Chapter 2
Properties of Critical Infrastructures

Physical-engineered critical infrastructures (CIs) are characterized as large scale, spatially distributed, complex networks—either open or closed. According to Dueñas-Osorio and Vemuru (2009), these systems are made of “a large number of interacting components (real or virtual), show emergent properties difficult to anticipate from the knowledge of single components, are characterized by a large degree of adaptability to absorb random disruptions and are highly vulnerable to widespread failure under adverse conditions.” Indeed, small perturbations can trigger cascades and large-scale consequences in CIs; furthermore, disruptions may also be caused by targeted malicious attacks.

2.1 Complexity

A recent National Science Foundation (NSF) workshop report (Guckenheimer and Ottino 2008) points at the fact that a complex system is characterized by an internal structure which may consist, besides many interacting components, of “a network that describes which components of the system interact, multiple scales of space and/or time, or symmetry. The components of many complex systems are heterogeneous and form a hierarchy of subsystems.” Furthermore, uncertainty is regarded as pervasive in complex systems, and its characterization and propagation through the system as key aspects for the reliable prediction of the system behavior and its effect and safe control.

The above attributes draw the boundary between simple and complex systems. Less trivial is to draw a boundary between complicated and complex systems. Table 2.1 attempts to do so by highlighting the very essence of a complex system, which is believed to lie in the degree and modality the parts interact and the overall behavior of the system that emerges from these. “The system must be analyzed as a whole; decomposing the system and analyzing subsystems does not necessarily give a clue as to the behavior of the whole” (Guckenheimer and Ottino 2008).

W. Kröger and E. Zio, *Vulnerable Systems*, DOI: 10.1007/978-0-85729-655-9_2,

Table 2.1 Characteristics of complicated versus complex systems, both entailing a large number of highly connected components

Complicated systems (mechanical watches, aircraft, power plants, etc.)	Complex systems (stock market, www, power grid, etc.)
Components have well-defined roles and are governed by prescribed interactions	Rules of interaction between the components may change over time and may not be well understood
Structure remains stable over the time. Low dynamics	Connectivity of the components may be quite plastic and roles may be fluid. Interactions are not always obvious
No adaptation. One key defect may bring system to a halt	System responds to external conditions and evolves
Limited range of responses to changes in their environment	Display organization without a central organizing principle (self-organization/emergence)
Decomposing the system and analyzing subparts can give us an understanding of the behavior of the whole, i.e., the whole can be reassembled from its parts	Respond to and interact with their environment
Problems can be solved through analytical thinking and diligence work	Inadequate information about the state of the influencing variables, nonlinearities
	Overall behavior cannot be simplified in terms of their building blocks. The whole is much more than the sum of its parts

2.2 Learning from Experience

Despite Cassandra, CIs have proved highly reliable in and beneficial for Western societies. Nevertheless major breakdowns have occurred, illustrating the complexity of system behavior and of the event sequences which may generate, and showing the negative consequences of dependencies leading to cascading effects.

In the electrical transmission CIs, for example, the analysis of recent major blackouts from 2003 to 2006 (Table 2.2) leads to drawing some conclusions on the main underlying causes and to carving some patterns of common behavior:

- Technical failures (Denmark/Sweden, two independent failures), external impacts (Tokyo, construction work; Brazil, extreme weather conditions) and adverse behavior of protective devices (London) are important triggering events, when not protected by the N-1 security criterion[1] and/or in combination with high-load conditions (Moscow).

[1] Definition of the N-1 security criterion specifies that “any probable single event leading to a loss of a power system element should not endanger the security of the interconnected operation, that is, trigger a cascade of trippings or the loss of a significant amount of consumption. The remaining network elements, which are still in operation, should be able to accommodate the additional load or change of generation, voltage deviation or transient stability regime caused by the initial failure.” (Union for the Coordination of Transmission of Electricity 2008).

