COMPERATVE EVALUATION OF MODELING AND SIMULATION TECHNIQUES FOR INTERDEPENDENT CRITICAL INFRASTRUCTURE

Associate professor Dimitrov D.L., Ph.D.
Institute of Metal Science Equipment and Technologies with Hydroaerodynamics Centre "Acad. A Balevski"
Bulgarian Academy of Sciences, Sofia, Bulgaria
E-mail: ddimitrov@ims.bas.bg

Abstract: *There are numerous methodical approaches to model, numerically analyses or/and simulate single systems' behavior. However, modeling interdependencies between different systems (so called system-of-systems) and to describe their complex behavior, necessarily by simulation, is still an unresolved issue.*
KEYWORDS: *CRITICAL INFRASTRUCTURE, VULNERABILITY, RISK ASSESSMENT, RISK MANAGEMENT, MODELING AND SIMULATION*

1. Introduction.

As is well known, a number of studies and attempts have been made to characterize the various infrastructures and their degree of criticality. Critical infrastructure analysis can focus on different goals (reliability, risk, vulnerability, etc.), may vary in scope (sectoral, system-wide or system-of-systems) and may follow different methodological approaches and / or competing approaches.

These facts usually create confusion and require comparative analysis with respect to different models and analytical techniques. The content of this report aims to establish clear criteria for such a comparison, with a focus on vulnerability of critical infrastructures and evaluation of modeling and simulation techniques.

These methodologies have been described and evaluated relatively successfully with respect to their overall suitability for critical infrastructure vulnerability assessment, with an emphasis on the role and impact of interdependencies, and for the purposes of the report will address some of the key benchmarks (e.g., " Types of interdependencies ";" Types of simulation events ";" Consequences of events ";" Need for data ", etc.)

On the one hand, critical infrastructures are defined as "a network of independent, large-scale, human-created systems that work together and in sync to produce a steady flow of essential goods and services" [1] and are also essential on economic development and social well-being. They are subject to a number of potential asymmetric threats (technical, intentional or unintentional - human-caused, physical, natural, cybernetic) that pose a risk to them.

Critical infrastructures are highly interdependent, both physically and in widespread use of information and communication technologies. In other words, critical infrastructures are characteristic of highly dynamic and complex systems, dependent on each other to varying degrees and with different intensities [2]. At the systemic level, critical infrastructure is viewed from a technical point of view as a problem for the security of logistical systems and their software.

Ensuring the continuous functioning of critical infrastructure sites, ie reducing the vulnerability to acceptable levels is one of the ideas behind the creation of the Competence Center "Quantum Communication, Intelligent Security and Risk Management" (Quasar) in the Republic of Bulgaria under Project BG05M2OP001-1.001-0006, funded by the European Union. Smart Growth Operational Program" [3].

On the other hand, we often define the vulnerability of critical infrastructure systems as gaps or weaknesses in their design, implementation, operation and / or management that make them susceptible to disruption / destruction, regardless of their ability to recover.

What does the term "vulnerability" mean in the context of critical infrastructure protection? Some researchers define the concept of vulnerability as follows: vulnerability is a manifestation of the inherent states of a system that make it susceptible to failure or loss. It is well described by a set of state variables that describe the weaknesses of the system and how they interact to cause loss due to a devastating event.

2. Requirements for methods and approaches for making comparative analysis.

2.1 Need for a systematic study.

There are a number of studies that call for and confirm the importance of understanding, modeling and simulating interdependent critical infrastructures.

Although there are studies on available techniques, it is clear that they lack comprehensive, clear criteria for assessing applicability. Therefore, the question of how to model the complex behavior of "system-of-systems" or which methods are best suited to accomplish this task is still open and provides a basis for finding additional approaches.

2.2 Objectives for comparative evaluation of techniques.

The main objective is to select, describe and evaluate techniques with a view to their adequacy in the preparation of vulnerability analysis of infrastructure interdependencies.

To this end, it is logical to distinguish between obvious and hidden vulnerabilities - reviewing the results of a statistical data analysis helps to identify obvious weaknesses if the statistics show some clear problem areas / scenarios - e.g. conclusions based on "power outages". Other indications of apparent vulnerability are operating errors, emergency procedures, etc.

