CIP

Schutz kritischer Infrastrukturen

Bundesamt für Bevölkerungsschutz (BABS)

Comparative Evaluation of Modeling and Simulation Techniques for Interdependent Critical Infrastructures

Scientific Report

Laboratorium für Sicherheitsanalytik

ETH

Eidgenössische Technische Hochschule Zürich

Swiss Federal Institute of Technology Zurich

Comparative Evaluation of Modeling and Simulation Techniques for Interdependent Critical Infrastructures

Scientific Report

Authors: Irene Eusgeld, David Henzi, Wolfgang Kröger

Der vorliegende, sprachlich überarbeitete Bericht ersetzt gemäss Beschluss an der Sitzung vom 25. April 2008 den ersten Entwurf vom 21. April 2008.

5. Juni 2008

Laboratorium für
Sicherheitsanalytik

ETH Zürich
Sonneggstrasse 3
8092 Zürich

www.lsa.ethz.ch

Laboratory for Safety Analysis
INSTITUTE FOR ENERGY TECHNOLOGY

Contents

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. The present report contains the results of a first-of-its-kind literature review of modeling and simulation techniques which has identified eight best practice methodologies such as Agent-based Modeling, System Dynamics, and Hybrid System Modeling. These methods are described and comparatively evaluated with regard to their general suitability for vulnerability assessment of critical infrastructures focusing on the role and impact of interdependencies. For this purpose nine evaluation criteria are proposed: 1. Modeling focus; 2. Methodical design strategies; 3. Type of interdependencies; 4. Types of events for simulation; 5. Event consequences; 6. Data needs; 7. Monitoring area; 8. Modeling and simulation paradigms; 9. Maturity. Thus, this report offers a state-of-the-art description and, more importantly, a helpful basis for the selection of appropriate single or combined techniques to model and simulate critical infrastructure interdependencies in view of the given scientific problem or task.

1 Introduction

1.1 Background

Various attempts have been made to characterize infrastructures and their degree of criticality [IRGC 2006]. The analysis of critical infrastructures may focus on different goals (reliability, risk, vulnerability, etc.), vary in scope (sector, whole system, "system-of-systems"), and follow fundamentally different methodical approaches and/or competing "schools-of-thought". This creates confusion and calls for a comparative analysis of different modeling and analytical techniques. The content of this report aims at defining clear-cut criteria for such a comparison focusing on vulnerability of critical infrastructures and evaluation of modeling and simulation (M&S) techniques with regard to their general suitability for critical infrastructures.

We define *vulnerability* of systems as the presence of flaws or weaknesses in its design, implementation, operation and/or management that render it susceptible to destruction or incapacitation by a threat, in spite of its capacity to absorb and recover ("resilience").

We also define *critical infrastructures* as "a network of independent, large-scale, man-made systems (set of hard and soft structures)… that function collaboratively and synergistically to produce a continuous flow of essential goods and services" [PCCIP1997] and are, finally, essential for economic development and social well-being. They are subject to multiple, potentially asymmetrical threats (technical, intentional or unintentional human, physical, natural, cyber, contextual) and may pose risks themselves. Critical infrastructures are highly interdependent, both physically and through a pervasive use of information and communication technologies. Most critical infrastructures are undergoing far-reaching changes, both technological and organizational, and incorporate technologies as soon as they are (commercially) available. In other words: Critical infrastructures stand for highly dynamic, complex systems being dependent upon each other to varying degrees [EuKr 2008].

1.2 Requirements for methods and approaches

The well known "classical" methods of reliability and risk analysis are widely applied to single complicated[1] systems; i.e. tabular techniques (FMEA, HAZOP), decomposition techniques and causal chains (Fault/Event Tree Analysis), logical representation tech-

[1] Complicated systems are highly integrated systems with low dynamic, which can be described with numerous variables. The decomposition of a system for analytical goals is reasonable.

niques (Markov graphs, Petri Nets), computational techniques (cut-sets, Binary Decision Diagrams, Monte-Carlo simulation).

Difficulties arise when applying these methods to model and analyze the behavior of highly complex[2] systems or even large scale interconnected infrastructures. Here, the subject of the analysis is no longer a single system but many interdependent structures of components, which result in an often spatially distributed “system-of-systems” (or “meta-infrastructure system”). This may show - besides strong interdependencies, dynamic and non-linear behavior, rippling effects, dependence on natural and operational environment, etc. Powerful methods are needed to describe the behavior of such a system as a whole (not as a sum of single systems) while taking into account various kinds of threats and failures as well as contextual factors.

Therefore, the approaches required to capture this holistic view should be based on “system thinking” and may embrace various methods and techniques.

A general framework for the description of infrastructure interdependencies has been proposed by Rinaldi et al [RiPe 2001], based on six dimensions (coupling and response behavior, type of failure, infrastructure characteristics, state of operation, and environment) and four types of interdependencies (physical, cyber, geographical, and logical).

1.3 Need for systematic survey

Numerous reports are available which recognize and confirm the importance of the understanding, modeling, and simulation of interdependent critical infrastructures [DeHo 2006, RoWo 98, etc.]. Although surveys on available techniques exist [RiDe 2006] they seem to suffer from a lack of comprehensive, clear-cut criteria for suitability assessment. Therefore, the question of how to model the complex behavior of a “system-of-systems”, or which methods suit best for this task, is still open and calls for additional work.

To answer this question almost 100 articles dealing with modeling and simulation techniques applied to infrastructures or complex systems in general were reviewed. This “first-of-its-kind” survey has drawn information from open literature for the period 1981-2007.

[2] Complex systems are systems with nonlinear adaptive emergent behavior and feedback loops. The system dynamic is not equal to the sum of a single systems’ elements’ behavior.

2 Goals

The main goal is to select, describe and evaluate techniques with a view to their adequacy for vulnerability analysis of infrastructure interdependencies. For this purpose it seems to be reasonable to distinguish between obvious and hidden vulnerabilities. Collective discussion of the results of statistical data analysis[3] helps to find obvious weaknesses, if statistical data already exhibit some clear problem areas/scenarios (e.g. lessons learned from "blackouts"). Other indications of obvious vulnerability are, e.g., reliability bottlenecks, errors in operating and emergency procedures, etc. Therefore, in an early project phase the main emphasis is often placed on experts' opinion, brainstorming, etc., rather than on application of detailed models. The techniques to find obvious vulnerabilities are not subject of this review.

If the indications assessment is not "clear-cut" and major hidden vulnerabilities still need to be expected, a more accurate analysis has to be undertaken. Special attention should be placed on interdependencies within or among systems. Simplifications made earlier (including "decoupling" of systems) need to be reassessed. As a result more sophisticated methods of analysis may be called for. To identify the methods for this phase of detailed analysis and to check the availability of pertinent data are the goals of the present work.

As regards the literature analysis related to these goals, a few remarks need to be made:

Firstly, it seems to be important to mention that, in general, the progress in the field of M&S of interdependent critical infrastructures has slowed down. We can observe October 1997 (data of the final report of the *President's Commission on Critical Infrastructure Protection* (PCCIP)) as a starting point of a growing academic and political interest in critical infrastructures research. On 24th January 2003 U.S. President Bush founded the Department of Homeland Security (DHS), one of the major tasks of which has consisted in carrying out a comprehensive analysis of critical infrastructures as well as in engaging in a national protective planning, the *Critical Infrastructure Protection* (CIP) [DeHo 2006]. This 35 Billion dollar project was launched in the aftermath of the terrorist attack on the two World Trade Center buildings on 11th September 2001 (9/11) and accelerated the research in critical infrastructure modeling and simulation, especially by the DHS founded National Laboratories. This lead to a considerable increase in intensity of research and, with growing researchers' interest in this field at international level to a rising number of presented publications regarding critical infrastructures. These publications describe mainly conceptual approaches for solving specific single systems'

[3] Statistical data analysis including root-cause and precursor analysis is promising as for most of the systems the population of data is sufficiently large and most infrastructures are self-supervising, respectively.

problems or try to come up with more specific definitions. However, since it became clear after a while that further progress would be slow and judging from the decreasing number of publications more recently, we deduce that less research in critical infrastructure protecting is ongoing. In other words: Since the hype was over, or after the real complexity of modeling and simulation was recognized, only a few continued to do research in this field. At present, only the DHS and its underlying national laboratories seem to make advances in the field of tools development and the results are not published in open literature.

Secondly, there are inconsistencies with definitions and taxonomy which depend strongly on the scientific field. In current scientific literature recent methodical approaches are often inadequately defined.

Finally, it is worth mentioning that the motive of our approach is not to crystallize “the best method”, mainly because the suitability of methods is highly dependent on the scientific problems to be solved, which may vary significantly. Rather, the aim is to discuss strengths and weaknesses of the various methodologies as well as to analyze, characterize, and hypothesize their suitability for modeling and simulation of interdependent critical infrastructures.

3 Criteria for comparative evaluation

In this chapter we define criteria to characterize and comparatively evaluate modeling and simulation techniques for infrastructures' interdependencies. The proposed *evaluation key* comprises the following seven criteria:

3.1 Modeling focus

In current literature, two main modeling and simulation approaches are described: *Interdependencies Analysis* which comprises **qualitative** approaches and *System Analysis* which encompasses rather **quantitative** approaches.

- *Interdependencies Analysis* [ReWe 2003, Rina 2004] comprises qualitative techniques for identifying critical infrastructures and for analyzing the characteristics and dimensions of their interdependencies. These techniques make extensive use of expert interview, round-table discussion or workshop, suitable questionnaire, etc. The models are relatively easy to be built, but they are restricted to the elements explicitly considered by the experts. They are not capable to systematically discover hidden critical elements and pertinent vulnerabilities.
- *System Analysis* [PaSe 2005] approaches tend to be rather quantitative techniques able to identify hidden interdependencies and are strongly related to computer simulations. These techniques need sophisticated computational architectures because the approaches are very detailed and time consuming.

3.2 Methodical design strategies

The most important aspect of estimation, not only in the development of optimal modeling and simulation design strategies but for almost any project, is the decision between two basic strategies: *bottom-up* and *top-down*. Combinations of the two may be applied as well:

- *Bottom-up approach:* The whole system is described starting from its individual parts [Lee 2007]. This kind of approach generally refers to Complex Adaptive Systems (CAS), which can be built on a population of interacting elements as the basic entities with a certain location, capabilities, and memory reflecting 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 in a software-code with relative ease. So long as components are

well-defined, it can produce very precise output data. However, exclusive use of a bottom-up approach can lead to significant system-level constraints being ignored, especially when used in the absence of sufficient input data.