Table 2.2 Recent major blackouts of electric power supply systems

Blackout		Load loss (GW)	Duration (h)	People affected	Main causes
Aug 14, 2003	Great Lakes, NYC	~60	~16	50 million	Inadequate right-of-way maintenance, EMS failure, poor coordination among neighboring TSOs
Aug 28, 2003	London	0.72	1	500,000	Incorrect line protection device setting
Sept 23, 2003	Denmark/Sweden	6.4	~7	4.2 million	Two independent component failures (not covered by N-1 rule)
Sept 28, 2003	Italy	~30	up to 18	56 million	High load flow CH-I, line flashovers, poor coordination among neighboring TSOs
July 12, 2004	Athens	~9	~3	5 million	Voltage collapse
May 25, 2005	Moscow	2.5	~4	4 million	Transformer fire, high demand leading to overload conditions
June 22, 2005	Switzerland (railway supply)	0.2	~3	200,000 passengers	Non-fulfillment of the N-1 rule, wrong documentation of line protection settings, inadequate alarm processing
Aug 14, 2006	Tokyo	?	−5	0.8 million households	Damage of a main line due to construction work
Nov 4, 2006	Western Europe ("controlled" line cut off)	~14	~2	15 million households	High load flow D-NL, violation of the N-1 rule, poor inter TSO–coordination
Nov 10, 2009	Brazil, Paraguay	~14	~4	60 million	Short circuit on key power line due to bad weather, Itaipu hydro plant (18 GW) shut down

- Organizational factors such as market liberalization and short-term contracting causing operation of the system beyond original design parameters (e.g., Great Lakes, Italy), and stressing operation conditions such as weakening maintenance work and/or inadequate integration of intermittent power generation (e.g., Western Europe) have proven to be outstanding causes.
- As the transmission system operators (TSOs) play a decisive role with regard to contingency management, lack of situational awareness and short-term preparedness, as well as limited real-time monitoring beyond control areas and poorly timed cross-border coordination (e.g., Great Lakes, Italy, Switzerland (rail)) build up as aggravating factors.
- The inadequacy of the N-1 security criterion and, even more importantly, of its inadequate evaluation/implementation in various cases have enforced attempts to make it more stringent and legally binding.

Also, lack of investment due to increasing economic pressure, public resistance, etc., can be observed in many countries and areas, leading to insufficient system monitoring, control, and automation as well as to insufficient grid extension and maintenance (including tree cutting programs [Great Lakes, Switzerland/Italy]), and thus contributing significantly to past blackouts.

As expected, disruption of electricity supply strongly affects our society and other infrastructures which depend on it. The Italian electric power blackout on September 28, 2003 at 3.01 a.m. (Sunday/Monday night) may serve as an example to further elucidate the course of events and delineate the associated consequences:

At the given date, one of the main north–south transit lines through Switzerland—the Lukmanier transmission line—shut down following a flashover between a conductor cable and a tree. This resulted in a redistribution of the electricity in accordance with the laws of physics, and a subsequent overload (110%) of another north–south transit line, namely the San Bernardino transmission line, which due to another flashover also shut down at 3.25 a.m. What followed was a series of cascading failures of other transmission lines in the border region. At that time, the Italian grid was completely separated from the UCTE[2] network. Despite primary frequency control, automatic disconnection of the pump storage plants in Northern Italy, and automatic load shedding (10 GW), the voltage and frequency drop within the Italian grid could not be mastered and generation plants started to trip. This in turn gave rise to a total blackout throughout Italy at 3.27 a.m. (except Sardinia).

After 3 hours, energy was restored in some regions connected to France (such as Liguria). Nine hours later, in the afternoon of September 28, electricity was restored gradually in most places, including Turin, Milan, Venice, and Rome. The energy not supplied due to the rotating outages totaled 12.9 GWh. Rolling blackouts continued to affect about 5% of the population on the next 2 days (September 29–30) as the electricity company ENEL continued its effort to restore supply. Restoring power to the whole country took 18 hours. As a consequence, other infrastructure sectors were affected showing their strong dependence on electricity supply (Fig. 2.1). The effects on the population, the economy and other infrastructures—in greater detail—are given in Table 2.3.

The role of failure cascades and (inter)dependencies among infrastructures (see Chap. 1 and Sect. 2.3) is highlighted in the real examples listed in Table 2.4. Details of the mini telecommunication blackout in Rome, Tor Pagnotta Street, on January 2, 2004 at 5.30 a.m., demonstrate the challenges to (inter)dependency analysis:

Flooding of a Telecom Italia major telecommunication service node occurred when a metallic pipe carrying cooling water for the air conditioning plant broke. The flooding led to several boards/devices failing due to short circuits and the main power supply going out of service. Diesel generators, part of the emergency power supply, failed to start due to the presence of water; only batteries provided power to the boards/devices still working, but finally dropped.

[2] Now ENTSO-E.

