A1 Key Terms

Agent-Based Modeling

See →*Agent-Based Modeling and Simulation (ABMS)*.

Agent-Based Modeling and Simulation (ABMS)

Agent-based models are computer-driven tools to study the intricate dynamics of →*Complex Adaptive Systems;* those real-world systems in which very complicated behaviors emerge from the relatively simple, local interaction of many different individual components. The primary assumption in ABMS is that system behavior can be explained by individual traits, as the individuals interact and adapt to each other and their environment. In ABMs, complex interactions are emergent, whereas in other models the types of interactions must be foreseen and written into the model.[1]

Broad Risk Areas

The Australian PreDict approach[2] has developed industry →*Vulnerability Profiles* for ten sectors and focused on the critical interdependencies between them. The magnitude of the identified vulnerabilities was assessed and categorized into 12 groupings of →*Broad Risk Areas*, namely: Political, Economic, Social/Environmental/Cultural, Technological, Supplier, Customer, Substitutes, Competitor, Barriers to Entry, Operations (Human Resources), Operations (Training), and Flexibility/Adaptability. The majority of the Broad Risk Area titles were drawn from the analytical perspective resulting from a →*PEST* and →*Porter's Analysis*.

Cascading Effect

A cascading effect occurs when a condition in one section of an infrastructure system causes a fault that then, in turn, causes another fault somewhere else in the system, and then ripples across the sector or the whole system of complex infrastructures.

1 http://www.cas.anl.gov/.
2 http://www.defence.gov.au/predict/.

Categories

Categories of risks, likelihood, impact, and consequences vary considerably and need to be defined thoroughly at the beginning of any risk assessment. Categorization might depend on the desired level of precision in the assessment, or on whether it is a →*Qualitative* or a *Quantitative Risk Assessment.* The most simple ranking can be expressed using the categories "high", "medium", and "low".

Causal Mapping

Causal mapping refers to the use of directed node and link graphs to represent a set of causal relationships within systems of complex relationships. Causal relations are represented as nodes and links, and concepts of cause and effect are established with direct or inverse directions. The method can be used to explore cognition and to develop maps that can provide a basis for confirmatory empirical testing.

Computer Emergency Response Team (CERT)

CERTs are an integral part of current early warning efforts in all surveyed countries. They are established on the premise that any understanding of current security problems and potential solutions has to be derived from an analysis of security incidents, intrusion techniques, configuration problems, and software vulnerabilities. Their role is to analyze the state of Internet security and convey that information to the system administrators, network managers, and others in the Internet community. The first CERT (today, the CERT Coordination Center, or CERT/CC) was founded in 1988 and is located at the Software Engineering Institute (SEI), a federally funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania.[3]

Common Criteria

The *Common Criteria for Information Technology Security Evaluation* (CC) defines general concepts and principles of IT security evaluation and presents a general model of evaluation. It presents constructs for expressing

3 http://www.cert.org/.

IT security objectives, for selecting and defining IT security requirements, and for writing high-level specifications for products and systems.[4]

Complex Adaptive Systems (CAS)

CAS are real-world systems that are characterized by apparently complex behavior, which emerges as a result of often nonlinear spatio-temporal interactions among a large number of component systems at different levels of organization.

Consequence

The consequences of an infrastructure disruption are sometimes also called →*Damage*, →*Harm*, or →*Impact*. Consequences usually entail either physical harm or injury that makes something less useful, valuable, or able to function; a harmful effect on somebody or something; or the cost or price of something.

Critical Information Infrastructure (CII)

Critical Information Infrastructure (CII) includes components such as telecommunications, computers/ software, the Internet, satellites, fiber optics, etc. The term is also used for the totality of interconnected computers and networks and their critical information flows, as well as for that part of the global or national information infrastructure that is essentially necessary for continuity of the critical infrastructure services.