- *Top-down approach:* First an overview of the considered system has to be provided. The distinctive feature of the top-down approach is its focus on overall system properties combined with its relatively easy applicability. However, the top-down approach is less suitable than the bottom-up approach for capturing lower-level factors, such as system-specific issues, application design features, and implementation-specific details, which tend to accumulate rapidly and can greatly affect the estimation [Temn 2007].

3.3 Types of interdependencies

This criterion describes the various types of interdependencies among infrastructures. Each type has its own characteristics and effects on infrastructures' entities. Usually, modeling and simulation approaches do not consider all types of interdependencies. According to [RiPe 2001] four general types of interdependencies among critical infrastructures can be distinguished:

- *Cyber interdependencies* connect infrastructures to one another via electronic, informational links; the outputs of the information infrastructures are inputs to other infrastructures, and the "commodity" passed between the infrastructures is information.
- *Geographic interdependencies* occur when elements of infrastructures are in close spatial proximity. For example, a damaged underground water pipe could create perturbations to close-by electrical lines and fiber-optic communication cables - so called causal failures.
- *Physical interdependencies* describe the material flow between infrastructures. Such interdependency arises from a physical linkage consisting of input and output commodities. For example, electric power systems and information and communication technology (ICT) are physically interdependent. Electricity powers ICT, while the ICT may supervise and control operational data for the well functioning of energy generation, transportation, and distribution.
- *Logical interdependencies* exist between infrastructures that do not belong to the above types. Often logical interdependencies are caused by human decisions and actions undertaken, as in the political or societal areas. For example, the amount of delivered oil and gas highly depends on the political decisions of the OPEC members.

3.4 Types of events

A significant challenge associated with modeling and simulation techniques may be to create “what-if” scenarios for the analysis of critical infrastructure interdependencies. According to [ElMe 2000] the following definition of terms for a triggering event are proposed:

- *Accident*: Accidents describe a broad range of randomly occurring and potentially damaging events, such as natural disasters; they usually originate outside a system.

- *Attack:* A series of potentially damaging steps taken by an intelligent adversary to achieve an unauthorized result. Cyber attacks include intrusion, probes, and denials of service. Moreover, the mere threatening gesture can have an impact on a system as severe as if a threat would materialize. A system that assumes an overly defensive position because of an attack threat may significantly reduce functionality and divert excessive resources to monitoring the environment and protecting system assets.

- *Failure:* A potentially damaging event resulting from deficiencies in a system or in an external element on which the system depends. Failures may be due to results from design, manufacturing and operation (human) errors, corrupted data etc.

3.5 Course of triggered events

Interdependencies affect the consequences of single or multiple failures or disruption in interconnected systems. Different types of interdependencies can induce feedback loops which have accelerating or retarding effects on systems’ response as observed in system dynamics. The following types of events are distinguished:

- *Cascading events:* address a situation where an adverse event in one part of an infrastructure snowballs into other parts. An example of a cascading event in electric power systems is the overload and outage of one transmission line of the power grid [DoCa 2004]. In such a case its load is shifted to a nearby transmission line which - without further load shedding – may also be shut-off and cause a large area blackout.
- *Escalating events:* can be seen as an extended result of a cascading event, i.e. an occurred “problem” in one infrastructure may snowball into other infrastructures causing their malfunction or disruption or exacerbating an independent disturbance in another infrastructure by increasing the severity or time of recovery. This in turn may affect the restoration of service provided by the initially defective infrastructure. For example, a bulk power grid outage could escalate be-

cause of a simultaneous congestion in the traffic network. This may delay the arrival of spare parts and affect emergency actions.

- *Common cause events:* are dependent failures in which two or more component fault states exist simultaneously or within a short time interval, being a direct result of a shared cause. For example, optic cables and power lines often share the funnel in tunnels or over bridges. If that tunnel or bridge is damaged, e.g. by a fire caused by a traffic accident, this could also disrupt telecommunication and energy supply secondary to the disruption in the traffic in a spatial network [MaRa 98].
- *Confined events:* occurring failures which have no cascading, escalating or common cause consequences on the considered infrastructures. For example, a disruption or a malfunction of a valve in a petroleum refinery rests confined if the n-1 rule (calling for redundancy) is well complied with.

3.6 Data needs

This criterion asks for general information about the quantity and quality of input data needed for an application of the respective methodical approach. Input data include information about the topology and lay-out of the system, commodity flows, functioning, etc. (“system description”) as well as numerical values for modeling parameters. The input data availability and their sufficient quality are essential for the practical use of modeling and simulation approaches; a lack of satisfying data is an ubiquitous problem of scientific analyses and may curtail the use of sophisticated approaches. Two scales are proposed:

- *High:* Methodical approach strongly depends on a high quantity and quality of input data to provide reasonable modeling outputs. This needs to be ensured before applying such an approach.
- *Low:* The methodology works also with nonconformities in the quality or quantity of input data given to provide plausible outputs, and/or the considered methodologies need to have a minimum quality or quantity of information.

3.7 Monitoring area

Depending on the criteria described above, the monitoring area refers to the modeling and simulation techniques, output data and information. Interdependency models can be grouped into four broad categories, depending on the required scenarios: vulnerability assessment, failure analysis, mitigation/prevention and self healing strategies, information generation.

- *Vulnerability assessment:* The goal is to identify and quantify vulnerabilities in a system. Vulnerability is defined as the probability of an accident, successful attack, or failure. Vulnerability assessments can be seen as an extended failure analysis of components with focus on the three different event simulations from the environment into infrastructures components [Lewi 2006].
- *Failure analysis:* Component failures and human errors can cause disruptions in infrastructure systems. Modeling and simulation techniques can yield a system analysis and reliability theory by identifying and analyzing most frequent failures. Failure analysis provides identification of critical components, helps to improve system redundancies and understand relationships among critical nodes of a network, etc. Failure analysis can be seen as basic assessment for further vulnerability assessments.
- *Mitigation, prevention, and self healing strategies:* The identification and understanding of the systems under study is preconditioned when dealing with these strategies [Amin 2001].
- *Information generation:* The aim is to analyze and to calculate black boxes to gain initial system data and information regarding interdependencies.

3.8 Modeling and simulation paradigms

Modeling and simulation of dynamical processes emulate changes of the system/components' state. "Simulation is the process of model "execution" that takes the model through (discrete or continuous) state changes over time" [BoKa 2002]. Of course, the combination of both these paradigms is possible.

- *Discrete events:* State variables change "jumping". Models consist of entities (units of traffic), resources (elements that service entities), and control elements (elements that determine the states of the entities and resources). Typical examples are break-down failures, factory operations, shipping facilities in which the material or information being simulated can be described as moving in discrete steps or packets, etc.
- *Continuous events:* State variables are described with continuous functions. If the material or information that is being simulated can be described as moving continuously, rather than in discrete steps or packets, the paradigm of continuous events is the most appropriate. The simulation is based on solving differential equations that describe the evolution of a system. Typical examples of continuous dynamic behavior are weary-out processes, water movement through reservoirs and pipes, etc.

3.9 Maturity

The selection of evaluated methods based on the literature review. The number of publications can be seen as a criterion of maturity of every technique for M&S of interdependent critical infrastructures. We distinguish between three levels of maturity:

- *High:* Many application examples of this method for M&S of interdependent critical infrastructures are found in scientific literature. Experience seems to be extensive and lets us assume a high maturity level.

- *Middle:* Some application examples of this method for M&S of interdependent critical infrastructures are found in scientific literature. Experience seems to be moderate and lets us assume a medium maturity level.

- *Poor:* Some application examples of this method for M&S **at least of one** critical infrastructure are found in the scientific literature. Experience in M&S of interdependencies seems to be scarce and lets us assume a poor maturity level.

4 Techniques of modeling and simulation

For the present comparative evaluation eight modeling and simulation techniques have been selected as representative based on literature review. Some methods which model infrastructures using very high level abstractions were not included, e.g. *Supply-Demand Graphs* [LeMi 2004] and the similar method *Game Theoretic Model* [ZhPe 2003].

On the other hand very promising but yet not established techniques of applied biology [Szal 2005] have not been taken into account either.

In the following chapters the eight methods are briefly described and evaluated regarding the criteria defined in chapter 3.

4.1 Agent-based Modeling

Agent-based models (ABM) consist of dynamically interacting, rule-based agents [DILu 2004, WoJe 95]. An agent-based model can exhibit complex behavior patterns and provide valuable information about the dynamics of the real-world system simulated.

An agent is a software object implemented on a computer network. Agents have access to certain information and they are able to "communicate" with each other. Additionally, agents' design can include an ability to learn about the environment and formulate unique sets of decision rules [BoKa 2002]. Agent-based models are often used to observe aggregate activity for a population of agents. ABM can also be seen as a *modeling framework* rather than a *methodology,* because it is based on further underlying techniques like Monte-Carlo, FTA, etc.

Own experience with simulation and analysis of Electric Power Supply Infrastructure (EPSI) has confirmed the suitability of the ABM approach for vulnerability assessment [ScKe 2008]. In order to integrate a comprehensive spectrum of different phenomena and to derive stochastic, time-dependent event chains an object-oriented[4] approach combining Monte Carlo and agent-based modeling techniques are applied. Agents represent both technical components such as generators and non-technical components such as grid operators. They interact with each other directly (e.g. generator dispatch) or indirectly (e.g. via the physical network). Those behavioral rules and interactions of the components given by the physical laws of the electric power network are modeled separately from those being independent from the network (see Fig. 4.1).

The major advantage of the ABM approach for modeling and simulation critical infrastructure interdependencies is the possibility to emulate an emergent behavior. The overall system behavior results from the interactions of the multiple single agents and

[4] Object-oriented approach is a M&S technique, which includes, amongst others, ABM.

is not specified on the system level. Detailed data is only needed on the agents' level (bottom-up principle), not on the system level.