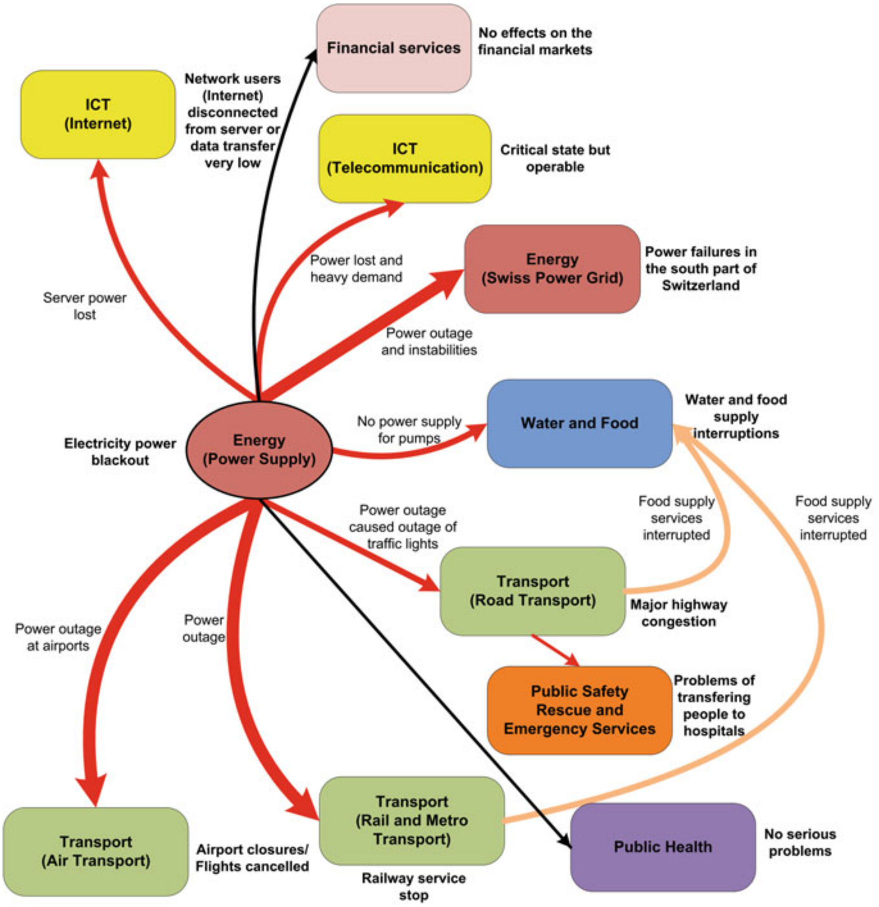

Financial services
No effects on the financial markets
ICT (Internet)
Network users (Internet) disconnected from server or data transfer very low
ICT (Telecommunication)
Critical state but operable
Energy (Swiss Power Grid)
Power failures in the south part of Switzerland
Power lost and heavy demand
Server power lost
Power outage and instabilities
Water and Food
Water and food supply interruptions
No power supply for pumps
Electricity power blackout
Energy (Power Supply)
Power outage caused outage of traffic lights
Food supply services interrupted
Food supply services interrupted
Transport (Road Transport)
Major highway congestion
Power outage at airports
Power outage
Public Safety Rescue and Emergency Services
Problems of transfering people to hospitals
Transport (Air Transport)
Airport closures/ Flights cancelled
Transport (Rail and Metro Transport)
Railway service stop
Public Health
No serious problems

Fig. 2.1 Impact of the Italian blackout on other infrastructure sectors

The Fire Brigade arrived at 7.30 a.m. and worked for pumping out the flooding water and finally individuating the point of the pipe breakage. To start the repair actions, technicians had to shut down the air conditioning plant. The mini blackout caused problems and delays in different infrastructures, including Fiumicino airport, ANSI print agency, post offices and banks, ACEA power distribution and the communication network (both fix-to-fix and fix-to-mobile), connecting the main Italian research institutions (Fig. 2.2).

As mentioned before, the Telco mini blackout also impacted services of ACEA electrical distribution power grid. ACEA has two Control Centres: manned Main Control Centre (Ostiense) and unmanned Disaster Recovery Control Centre (Flaminia). All the tele-measures, commands, and alarms managed by the unmanned control centre are dispatched to the manned one using two redundant TELCO communication links at 2 Mbits/s. One is the main link, the other one a

