Critical Infrastructure Modelling

Robert Gogela **Luděk Novák** **Antonín Šefčík**

robert.gogela@bdo-it.com ludek.novak@bdo-it.com antonin.sefcik@bdo-it.com

BDO IT a. s.
Olbrachtova 5/1980
140 00 Prague, Czech Republic

Abstract

One of the key points of Critical Infrastructure Protection is to have a deep knowledge of Critical Infrastructure (CI) interdependencies. CI modelling is a valuable tool for obtaining important and useful information about a real situation. This article explains the basic approaches commonly used in CI modelling. The focus is concentrated on two CI models – the CI Layer Model and the CI Element Chain Model.

Keywords: Critical Infrastructure, Critical Information Infrastructure, Critical Infrastructure Protection, Critical Infrastructure Modelling.

1 Introduction

The nature of risks and vulnerabilities in modern information society is becoming more and more transnational today. An open dialog on newly recognized vulnerabilities at the physical, cyber, and psychological level is needed to create new knowledge and a better understanding of new risks and of their causes, interaction, probabilities, and costs.

Modern society increasingly depends on networked information systems. The information infrastructure is becoming one of the backbones of our societies. Whereas the opportunities for a wide application of modern Information and Communication Technology (ICT) are known and exploited, the negative consequences are not yet thoroughly understood. The global use of ICT means a broad dependence upon and among critical infrastructures. Also there are growing needs for security and protection.

The complicated interdependencies in a complex infrastructure's environment require special vigilance. Consequently governments are starting to dedicate an extraordinary amount of attention to the Critical Infrastructure and its effective protection.

Critical Infrastructure (CI) includes all systems and assets whose incapacity or destruction would have a debilitating impact on the national security, and the economic and social well being of a nation.

Critical Information Infrastructure (CII) includes components such as telecommunications, computers/software, Internet, satellites, fibre optics, etc. The term is also used for the totality of interconnected computers and networks and their critical information flows.

Critical Infrastructure Protection (CIP) includes measures to secure all systems and assets whose incapacity or destruction would have a debilitating impact on the national security, and the economic and social well being of a nation.

Critical Information Infrastructure Protection (CIIP) is a subset of the Critical Infrastructure Protection. CIIP focuses on the protection of systems and assets including components such as telecommunications, computers/software, Internet, satellites, fibre optics, etc., and on interconnected computers and networks, and the services they provide.

2 CI Modelling

Modelling involves the use of mathematical relationships to describe a system. The user needs to have a solid understanding of the system: specially the relationships between events, factors and variables within the model, and secondly the magnitude of those relationships.

A model is simplified representation of reality. In this sense, therefore, you must have a 'model' of the world (a notion on how the world works) before you can write detailed scenarios.

3 CI Layer Model

The CI Layer Model shows parts of infrastructure systems or the totality of a nation's critical infrastructures and their relationship to each other, and often serves as a global picture of interdependencies among the elements. The model includes the overall perspective and is mainly used as illustrations for how critical infrastructures are organized. The overall perspective of the model allows users to model global dependency and relationships within CI.

The CI Layer Model is a combination of the tree following critical infrastructure dimensions: (1) critical infrastructure sectors, (2) critical infrastructure administration areas, and (3) critical infrastructure management fields. There can be used different overviews based on a combination of the dimensions.

3.1 CI Sectors

The model divides the whole CI environment into eight critical infrastructure sectors (the first dimension). The CI sector represents a separate functional unit of the whole critical infrastructure focused on providing a defined kind of the critical services.

Critical Infrastructure Sector	Basic description
Information and Communication Services	include telecommunication, information distribution and broadcasting services (mainly electronic), hardware and software components of data networks, etc.
Electric Power Services	include electric power plants, electric distribution lines, transmission and substation networks, electronic power management systems, etc.
Gas and Oil Services	include production, storage, and transportation of natural gas, oil, coal, heat, and other energy services, etc.
Banking and Finance Services	include banks, insurance companies, lending and credit institutions, oversight and regulatory agencies and support systems that facilitates lending, borrowing, issuing, trading in or caring for money, purchase and sales of shares and bonds, credits and other representations of value, etc.
Transportation Services	sector mainly includes all (air, rail, marine, and surface) transport components like aviation, highways, mass transit, railways, etc.
Water and Food Services	include drinking water supply systems, water filtration, cleaning and treatment and transport systems, food distribution services, water management, etc.
Emergency and Health Services	include emergency (medical, police, fire, and rescue systems), public health like prevention, laboratories, personal health services, nuclear safety, prevention of industrial hazards and pollutions, etc.
Government Services	include national and civil defence, public administration, justice, public order, social security and welfare, etc.

