10.53477/2668-2028-21-47

MODELING AND SIMULATION IN CRITICAL INFRASTRUCTURES PROTECTION

Sorina-Denisa POTCOVARU, PhD Candidate
Lieutenant, Doctoral School, "Carol I" National Defense University
sorina.potcovaru@yahoo.com

Abstract: *Critical infrastructure protection is a complex field that involves using specific research methods, capturing the dynamic and complex reality in which infrastructure systems evolve. Modeling and simulation provides particular tools and approaches adapted to the field of critical infrastructure protection. A good knowledge of the methodology and using the appropriate tools can lead to improvements in the security of critical infrastructures. Creating models for infrastructures or systems facilitates research, followed by the simulation of potential events with a negative impact. The studies carried out at the intersection of the two fields open new research opportunities to improve the modeling and simulation tools and increase the resilience of critical infrastructures. The specific modeling and simulation methods find their applicability at the operator's or owners' activity for the elaboration of the security plans and their validation.*

Keywords*: modeling and simulation; methodology; critical infrastructures; protection.*

Modeling and simulation for critical infrastructures in literature

Modeling and simulation has applicability in several fields of activity, generating a wide field of scientific research in the area. Modeling and simulation in the field of critical infrastructures takes place in space and time and involves a significant institutional and social component. In one of the scientific papers representing a meta-study in the field of modeling and simulation, the authors identified six categories of methods following the analysis of published studies: "mathematical model, modeling objective, the scale of analysis, quantity and quality of input data, targeted discipline, and end-user type"[1].A brief presentation of the classification made by the authors is given in table no.1.

Table 1 Synthesis of Modeling and Simulation Methods

Category	Attribute
Mathematical model	agent-based; input-output; graph theory; other emerging models (ex: petri nets, Monte Carlo)
Modeling objective	risk and vulnerability analysis; risk mitigation measures and infra-structure protection; failure propagation prediction, interdependence modeling and simulation
Scale of analysis	system of systems; network; advanced network
Quantity and quality of input data	public/private sector published data; extreme event reported data; directly elicited data.
Targeted discipline	engineering; social-technical; economic.
End user type	industry professionals; government agencies; scholarly re-searchers and scientists.

[1] Satumtira Dueñas-Osorio, Leonardo Dueñas-Osorio, *Synthesis of Modeling and Simulation Methods on Critical Infrastructure Interdependencies Research*, in Sustainable and ResilientCritical InfrastructureSystems, Chennai, India, Springer, 2010, p. 10.

One of the attributes identified within the category of mathematical models is Agent-based. The components of the infrastructure are represented by agents defined by specific rules that prescribe their action in response to the action of another agent. Thus, the system of an infrastructure consists of several agents' interactions, according to the Complex Adaptive Systems approach. Various modeling and simulation programs have been developed, such as N-ABLE, used for economic activities and energy infrastructures or SCIMOD Simulator (Simulation of Interdependence of Critical Infrastructures and MODeling of users' behavior) to address the interdependencies between energy and transport infrastructures. Agend-based methods are suitable for modeling reactions and the evolution over time of the behaviors of the elements of a system.

The IIM-inoperability Input-Output Model is used to analyze the propagation of adverse effects from the affected infrastructure to other infrastructures at the level of goods input-output relations. The model starts from Wassily Leontief's equation for studying the equilibrium conditions in economics. These models analyze the impact on the ability of the infrastructure to generate resources in terms of capacity losses or other disruptions and malfunctions and the effect on other infrastructures for which those resources are input.

Network theory and graph theory also use the representation of the components of infrastructure through nodes and links. Nodes are the units of an infrastructure that consumes or produces resources, and connections are how resources flow from one node to another. The structure presented in this meta-study, organized in the form of a literature matrix, leads to the formulation of essential aspects, preliminary to the organization of research in the field of critical infrastructure protection through modeling and simulation.

First of all, it is vital to establish the objective of the research by simulation modeling. The author proposes a comprehensive set of goals, which are subsequent to the general objective of improving the protection and increasing the resilience of the modeled infrastructure.