Critical Information Infrastructure Protection (CIIP)

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

4 http://www.commoncriteria.org/index.html.

Critical Infrastructure (CI)

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

Critical Infrastructure Protection (CIP)

Critical Infrastructure Protection (CIP) includes measures to secure all systems and assets whose incapacity or destruction would have a debilitating impact on national security, and the economic and social well-being of a nation. CIP is more than CIIP, but CIIP is an essential part of CIP.

Criticality Matrix

Criticality, e.g. the criticality of processes, can be derived from the combination of effects and failure probability (see Table 2).

Failure Probability						
	Virtually Certain	Significant	Significant	High	High	High
	Probable	Intermediate	Significant	Significant	High	High
	Possible	Low	Intermediate	Significant	High	High
	Improbable	Low	Low	Intermediate	Significant	High
	Highly Unlikely	Low	Low	Intermediate	Significant	Significant
		Insignificant	Minor	Moderate	Major	Catastrophic
		Effects/Degree of Damage				

Table 2: Assessment of Criticality

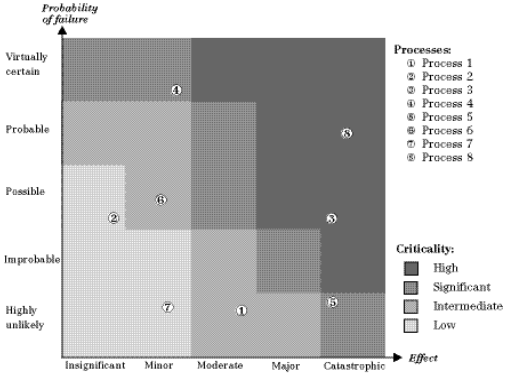
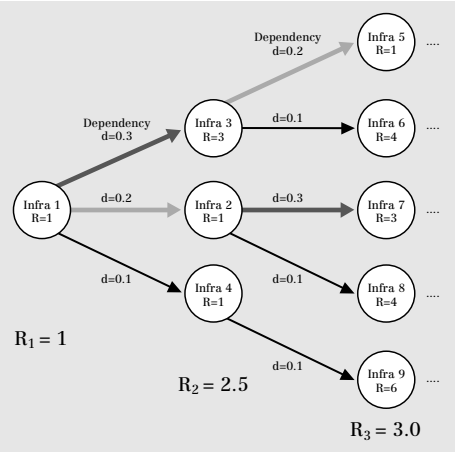


Figure 1:
Criticality Matrix for Processes[5]

5 Reinermann, Dirk and Joachim Weber. *Analysis of Critical Infrastructures: The ACIS Methodology (Analysis of Critical Infrastructural Sectors)* Paper presented at the Critical Infrastructure Protection (CIP) Workshop (Frankfurt a.M., 29–30 September 2003).

The result of the criticality analysis can then be entered into the criticality matrix, which is a graphical representation of the failure mode and effects, usually graphed as the probability of occurrence vs. severity level.

Cumulative Risk Assessment



A cumulative risk assessment is the process of evaluating the combined exposure and hazard of a subject from all factors that share a common mechanism of danger. In CIIP, the risk of dependencies propagates and the risk to infrastructures accumulates. In Figure 2, the cumulative risk to Infrastructure 1 rises from 1 to 2.5 to 3.0 (etc.) as one goes into more depth.

Figure 2: Cumulative Risk Tree[6]

Damage

Damage is also called →*Harm*, →*Impact*, or →*Consequence*. It is manifested either as physical harm or injury that makes something less useful, valuable, or able to function; as a harmful effect on somebody or something; or as the cost or price of something.

Denial of Service (DoS)-Attack

A denial of service (DoS) attack is any attack that occupies enough of a limited resource to make the resource unusable for legitimate purposes. There are two types of DoS attacks: local and distributed.