Table 2.3 Effects of the Italian blackout, September 28, 2003

Impact on the population: strong
About 56 million people have been affected, five elderly persons died
Hundreds of people have been trapped in elevators
Economic losses: moderate
About 120 million € due to spoiled foodstuff
Several hundred thousand € due to the interruption of continuously working industries (e.g., steel, cement or plastic factories); no effects on the financial markets
Impact on dependent critical infrastructures: varying
About 110 trains with more than 30,000 passengers stopped as well as subways in Rome and Milan. Flights were cancelled or delayed. Outage of traffic lights partly led to chaotic situations in major cities, no severe accidents
In some southern regions interruptions of water supply for up to 12 h.
Telephone and mobile networks in a critical state but operable; Internet providers shut down their servers (data transfer rate went down to 5% of normal)
Hospitals without serious problems due to the use of emergency power generators

backup link that is always in stand-by state. Such links were expected to be located on two different geographical paths. Due to a maintenance operation, both links were traversing the same flooded node. Therefore, both links were out of service during the blackout. As a consequence, there was no chance to exchange alarms and signals on the status of power distribution network, and commands between the unmanned centre and the manned one. In such a situation, ACEA completely lost the monitoring and control of all the remote substations managed by the unmanned control centre for a total of 1 h and 23 min. The difficulty of the manual diagnostic and recovery actions by ACEA operators were further increased due to partial out-of-service of fixed and mobile phones.

Fortunately, conditions were very favorable during the blackout so that the power grid required no control actions from ACEA Control Centres to its Remote Terminal Unit, within the duration of the Telco mini blackout.

2.3 Dimensions of Interdependencies

As clearly demonstrated by experienced events, dependencies and in particular interdependencies bear significant practical relevance rather than being a (fairly) new theoretical concept (Rinaldi et al. 2001) introduced six dimensions for their description, and a categorization into four general "types of interdependencies" (Fig. 2.3):

- Physical interdependencies—the state of each is dependent on the material output(s)/flows(s) of the other, e.g., a pipeline network provides gas to fuel a gas-fired power station while the electricity generated is used to power compressors and controls the gas supply network.

Table 2.4 Examples of the importance of interdependencies between critical infrastructures (based on ETH–Laboratory for Safety Analysis 2008)

Event	Duration	Cause	Affected infrastructures	Consequences	Vulnerabilities
May 19, 1998 Failure of Galaxy IV satellite (CRE)	2 days Galaxy IV was not restored	Failure of satellite's primary control processor (technical)	ICT Finance service	45 million customers lost pager service Loss of TV/radio service Disruption of bank card service	Almost all the satellites are not well protected due to their inherent designs and operating environment (design) The replacement of failed satellite is extremely slow and expensive (operational)
July 18, 2001 Baltimore Howard Street Tunnel fire (CIE)	The tunnel entrance was blocked for about 5 days	A freight train detailed while passing through Howard Street Tunnel in Baltimore and caused the fire explosion due to the subsequent ignition of the flammable liquid (technical)	Transport (rail transport) → water and food (geospatial) Transport (rail transport) ↔ ICT (radio) (physical) Transport (rail transport) → energy (power supply) (geospatial) Water and food (water supply) → ICT (Internet/ telecommunication) (geospatial) Water and food (water supply) → energy (power supply) (geospatial)	12 million USD associated with incident 23 bus lines and several train services suspended or delayed Delays of coal and limestone services Extremely heavy road congestion in Baltimore 14 million gallons of water lost (water supply system) 1,200 Baltimore buildings lost electricity Service disruptions for phone/cell phone and	Significance of this rail route was not fully recognized (organizational) Many structures, services, and private utility lines all coexisted within a relatively compact area (design)

(continued)

Table 2.4 (continued)

Event	Duration	Cause	Affected infrastructures	Consequences	Vulnerabilities
				slowed Internet service	
August 23-31, 2005 Hurricane Katrina (CCIE)	Katrina, a category 4 hurricane dissipated 7 days after it formed. Repair and recovery last more than four years	Hurricane Katrina caused severe damage along the Gulf coast from Central Florida to Texas, especially in New Orleans, Louisiana (natural)	Energy (power supply) → Water and food (water supply) (physical) ICT (telecommunication) → public safety, rescues, and emergency service (physical) ICT (telecommunication) → energy (power supply) (logical) Energy (power supply) → ICT (radio) (physical) Transport (road transport) → public health (medical care and hospitals) (physical) Energy (power supply) → public health (medical care and hospitals) (physical) ICT (radio) → public health (medical care and hospitals) (physical)	Damages cost more than 100 billion USD 1,836 fatalities 80% of New Orleans city flooded Drinking water contamination 890,300 customers in Louisiana lost power 30 oil drilling platforms destroyed or damaged 24% of annual oil production and 18% of annual gas production reduced 3 million customers lost phone lines of 2,000 cell sites, out of service Most of major roads in New Orleans area damaged 7 million gallons of oil and 1–2 million gallons of gasoline spilled into southeast Louisiana	The original levees in New Orleans was not prepared to category 4 or 5 hurricane (design) Massive inoperability problems between communication and power supply systems (design/operational) Lack of backup communication devices, such as satellite phone(organizational) Responsibilities (city, state, federal) turned out to be impending (organizational)