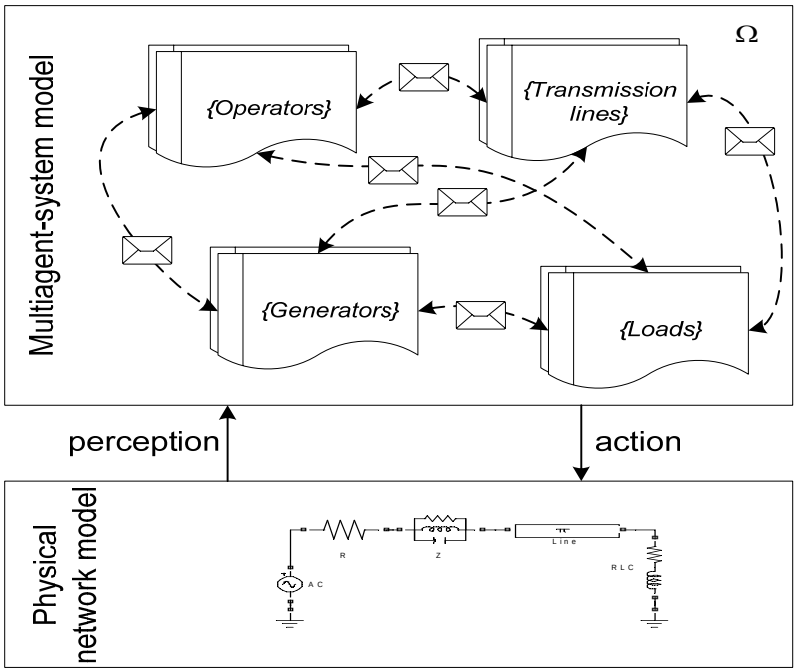

Figure 4.1 Two-layer-approach to model the Electric Power Supply Infrastructure [Kroe 2008]

Each modeled agent consists of a set of rules, supporting a decision making. These rules consist of three basic characteristics, namely *location, capabilities*, and *history* [PaSe 2004, BaSt 2000]:

- The agent's *location* describes where it is in a physical space. This physical space is defined by coordinates for a geographic region or an abstract space.
- The agents' *capabilities* describe how agents can react to environmental changes, how they can share knowledge among each other, and how they can adopt to changes in their environment.
- The agents' *history* is equal to memory. This memory includes information about previous experiences like overuse, stress, and aging.

Although ABM has demonstrated its attractiveness for the simulation of infrastructures [ScKe 2008], it should be noted that each simulation is very time consuming and a larger number of parameters need to be set, the data for which may not be readily available in practice.

ABM has successfully been used in several scientific areas, e.g. economics (supply chain optimization and logistics, consumer behavior, etc.) and informatics (distributed

computing, traffic congestion, etc.). Many ABM approaches for modeling and simulation of critical infrastructures interdependencies can be found in literature.

Table 4.1 Evaluation of ABM based on literature review and developed criteria

	Modeling Focus	**Design Strategies**	**Types of Interdependencies**	**Types of Events**	**Course of Triggered Events**	**Data Needs**	**Monitoring Area**	**Paradigm**	**Maturity**
Agent-based modeling		a) Bottom up	a) Physical	a)Accidents	a) Cascading	a) High		a) Discrete	a) High
	b) System Analysis		b) Cyber	b) Attacks	b) Escalating	b) Low	b) Failure Analysis		
			c) Geographic	c) Failures	c) Common cause				
			d) Logical		d) Confined		d) Information gen		

4.2 System Dynamics

System Dynamics is a method for studying and understanding the behavior and the underlying structure of a complex system over time. System Dynamics represents a fundamentally interdisciplinary top-down approach. Grounded in the theory of nonlinear dynamics and feedback control, the System Dynamics method deals with internal feedback processes (loops) and time delays that influence the whole system. All dynamics in a system are assumed to arise from the interaction of two types of feedback loops, positive and negative ones [Ster 2002]. These loops are represented in loop diagrams. A diagram includes stocks (the accumulation of resources in a system), flows (the rates of change that alter those resources) and information (about the value influences based on changes in the regarded stocks). Changes in stocks and flows are described with differential equations.

The elements of a system dynamics diagrams are shown in Figure 4.2. There are two diagrams used to build up the structure of systems: (a) causal-loop diagrams and (b) stock-and-flow diagrams [Kirk 98, Min 2005]. Typically, the first step is to construct the causal-loop diagram and to capture the strengths of the basic interactions between the system components. In Figure 4.2a the components are represented by *potential customers and actual customers* (which represents the stocks or accumulation) and *sales* (which represents the flows or rates). The strengths of the interactions are variables which directly influence the components and connect them with a directional arrow including a “+” or “-“ sign. A “+” sign denotes that the causal link is positive or a change in potential customers produces a change in sales in the same direction. A “-“ sign denotes a negative causal link or a change in sales produces a change in potential customers in the opposite direction. An aggregation of such arrows to a closed *feedback loop* can produce positive (reinforcing) or negative (balancing) feedback loops in addition to the signs on each link. This principle can be used for the modeling of interdependencies. However, it is hard to see any physical information for configuration or flow. Therefore, the second step implements the stock-and-flow diagrams (Fig. 4.2b). The stock-and-flow diagram conducts the differential equation that causes the evolution of the system.

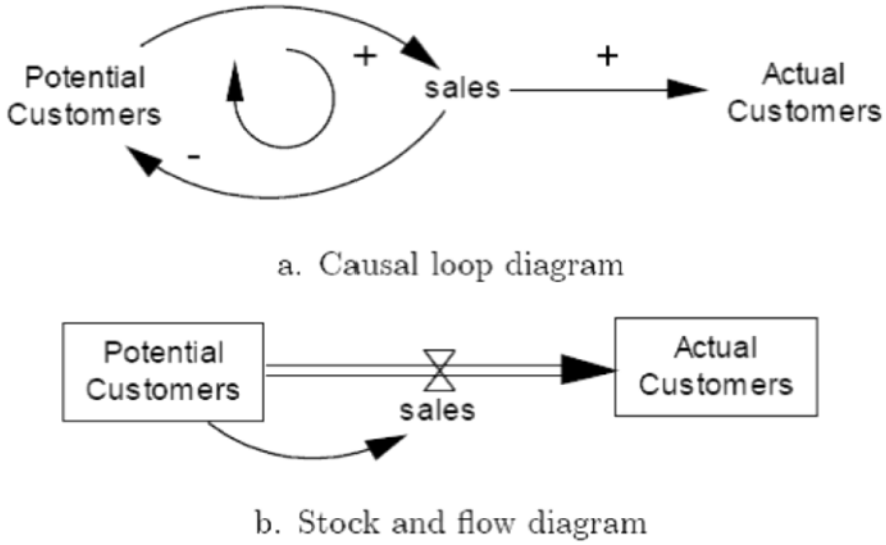

Figure 4.2 Advertising example of Causal-loop and Stock-and-Flow diagram [Kirk 98]

System Dynamics is widely used in environmental modeling, in economics, and in analysis of infrastructure interdependencies, e.g. [LeRe 2005]. This approach is also used in modeling and simulation of critical infrastructure systems, e.g. [Conr 2006], [Min 2005].

Table 4.2 Evaluation of SD based on literature review and developed criteria

	Modeling Focus	**Design Strategies**	**Types of Interde-penden-cies**	**Types of Events**	**Course of Trig-gered Events**	**Data Needs**	**Moni-toring Area**	**Paradigm**	**Maturity**
System Dynamics	a) Inter-depend-ency Analysis		a) Physical		a) Cas-cading			a) Discrete	a) High
	b) System Analysis	b) Top down	b) Cyber			b) Low		b) Con-tinuous	
				c) Failures					
					d) Con-fined		d) In-forma-tion gen		

4.3 Hybrid System Modeling

The term “Hybrid System” here is related to mathematical methodologies for the modeling and simulation of complex computational systems which display *discrete and continuous* system behaviour, e.g. [Wits 66]. The primary goal of hybrid system architecture is to facilitate the simulation of interdependent systems, which includes time dependent changes and jumping events. Mostly discrete and continuous events are separated in two different layers. Continuous behavior is specified as a set of algebraic-differential equations and discrete events are represented with a state of a state machine. That means a continuously changing variable describing the change of systems behavior over time can trigger a state machine transition, which means an occurrence of a discrete event. On the other hand a state can change as a result of some discrete events which are directly linked to the continuous system behavior [BoKa 2002] (s. Fig. 4.3).

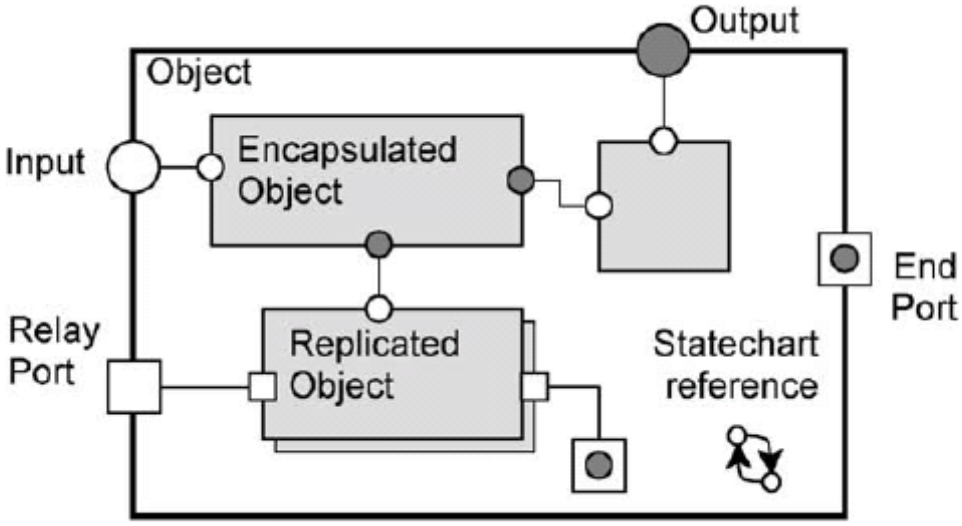

Figure 4.3 Example of Hybrid System Model [BoKa 2002]

In general this approach provides relative higher computational speed due to a substantial decrease in system complexity. The new hybrid modeling language is designed to mainly focus on flexibility in connecting with control software and model reusability. Nevertheless, to complete the simulation runs of large scale and complex models requires considerable computer capacity and is time consuming.

Hybrid System Modeling applies mainly to the huge group of continuous systems controlled by discrete events, such as systems coordinating processes (e.g. air and ground transportation), infrastructures, robots, etc.

Table 4.3 Evaluation of HSM based on literature review and developed criteria

	Modeling Focus	**Design Strategies**	**Types of Interde-penden-cies**	**Types of Events**	**Course of Trig-gered Events**	**Data Needs**	**Monitoring Area**	**Paradigm**	**Ma-turity**
Hybrid System Modeling			a) Physical	a)Accidents	a) Cas-cading		a) Vulner-ability As-sessment	a) Discrete	
	b) System Analysis	b) Top down	b) Cyber	b) Attacks		b) Low	b) Failure Analysis	b) Con-tinuous	
			c) Geo-graphic	c) Failures					c) Poor
			d) Logical		d) Con-fined		d) Informa-tion gen		

4.4 Input-Output-Model

The Nobel prized Leontief's Input-Output Model (IOM) is capable of describing the ripple effects of disruptions to interdependent systems [Joos 2006]. IOM has frequently been used in economics to predict commodity or information flow between economic sectors.