6 Grenier, Jacques. "The Challenge of CIP Interdependencies". *Conference on the Future of European Crisis Management.* (Uppsala, Sweden, 19–21 March 2001). http://www.ntia.doc.gov/osmhome/cip/workshop/ciptf_files/frame.htm.

Distributed Denial of Service (DdoS)-Attack

A DdoS-Attack is a →*Denial of Service (DoS)-Attack* involving two or more machines. DDoS attacks entail breaking into hundreds or thousands of machines all over the Internet. Then the attacker installs DDoS software on them, allowing them to control all these stolen machines to launch co-ordinated attacks on victim's internet sites. These attacks typically exhaust bandwidth, CPU capacity, or other resources, breaking network connectivity to the victims.

Dependability

Dependability is the collective term used to describe availability performance and factors influencing it: reliability performance, maintainability performance, and maintainability support performance. The term "Dependability" is used only for general descriptions in non-quantitative terms.[7]

Dependency

Dependency may exist between two components, often within a sector. The term describes a specific, individual connection between two infrastructures, such as the electricity used to power a telecommunications switch. Usually, this relationship is unidirectional. Dependency is, therefore, a linkage or connection between two infrastructures through which the state of one infrastructure influences or is dependent on the state of the other.

Dependency/Interdependency Matrices

Dependency/Interdependency Matrices often serve as a tool for visualizing the strength of interdependencies between different sectors. Often, different colors representing values (→*Categories*) such as "high", "medium", "low", or "none" are used to show the strength of interdependencies. These matrices are read horizontally by industry sector, where each field describes the level of dependency on the sector in the vertical column.

7 http://www.asq-rd.org/depend.htm.

Sector	Element	Electrical Power	Water Purification	Sewage Treatment	Natural Gas	Oil Industry	Customs and Immigration	Hospital & Health Care Services	Food Industry
		Energy & Utilities					Services		
Energy & Utilities	Electrical Power		L			M			
	Water Purification	H				M			
	Sewage Treatment	M	H			H			
	Natural Gas	L				L			
	Oil Industry	H	L						
Services	Customs & Immigration	H	L	L	L	L		L	
	Hospital & Health Care Services	H	H	L	H	H	M		H
	Food Industry	H	H	H	L	M	M	L	

Key: H High M Medium L Low

Figure 3: Dependency / Interdependency Matrix

Direct Vitality

Direct Vitality is the contribution that a product or service delivers to the continuity of the society, which is equivalent to the amount of direct (first-order) damage caused by a loss or serious disruption of the product or service.

Emergent Behavior

The idea behind emergent behavior is that from simple interactions and/or rules, complex behaviors can emerge at the group level that would not at the individual level. An emergent property is one that appears as the unpredictable result of the complex interactions of parts that themselves obey simple rules or laws.

Event Tree Analysis

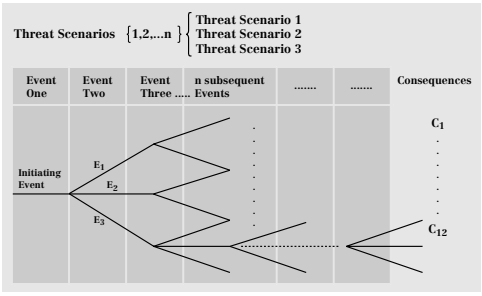


Figure 4: Event Tree (Source: Ezell, Farr, Wiese)

Event tree analysis asks "what if" to determine the sequence of events that lead to consequences. From the event tree, one can deduce a probability density and an exceedance probability. Event trees help to understand how an outcome is determined by mitigating events. The failure of each mitigating event may be estimated through expert assessment or, in some cases, through an additional →*Fault-Tree Analysis*. Figure 4 is an example of an event tree.

Expert Assessment/ Interviews

A very effective way of getting information on various aspects of CII is to circulate a questionnaire among key persons and experts, or to interview them. A questionnaire can contain multiple-choice answers that can be assessed afterwards with the help of an evaluation key, or questions can be phrased to leave more latitude for semi-structured answers.