(continued)

Table 2.4 (continued)

Event	Duration	Cause	Affected infrastructures	Consequences	Vulnerabilities
				Population in New Orleans reduced half after Katrina	
August 17, 1999 Kocaeli Earthquake (CCIE)	Restoration process lasted from a few days (power supply) to months (transport infrastructure) and up to many years for total recovery	A Mw 7.4 earthquake along the North Anatolian Fault in northwestern Turkey (natural)	IE → ICT (Internet/telecommunication), energy (power supply, oil supply), chemical industry, transport (road/rail), water and food, public safety, rescues, and emergency services, financial services Energy (power supply) → ICT (telecommunication) (physical) Energy (power supply) → transport (rail/road) (physical) Energy (power supply) → water and food (water and food supply) (physical) Energy (oil supply) → transport (road) (physical) Transport (road) → public safety, rescues,	Around 15 billion USD losses Official death toll at 17,127 (unofficial figure closer to 40,000), 43,959 injured, around 500,000 homeless Loss of electricity due to damaged transmission lines and substations Oil sector affected due to damages on industrial plants Various industrial facilities affected including petrochemical plants, pharmaceutical firms, car manufactures, tire companies, paper mills, steel fabrication plants, etc. Loss of water supply services due to	Some heavy populated districts built on ground mainly composed of sea soil which made them vulnerable to any earthquake (organizational/technical) Inadequate seismic design and construction practices lead to collapses (technical) Inadequate earthquake risk management (organizational) Food, clothing, and sheltering efforts generally lagged behind the needs of the people (organizational)

(continued)

Table 2.4 (continued)

Event	Duration	Cause	Affected infrastructures	Consequences	Vulnerabilities
			and emergency services (physical)	failures of pipelines Motorways and railway tracks damaged Telephone service disruptions	
January 2, 2004 Mini Telecommunication Blackout in Rome (CIE)	The communication blackout lasted around 2 h	In the major Telco node, the breakage of a metallic pipe carrying cooling water caused the node failure and cascading failures in the other infrastructures (technical)	ICT (geospatial) Energy (cyber) Transport (cyber) Finance Services (cyber)	ACEA power grid lost the monitoring and control of all the remote substations managed by the unmanned Control Centre Major node failure and all connections connected to the node failed Delays and services perturbations at banks Delays and check-in troubles in Fiumicino airport Delays and services perturbations in ANSI print agency, post offices	The facilities and apparatus in the major Telco node were not checked and maintained carefully and regularly (operational) Because of a maintenance operation, two redundant communication links between two control centers of ACEA power grids were actually routed through the same Telco node. Both links failed too due to geospatial common cause failures (design/operational) Emergency power

(continued)

Table 2.4 (continued)

Event	Duration	Cause	Affected infrastructures	Consequences	Vulnerabilities
					supply like diesel generators was not kept safely enough and failed to start due to the presence of water (operational)
September 11, 2001 World Trade Center Attack (CCIE)	Part of energy supply and telecommunication were restored within 1 week. More services were restored in 1 year. The complete rebuilding of WTC is still underway	Terrorist attack with two hijacked planes caused the collapse of WTC (malevolent acts)	ICT (geospatial and physical) Energy (geospatial and cyber) Transport (physical and logical) Finance services (geospatial, physical, and cyber) Water and food (geospatial) Public safety, rescue and emergency services (geospatial, physical and cyber) Public health (logical)	Four airplanes crashed *Twin Towers collapsed, destruction of nearby buildings In total, 2,993 people were killed, more than 6,000 injured Loss of power supply in a big area Loss of gas and steam supply A lot of phone lines and data lines damaged, most communication traffic rerouted New York Stock Exchange closed,	Geospatial concentrations of critical infrastructure may be distinctly vulnerable to catastrophic disruption (design and operational) Lack of interoperability results in police and fire not being able to communicate with one another during an emergency (organizational and operational) Revealed shortfalls in the emergency

(continued)

Table 2.4 (continued)