Table 1: Critical Infrastructure Sector Overview.

There are other approaches to arrange critical infrastructure sectors. Some models use the five following sectors (1) Information and Communication Services, (2) Energy Services (including Electric Power Services and Gas and Oil Services), (3) Banking and Finance Services, (4) Transportation Services, (5) Vital Human Services (including Water and Food Services, Emergency and Health Services and Government Services).

Other model variations are based on the six sectors (1) Information and Communication Services, (2) Energy Services (including Electric Power Services and Gas and Oil Services), (3) General Services (including Banking and Financial Services and Water and Food Services), (4) Transportation Services, (5) Emergency and Health Services, (6) Government Services.

The first dimension helps to model and assess interdependency among CI sectors. The extent of a direct dependency between two CI sectors is assigned by a proper scale of magnitude values. The most common scales are based on 3 or 5 values. The 3-value scale uses the following levels: High – H, Middle – M, Low – L. The 5-value scale distinguishes these levels: Critical – C, High – H, Middle – M, Low – L, None – N.

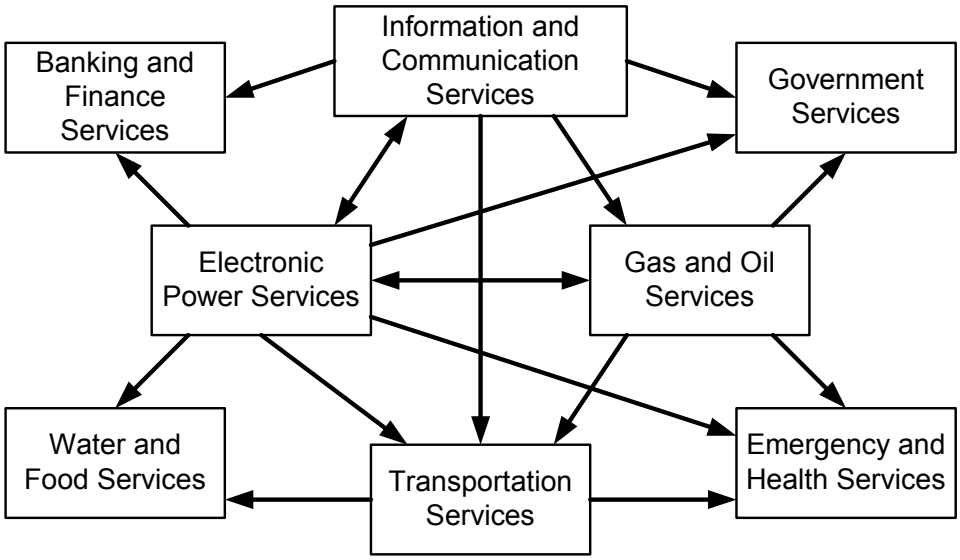

Figure 1: Graph of Sector Interdependencies.

The oriented graph (figure 1) and the matrix (figure 2) are helpful examples of results. Figure 1 presents the graph of key interdependencies among the CI sectors. The table in figure 2 is a sample of 3-value interdependency matrix.

	IC Services	EP Services	GO Services	BF Services	Transp Services	WF Services	EH Services	Gov Services
Information and Communication Services	–	H	M	M	L	L	M	M
Electric Power Services	H	–	H	M	M	M	M	M
Gas and Oil Services	H	H	–	M	H	M	M	M
Banking and Finance Services	H	H	M	–	M	L	L	M
Transportation Services	H	H	H	M	–	L	L	M
Water and Food Services	M	H	M	M	H	–	M	L
Emergency and Health Services	H	H	H	M	H	M	–	M
Government Services	H	H	H	M	M	L	M	–

Figure 2: Sector Interdependency Matrix.

There is a need to study the CI interdependencies more closely sometimes. In this case, it is possible to identify additional details and specify relevant items within each CI sector. The presented tools are useful for understanding various relationships inside any CI sector and its components.