Fault Tree Analysis

A fault tree analysis is a deductive, top-down method of analyzing system design and performance. It involves specifying an (often undesirable) top event for analysis, followed by the identification of all associated elements in the system that could cause that top event to occur. Fault trees can be used to assess the probability of failure of a system or of a top event occurring, to compare design alternatives, to identify critical events that will significantly contribute to the occurrence of the top event, and to determine the sensitivity of the probability of failure of the top event to various contributions of basic events. Fault tree analyses are generally performed graphically using a logical structure of "AND" and "OR" gates (Figure 5).

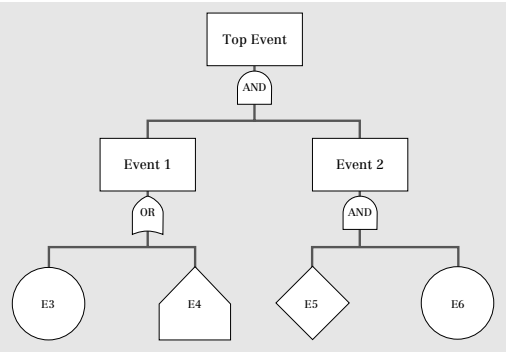


Figure 5: Example of a Simple Fault Tree

Harm

Harm to CI/CII is also called →*Damage*, →*Impact*, or →*Consequence*. It is either physical harm or injury that makes something less useful, valuable, or able to function; a harmful effect on somebody or something; or the cost or price of something.

Impact

The Impact of a disruption in CI/CII is also called →*Damage*, →*Harm*, or →*Consequence*. It manifests itself either as physical harm or injury that makes

something less useful, valuable, or able to function; as a harmful effect on somebody or something; as or the cost or price of something.

Impact Assessment

Impact assessment is one step within the whole risk analysis process that aims to determine the impact resulting from a successful threat exercise of a vulnerability. The grade of possible harm to an asset must be determined by a number of experts familiar with the assets, be they executives such as experts within the administration, asset owners, or asset managers.

Indicator

There are many definitions for the term "Indicator" in many different communities. It can be understood as a way of measuring, indicating, or identifying more or less exactly a sign, symptom, or index of a system.

Indirect Vitality

Indirect Vitality is the extent to which other vital products and services contribute to the dependability of the vital service or product

Information and Communication Technologies (ICT)

Information and Communication Technologies are characterized by (1) computing and telecommunications equipment, software, processes, and people that support the processing, storage, and transmission of data and information, (2) the processes and people that convert the data into information and information into knowledge, and (3) the actual data and information.

Information Security Guidelines

Information Security Guidelines are suggested actions or recommendations to address an area of →*Information Security Policy*. A security guideline is not a mandatory action. However, Information Security Guidelines are considered best practices and should be implemented whenever possible.

Information Security Policy

Information Security Policy is an organizational document usually ratified by senior management. It aims to reduce the risk of, and minimize the effect (or cost) of, security incidents. It establishes the ground rules for the organization's information systems operations. The formation of an Information Security Policy is driven by many factors, the key part of which is →*Risk*.[8]

Infrastructure

The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services. Infrastructures provide a reliable flow of products and services essential to defense and economic security, the smooth functioning of governments at all levels, and society as a whole.

Interdependency

An interdependency is a bi-directional relationship between two infrastructures through which the state of each infrastructure influences or is correlated to the state of the other. More generally, two infrastructures are interdependent when each is dependent on the other.

Interdependency Chart

See →*Dependency/Interdependency Chart*.

IT-Security Objectives

There are four basic IT-security objectives:[9]

(1) Availability (of systems and data for intended use only): Availability is required to assure that systems work promptly and service is not denied

8 http://www.yourwindow.to/information-security.