With IOM a system-wide solution can be determined for the cascading effects caused by a single perturbation. If for example the operability of one producer decreases by a certain amount, this model can calculate how the operability of all interconnected producers is affected (including an amplification of the inoperability of the originally affected producer) [RiDe 2006].

Based on Leontief's work, the so called *physical-based* Input-Output-Model *(IIM)* which considers multiple intra- and interconnected systems was developed by Haimes and Jiang [HaJi 2001]. This model assumes the output is the inoperability that can be triggered by one or multiple failures due to their inherent complexity or to external perturbations (e.g., natural hazards, accidents, or acts of terrorism). In this approach several time frames - or regimes - exhibit different features of interdependencies following an attack or other extreme event affecting the infrastructure. The nature and extent of sector interactions will vary from one time frame to the next. Within each time frame, the inoperability *Input-Output risk model* can describe a conceptual situation of equilibrium. Before an equilibrium is reached, the system will have evolved to a distinct and new frame of interactions. A sample of several time frames that will be addressed by IIM is presented in Fig. 4.4.

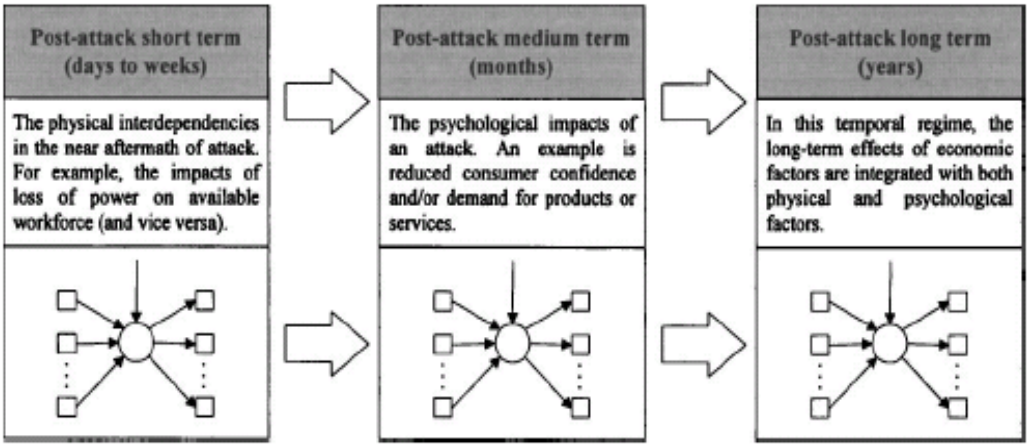

Figure 4.4 Example of three temporal regimes of recovery considered in IOM/IIM analysis of attack impacts [HaHo 2005]

The Input-Output Model was successfully implemented e.g. for the forecasting of economic activity for the Chicago Region. This method has also been used in local urban ecnomics. Olsen et al. [OlBe 97] developed an IOM for risk analysis of distributed flood protection. For modeling and simulation of critical infrastructures, Haimes [HaPu 2001]

applied IOM to examine and predict the effect of changes in one infrastructure system on others.

Table 4.4 Evaluation of IOM based on literature review and developed criteria

	Modeling Focus	**Design Strategies**	**Types of Interde-penden-cies**	**Types of Events**	**Course of Trig-gered Events**	**Data Needs**	**Monitoring Area**	**Paradigm**	**Maturity**
Input-Output Model	a) Inter-depend-ency Analysis		a) Physical		a) Cas-cading				
		b) Top down				b) Low	b) Failure Analysis	b) Continu-ous	b) Middle
				c) Failures					
					d) Con-fined				

4.5 Hierarchical Holographic Modeling

The term *hierarchical* refers to an understanding of risks due to different levels in a hierarchy (i.e. risks at “system-of-systems” level, individual system level, sub-system level and component level). The term *holographic* modeling refers to a multi-view image of a system with regard to indentifying vulnerabilities.

Central to the mathematical and systems basis of hierarchical holographic modeling (HHM) is the overlapping among various holographic models with respect to the objective functions, constraints, decision variables, and input-output relationships of the basic system. Through HHM [Haim 81], multiple models can be developed and coordinated to capture the essence of many dimensions, visions, and perspectives of infrastructure systems. One example is the study conducted for the President’s Commission on Critical Infrastructure Protection on the U.S. water supply system (see Fig. 4.5). In applying the HHM philosophy the risk to a water supply infrastructure is decomposed into 16 major categories. The categories represent the risks to a water supply system from the multifaceted dimensions of each major category including the likelihoods, root causes, consequences, and direct and indirect impacts.

The HHM approach to reduce infrastructure vulnerability addresses its holistic nature in terms of its hierarchical institutional, organizational, managerial, and functional decision making structure in conjunction with factors that shape that hierarchical structure. These include the hydrologic, technologic, and legal aspects as well as time horizons, user demands on the infrastructure, and socioeconomic conditions. Unfortunately no real-time simulation is possible.

HMM has been applied to study risks for agencies in the U.S. such as – besides the PCCIP - the FBI, the NASA, the Virginia Department of Transportation (VDOT), and the National Ground Intelligence Center [HaKa 2002].

Table 4.5 Evaluation of HHM based on literature review and developed criteria

	Modeling Focus	**Design Strategies**	**Types of Interde-penden-cies**	**Types of Events**	**Course of Trig-gered Events**	**Data Needs**	**Monitoring Area**	**Paradigm**	**Maturity**
Hierarchical holographic modeling	a) Inter-depend-ency Analysis		a) Physical	a)Accidents		a) High	a) Vulner-ability As-sessment		
		b) Top down		b) Attacks				b) Con-tinuous	b) Middle
			c) Geo-graphic		c) Com-mon cause				
			d) Logical		d) Con-fined				

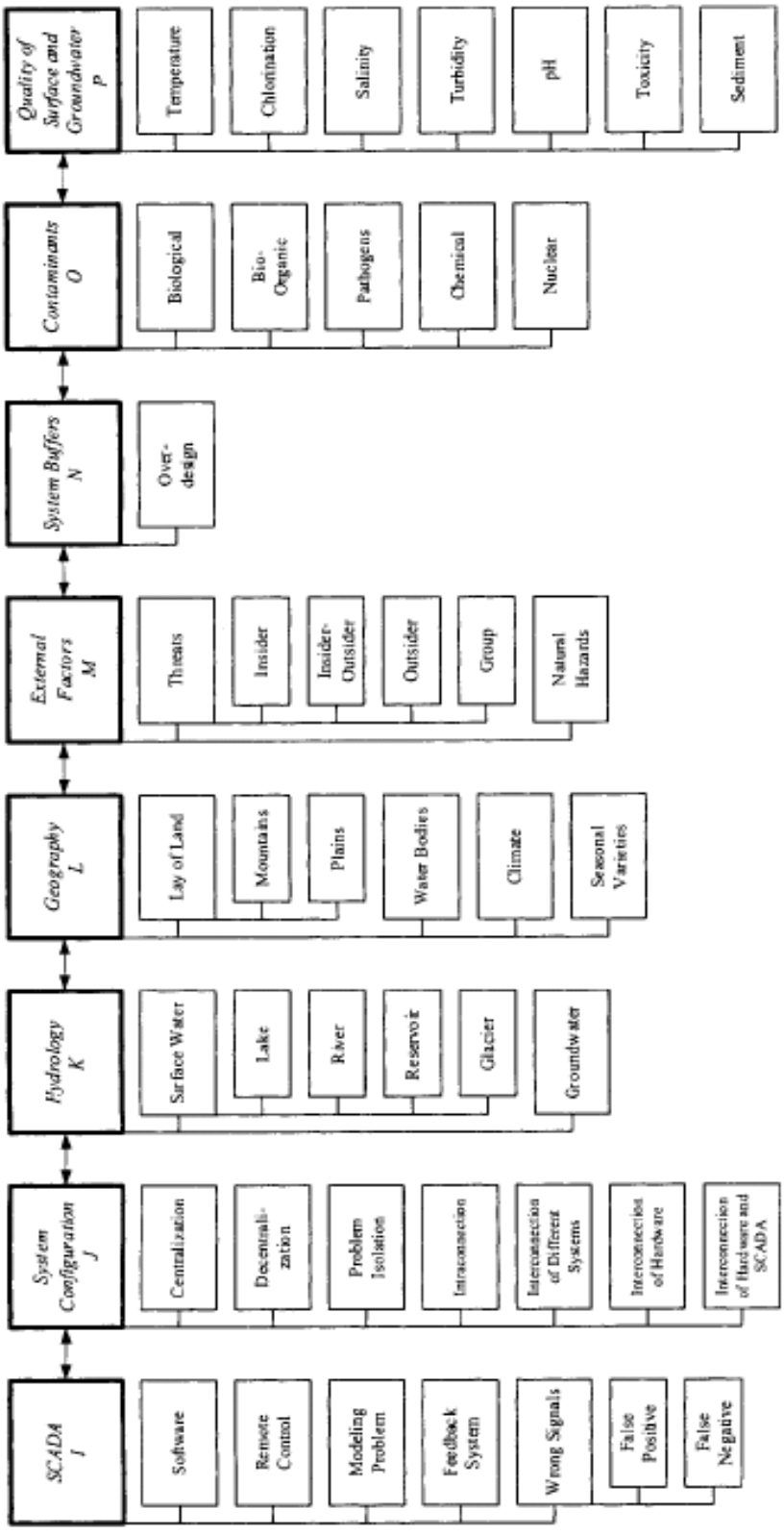

Figure 4.5 HHM approach to hardening the water supply infrastructure (extract of) [Haim 2004]

4.6 Critical Path Method

The Critical Path Method (CPM) represents one of several mathematically based engineering and project managing techniques for scheduling a set of project activities (s. Fig. 4.6). CPM uses a network diagram. The method considers logical interdependencies between activities, events, costs, and resources for the process execution and aims to identify the critical paths of a given project or process [Bake 2004]. Originally, the critical path method considered only logical dependencies between terminal elements.

