI, RIA, RMP, EE). CIDA is a hybrid (empirical and network based) tool that employs several growth models and fuzzy logic to consider the effects of dependencies; it covers the last three risk management stages (RP, RMP, EE). Athena only supports the risk impact assessment (RIA) stage and can be used to model a number of different risk events in various sectors. Of all the tools mentioned above, CIDA is the only one that is publicly available.

With regard to the risk identification (RI) and risk prioritization (RP) stages, CARVER-2 [5, 15] and MUNICIPAL [8, 22] appear to be effective at analyzing multiple critical infrastructure components in order to identify and prioritize them according to the severity of failure impacts, albeit using technical approaches. CARVER-2 uses rating matrices to generate hazard maps whereas MUNICIPAL relies on a relational database that maintains network asset inventories.

IEISS [10, 22] is well suited to risk mitigation planning (RMP) in the energy, water and wastewater systems, nuclear reactor materials and waste sectors. It simulates dynamic behavior, including the effects of system interdependencies. IIM [22] is a continuous input-output model that uses analytical models to determine the impacts of attack on infrastructures and their cascading effects in all the interconnected infrastructures [10]; like IIM, it uses continuous simulation and is employed in the energy and water and wastewater sectors. Both IEISS and IIM are designed for risk identification, risk prioritization and risk mitigation planning. IIM has wider sector coverage compared with IEIIS. IEISS uses a multi-agent system with Monte Carlo simulation as a supplementary technique while IIM uses rating matrices and network theory with continuous time-step simulation.

*Table 10.* Number of sectors per modeling approach.

| Modeling Approach | 1 to 3 Sectors | 4 to 6 Sectors | 7 or More Sectors |
|---|---|---|---|
| Agent Based | 16 | 7 | 2 |
| Network Based | 13 | 4 | 2 |
| Empirical | 5 | 0 | 2 |
| System Dynamics Based | 4 | 3 | 2 |
| Other | 3 | 3 | 2 |

## 3.2 Technical Approach Based Comparison

Comparison of the modeling approaches used by the tools against the risk management stages they cover reveals that empirical tools mostly cover the early risk management stages (RI, RP). Agent based tools are mostly popular for RI while network based approaches usually cover three risk stages (RI, RIA, RMP). System dynamics and network based approaches are mainly used by the few tools that cover four risk management stages. Even fewer (only three) tools cover all five risk management stages, but there is no discernible trend with regard to the specific approaches that are used.

Critical infrastructure modeling tools mainly use mathematical models and simulation techniques combined with the above supplementary computational techniques. Table 10 shows the number of sectors per modeling approach. The majority of the agent and network based tools support up to three critical infrastructure sectors. Most tools that cover one or two sectors are geared for the energy, transportation and/or public health sectors. Multi-agent systems and system dynamics techniques appear to combine well with computational methods such as Monte Carlo simulation, discrete time-step simulation and continuous time-step simulation and are most suitable for obtaining optimal solutions [14, 22]. Agent based simulations combine well with geographical information systems to predict the performance of infrastructures during emergencies in specific geographical areas.

Relational databases are currently the predominant choice for storing data and records pertaining to critical infrastructure system properties. Relational databases are widely used in asset identification and can be combined with event monitoring, real-time recording, geographical information systems, error logs, access control, risk components, etc.

Rating matrices are useful for assessing risk severity and event occurrence. The modeling techniques include data processing in risk analysis and risk mapping to support decision making. Rating matrices are popular because they tend to combine well with every computational technique and also facilitate sensitivity analysis. Additionally, they are appropriate for data classification using geographical information systems and for monitoring events.

Graph theory is used to identify the most critical components or nodes in infrastructures using graphical models that depict relations and properties of

system components in a precise manner. The complexity of network theory models, however, can increase exponentially for large infrastructures.

The majority of the tools – 39 out of 69 tools – are dedicated to specific sectors (or one or two similar sectors), with the energy and transportation sectors being the most popular. NGAT, RTDS, FEPVA and EPRAM [6, 9, 16, 18] are dedicated to the energy sector. Some tools, namely ATOM, SIERRA, FastTrans [11, 21] and AIMSUN [1] are designed for the transportation sector. ATOM and SIERRA [11] cover more than four risk management stages and both tools incorporate network based method approaches. FastTrans is an agent based tool that covers three risk management stages (RI, RIA, RP).

SimCore is a meta-tool that combines multi-agent modeling with discrete time-step simulation. It utilizes a collection of simulation applications (ActivitySim, DemandSim, SessionSim, FastTrans and MIITS-NetSim), all of which engage the SimCore modeling paradigm as a library for building large-scale distributed memory discrete event simulations.

## 4. Conclusions

The primary goal of critical infrastructure protection tools is to help risk assessors and decision makers evaluate risk. The research has identified, classified and compared a number of tools that have been developed for analyzing critical infrastructures and supporting risk management. Emphasis has been placed on comparing similar tools based on their purpose and modeling approach.

The classification and comparison of tools based on the risk assessment stages in which they are used provide a valuable perspective. The analysis identifies the models used in each stage of risk assessment and mitigation, and reveals that most tools focus on the risk identification and risk impact assessment stages.

Classifying technical modeling approaches also provides useful information – most of the tools utilize multi-agent systems coupled with system dynamics, network theory and/or empirical approaches. The analysis reveals that multi-agent and network based modeling techniques are most commonly used in critical infrastructure protection tools.

As expected, no critical infrastructure tool is a "jack of all trades." Indeed, the vast majority of tools specialize in specific parts of the risk management process.

It is important to note that the taxonomy is incomplete because many tools have been built for in-house use and few details are available about them. Additionally, many tools are unsupported, some of them are left unsupported as soon as one year after their development.