9 Cf. Stoneburner, Gary. *Computer Security. Underlying Technical Models for Information Technology Security. Recommendations of the National Institute of Standards and Technology*. NIST Special Publication 800–33. (Washington, D.C.: U.S. Government Printing Office, December 2001). http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf.

to authorized users. This objective protects systems against intentional or accidental attempts to either perform unauthorized deletion of data or otherwise cause a denial of service or data, and against attempts to use a system or data for unauthorized purposes.

(2) Integrity of system or data: Integrity is required on two levels:

- Data integrity (the requirement that data not be altered without authorization while in storage, during processing, or while in transit), and
- System integrity (the quality that a system has when performing the intended function in an unimpaired manner, free from unauthorized manipulation).

(3) Confidentiality of data and system information: Confidentiality is the requirement that private or confidential information not be disclosed to unauthorized individuals. Confidentiality protection applies to data in storage, during processing, and while in transit.

(4) Accountability (to the individual level): Accountability is the requirement that actions of an entity may be traced uniquely to that entity.

As a fifth objective, the assurance that the other four objectives have been met is sometimes mentioned.

Layer Model

Layer models show parts of infrastructure systems or the totality of a nation's critical infrastructures and their relationship to each other, and often serve to picture interdependencies between the elements.

Logarithmic Scale

On a linear scale, the ratio of successive intervals is equal to "1". A logarithmic scale is different in that the ratio of successive intervals grows exponentially. Each interval on a logarithmic scale exceeds the previous interval by an order of magnitude. A typical ratio is 10, so that the marks on the scale read: 1, 10, 100, 1'000, 10'000, etc. Such a scale is useful if you are plotting a graph of values which have a very large range The logarithmic scale allows for much greater granularity at the lower end of the axis. Gradations in the scale for social and political impacts can also be set out. Social and political scales will be more subjective, using examples rather than number ranges.

Model

A model is a simplified representation of a system at some particular point in time or space, intended to promote understanding of the real system. System modeling is the process of describing both natural and engineered systems in precise mathematical terms. Thus, a model is a simplified representation of the real system intended to promote the development of understanding.

Multi-Criteria Decision Approach

The multi-criteria decision approach (MCDA) is both an approach and a set of techniques, with the goal of providing an overall ordering of options, from the most preferred to the least preferred option. MCDA involves structuring the research problem into a multi-criteria hierarchy, where measures are linked to a top-level goal through several levels of decision criteria. The top-level goal is the overall objective of the system of analysis.

Multi-Criteria Model

See →*Multi-Criteria Decision Approach*.

PEST (Political, Economic, Social, Technological) Analysis

A PEST analysis is usually conducted to obtain an understanding of the macro-environment affecting the business or sector under consideration (political, economic, social, and technological factors). The concept of the PEST analysis is to look at external factors that influence the business. Table 3 shows an example of a PEST analysis table.

	Political	Economic	Social	Technological
Macro Overview	- Globalization - Privatization	- Economic development - Inflation - Unemployment	- Population - Education	- PC penetration - Reliance of key infrastructure on technology systems - Internet access
Specific Sector Drivers	- Establishment of federal ministries - Organizations	- Importance of industry - R&D	- Improve quality of life - Global community - Knowledge-sharing	- Technological breakthroughs

Table 3: PEST Example

Porter's Analysis

Michael Porter's analysis looks at the competitive forces at work in a particular sector or industry. Important criteria in this analysis are intensity of rivalry; competitors, barriers to entry, or the threat of substitutes; supplier power, and buyer power. Figure 6 shows Porter's "five forces" model.