3.2 CI Administration Areas

The second dimension of the layer model creates five administration areas. The area represents a part of the organization structure associated with CI management and control measures. The areas mostly correspond to a government and public administration arrangement, structure, etc.

Administration Area	Basic description
Private Area	involves private responsibilities associated with home and family issues.
Municipal Area	involves responsibilities of local government, small organizations and/or companies with influence limited to a small territory.
Regional Area	involves responsibilities of regional government, middle organization and/or companies with influence to a large territory within a state.
National Area	involves responsibilities of state government, large organizations and/or companies with influence covered a whole state.
International Area	involves international cooperation, cross-board relationships, global companies with worldwide influence and consequences.

Table 2: Administration Area Overview.

The second dimension brings a possibility to model and assess dependencies between the CI sectors and the CI administration areas. The dependencies represent any direct involvements and supervision controls of the CI administration area over the CI sectors. The value scales for the second dimension are the same like for the first one.

	Private Area	Municipal Area	Regional Area	National Area	International Area
Information and Communication Services	M	H	H	H	M
Electric Power Services	L	M	H	H	L
Gas and Oil Services	M	M	M	H	H
Banking and Finance Services	L	M	M	H	M
Transportation Services	M	H	H	M	L
Water and Food Services	M	H	M	M	L
Emergency and Health Services	M	H	H	M	M
Government Services	L	M	H	H	M

Figure 3: Sector – Administration Area Dependency Matrix.

An example of a two dimensional perspective is presented in the matrix on the figure 3. The matrix says that information and communication services are highly dependent on tree administration areas (municipal, regional,

national). These areas must provide proper information and manage related information and communication services distributing information to depended bodies.

3.3 CI Management Fields

The third dimension, if applicable, includes several management fields. The dimension describes information, management and steering characteristics connected with critical infrastructure environment, and shows various kinds of executive and operational context.

Management Field	Basic description
Social Field	signifies social, political and economical influences and impacts which affect people and their quality of life.
Organization Field	qualifies government and business policies, strategies, structures, regulations and other management issues concerning to the critical infrastructure and represents interdependencies among critical infrastructures and their information and communication systems.
Information Field	means an information and communication system (not necessary based on modern technology), which supports a given set of critical infrastructure services as a complex.
Application Field	stands for an individual integral functional complex which provides a basic application background supporting a part of a critical infrastructure service.
Technological Field	represents a technological components (hardware, software etc.) and their integration to a basic functional blocks.
Feature Field	is a common foundation field, which describes the general character of the surrounding environment. Typical parameters express quality of road and rail networks, different facilities, nature and terrain characteristic, etc.

Table 3: Management Field Overview.

The management fields represent a level of studied CI components and range of their integration. The fields are important for studying a special part of the critical infrastructure, which is called Critical Information Infrastructure (CII). CII deals with information and communication technology (ICT) applied in and supported various critical infrastructures. In this case, the fields represent a different level of ICT complexity and its impacts on the critical information infrastructure.

Using of the fields is also discussed in the following model (see chapter 4).

4 CI Element Chain Model

The CI Element Chain is the second model focused on a detail description of functional relationships within a critical service.

Critical Service (CIS) is that service whose interruption would have a serious adverse on a nation as a whole or on a large proportion of the population, and which would require immediate reinstatement.

In the CI Element Chain Model, the CI service is an explored service, which is a component of the critical services. The model describes CI primitive elements, connected with the critical service, and their bindings. The CI primitive elements are following (see figure 4):

- CIS Customer – uses some amount of CI Services from one or more CIS Providers through appropriate CIS Operators.
- CIS Provider – offers some CI resources/services for CIS Customers.

- CIS Operator – is a connection between one CIS Provider and one CIS Customer used for proper delivery of CIS.
- CIS Management Structure – is a steer element, which mediates administrative and control information among CIS Customer, CIS Provider, CIS Operator and other CI Members.
- CIS Support Structure – is a general environment necessary for providing and/or delivering CIS (i.e. transportation roads, gas or oil pipelines).