Event	Duration	Cause	Affected infrastructures	Consequences	Vulnerabilities
				international economy affected Loss of water supply All air and subway services suspended	services sector being able to respond to large-scale terrorist incidents and other catastrophes disasters that required extensive cooperation among local, state, and federal emergency response organizations (organizational and operational) Communications and business continuity will further deteriorate after the initial impact of a disaster if backup power generation facilities are not provided with guaranteed access to fuel and maintenance (organizational)

CRE cascade resulting event, *CIE* cascade initiating event, *CCIE* common cause initiating

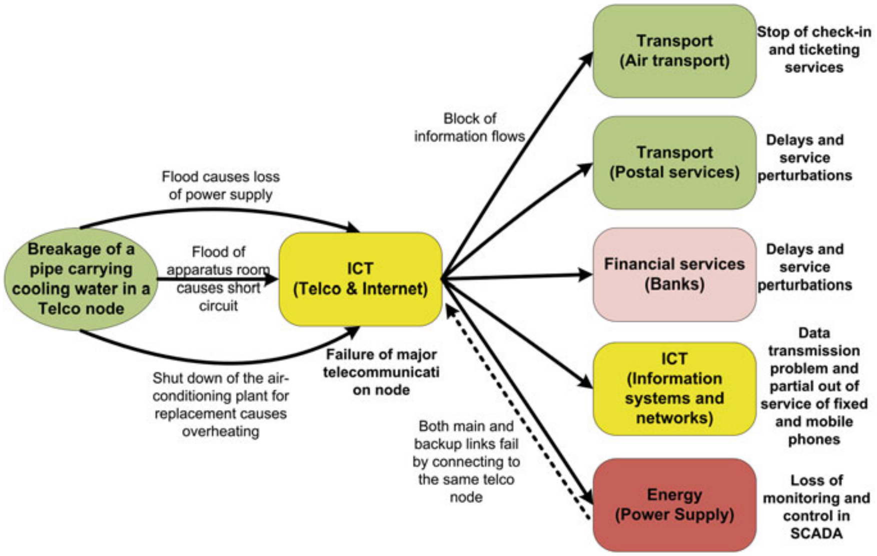
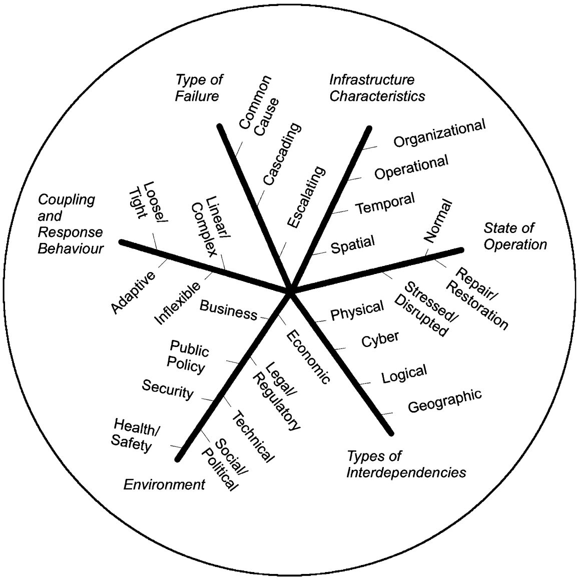

Breakage of a pipe carrying cooling water in a Telco node
Flood causes loss of power supply
Flood of apparatus room causes short circuit
Shut down of the air-conditioning plant for replacement causes overheating
ICT (Telco & Internet)
Failure of major telecommunicati on node
Block of information flows
Both main and backup links fail by connecting to the same telco node
Transport (Air transport)
Stop of check-in and ticketing services
Transport (Postal services)
Delays and service perturbations
Financial services (Banks)
Delays and service perturbations
ICT (Information systems and networks)
Data transmission problem and partial out of service of fixed and mobile phones
Energy (Power Supply)
Loss of monitoring and control in SCADA

Fig. 2.2 Infrastructures affected by the mini telecommunication blackout in Rome, 2004

Fig. 2.3 Dimensions for describing infrastructure interdependencies (Rinaldi et al. 2001)



- Geographic interdependencies—elements are in close spatial proximity and a local environmental event affects components across multiple infrastructures, e.g., earthquake, flooding or a fire.
- Cyber interdependencies—connect infrastructures to one another via electronic, informational links, e.g., a supervisory control and data acquisition (SCADA)

system monitors and controls elements of the electric power grid—likewise, it may provide pieces of information or intelligence supporting another infrastructure or a decision-making process elsewhere.