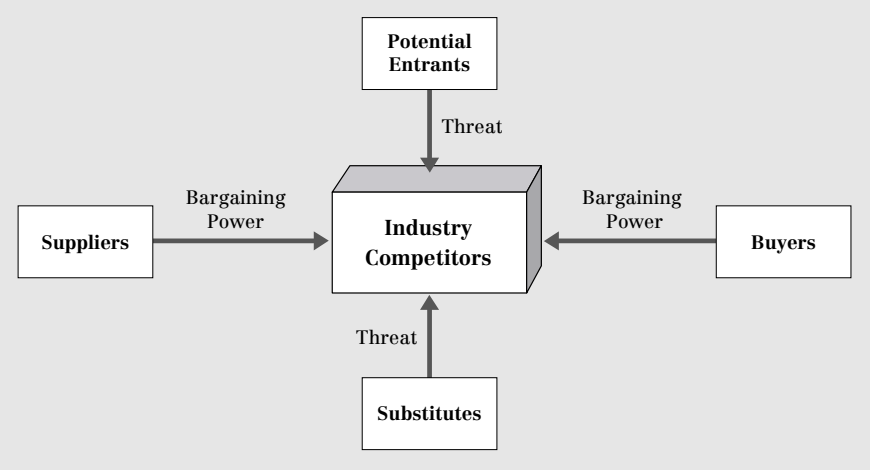


Figure 6: Porter's Five Forces Model

Qualitative and Quantitative Risk Assessment

A *quantitative* risk assessment expresses threat likelihood, impact, and risk in terms of a numeric value, whereas a *qualitative* assessment uses ratings such as "high", "medium", or "low" to express the value. The major advantage of the quantitative approach is that it is precise and provides a measurement that can be fed directly into a cost-benefit analysis. Many approaches today start out by using qualitative rankings ("high", "medium", or "low") and attribute a range of values to each.

Questionnaire

A Questionnaire is a set of specially designed questions to which answers are written on a pre-prepared form. Questionnaires are used in CIP/CIIP to get crucial information from stakeholders on issues such as products and services regarded vital, underlying processes and dependencies, or possible damage.

Risk

Risk is often defined quantitatively as a function of the *likelihood* of a given *threat source* displaying a particular potential *vulnerability*, and the resulting *impact* of that adverse event. However, risk sociologists have identified the importance of a third element: the ability of humans to influence both the probability of a risk occurring and the extent of the damage.

Risk / Impact Scattergram

When assessing impact of incidents, a scattergram plotting the relative rated criticality of the infrastructure elements (increasing from bottom to top) against their relative risk value (increasing from left to right) can be used (Figure 7).

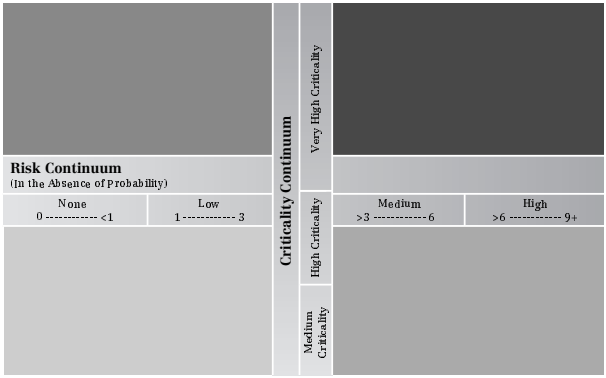


Figure 7: Risk/ Impact Scattergram

This creates four quadrants in which crucial elements of a sector (e.g. communication satellites or telecom systems for the communications sector) can be positioned. This is a way to show which element needs special attention.

Risk Analysis

Risk analysis is a systematic approach to gaining a more comprehensive assessment of risks that aims at bringing transparency into complexity and at addressing uncertainties or knowledge gaps. It supports risk management decisions and communication about risk. It is a procedure that helps to identify threats and vulnerabilities, analyze them to ascertain the exposures, and highlight ways in which the impact can be eliminated or reduced.

Risk Level Matrix

A risk level matrix is used in connection with a →*Risk Scale* to determine and describe the intensity of risk. It establishes a relationship between two categories (such as threat likelihood and impact) and multiplies the values assigned to each category (Figure 8).