Future research should focus on tools geared for the later stages of risk assessment (RMP, EE) and tools that perform qualitative rather than quantitative analyses. Two approaches are suggested for developing new tools with the most utility – one approach is to create holistic meta-tools that can model all critical infrastructure sectors; the other is to create tools that focus on specific problems in specific sectors.

## References

[1] J. Barcelo and J. Casas, Dynamic network simulation with AIMSUN, in *Simulation Approaches in Transportation Analysis: Recent Advances and Challenges*, R. Kitamura and M. Kuwahara (Eds.), Springer, New York, pp. 57–98, 2005.

[2] B. Bush, L. Dauelsberg, R. LeClaire, D. Powell, S. DeLand and M. Samsa, Critical Infrastructure Protection Decision Support System (CIP/DSS) Project Overview, LA-UR-05-1870, Los Alamos National Laboratory, Los Alamos, New Mexico, 2005.

[3] R. Chamberlain, W. Duquette, J. Provenzano, T. Brunzie and B. Jordan, Athena, *NASA Tech Briefs*, p. 12, December 2011.

[4] D. Dudenhoeffer, CIMSuite: Critical Infrastructure Modeling, Idaho National Laboratory, Idaho Falls, Idaho (`www4vip.inl.gov/factsheets/docs/cimsuite.pdf`), 2007.

[5] G. Giannopoulos, R. Filippini and M. Schimmer, Risk Assessment Methodologies for Critical Infrastructure Protection, Part 1: A State of the Art, JRC 70046, European Commission Joint Research Centre, Ispra, Italy, 2012.

[6] J. Kavicky, M. Jusko, B. Craig, E. Portante and S. Folga, A natural gas modeling framework for conducting infrastructure analysis studies, *Proceedings of the Winter Simulation Conference*, pp. 2891–2901, 2009.

[7] E. Lee, J. Mitchell and W. Wallace, Network flow approaches for analyzing and managing disruptions to interdependent infrastructure systems, *Wiley Handbook of Science and Technology for Homeland Security*, vol. 2(5), pp. 1–9, 2009.

[8] E. Lee, W. Wallace, J. Mitchell and D. Mendonca, Decision technologies for protection of critical infrastructures, *Proceedings of the Working Together: R&D Partnerships in Homeland Security*, 2005.

[9] S. McBride and G. West, Real Time Digital Simulator, Idaho National Laboratory, Idaho Falls, Idaho (`www4vip.inl.gov/research/real-time-digital-simulator/d/real-time-digital-simulator.pdf`), 2014.

[10] C. McLean, Y. Lee, S. Jain and C. Hutchings, Modeling and Simulation of Critical Infrastructure Systems for Homeland Security Applications, NISTIR 7785, National Institute of Standards and Technology, Gaithersburg, Maryland, 2011.

[11] National Infrastructure Simulation and Analysis Center, Network Optimization Models (RNAS and ATOM), Sandia National Laboratories, Albuquerque, New Mexico (`www.sandia.gov/nisac/capabilities/network-optimization-models`), 2012.

[12] B. Obama, Presidential Policy Directive – Critical Infrastructure Security and Resilience, PPD-21, The White House, Washington, DC, 2013.

[13] M. Ouyang, Review on modeling and simulation of interdependent critical infrastructure systems, *Reliability Engineering and System Safety*, vol. 121, pp. 43–60, 2014.

[14] P. Pederson, D. Dudenhoeffer, S. Hartley and M. Permann, Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research, INL/EXT-06-11464, Idaho National Laboratory, Idaho Falls, Idaho, 2006.

[15] R. Peimer, Target analysis, *Emergency Management* (`www.emergency mgmt.com/safety/Target-Analysis.html`), November 27, 2006.

[16] C. Shih, C. Scown, L. Soibelman, H. Matthews, J. Garrett, K. Dodrill and S. McSurdy, Decision support framework for electricity production vulnerability assessment, in *Computing in Civil Engineering*, L. Soibelman and B. Akinci (Eds.), American Society of Civil Engineers, Reston, Virginia, pp. 427–434, 2007.

[17] K. Simunich, T. Perkins, D. Bailey, D. Brown and P. Sydelko, Demonstration of CBR Modeling and Simulation Tool (CBRSim) Capabilities, ERDC/CERL TR-09-39, Engineer Research and Development Center, U.S. Army Corps of Engineers, Champaign, Illinois, 2009.

[18] K. Stamber, T. Brown, D. Pless and A. Berscheid, Modeling and simulation for homeland security, *Proceedings of the Twentieth International Congress on Modeling and Simulation*, pp. 1103–1109, 2013.

[19] G. Stergiopoulos, P. Kotzanikolaou, M. Theocharidou, G. Lykou and D. Gritzalis, Time-based critical infrastructure dependency analysis for large-scale and cross-sectoral failures, *International Journal of Critical Infrastructure Protection*, vol. 12, pp. 46–60, 2016.

[20] U.S. Department of Homeland Security, National Infrastructure Protection Plan, Washington, DC, 2006.

[21] S. Thulasidasan, S. Kasiviswanathan, S. Eidenbenz, E. Galli, S. Mniszewski and P. Romero, Designing systems for large-scale, discrete-event simulations: Experiences with the FastTrans parallel microsimulator, *Proceedings of the International Conference on High Performance Computing*, pp. 428–437, 2009.

[22] J. Yusta, G. Correa and R. Lacal-Arantegui, Methodologies and applications for critical infrastructure protection: State-of-the-art, *Energy Policy*, vol. 39(10), pp. 6100–6119, 2011.