The analysis level is another aspect that needs to be clarified in the formulation stage of the problem. In addition to the system and network approach, the literature recommends the simultaneous use of the scale with the local, regional, national and international levels. The choice of the study area is essential in choosing the extensions for the visualization of the terrain, in the modeling of the extended networks, and for the follow-up of the propagation of the effects, especially at the international level[2] to identify the potential European critical infrastructures.

Establishing the necessary data and potential sources of information, in terms of quantity and quality, is a challenge and a key factor for the success of the modeling-simulation activity. The data needed to use the modeling and simulation method for critical infrastructures efficiently can be grouped into the following three categories:

- data necessary for the construction of the model (data about the infrastructure or the infrastructure system);
- data required for the construction of the scenario (data on the manifestation of the event to be simulated);
- data necessary for interpreting the results (from the stage of defining the situation must be formulated the questions to which answers must be found following the method).

In choosing simulation modeling methods and tools, essential factors are the discipline, especially in the context of scientific research subscribed to a particular field of study and the end-user. The logical link between objectives, disciplines, and the user must be established so that the results of the simulation modeling activity can be translated into effective measures and responses for decision-makers.

[2] Satumtira and Leonardo Dueñas-Osorio, *Synthesis of Modeling and Simulation Methods on Critical Infrastructure Interdependencies Research*, in Sustainable and ResilientCritical InfrastructureSystems, Chennai, India, Springer, 2010, p. 21.

As for the category related to the target discipline, that it is necessary to introduce the military field, as a separate field, with specific methods, tools, and purposes from the point of view of security infrastructure and the point of view of defending infrastructure objectives, during a potential armed conflict. Input-output mathematical models can also be used to analyze the flow of vital resources needed to support military action and to ensure freedom of movement for the armed forces. Also, the results of a simulation exercise should be validated and exploited to bring integrated benefits to the three categories of users. Research results can be transformed into industrial innovations and governmental and public policy decisions.

The importance of critical infrastructures has increased with their vulnerability to various types of risks and threats. Negative events with an impact on infrastructure objectives have underlined their vitality and contributed to strengthening critical infrastructure protection, initially as an integral part of the fight against terrorism. From this point of view, the empirical approach to modeling and simulation is relevant. The empirical approach involves the analysis of interdependencies at the level of critical infrastructures, based on data on accidents and incidents in the history of infrastructure and based on the experience of specialists in the field. The challenge for this approach results from the data collection activity. The specialized literature recommends the following sources of information: "newspapers, media reports, internet news outlets, official ex-post assessments, and utility owners and operators."[3]

Applicability of modeling and simulation in critical infrastructure protection activity

From the point of view of modeling and simulation, a crucial aspect is methodology, which represents the principles of the method used to solve problems or make decisions in critical infrastructure protection. Using simulation modeling tools to solve problems involves three main elements: the user, the methodology, and the situation[4]. In the literature, the connection between these elements is described by the LUMAS model: learning, user, methodology, approach and situation.

Thus, it starts from a user who knows a methodology and has a real problem to solve. The user uses the methodology with a specific approach to improve the real situation, generating solutions and thus learning. Starting from the LUMAS model, the question arises: What is the real situation that can be improved in critical infrastructures? In this case, the subject of a problem is the risk, and there is a vulnerability or threat to the infrastructure that needs to be reduced in order to improve protection. The solutions thus identified strengthen the degree of infrastructure protection, performance and resilience. Correctly identified, implemented and disseminated solutions generate learning, constituting even learned lessons of simulated reality. One of the most important products of modeling and simulation application for infrastructures is the threat scenario. A viable security plan contains conclusive threat scenarios based on realistic estimates to identify the best course of action in a risk event.