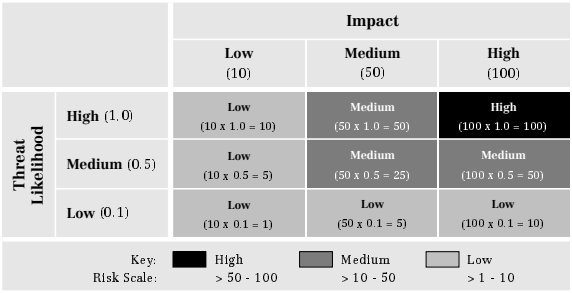


Figure 8:
Typical Risk Level Matrix

Risk Rating Matrix

After the evaluation of threat and vulnerability for single components of an infrastructure element, risks can be determined based on a matrix that multiplies the assigned values for threat and vulnerability (Figure 9). This method allows for a comparison of relative risks between components of an infrastructure element, between layers in the infrastructure model, and between infrastructures.

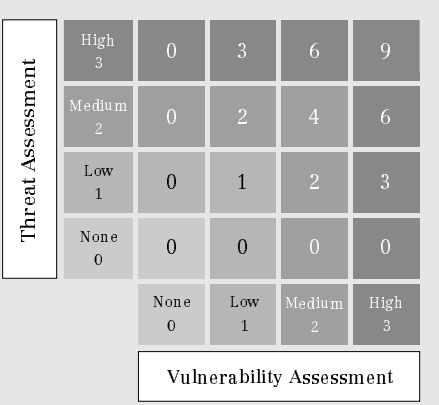


Figure 9: Basic Risk Rating Matrix

Risk Scale

A risk scale assigns numeric values to →*Categories* of risk, such as “high”, “medium”, or “low”. (See Figure 8).

Roundtable

A Roundtable is a discussion group for professionals in any industry who come together to discuss a number of issues.

Scenarios/ Scenario Technique

The scenario technique enables the generation of scenarios that serve to determine strategies in order to control or at least influence the unknown developments of complex systems as favorably as possible with regard to own objectives and interests. There are various techniques and even software tools to develop scenarios.[10]

Sector

a) One of the two divisions of the economy (private or public); b) a group of industries or infrastructures that perform similar functions within a society (e.g., vital human services)

Sector Analysis

Sector analysis adds to an understanding of the functioning of single sectors by highlighting various important aspects of the sector.

Sector Model

Sector and layer models are mainly used as illustrations of how critical infrastructures are organized. They vary considerably from country to country

Seminar Games

Seminar gaming is an approach to understanding complex problems that capitalizes on the inherent expertise of groups of participants, who discuss complex topics by way of scenarios.

Simulation

A *Simulation* is the manipulation of a model in such a way that time or space are compressed, thus enabling one to perceive the interactions that would not

10 Cf. von Reibnitz, Ute. *Szenario-Technik: Instrumente für die unternehmerische und persönliche Erfolgsplanung.* (Wiesbaden, 1992).

otherwise be apparent because of their separation in time or space. Simulation is the exploitation of a model in order to predict logical consequences of hypothetical situations. A simulation is generally used to study the implications of the defined interactions of developed models running over time.

Sub-Sector

A sub-sector is the next smallest unit within a →*Sector*, often in terms of organizational standpoints or services delivered.

SWOT (Strength, Weakness, Opportunities, Threats)

A SWOT analysis, which focuses on strength, weakness, opportunities, and threats, is usually conducted at the micro-level, or business unit level, but can also be conducted at the sector level. Table 4 shows a typical SWOT worksheet.