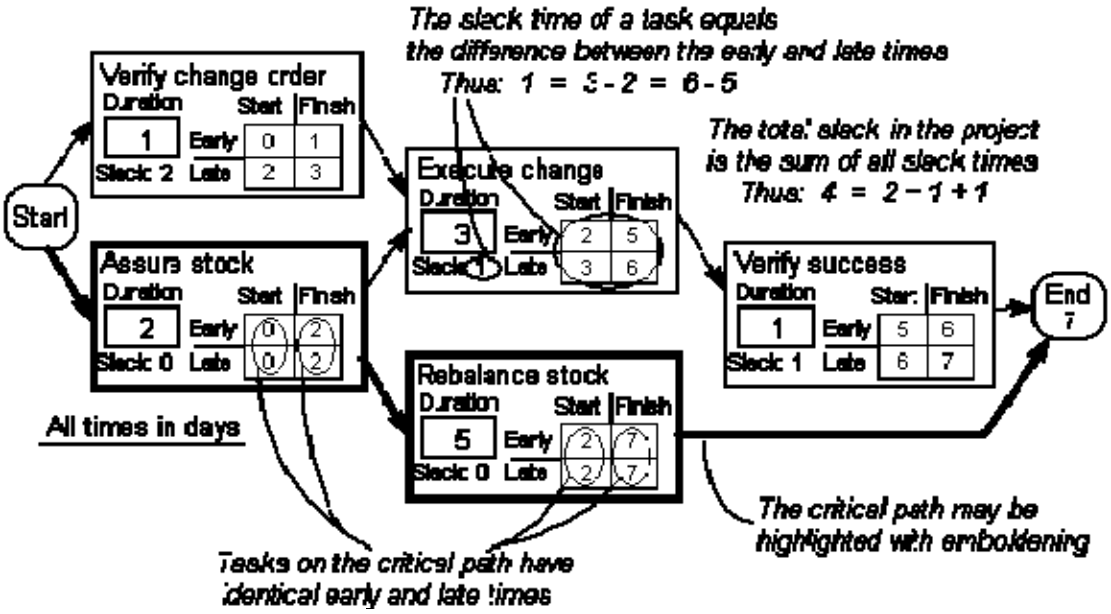

Figure 4.6 Finding the Critical Path [QuWo 97]

In construction projects, for the process of planning, scheduling, and control, CPM is one of the most popular and practical methods because it supports manual practice and computerized applications. There is very little evidence of a use of CPM as a modeling and simulation approach in critical infrastructures matters. Usually, CPM serves to quantify robustness and stability in time dependent projects such as timetable management in railway systems or in grid computing economy.

Table 4.6 Evaluation of CPM based on literature review and developed criteria

	Modeling Focus	**Design Strategies**	**Types of Interde-penden-cies**	**Types of Events**	**Course of Trig-gered Events**	**Data Needs**	**Monitoring Area**	**Paradigm**	**Maturity**
Critical Path Method	a) Inter-depend-ency Analysis		a) Physical		a) Cas-cading	a) High		a) Dis-crete	
	b) System Analysis	b) Top down	b) Cyber				b) Failure Analysis		c) Poor
			c) Geo-graphic	c) Failures					
			d) Logical		d) Con-fined		d) Informa-tion gen		

4.7 High Level Architecture

High Level Architecture (HLA) is a general architecture for modeling and simulating complex distributed systems [DeDe 97]. This technique breaks the entire system down into individually operating sub-systems. Communication within a “system-of-systems” is managed by a runtime infrastructure (RTI) which represents a very powerful tool. A single simulation is referred to as a federate. The total of single simulations connected via RTI is called federation. An example is shown in figure 4.7 [SeKr 99] where federates are informed by the federation management about the instances of order and company classes created by other federates. It is the task of the federation management to keep the federates informed about ongoing changes in existence and state of the objects.

There are many software tools supporting this methodical approach. These tools build on a standard layered software framework with a communication protocol [IEEE 1516-1516.2]:

- HLA-Rules: It defines the rules to which a simulation must keep to be standard-compliant and which represents the behavior of the overall distributed simulation (federation) and their associated sub-simulations (federates).

- Interface Specification: This defines the interface between sub-simulations (federates) and the RTI. The specific program libraries contain the functions and data structures for the communication and coordination between RTI and federates.

- Object Model Template (OMT): This provides a framework for the communication between individual HLA simulations. An OMT consists of a “federation object model” describing the shared object for the whole federation, and “simulation object model” describing the shared object for a single federate.

High Level Architecture has many advantages especially for the modeling and simulation of dynamic behavior of “system of systems”. Nevertheless, it should be noted that similar to ABM each simulation is very time and recourse consuming.

HLA has widely been used in the development of military software systems as well as in multiplicity fields for computer based tool development.

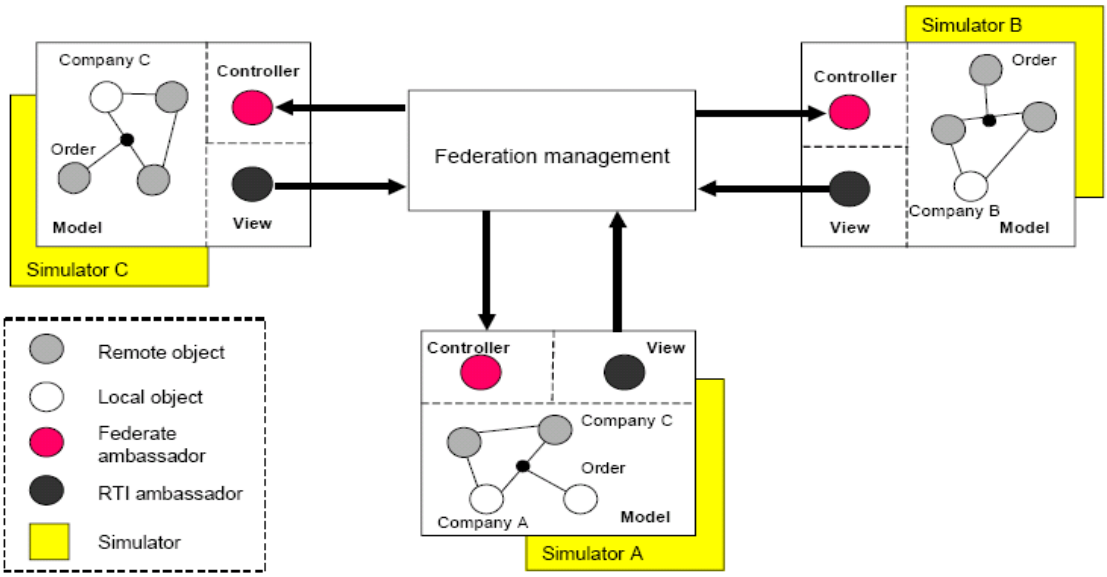

Figure 4.7 Example: Meta-Model in HLA [SeKr 99]

Table 4.7 Evaluation of HLA based on literature review and developed criteria

	Modeling Focus	**Design Strategies**	**Types of Interde-penden-cies**	**Types of Events**	**Course of Trig-gered Events**	**Data Needs**	**Monitoring Area**	**Paradigm**	**Maturity**
High Level Architecture	a) Inter-depend-ency Analysis	a) Bottom up	a) Physical	a)Accidents	a) Cas-cading			a) Dis-crete	
	b) System Analysis	b) Top down	b) Cyber	b) Attacks	b) Esca-lating	b) Low	b) Failure Analysis		
			c) Geo-graphic	c) Failures	c) Com-mon cause		c) Mitiga-tion/ Pre-ventation		c) Poor
			d) Logical		d) Con-fined				

4.8 Petri Nets

Stochastic Petri Nets (in short SPN) are a time enhanced variant of place- and transition nets which are mathematical models of non-deterministic and discrete distributed systems. A Petri Net model is a bipartite directed graph. It consists of places and transitions. Places may contain any number of tokens. When a transition switches (“fires”), it consumes the tokens from its input places, performs some processing task, and places a specified number of tokens into each of its output places.

Generalized Stochastic Petri Nets (GSPNs) are an extension of SPNs which allow timeless as well as timed (exponential) transitions. Petri nets are a well known technique to implicitly define large automatons needed to model distributed systems. Petri nets have an advantage in that the size of the net, i.e. the number of places and transitions, grows but in linearity with the number of components.

Figure 4.8.2 [GuDe 2003] shows a Petri net model of infrastructure interdependencies presented in Figure 4.8.1 [RiPe 2001].

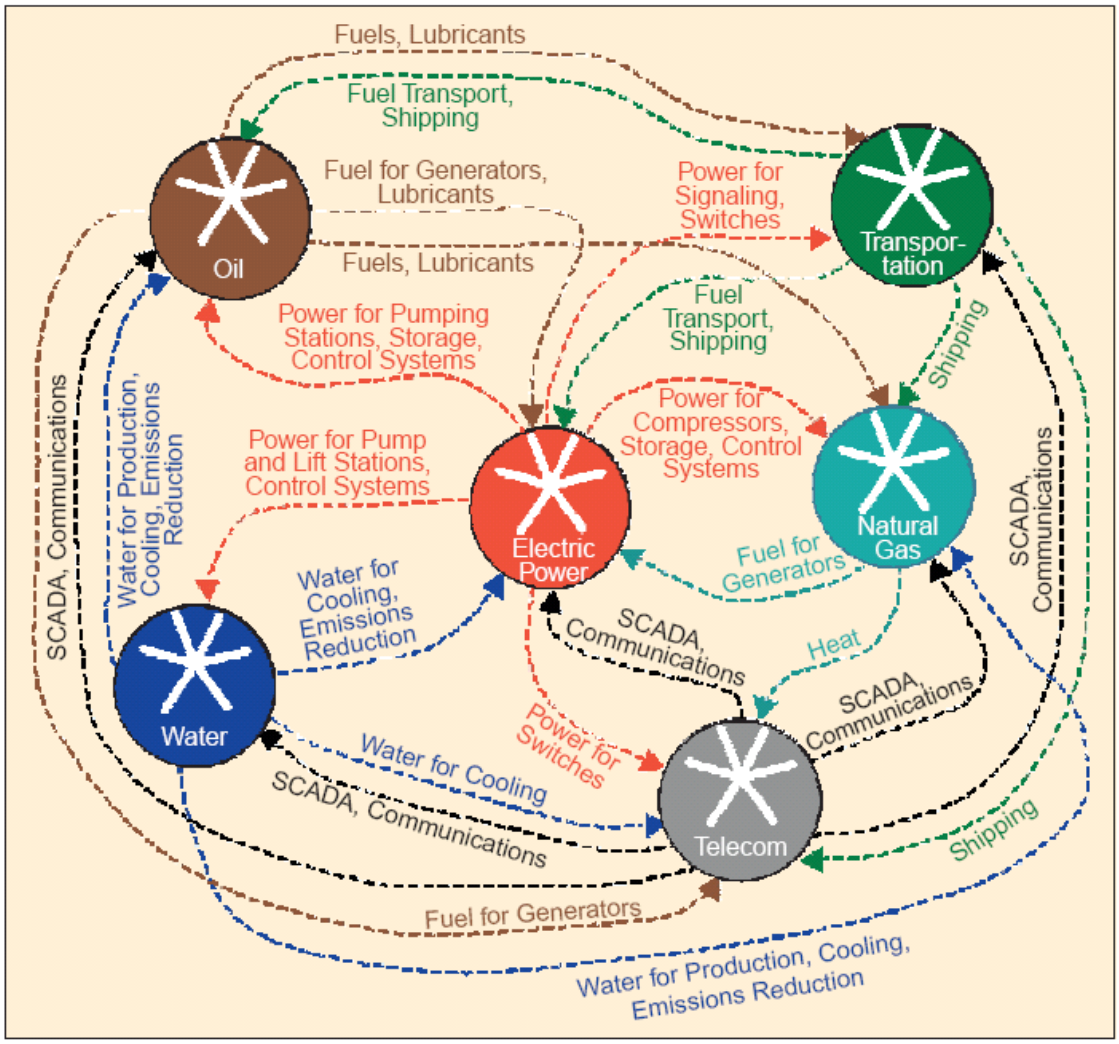

Figure 4.8.1 Examples of infrastructure interdependencies [RiPe 2001].