Modeling and simulation also provide relevant tools for testing the viability of the security plan and updating it as a result of the dynamics of risks and threats. The threat scenario must contain a detailed description of the adverse event that may occur with implications for the safe performance and continuity of the infrastructure. Moreover, the threat scenario must provide data on damage, casualties, lost performance, and recovery time. With the help of appropriate modeling and simulation methods, one can answer what would happen if the threat scenario materialized in terms of impact on critical infrastructure. Based on this response, the necessary measures can be identified to improve protection and increase resilience. Furthermore, to test whether the identified solution is useful, it can be tested by simulation modeling methods.

---

[3] Min Ouyang, *Review on modeling and simulation of interdependent criticalinfrastructure systems*, în Reliability Engineering and System Safety, 121/ 2014. p. 46.

[4] Charles McLean, Y. Tina Lee, Dr. Sanjay Jain, Dr. Charles Hutchings, *Modeling and Simulation of Critical Infrastructure Systems for Homeland Security Applications*, National Institute of Standards and Technology, 2011, p. 6.

All these answers are used as arguments for the decision-making process regarding implementing the measures that proved to be viable following the testing. In the decision-making process is important the cost of implementing the measures, the decision-maker wondering how much does the implementation of the solution cost. But how much does it cost to not implement the measure? Answers to this decision-making stage can also be found by using appropriate mathematical models, with applicability in the economic environment that can predict large-scale economic effects.

The process of solving a critical infrastructure protection problem in terms of risks using modeling and simulation, is described in Figure 1. As can be seen from the graphical representation, modeling and simulation has multiple uses in critical infrastructure protection management.

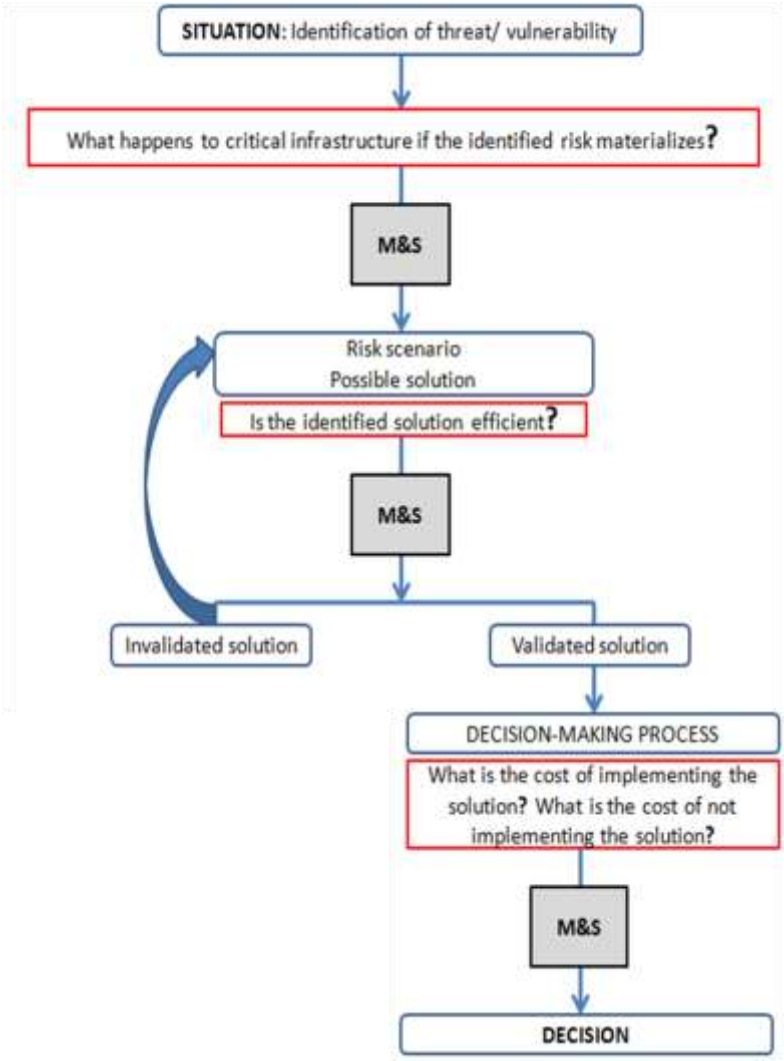

Figure 1: Using modeling and simulation in critical infrastructure protection

The LUMAS model's key element is the user, who must correctly identify the real situation, formulate the problem to be solved, choose the right methods, know the methodology, and have an approach that generates answers. Thus, the user's role cannot be played only by the security liaison officer, but a multidisciplinary team of specialists must be set up. The multidisciplinary team can be made up of key personnel, knowledgeable of specific technical processes, specialists in various fields necessary for an all-hazards approach analysis, modeling and simulation specialists to handle software and methodological tools.