A more accurate analysis must be adopted if the evaluation of the readings is not "clearly outlined" and the underlying hidden vulnerabilities are still expected. Particular attention should be paid to interdependencies within or between systems, and simplified procedures prepared at an earlier stage (including "system separation") should be evaluated.

For these and other reasons, as we know, on January 24, 2003, US President George W. Bush created the Department of Homeland Security (DHS), one of the main tasks of which is to conduct a comprehensive analysis of critical infrastructures as well as an organized national planning and protection process - CIP [4].

The $ 35 billion project was launched as a result of the terrorist attack on the two World Trade Centers on September 11, 2001 and accelerated the process of exploration for modeling and simulation of critical infrastructures. This fact has led to a significant increase in the intensity of research and, at the same time, the international interest in this field and the number of publications on these infrastructures.

Secondly, there are a number of inconsistencies in definitions and classifications that depend heavily on the scientific field. In the current scientific literature, recent methodological approaches are often incorrectly defined.

Therefore, the purpose of comparative evaluations of different techniques is to analyze the strengths and weaknesses of different methodologies, as well as to analyze, characterize and propose appropriate techniques for modeling and simulating interdependent critical infrastructures[5].

3. Basic benchmarks

3.1. Basic modeling approaches.

Two main approaches to modeling and simulation have been described in the contemporary literature: Interdependence analysis, which includes qualitative approaches, and Systematic analysis, which rather covers quantitative approaches.

Interdependence analysis [6] - includes qualitative techniques for identifying critical infrastructures and for analyzing the characteristics and dimensions of their interdependence. These techniques include extensive use of expert interviews, roundtables or seminars, appropriate questionnaires, and more. Models are relatively easy to build, but are limited to items explicitly examined by experts and are not able to systematically detect hidden critical elements and their respective vulnerabilities.

Systems Analysis [7] - uses approaches that are more quantitative techniques, can identify hidden dependencies, and are strongly associated with computer simulations. These techniques require sophisticated computer architectures as the approaches are very detailed and time consuming.

3.2. Modeling and simulation strategies.

The most important aspect of evaluation, not only in the development of optimal modeling and simulation strategies, is the decision to choose between two basic strategies: bottom-up and top-down, and a combination of both can be applied:

Bottom-up approach: the whole system is described starting with the individual parts [8]. This type of approach usually refers to complex adaptive systems that can be built on the results of interacting elements, such as basic entities with specific locations, capabilities, and memory that reflect their identification.

The bottom-up approach is generally considered to be more intuitive and less error-prone than the top-down approach and can usually be implemented with relative ease in software code. While the components are well defined, it can produce very accurate output. However, the exceptional use of the bottom-up approach can neglect significant system-level constraints, especially when used in the absence of sufficient input;

Top-down approach: The distinctive feature of the top-down approach is its focus on the overall properties of the system, combined with its relatively easy applicability. However, this approach is less appropriate than the bottom-up approach of capturing lower-level factors, such as problems with system-specific issues, as well as details of the implementation of specific details that tend to accumulate quickly and can significantly influence the evaluation [9].

3.3. Types of interdependencies.

This criterion describes the different types of infrastructure dependencies. Each type has its own characteristics and effects on infrastructures, but usually modeling and simulation approaches do not take into account all types of dependencies. There are four main types of interdependencies between critical infrastructures [10]:

Cyber interdependencies - connect infrastructures to each other through electronic, information links; outputs of information infrastructures are inputs to other ones;

Geographic interdependencies - observed when elements of an infrastructure are in close spatial proximity. For example, a damaged underground water main may cause interference to power lines and optical communication cables in a collector - the so-called "causal failures";

Physical interdependencies - describe the material flow between different infrastructures. Such interdependence arises from a physical connection consisting of input and output streams. For example, electrical systems and information and communication technologies (ICTs) are physically interdependent. Electricity supplies ICTs while they can control and manage the operational data for the proper functioning of that energy production, transmission and distribution;

Logical interdependencies - dependencies that exist between infrastructures but do not belong to the above types. Often logical dependencies are caused by human decisions and actions taken in both political and public fields, e.g. the volume of oil and gas supplied is highly dependent on the political decisions of OPEC members.