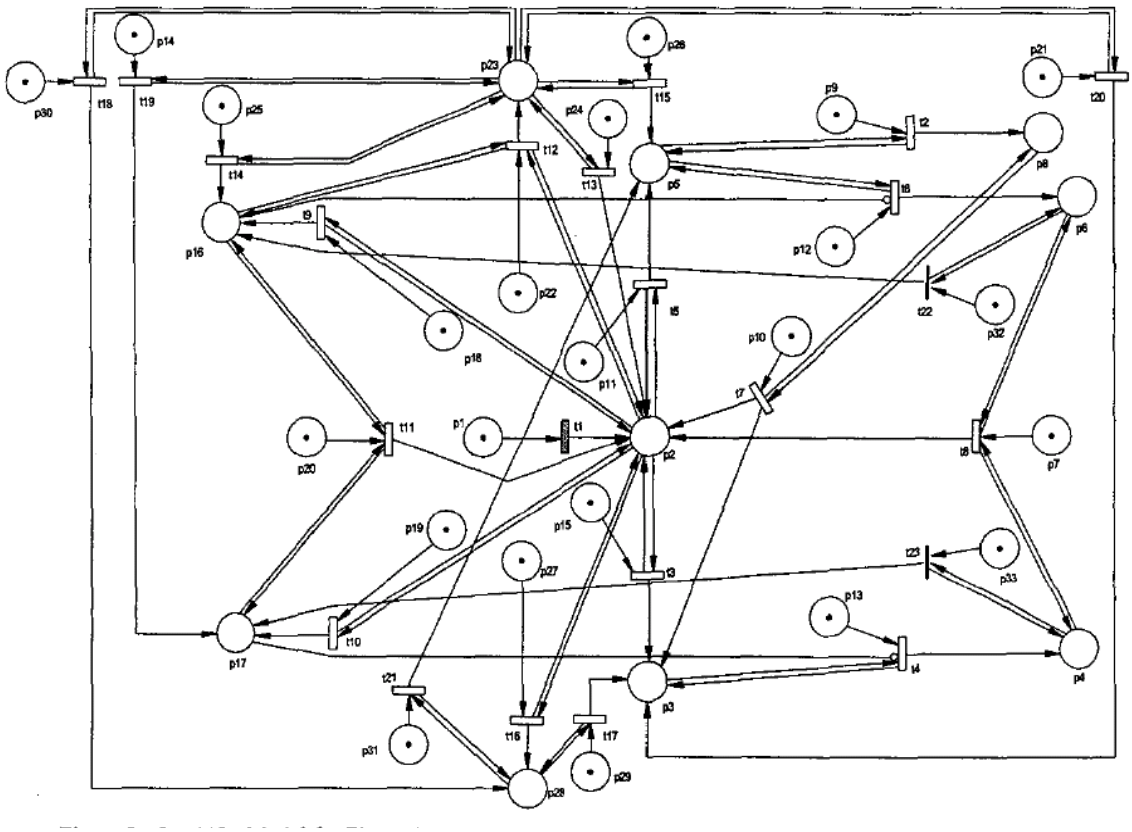

Figure 4.8.2 Petri Net Model of infrastructure interdependencies presented in Figure 5.8.1 [GuDe 2003]

Table 4.8.1 Legend for Petri Net Model in Fig. 5.8.2 [GuDe 2003]

TRANSITIONS	**PLACES**
1 "Electric Power is Disrupted" 2 "Lubricants in Reserves are Consumed" 3 "Power Disruption Affects Natural Gas Production" 4 "Natural Gas in Reserves is consumed ***5*** "Power Disruption affects OivLuhricants Production" 6 "Oil in Reserves is Consumed" 7 "Lubricants are Disrupted" 8 "Both Oil and Natural Gas are Disrupted" 9 "Power Disruption Affects Oil Transportation" 10 "Power Disruption Affects Natural Gas Transportation" 1 1 "Transportation Affects Electric Power Generation" 12 "Power Disruption Affects Telecommunication" …….. 23 "Consumed Natural Gas Affects Transportation"	1 "Electric Power ON" 2 "Electric Power **OFF"** 3 "Natural Gas Production Stops" ***4*** "Consumed Natural **Gas"** **5** "OiVLubricant Productions Stop" **6** "Consumed **Oil"** 7 8 "Consumed Lubricants" 9 "Lubricant Production Stops Mirror" IO "Consumed Lubricants Mirror" 11 "Electric Power OFF Mirror (for Oil Production)" **12** "Oil Production Stops Mirror" 13 "Natural Gas Production Stops Mirror" 14 "Telecommunication OFF Mmor (for Natural Gas …… 33 "Consumed Natural Gas Mirror (for Transportation)"

SPN can be applied to model common mode failures and cascading effects in complex systems, e.g. [KrOm 2003], as well as to analyse the impact of communication on power grids [ScLi 2006]. GSPNs are also suitable for formalizing and simulating dynamic aspects describing the semantics and activities of e. g. workflow systems and distributed and concurrent computing systems.

Table 4.8.2 Evaluation of Petri Nets based on literature review and developed criteria

	Modeling Focus	**Design Strategies**	**Types of Interdependencies**	**Types of Events**	**Course of Triggered Events**	**Data Needs**	**Monitoring Area**	**Paradigm**	**Maturity**
Petri Nets	a) Interdependency Analysis		a) Physical		a) Cascading	a) High		a) Discrete	
	b) System Analysis	b) Top down				b) Low	b) Failure Analysis		b) Middle
				c) Failures	c) Common cause				
					d) Confined		d) Information gen		

5 Results of comparative evaluation

The proposed nine evaluation criteria reflect important requirements for the modeling and simulation of a complex “system-of-systems” like interdependent critical infrastructures.

The goal of the evaluation code introduced is to provide an overview of the general capacity and suitability of methods in this field, which can help to identify good practice methods or a combination of them, depending on the objective of the analysis/task.

It is very important to be aware of the difficulties and limitations of such comparisons. The following evaluation key and the resulting evaluation code provide a first overview of the potential of each method considered, based on a scientific literature survey. Some methods vary significantly in the degree of abstraction and belong to various classification categories. Nevertheless, the evaluation code highlights individual characteristics of modeling and simulation methodologies in the context of critical infrastructure interdependencies’ analysis.

In Table 5.1 methods are evaluated comparatively making use of the nine evaluation criteria. In the left column the eight methodical approaches examined (see chapter 4) are listed and labeled with **a-b-c-d** while the scales are explained the Table 5.2.
For example *Petri Nets* provide the code (a,b),(b),(a),(c),(a,c,d),(a,b),(b,d),(a),(b). This indicates that this method was applied for interdependency analysis (a) as well as for system analysis (b); the design strategy used is top down (b); it was applied to modeling and simulation of physical interdependencies (a); it allows to simulate the failures of components/subsystems (c) of the following types: cascading, escalating, and common causes (a,b,c); monitoring areas are failure analysis and generation of information about system behavior (b,d); modeling and simulation of dynamical processes emulate discrete changes of the system/components state (a); some application examples of PN for M&S of interdependent critical infrastructures could be found in the scientific literature – this case corresponds to a middle maturity level (b).

With respect to the evaluation code Agent-based Modeling, Hybrid System Modeling and High Level Architecture cover the largest spectrum of characteristics. At first sight, these methods seem to be more universal than the others.

Nevertheless it seems to be important to note that HSM and HLA have a lowest maturity level (c). In contrast, ABM represents **the most used technique** in the area of interdependency modeling and simulation of critical infrastructures. The (literature based) analysis of 33 **simulation tools** (see chapter 6) for modeling and simulation of interdependent critical infrastructures with regard to underlying methodologies has shown that every third tool applies ABM besides other methods, including “traditional” methods such as graphs or GIS, depending on the subject and objective. This example demonstrates the significance of the evaluation code.

On the basis of the evaluation code, general comparative statements about the methodologies can be made. Depending on the objectives and tasks good or even best practice methods or a combination of them can be identified.

Table 5.1 Comparative evaluation of methods: Evaluation code

	Modeling Focus	Design Strategies	Types of Interdependencies	Types of Events	Course of Triggered Events	Data Needs	Monitoring Area	Paradigm	Maturity
Agent-based modeling	b)	a)	a),b),c), d)	a),b),c)	a),b),c), d)	a),b)	b), d)	a)	a)
System Dynamics	a),b)	b)	a),b)	c)	a),d)	b)	d)	a),b)	a)
Hybrid System Modeling	b)	b)	a),b),c), d)	a),b),c)	a),d)	b)	a),b),d)	a),b)	c)
Input-Output Model	a)	b)	a)	c)	a),d)	b)	b)	b)	b)
Hierarchical holographic modeling	a)	b)	a),c), d)	a),b)	c), d)	a)	a)	b)	b)
Critical Path Method	a),b)	b)	a),b),c), d)	c)	a), d)	a)	b), d)	a)	c)
High Level Architecture	a),b)	a),b)	a),b),c), d)	a),b),c),	a),b),c), d)	b)	b),c),	a)	c)
Petri Nets	a),b)	b)	a)	c)	a),c), d)	a),b)	b), d)	a)	b)

Table 5.2 Evaluation key

	Modeling Focus	Design Strategies	Types of Interde-pendencies	Types of Events	Course of Triggered Events	Data Needs	Monitoring Area	Paradigm	Maturity
a)	Interde-pendency Analysis	Bottom up	Physical	Accidents	Cascading	High	Vulnerability Assessment	Discrete	High
b)	System Analysis	Top down	Cyber	Attacks	Escalating	Low	Failure Analysis	Continuous	Middle
c)			Geographic	Failures	Common cause		Mitigation/ Preventation		Poor
d)			Logical		Confined		Information gen		

6 Modeling and simulation tools

Tools for modeling and simulation critical infrastructures play an important role in the analysis of interdependencies' behavior.