Hence the need to train specialists in critical infrastructure protection in the field of modeling and simulation. Do security liaison officers need to be specialists or is it enough for them to work with other specialists in a multidisciplinary team? The optimal solution is that of a multidisciplinary team. The critical infrastructure protection officer's key role is to identify the problem, formulate the situation together with the other specialists, and provide the necessary data and variables. It is also essential how the simulation results are interpreted and their transposition into threat scenarios and additional protection measures. Identifying and then implementing additional protection measures is a decision-making process that considers both the cost of security and the cost of manifesting what is likely or even unlikely.

The challenge of applying the modeling and simulation methods is to provide answers in cross-cutting criteria established by European legislation on critical infrastructure protection. Directive 2008/114[5] establishes three cross-cutting criteria: victims, economic effects, public effects. A simulation to describe the impact of a negative event that may disrupt or destroy critical infrastructure must provide data on the three cross-cutting criteria. Thus, the model is a more complex one requiring an abstraction of the infrastructure and a representation of systems composed of interdependent infrastructure objectives and connections established with the social macrosystem. With the help of appropriate simulation modeling tools, estimation data can be provided on the number of victims in terms of injuries and deaths and economic and environmental effects. However, it is difficult to simulate the third criterion, which involves transposing into quantitative data and mathematical algorithms the elements related to the impact on public confidence, physical suffering, and disruption of daily life, including the loss of essential services. In addition to the data on the modeled system and the simulated event, a good knowledge of social phenomena through qualitative and quantitative methods is required.

Modeling and simulation is used both in the field of critical infrastructure but especially in the military. New perspectives for research appear at the intersection of the two fields. The finality of the modeling and simulation processes is integrating critical infrastructures in planning and conducting military action by exploiting the common points of the threat scenario and course of action. Thus, it is possible to analyze the impact of a certain course of action on infrastructure or a complex system built by the relations of influence and interdependence between infrastructures. Simulating a military attack on critical infrastructure can provide relevant data for building the defense of the infrastructure target. It can also simulate military action by limiting or stopping the flow of vital resources provided by critical infrastructures, such as transport, energy, or communications services, indispensable for ensuring freedom of action. Implementing such simulation modeling methods is possible in military exercises in the field of critical infrastructure protection in a framework of interinstitutional cooperation. Similarly, it is possible to simulate terrorist attacks on critical infrastructure through a joint exercise of the authorities responsible for protecting critical infrastructure and members of the National System for Preventing and Combating Terrorism.

Modeling and simulation provide specialists with relevant tools and data for the process of identifying European critical infrastructure, defined by European and national legislation as a critical infrastructure located in the territory of a Member State and whose destruction has a significant impact in at least 2 Member States. This analysis requires the model to reproduce the extended infrastructure system and use tools to visualize and analyze the terrain corresponding to the territory of the Member States in the vicinity of the infrastructure objective. Specialists need to identify potential adverse events that may have such a significant impact to simulate them. The simulation should allow the analysis and observation of the spread of effects and consequences at the level of neighboring Member States and provide data to assess the cross-cutting criteria according to the legislator's thresholds set by the legislator.

[5] Council Directive 2008/114/EC of 8 December 2008 *on the identification and designation of European critical infrastructures and the assessment of theneed to improve their protection*, Official Journal of the European Unio, L345/75.

Simulation of unlikely events with serious consequences

Is it worth simulating what is unlikely but with severe effects for when the event will occur?