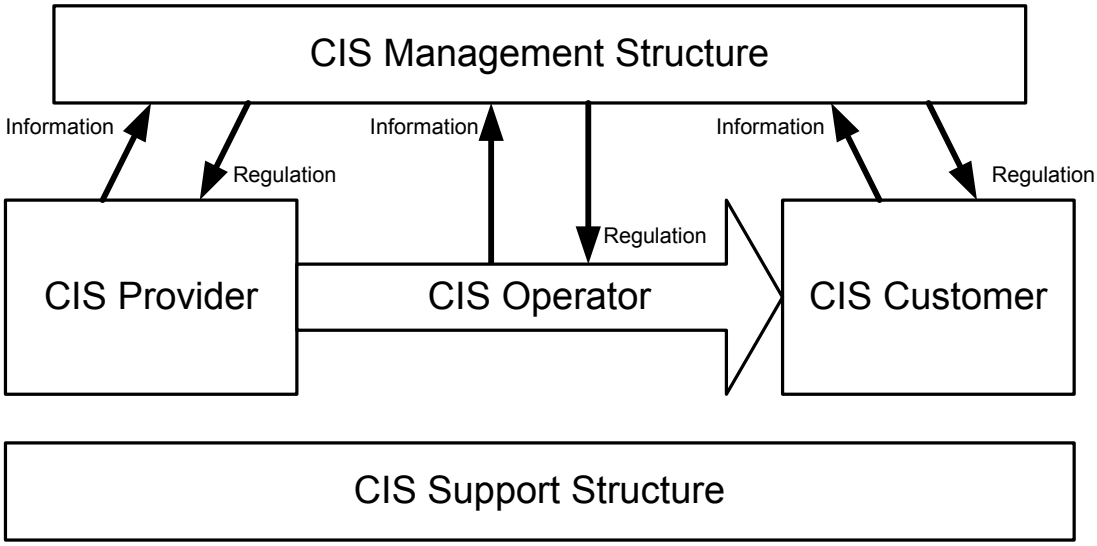

Figure 4: CI Element Structure.

The purpose of this model is to improve understanding of the operability of a critical service as an elementary piece of any critical infrastructure. The model helps to forecast and quantify effect linked with the critical service. A kernel is two relations: CIS Customer – CIS Operator and CIS Operator – CIS Provider. To provide CIS, these subjects need a defined amount for resources, which can be expressed as required CIS consumption, CIS quality (of service), CIS time of delivery, CIS location of delivery etc.

If the CIS Customer demonstrates its CIS demands, it is possible to calculate quantities of all resources required by the CIS Operator and CIS Provider. And the CIS Operator and the CIS Provider are just a CIS Customer, if they need to use any critical service to fulfil their services. According to this series, a chain of critical services is established and helps to quantify complex set of demands.

The Model includes the CIS Management Structure and CIS Supporting Structure. Both present complex dependencies related to the CI management fields (see table 3). The CIS Management Structure reflects high level fields (Social, Organization, and Information) and the CIS Support Structure relates to the lowest level called Feature Field.

In the CI Element Chain Model, the CI Service is described as a suitable relation among the CI primitive elements. By a chain of CI Services users can formulate complicated relations inside a studied segment of CI including it's complex dependencies. For this reason, the CI Element Chain model is a helpful instrument for describing CI.

5 CI Simulations and Scenarios

Modelling involves the use of formal relationships to describe a system. The user needs to have a solid understanding of the system: specifically the relationships between events, factors and variables within the model, and secondly the magnitude of those relationships.

The discussed CI Models describe a studied reality quite deterministic, so they bring limited knowledge of the behaviour of the critical infrastructures. The ultimate aim is to model the behaviour of the critical infrastructures as a complete and integral organism and understand CI reliance on information and communication technology.

This can be achieved through the application of such analytical tools and techniques as simulations and scenarios.

The simulations can be defined as the mimicking of a system with its dynamic and temporal processes in an "experimentable" model, with the overall aim of gaining insight that can be applied to real-life situations.

The scenarios are focused analyses of different futures presented in a coherent script-like fashion. They are not predictions but possibilities with the aim to trigger "what-if" thinking in a strategic process and thus handling uncertainty. They include coherent pictures of plausible future dealing with uncertainty about what the future could bring. A scenario can be desirable, an undesirable, or just a possible future or even a range of plausible futures.