- Logical interdependencies—exist between infrastructures that do not fall into one of the above categories.

The "coupling[3] and response behavior" of interdependent CI deserves special attention, as it directly influences whether the infrastructures are adaptive or inflexible when perturbed or stressed. Rinaldi et al. (2001) introduce three primary coupling characteristics:

- The degree of coupling either tight or loose addressing the nature of correlation of a disturbance in one agent to those in another; e.g., the gas-fired spatial heating system without storage is closely coupled to the gas supply system without "time to give" or slack.
- The coupling order either directly connected (first-order effect) or indirectly through one or more intervening infrastructures (second-order up to *n*-order effects); e.g., loss of electric power may directly affect the pumps and control of the spatial heating system directly and indirectly affects the fuel supply via the compressors of the gas supply system, if they are electrically driven.
- The linearity or non-linearity/complexity of the interaction; i.e., whether or not agents can interact with other agents outside the normal scheme, or production, or operational sequence, not intended by design as being subtle and difficult to detect, showing unfamiliar feedback loops; e.g., a large scale areal event such as extreme heat affecting various agents simultaneously.

Figure 2.4 depicts all this by taking the prolonged electric power problems in California as the basis. Elements of other dimensions, in particular "environment" (business and economic [deregulation], legal and regulatory [public policy]) and "type of failure" (subset of common causes) might be added to the four above categories of types of interdependencies, or used to specify "logical interdependencies". The latter has been proposed by (Pederson et al. 2006) who slightly expanded the above taxonomy from physical, cyber (renamed informational), and geographic (renamed geospatial) to policy/procedural, and societal interdependencies. These types of interdependencies carry a state, or consequences from events in one infrastructure to other infrastructures, although no direct linkage or relationship in a physical sense exists; halt of air traffic for more than 24 h in the US and air traffic drop worldwide following the "September 11 attack" may serve as reference examples.

Relating to physical-engineered CIs, the six dimensions proposed by (Rinaldi et al. 2001) still seem to be appropriate to facilitate the identification, understanding, and analysis of interdependencies as well as of dependencies, and to frame the requirements for modeling and simulation approaches. A multiple/combined (rather than "silver bullet" single) approach is needed to address, in a

[3] According to *Webster Dictionary*: The act of bringing or coming together. (Mech.) A device or contrivance which serves…. to connect adjacent parts.

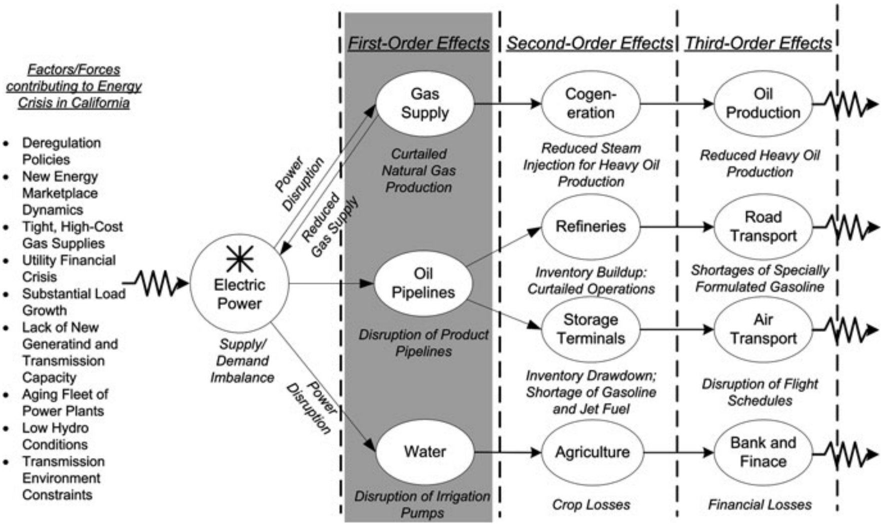
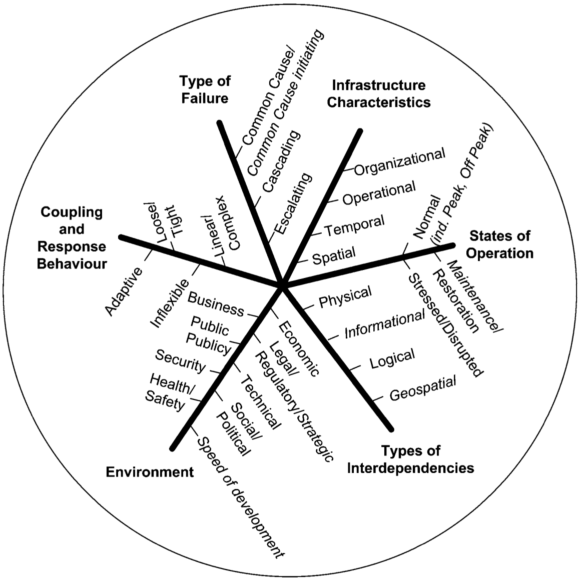