Due to the fact, that the complex models of "system-of-systems" can not be solved analytically, computer simulation is necessary. "Simulation is the process of model "execution" that takes the model through (discrete or continuous) state changes over time" [BoFi 2004].

Efforts have been made to develop models that accurately simulate critical infrastructure behavior and can thus identify interdependencies and pertinent vulnerabilities. Developed tools are mostly in confidential use by private companies, military, and government agencies, and serve different goals e.g. preparing for emergencies, reducing costs, enhancing redundancy, improving commodities flows, etc. [Pede 2006].

This chapter presents the leading research efforts in tool development. The survey is based on an open source material research, mainly from publications and online presentations.

6.1 Tool developing organizations

The modeling and simulation of critical infrastructures' interdependencies via tools is an essential attempt in the collection of knowledge about these systems, such as infrastructure expertise, data accessibility, etc. The U.S. government agencies have triggered most of the research in this area. The three U.S. departments most strongly involved in the development of modeling and simulations tools for protecting and securing nation's critical interdependent infrastructures are:

- *Department of Homeland Security (DHS)* - The DHS is a Cabinet department of the Federal Government of the United States with the responsibility of protecting the State territory from terrorist attacks and responding to natural disasters. The DHS works in the civilian sphere.
- *Department of Defense (DOD)* - The DOD is charged with coordinating and supervising all agencies and functions of the government relating directly to national security and the military. The DOD is the major tenant of The Pentagon and has three main components - the Department of the Army, the Department of the Navy, and the Department of the Air Force.
- *Department of Energy (DOE)* – The DOE is a Cabinet-level department of the US government responsible for energy policy and nuclear safety. Its purview includes the nation's nuclear weapons program, nuclear reactor production for

the United States Navy, energy conservation, energy-related research, radioactive waste disposal, and domestic energy production. The DOE also sponsors more basic and applied scientific research than any other US federal agency.

The DOE associates with many of the most important national laboratories which are leading in modeling and simulation of interdependent critical infrastructures, e.g.:

- Argonne National Laboratories (ANL)
- Idaho National Laboratories (INL)
- Los Alamos National Laboratories (LANL)
- Oak Ridge National Laboratories (ORNL)
- Sandia National Laboratories (SNL)

6.2 Brief tools survey

Modeling and simulation of critical infrastructures' interdependencies is a very challenging task, particularly when considering a system of multiple interconnected infrastructures. The presented modeling and simulation tools comprise multi system approaches considering combinations of more than one layer of one or multiple infrastructures. The presented survey implies 33 different tools [Pede 2006]. The modeling and simulation approaches, as well as the objectives of the different efforts vary significantly.

In the survey [Pede 2006] six categories were considered, which characterize the different modeling and simulation tools:

- **Infrastructures***:* In this survey a total of 12 different critical infrastructure sectors were considered. Each infrastructure can contain individual subsystems such as transportation: rail systems, highways; energy: electric power generation, transmission, distributions, dispatch, oil pipelines, refineries, etc.

  These 12 infrastructures are:

  1. Agriculture and food
  2. Banking and finance
  3. Defense industrial base
  4. Emergency services
  5. Energy
  6. Government
  7. Industry/manufacturing
  8. Information and telecommunication technology

9. Postal and shipping
10. Public health and safety
11. Transportation
12. Water

- **Modeling and simulation technique***:* The underlying methodologies are discussed in chapter 5.
- **Integrated vs. coupled models***:* Two different approaches were often used to conduct the analysis.
    1. Creating an integrated system model trying to model multiple infrastructures together.
    2. Coupling of a series of individual infrastructures' simulations, which simulate the cascading influence of a causing event.
- **Hardware/software requirements:** Here the portability and exportability of the tool programs considered and data are listed.
- **Intended user***:* Information related to tool access: are the tools for internal use only or also for external use, i.e. outside the developing organization? This adverts to the level of expertise required to use the product.
- **Maturity level of the tool***:* The survey considers four different maturity categories:
    1. Research level – the product level is still conceptual.
    2. Development level – the product has been used by internal customers.
    3. Mature analytic – the product has reached a mature level but is still for internal use only.
    4. Mature commercial – the tool has reached the level of a commercially licensed product.

In Table 6.1 an overview of the 33 investigated tools is presented. More detailed information about each tool can be found in [Pede 2006]. Most efforts have been made in the sectors *electricity, information and telecommunication technology, and transportation*, but further infrastructure sectors are also considered (12 sectors in total). Some of the approaches consider more than one infrastructure sector but this **does not mean** that they can provide combined modeling and simulation.

In the Table 6.2 the linking possibilities give information about combined modeling and simulation. As mentioned before, the user and the maturity level show the development state of the tools. The simulation type describes simulation paradigm.

The underlying methods from the 33 different tools give an interesting overview about the practical experience. Nine different underlying methodologies have been found (s. Table 6.3). The most used method is the agent based approach.

	Simulation Name	Developper	Area Model by Infrastructure Sector															
			Electric Power	Natural Gas	Drinking Water	Sewage Water	Storm Water	Human Activity	Financial Networks	SCADA	Telecom	Computer Networks	Oil Pipeline	Rail System	Higway System	Waterway System	Police/ Regulation Constraints	# of CIS
1	AIMS	UNB														X		1
2	Athena	On Target Technologies, Inc.	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	15
3	CARVER2	National Infrastructure																0
4	CI	ANL	X	X						X	X							4
5	CIMS	INL	X					X		X								3
6	CIP/DSS	LANL, SNL, ANL	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	15
7	CIPMA	Australia	X	X					X		X							4
8	CISIA	University Roma Tre	X							X								2
9	COMM-ASPEN	SNL							X		X							2
10	CounterMeasures	Alion Science & Technology												X	X			2
11	DEW	EDD	X							X								2
12	EMCAS	ANL	X						X							X		3
13	FAIT	SNL	X	X												X		3
14	FINSIM	LANL							X		X							2
15	Fort Future	USACE	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	15
16	IEISS	LANL	X	X														2
17	IIM	UV	X						X		X							3
18	Knowledge Management and Vizualisation	CMU	X											X	X	X		4
19	MIN	Purdue						X							X			2
20	MUNICIPAL	RPI	X								X			X				3
21	N-ABLE	SNL	X						X					X				3
22	NEMO	SPARTA	X	X	X									X			X	5
23	Net-Centric GIS	York University												X	X	X		3
24	NEXUS Fusion	IntePoint, LCC.	X					X			X			X	X			5
25	Ngtools	ANL	X	X														2
26	NSRAM	JMU	X								X						X	3
27	PFNAM	ANL		X									X					2
28	RAPIDware	Michigan State Uni	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	15
29	SAPHIRE	Idaho Falls	X															1
30	TRAGIS	ORNL												X	X	X	X	4
31	TRANSIMS	LANL						X										1
32	UIS	LANL			X	X	X	X			X				X	X		7
33	WISE	LANL			X	X	X											3
		# of Activities	21	11	7	6	6	9	10	8	13	4	5	12	11	11	7	

Table 6.1 Tools for modeling and simulation of critical infrastructures (developers and areas)

	Simulation Name	Developper	User and Maturity		Linking possibilities	Simulation Type		System Model		Hardware		Software Requirements		
			Users	Maturity Level	Single-/Combined Approach	Continuous	Discrete	Integrated	Coupled	PC	HPC	Windows	Linux	Solaris
1	AIMS	UNB	IA	RS	Single Approach	x	-	x	-	-	-	-	-	-
2	Athena	On Target Technologies, Inc.	EA	MI	Combined Approach	x	A	x	A	x	-	x	-	-
3	CARVER2	National Infrastructure Institute	B	MC	Single Approach	-	-	-	-	x	-	x	-	-
4	CI	ANL	B	MI	Single Approach	x	-	x	-	-	-	-	-	-
5	CIMS	INL	B	DV	Combined Approach	-	A	x	-	x	x	x	x	x
6	CIP/DSS	LANL, SNL, ANL	-	MI	Single Approach	x	-	x	-	x	-	x	-	-
7	CIPMA	Australia	B	MI	Single Approach	x	-	-	-	-	-	-	-	-
8	CISIA	University Roma Tre	-	-	Combined Approach	-	-	-	-	-	-	-	-	-
9	COMM-ASPEN	SNL	IA	DV	Single Approach	-	-	x	-	x	-	-	-	-
10	CounterMeasures	Alion Science & Technology	B	MC	Single Approach	x	-	x	-	x	-	x	-	-
11	DEW	EDD	B	MC	Combined Approach	-	-	-	-	-	-	-	-	-
12	EMCAS	ANL	IA	MI	Combined Approach	-	A	x	-	x	-	-	-	-
13	FAIT	SNL	IA	DV	Single Approach	I	-	x	-	x	-	x	x	-
14	FINSIM	LANL	IA	DV	Combined Approach	x	-	-	A	-	-	x	-	-
15	Fort Future	USACE	B	MC	Combined Approach	-	-	-	-	-	-	-	-	-
16	IEISS	LANL	IA	MI	Combined Approach	x	-	-	A	x	-	x	x	-
17	IIM	UV	IA	RS	Single Approach	I	-	x	-	-	-	-	-	-
18	Knowledge Management and Vizualisation	CMU	IA	RS	Single Approach	-	-	-	-	-	-	-	-	-
19	MIN	Purdue	-	-	Single Approach	-	-	-	-	-	-	-	-	-
20	MUNICIPAL	RPI	-	-	Single Approach	-	-	-	-	-	-	-	-	-
21	N-ABLE	SNL	IA	M	Single Approach	-	A	x	-	-	-	-	-	-
22	NEMO	SPARTA	-	DV	Combined Approach	x	-	x	-	-	-	-	-	-
23	Net-Centric GIS	York University	IA	RS	Single Approach	-	-	-	-	-	-	-	-	-
24	NEXUS Fusion Framework	IntePoint, LCC.	B	MC	Combined Approach	-	-	-	-	-	-	-	-	-
25	Ngtools	ANL	B	MI	Single Approach	-	-	-	-	-	-	-	-	-
26	NSRAM	JMU	-	RS	Single Approach	-	x	-	-	-	-	-	-	-
27	PFNAM	ANL	-	-	Single Approach	-	-	-	-	-	-	-	-	-
28	RAPIDware	Michigan State Uni	B	MI	Single Approach	x	-	-	-	x	-	x	x	-
29	SAPHIRE	Idaho Falls	-	-	Single Approach	x	-	-	-	x	-	x	-	-
30	TRAGIS	ORNL	-	MI	Single Approach	-	-	-	-	-	-	-	-	-
31	TRANSIMS	LANL	B	MC	Combined Approach	-	A	-	A	-	x	-	x	-
32	UIS	LANL	IA	MI	Combined Approach	x	A	-	A	-	x	-	x	-
33	WISE	LANL	IA	DV	Combined Approach	x	-	-	A	-	-	x	-	-