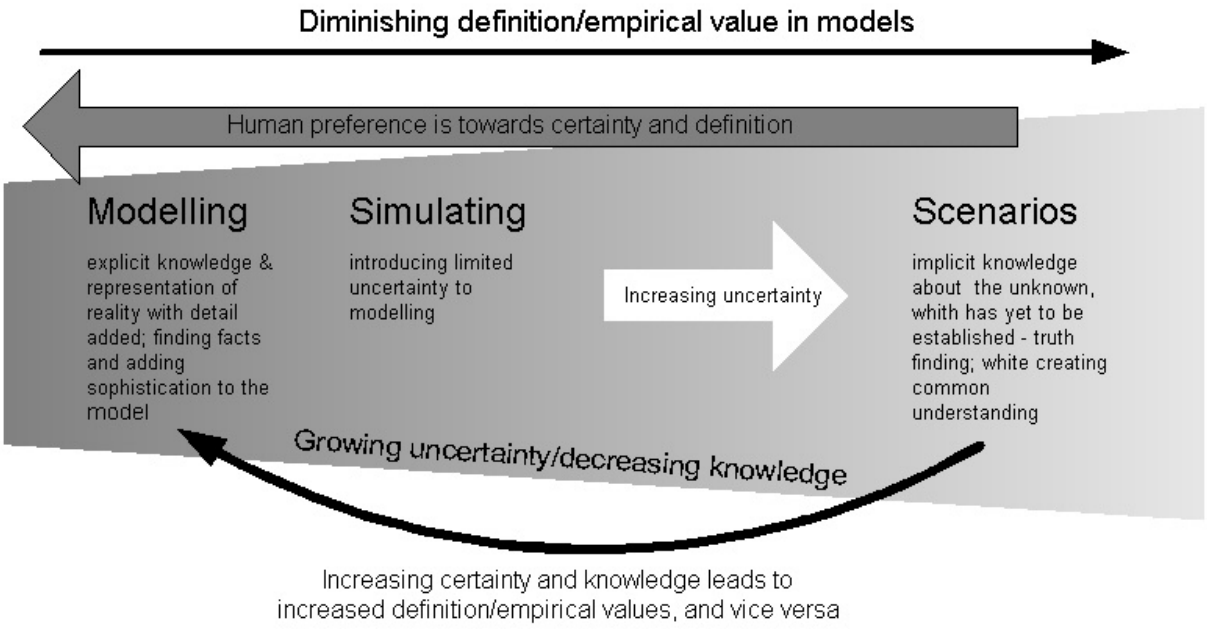

Figure 5: Knowledge and Certainty Progress.

Generally speaking, the models can be used in designing scenarios so that the relations between different factors can be understood. The models are a simplified representation of reality constructed to explore particular aspects or properties. The scenarios are complex methodologies which integrate with and rely heavily on all aspects of future analysis and can be used for the full range of challenges. So the scenarios must be aimed at bridging the gap between the required implicit knowledge and the explicit knowledge of the empirical values included in the models.

6 Conclusion

The CI modelling is a critical piece of CIP. The presented models serve for a better understanding of CI and it's included dependencies. The CI Layer model describes the general overview and the CI Element Chain model concentrates on the required details. The basic advantage is in combinations of both models. The combination can be used as a skilful fundament of more sophisticated methods built on the simulations and scenarios.

References

[1] The International Critical Infrastructure Protection Handbook: Exploratory Study, Swiss Federal Institute of Technology, Zurich, 2001.

[2] The National Strategy to Secure Cyberspace, The President's Critical Infrastructure Protection Board, Washington, 2002.

[3] Wenger, A., Metzger, J. and Dunn, M.: International Critical Information Infrastructure Protection Handbook, Swiss Federal Institute of Technology, Zurich, 2002.

[4] Architecture of an Integrated Model Hierarchy, ACIP, European Union, 2003.

[5] Using Scenarios to Support Critical Infrastructure Analysis and Assessment, ACIP, European Union, 2003.

[6] Šiška, V.: Critical Infrastructure Protection of Unclassified Information Systems, in *Proc. Of Emergency 2002,* article 29, 2002. in Czech

[7] Šmíd, J.: Critical Infrastructure Security in Information Society, in *Proc. Of Emergency 2002,* article 30, 2002. in Czech

[8] Towards a Centre for Critical Infrastructure Protection, CCIP, New Zealand 2001.