In 2019, in October, shortly before the onset of the Covid pandemic19, an Event 201 exercise was held, organized by the Johns Hopkins Center for Health Security. The exercise simulated a global pandemic with one of the types of coronavirus, spread from animals to humans very quickly and with long-term economic and social effects.

The exercise was based on a scenario, delivered to participants through videos with pre-recorded news and data on the evolution of the pandemic over time, covering 18 months with 65 million deaths. The exercise has governmental decision-makers and representatives of the private sector who trained for inter-institutional cooperation globally. The exercise lasted 3.5 hours with the subject of a hypothetical pandemic, but scientifically possible[6]. The exercise raised several questions that are still being answered in the context of the current pandemic, questions related to the supply of medical materials and equipment, healthcare, the management of infected people, or the production of vaccines. Moderate discussions during the year also identified gaps in the health system and related sectors of activity and gaps in cooperation.

Based on the scientific probability of a pandemic, this exercise has provided valuable results for a global organization in the event of a pandemic. The involvement of representatives of several sectors of activity and the questions each participates in solving the pandemic equation are indicators of the possible effects on the different critical infrastructure sectors. These possible effects but also the identified gaps were validated by the pandemic that broke out in 2019. If this exercise had been more widely disseminated, the conclusions of the simulations would have contributed to a global response efficient and coordinated in the face of the global pandemic that validated the exercise hypothesis.

Conclusions

One of the limitations of using modeling and simulation for critical infrastructures is data. The researcher must first determine what data he needs and where he can collect the data. The main limitation is given by the classified character of the critical infrastructure objectives, so an abstract and fictitious model of infrastructure represents a necessary tool, providing the object of study. A practical method of data collection may be the interview with specialists and managers in the field, but most of the time, researchers have been reluctant to discuss the vulnerabilities and risks to which the target is subjected.

From this point of view, the data represent a significant and important qualitative and quantitative aspect for the application of modeling and simulation. However, the studies and tools already developed represent a point of reference for future studies. Models have been developed for different types of infrastructure systems and software tools with different simulation capabilities. The data are still needed to correctly define the situation and choose the best methods and tools for modeling and simulation to achieve the goal. Another challenge encountered in research is access to specific software tools. Specialists have created over time various software applications for modeling and simulation in the field of critical infrastructures.

Further research in the field will focus either on the development of new modeling and simulation tools or on using these methods to generate new results that will contribute to the improvement of critical infrastructure protection. The second option involves using tools already developed for modeling and simulation, and whether access to these software products in an institutional context or not is often a limitation for research. Finally, one of the constraints

[6] About Event 201, a high-level pandemic exercise on October 18, 2019 (centerforhealthsecurity.org), accessed on 02.02.2021.

of the research activity is the know-how, digital skills, and specific knowledge for the use of simulation modeling tools to achieve the research objectives.

From this point of view, modeling and simulation appear as a necessity in preparing and training specialists in critical infrastructure protection. The person responsible for critical infrastructure protection must know about modeling and simulation to identify the applicability for solving problems related to infrastructure security. The approaches organized in the form of simulation exercises involve establishing a multidisciplinary team in which to find specialists in modeling and simulation, adopt the best approach and the best tools to achieve the objectives of the research approach.

BIBLIOGRAPHY

1. DUEÑAS-OSORIO Satumtira, Dueñas-Osorio Leonardo, "Synthesis of Modeling and Simulation Methods on Critical Infrastructure Interdependencies Research", in *Sustainable and Resilient Critical Infrastructure Systems*, Chennai, India, Springer, 2010.
2. MCLEAN Y. Charles, Tina Lee Dr. Sanjay Jain Dr. Charles Hutchings, *Modeling and Simulation of Critical Infrastructure Systems for Homeland Security Applications*, National Institute of Standards and Technology, 2011.
3. OUYANG Min, "Review on modeling and simulation of interdependent critical infrastructure systems", in *Reliability Engineering and System Safety*, 121/ 2014.
4. ***, *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*, Official Journal of the European Unio, L.345/75.
5. about event 201, a high-level pandemic exercise on october 18, 2019 (center forhealthsecurity.org)