		Environment Analysis	
		Opportunities (1) Opportunity 1 (2) Opportunity 2 (n) Opportunity n	**Threats** (1) Threat 1 (2) Threat 2 (n) Threat n
Situation Analysis	**Strengths** (1) Strength 1 (2) Strength 2 (n) Strength n	SO-Strategies Examples: *S1O1: Specific strategy* *S1SnO1: Specific strategy* ...	ST-Strategies Examples: *S1S3T2: Specific strategy* ...
	Weaknesses (1) Weakness 1 (2) Weakness 2 (n) Weakness n	WO-Strategies Examples: *W1O1O2: Specific strategy* ...	WT-Strategies Examples: *W2T2: Specific strategy* ...

Table 4: Typical SWOT Worksheet

System

A system can be a compound of several CI, a single infrastructure, an infrastructure-dependent enterprise, or a particular system within a given infrastructure, according to four hierarchy levels: 1) The system of systems; 2) individual infrastructures; 3) the individual system or enterprise; and 4) technical components.

System of Systems

The term "system of systems" has no clear and accepted definition, but the phenomenon is widespread and generally recognized. It can be seen as an emergent class of systems that are built from components which are large-scale systems in their own right (e.g., the energy system).

Threat Assessment

Threat assessment in the risk analysis context includes the determination of (1) the nature of external and internal threats, (2) their source, and (3) the probability of their occurrence, which is a measure of the likelihood of the threat being realized. However, when dealing with human actor-based threats such as terrorism, we are dealing with a "people business" that is intrinsically non-quantifiable – and thus poses significant problems for traditional risk analysis aproaches.

Values

See →*Categories*.

Vulnerability

Vulnerability can be understood as the collective result of risks and as the ability of a society, local municipal authority, company, or organization to deal with and survive external and internal emergency situations. The vulnerability analysis covers a long-term perspective and gives focus to a sequence of events, from the moment an emergency situation occurs until a new stable situation has been reached (see also →*Vulnerability Assessment*).

Vulnerability Analysis

See →*Vulnerability Assessment*.

Vulnerability Assessment

Vulnerability assessment is one step within risk analysis methodology. Its goal is to develop a list of vulnerabilities that could be exploited by a potential threat-source ("exposure analysis"). There are several sophisticated approaches to Vulnerability Assessment

Vulnerability Profile Chart

A vulnerability profile chart visually represents vulnerability rankings, often with a focus on interdependencies. Each profile may represent a single sector. The vulnerability ranking is done in order to compare and contrast vulnerabilities between sectors. One possible approach is the definition of "risk areas" in order to group vulnerabilities into common areas for analysis.

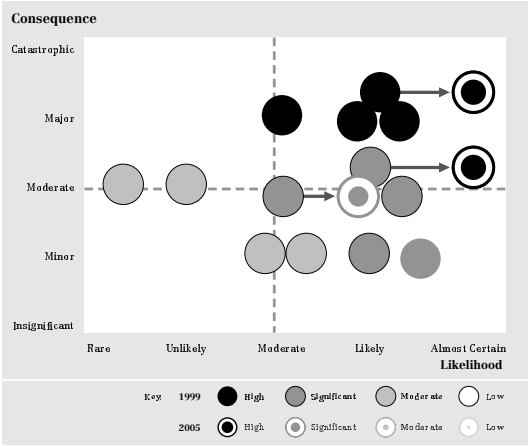


Figure 10: Vulnerability Profile Chart (Source: PreDICT)

Vulnerability Rating Table

Vulnerability is sometimes defined as a function of likelihood and consequences. Through the separate analysis of each, the vulnerabilities can be rated using the product of the "Consequence" and the "Likelihood" ratings, displayed as a rating table (Figure 11).

		Consequences				
		Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood	Almost Certain					
	Likely					
	Moderate					
	Unlikely					
	Rare					

Key: High Significant Moderate Low

Figure 11: Vulnerability Rating Table

Center for Security Studies, ETH Zurich
Volume 2, Zürich 2004.

The International CIIP Handbook 2004: An Inventory and Analysis of Protection Policies in Fourteen Countries

Myriam Dunn and Isabelle Wigert

edited by
Andreas Wenger and Jan Metzger