3.4. Types of simulation events.

A significant challenge related to modeling and simulation techniques may be to create a "what-if" scenario for critical infrastructure interdependence analysis. The following information for a subsequent event is possible [11]:

Incident: The incident describes a wide range of accidental and potentially damaging events, such as natural disasters, whose origin is usually outside and independent of the system;

Attack: A series of potentially damaging actions taken by an intelligent opponent to achieve certain results. Cyber-attacks include penetration, probing and denial of service. In addition, the idea itself can have as much impact on a system as if it actually materialized. A system that takes an overly defensive position because of the threat of attack can significantly reduce its functionality and reallocate excessive resources to monitor the environment and protect the assets of the system;

Failure: A potentially damaging event due to defects in one system or in an external element on which the system depends. Damage can result from incorrect design, production and operational (human) errors, corrupted data, etc.

3.5. Consequences of events.

Interdependencies affect the effects of single or multiple failures or interruptions within interconnected systems. Different types of dependencies can trigger feedback circuits that have accelerating or delaying effects on systems response, as observed in dynamics.

The following types of events are distinguished:

Cascading events: A situation where an adverse event occurs in one part of the infrastructure and the effect of them in the other parts. An example of a cascading event in electrical systems is the congestion and interruption of a transmission line from the electricity grid [12]. In that case, its load will be shifted to a nearby electricity transmission line, which - even without additional load - can also be switched off and without electricity leaving much of a region;

Increasing events: can be seen as a consequence of cascading events, ie. the resulting "problem" in one infrastructure can affect other infrastructures, causing them to malfunction or interrupt into other infrastructure by increasing the burden or recovery time. This in turn may affect the recovery of the service provided by the infrastructure initially affected;

Common cause events: Dependent failures in which two or more malfunctions occur simultaneously or within an interval of time as a direct result of the common cause. For example, fiber optic cables and power lines often share a common funnel in tunnels or over bridges. If this tunnel or bridge is damaged by a fire caused by a road accident, it may also disrupt telecommunications and energy supply as a result of disruption of spatial traffic [13];

Closed events: damages that do not have a cascading, escalating or general impact on the infrastructures under consideration.

3.6. Need for data (information).

This criterion requires the availability of general information on the quantity and quality of input required to apply the appropriate methodological approach[14]. Input data includes information about the topology and layout of the system, the flow of the product, its operation, as well as numerical values of the modeling parameters.

The availability of inputs and their quality are essential for the practical use of modeling and simulation approaches; lack of sufficient data is a widespread problem in scientific analysis and may reduce the use of sophisticated approaches. Two dimensions are known:

High: The methodological approach is highly dependent on the high quality and quantity of input data to provide applicable modeling approaches. These factors must be ensured before such an approach is implemented.

Low: The methodology can be applied with discrepancies in the quality or quantity of input submitted to ensure reliable results. In these cases, a minimum quality or quantity of information is required.

3.7. Observation scenarios.

Depending on the criteria described above, the observation scenarios relate to modeling and simulation techniques, baseline data and available information. Interdependent models can be grouped into the following main categories, depending on the scenarios required:

Vulnerability assessment: the purpose is to identify and quantify vulnerabilities in the system. Vulnerability is defined as the likelihood of an accident, successful attack or failure. Vulnerability assessments can be seen as an extended analysis of element damage;

Malfunction Analysis: Human errors can cause disruption to infrastructure systems. Modeling and simulation techniques can provide systematic analysis and reliability theory by identifying and analyzing the most common failures. The failure analysis provides the identification of the critical components, helps to improve the system, as well as to understand the connections between the critical nodes of the network as a whole.

3.8 Modeling and Simulation Paradigms.

Modeling and simulation of dynamic processes lead to changes in the state of the system / its components. Simulation is an "execution" process that takes over the model through discrete or continuous changes in its state over time "[15]. A combination of the two paradigms is also possible.

Discrete Events: The state is changed by "jumps". The models consist of entities (units of motion), resources (elements that provide the service), and control elements (elements that determine the states of entities and resources);

Continuous events: These describe changes in the state of continuous functions. If the material or information being simulated can be described as continuously moving rather than in separate steps or packages, it is most appropriate to use the continuous event paradigm. The simulation is based on solving differential equations that describe the development of the system.