Maturity:
RS: Research
DV: Development
MI: Mature Internal
MC: Mature Commercial

Users:
IA: Internal Analyst
EA: External Analyst
B: Both

Simulation Type:
I: Input-Output Model
A: Agent-based

- no informations available

Table 6.2 Tools for modeling and simulation of critical infrastructures (characteristics)

No.	Underlying Methodologies	Abbreviations	No. of Methods	Tool Nr.
1	Agent-Based Method	ABM	13	1, 5, 8, 9, 11, 13-15, 18, 20, 23, 24, 28, 29
2	Geografic Information System	GIS	6	19, 21, 22, 23, 24, 30
3	System Dynamics	SD	4	6, 7, 15, 26?, 30
4	Statistical Data Analysis	SDA	3	3, 17, 17
5	Monte Carlo	MC	2	4, 6
6	Input-Output Methods	IOM	2	12, 16
7	Graph Theory	GT	1	10
8	Control Theory	CT	1	27
9	Miscellaneous	MI	1	2

Table 6.3 Tools for modeling and simulation of critical infrastructures (underlying methods)

7 Conclusions

Although many techniques for analyzing individual critical infrastructures already exist (e.g. for electric power networks, traffic networks, etc.), neither an universal method nor a general tool for interdependency modeling and simulation has been established so far and discussions about suitability of different approaches are ongoing.

This first-of-its-kind approach to comparatively evaluate methods for modeling and simulation adequate for vulnerability analysis of critical infrastructures is based on an open scientific literature review and, partially, own experience. Its results need to be taken with caution as major developments, e.g. in the U.S. the work of National Labs for the Department of Homeland Security, may be confidential and thus not included here.

Nine evaluation criteria are defined and eight good practice methods have been selected and described. Analysis of the simulation and modeling techniques is undertaken and reasons for their use are hypothesized. Resulting is an overview of strengths and weaknesses of applied methods offering a basis for decision on appropriate single or combined methods, depending on the research scenario, to model and simulate critical infrastructures interdependencies.

The evaluation key is not weighted. Such a weighting would be essential for a qualitative rating and ranking and subject of a further research topic.

References

[Amin 2001] M. Amin. "*Toward Self-healing Energy Infrastructure System",*IEEE Computer Applications in Power, 32, pp.260-268, (2001).

[Bake 2004] S. Baker. "*Critical Path Method (CPM)",* University of South Carolina: South Carolina, (2004)

[BaSt 2000] D.C. Barton, and K.L. Stamber. "*An agent-based microsimulation of critical infrastructure systems"*, United States, (2000)

[BoKa 2002] 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)

[Bouc 2006] Bouchon, S., *The Vulnerability of interdependet Critical Infrastruc tures Systems: Epistemological and Conceptual State-of-the-Art.* European Commisssion, Joint Research Center, 2006.

[Conr 2006] St. H. Conrad et al. "*Critical national infrastructure reliability modeling and analysis",* Bell Labs Technical Journal,. 11(3): pp. 57-71, (2006)

[DeDe 97] Department of Defense, "High Level Architecture Run-Time Interface Programmers Guide", p. 7-13, (1997).

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

[DILu 2004] M. D'Inverno and M. Luck, "*Understanding Agent System",* Berlin: Springer, (2004).

[DoCa 2004] 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)

[ElMe 2000] 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).

[EuKr 2008] 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).

[GuDe 2003] O. Gursesli, A. Desrochers, “Modeling Infrastructure Interdependencies Using Petri Nets”. Proceedings of *IEEE International Conference on Systems, Man and Cybernetics, 2003*.

[Haim 81] Haimes, Y. Y., Hierarchical holographic modeling, IEEE Transactions on Systems, Man, and Cybernetics 11(9), 606-617, (1981)

[Haim 2004] Haimes, Y. Y. Risk Modeling, Assessment, and Management, 2nd Edition. John Wiley & Sons, Inc., (2004)

[HaKa 2002] Y.Y. Haimes, S. Kaplan, and J.H. Lambert. “*Risk Filtering, Ranking, and Management Framework Using Hierarchical Holographic Modeling*”. Risk Analysis, 22(2), pp. 383-397, (2002).

[HaPu 2001] Y.Y. Haimes, and J. Pu, *Leontief-Based Model of Risk in Complex Interconnected Infrastructures.* Journal of Infrastructure Systems,. 7(1), pp. 1-12, (2001).

[IEEE 1516] Standard for Modeling and Simulation(M&S) High Level Architecture (HLA)-Framework and Rules-IEEE Computer Society Document, (2000)

[IEEE 1516.1] Standard for Modeling and Simulation(M&S) High Level Architecture (HLA)- Federate Interface Specification-IEEE Computer Society Document; (2000)

[IEEE 1516.2] Standard for Modeling and Simulation(M&S) High Level Architecture (HLA) - Object Model Template (OMT) Specification-IEEE Computer Society

[IRGC 2006] White Paper on “Managing and Reducing Social Vulnerabilities from Coupled Critical Infrastructures”, IRGC, (2006).

[Joos 2006] R.S. Joost. “*Inoperability input-output modeling of disruptions to interdependent economic systems”,* Systems Engineering, 9(1), pp. 20-34, (2006).

[Kirk 98] C. Kirkwood. “*System Dynamics Methods: A Quick Introduction”*, ed. C.o. Business. Arizona State University, (1998).

[KrOm 2003] A. Krings and P. Oman. “*A simple GSPN for modelling common mode failures in critical infrastructures”,* (2003).

[Kroe 2008] W. Kröger, W. *“Critical Infrastructures at Risk: A Need for a New Conceptual Approach and Extended Analytical Tools”*, Reliability Engineering & System Safety, Elsevier, (accepted).

[LeCl 2005] R.J LeClaire,. and G.O. Reilly. “*Leveraging a High Fidelity Switched Network Model to Inform System Dynamics Model of the Telecommunications Infrastructure”,* Systemdynamics. (2005).

[Lee 2007] S. Lee. et al. "*A framework for supporting bottom-up ontology evolution for discovery and description of Grid services".* Expert Systems with Applications, 32(2): pp. 376-385, (2007).

[LeMi 2004] E. E. Lee, J. E. Mitchell, W.A. Wallace, "Assessing Vulnerability of Proposed Designs for Interdependent Infrastructure Systems.", Proceedings of the *37th Hawaii International Conference on System Sciences 2004*.

[Lewi 2006] T. Lewis. "*Critical Infrastructure Protection in Homeland Security; Defending a Networked Nation"*, Wiley, (2006).

[MaRa 98] 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).

[Min 2005] Min, H., et al., *Toward modeling and simulation of critical national infrastructure interdependencies.* IIE Transactions, 2005. 39:1(57-71).

[OlBe 97] Olsen, J. R., Beling, P. A., Lambert, J. H., and Haimes, Y. Y. 1997. "Leontief input-output model applied to optimal deployment of flood protection." *J. Water Resour. Plan. Manage.* 124~5!, 237–245.

[PaSe 2004] S. Panzieri, R. Setola and G. Ulivi "*An Agent Based Simulator for Critical Interdependent Infrastructures"*, Securing Critical Infrastructures, Grenoble, (2004).

[PaSe 2005] S. Panzieri, R. Setola, and G. Ulivi. "*An approach to model complex interdependent infrastructures"*, Universita "Roma Tre", Roma., (2005).

[Pede 2006] Pederson, P., et al., *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research*. 2006, Idaho National Laboratory: Idaho.

[PCCIP 1997] Critical Foundations: Protecting America's Infrastructures, Report of the President's Commission on Critical Infrastructure Protection, Washington D.C., 1997

[ReWe 2003] D. Reinermann and J. Weber. "*Analysis of Critical Infrastructues: The ACIS Methodology (Analysis of Critical Infrastructural Sectors)"*, Critical Infrastructure Protection Workshop. Frankfurt, (2003).

[RiDe 2006] T. Rigole and G. Deconinck, "*A Survey on Modeling and Simulation of Interdependent Critical Infrastructures",* 3rd IEEE Benelux Young Researchers Symposium in Electrical Power Engineering, Gent, Belgium, April 27-28, (2006).

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

[RiPe 2001] S. Rinaldi, J. Peerenboom and T. Kelly. "*Critical Infrastructure Interdependencies",* IEEE Control Systems Magazine, (2001).

[RoWo 98,] C. Robinson, J. Woodard and S. Vamado. "*Critical Infrastructure: Interlinked and Vulnerable",* Issues in Science and Technology, (1998).

[ScKe 2008] M. Schläpfer, T. Kessler, W. Kröger, "Reliability Analysis of Electric Power Systems Using an Object-oriented Hybrid Modeling Approach", Power Systems Computation Conference 2008, Glasgow (accepted).

[ScLi 2006] K. Schneider, C. C. Liu, and J.-P. Paul, "Assessment of Interactions between Power and Telecommunications Infrastructures,"*IEEE Trans. Power Systems*, Aug. 2006.

[SeKr 99] G. Seliger and D. Krützfeldt, "*On the HLA- and Internet-based coupling of commercial simulation tools for production networks"*, Institute for Machine Tools and Factory Management, Technical University of Berlin: Berlin, (1999).

[Ster 2002] J.D Sterman. "*Systems dynamics modeling: tools for learning in a complex world",* Engineering Management Review, IEEE, 30(1): pp. 42-52, (2002).

[Szal 2005] Szallasi System Modeling in Cellular Biology: From Concepts to Nuts and Bolts, 2005, MIT Press.

[Temn 2007] V. Temnenco. "*Software Estimation",* Enterprise-Wide. (2007).

[QuWo 97] Critical Path Method, in Quality World, the journal of the Institut for Quality Assurance, 16 Jul (1997), http://syque.com/quality_tools/tools/TOOLS16.htm

[Wits 66] H. Witsenhausen, "*A class of hybrid-state continuous-time dynamic systems.* IEEE Transactions on Automatic Control, 11(2): pp. 161-167, (1966).

[WoJe 95] M. Wooldridge and N.R. Jennings. *"Intelligent agents: Theory and practice",* Knowledge Engineering Review 10 (2), pp. 115–152, (1995).

[ZhPe 2003] P. Zhang, S. Peeta, and T. Friesz, "Dynamic Game Theoretic Model of Multi-Layer Infrastructure Networks", Proceedings of 10th International Conference on Travel Behaviour Research, Lucerne, 10-15 August 2003.