4. Conclusion.

Although there are many techniques currently available for analyzing the individual critical infrastructures, no universal method or common interdependent modeling and simulation tool is widely accepted, and therefore discussions continue on the suitability of different approaches.

In terms of the dynamics of a person's systems, a serious argument is offered that offers ways of possibly improving the analysis, security, functional understanding, and strategic management of critical infrastructure systems that will assist in the perception of the operation of the system and its changes over time.

Because efficiency reflects the state of resources or the provision of services, strategies can be developed and tested when modeling systems before policies are developed, physically implemented, and security decisions addressed to deviations from normal functioning, the presence of unexpected challenges.

With all of this in mind, it is quite possible to develop adverse scenarios that can be applied to critical infrastructure models to demonstrate such threats and vulnerabilities that would impact business continuity, accident management, and their consequences, attacks on information systems, cybercrime, protection of key sites against attacks, chemical, biological and radiological hazards, provision of water and food, identification and protection of adjacent droughts It is logical to apply maritime infrastructure to models of critical infrastructure.

Modeling system dynamics allows not only to monitor normal activity, but also functionality in adverse change and its effect on critical infrastructure systems as a whole, since without this knowledge critical infrastructure owners / operators will be very difficult and unprepared for all that is likely to happen.

Effective modeling of critical infrastructure would enable both public administration and critical infrastructure owners to analyze, identify and effectively manage and maintain stability, security and access to that infrastructure by developing solutions to unexpected or other sustainability challenges.

Literature

[1]. Critical Foundations: Protecting America's Infrastructures, Report of the President's Commission on Critical Infrastructure Protection, Washing-ton D.C., 1997;

[2]. Eusgeld, I., Kröger, W., Sansaviini, G., Schläpfer, M., Zio, E." Investigations on the role of network analysis and agent-based modeling within a framework for the vulnerability analysis of critical infrastructures" (working paper). 5. Juni 2008 48/50;

[3]. Panevski V., Competence centres and intelligent security systems in Bulgaria, International Scientific Journal "Security & Future", YEAR III, ISSUE 1, НТС по машиностроене, 2019, ISBN:WEB ISSN 2535-082X, 14-16 2019;

[4]. Department of Homeland Security. "National Infrastructure Protection Plan", DHS, (2006);

[5]. Georgiev Nikolai, "Quality indicators for protection systems", International Journal of Economics, Commerce and Management, vol VI, issue 4, ISSN 2348-0386, 2018,p.836-842;

[6].S. Rinaldi, "Modeling and Simulating Critical Infrastructures and Their Interdependencies", Proceedings of the 37th Hawaii International Cconference on System Science. Hawaii, (2004);

[7]. S. Panzieri, R. Setola, and G. Ulivi. "An approach to model complex in-terdependent infrastructures", Universita "Roma Tre", Roma. (2005);

[8]. S. Lee "A frame work for supporting bottom up ontology evolution for discovery and description of Grid services". Expert systems with Applications, 32(2):pp.376-385, (2007);

[9]. V. Temnenco. "Software Estimation", Enterprise-Wide. (2007);

[10]. S. Rinaldi, J. Peerenboom and S. Kelly "Critical Infrastructure Interdependencies", IEE Control Systems Magazine, (2001);

[11]. R.J. Ellison, N.R. Mead, T. A. Longstaff and R. C. Linger. ,, The Survivability Imperative: Protecting Critical Systems", The Journal of Defense Software Engineering, (2000);

[12]. I. Dobson, B. Carreras, V. Lynch and D.E. Newman. ,, Complex systems analysis of series of blackouts: cascading failure, criticality, and self-organization", Bulk Power System and Control, Cortina d' Ampezzo, Italy, (2004);

[13]. F.M. Marshall, D. M. Rasmuson and A. Mosleh. "Common Cause Failure Data Collection and Analysis System", 1, U.S. Nuclear Regulatory Commission, NUREG/CR-6268, (1998);

[14]. Georgiev Nikolai, "Quality criteria for critical infrastructure protection systems", International Journal of Economics, Commerce and Management, vol VI, issue VI, ISSN 2348-0386, 2018, p. 265-271;

[15]. Borshchev, A., Y. Karpov, and V. Kharitonov, Distributed simulation of hybrid systems with AnyLogic and HLA. Future Generation Computer Systems, 2002. 18(6): p. 829-839 (2002).