First-Order Effects
Second-Order Effects
Third-Order Effects
Factors/Forces contributing to Energy Crisis in California
Deregulation Policies
New Energy Marketplace Dynamics
Tight, High-Cost Gas Supplies
Utility Financial Crisis
Substantial Load Growth
Lack of New Generatind and Transmission Capacity
Aging Fleet of Power Plants
Low Hydro Conditions
Transmission Environment Constraints
Electric Power
Supply/ Demand Imbalance
Power Disruption
Reduced Gas Supply
Power Disruption
Gas Supply
Curtailed Natural Gas Production
Oil Pipelines
Disruption of Product Pipelines
Water
Disruption of Irrigation Pumps
Cogen-eration
Reduced Steam Injection for Heavy Oil Production
Refineries
Inventory Buildup: Curtailed Operations
Storage Terminals
Inventory Drawdown; Shortage of Gasoline and Jet Fuel
Agriculture
Crop Losses
Oil Production
Reduced Heavy Oil Production
Road Transport
Shortages of Specially Formulated Gasoline
Air Transport
Disruption of Flight Schedules
Bank and Finace
Financial Losses

Fig. 2.4 Examples of nth-order interdependencies and effects (Rinaldi et al. 2001)

Fig. 2.5 Dimensions for describing infrastructure interdependencies (according to (Rinaldi et al. 2001), modified by authors in italic)



consistent manner, all of these interrelated factors and system environment classes/attributes, respectively.

The following extensions to the six dimensions and related elements are here proposed (see Fig. 2.5 as a modification of Fig. 2.3) to strengthen their representation:

"*State of operation*":	"normal"—distinction between nominal, peak, off peak "repair" extended to maintenance during continuous operation or down states
"*Type of failure*":	"common cause initiating" added to "common cause"
"*Types of interdependencies*":	"cyber" changed to informational including hard- and software "geographical" changed to geospatial Note "logical" includes lacking diversity, functional, etc.
"*Environment*":	"Speed of developments/changes" added

In general, it is difficult to clearly define the boundaries of individual infrastructures and model (inter)dependencies among them adequately. Often, infrastructures are decomposed into a physical and supporting/controlling part and modeled in a linear fashion. Let us take the electrical power grid (physical system under control) and the monitoring and control (SCADA) system as examples. Only if the SCADA system is dedicated, does not make use of commercial systems to transfer data and commands, e.g., the open Internet, and does not incorporate common hardware and software, then it can be modeled as part of the electric power infrastructure, including dependencies within. If not, as it is obviously the case in many countries, it would be closely linked to the information and communication infrastructure and must be modeled in a less simplistic way, "not to overlook the true complex nature of interconnected infrastructures" (Rinaldi et al. 2001). Taking this into account, many vulnerability analysts call for a "system-of-systems" approach.

Failures (negative impact) that arise from (inter-)dependencies can be classified as follows:

(1) One event causing failure or loss of service of more than one infrastructure, such as areal external events (earthquakes, floods, extreme weather conditions, etc.), due to spatial proximity (called *common cause initiating events*).
(2) Failure of one infrastructure causing failure or loss of service of at least another infrastructure, e.g., rupture of mains of the water supply system (called *cascade initiating events*).
(3) Failure or loss of service resulting from an event in another infrastructure, e.g., failure of gas lines due to loss of main electricity supply if compressors are electronically driven (called *cascade resulting events*).
(4) Failure or loss of service of one infrastructure escalating "domino effect" because of failure of another affected infrastructure, e.g., failure of the electric power system leading to failure of the SCADA system and by this affecting restoration of the electric power system (called *escalating events*).

Events being neither one of these four types maybe called independent. The types of non-independent events are not mutually exclusive.

2.4 Empirical Investigations on Critical Infrastructure (Inter)Dependencies

As outlined before, interdependencies within and among CIs are recognized as both opportunities, e.g., increased coping capacity and elements of increased vulnerability. With regard to the latter, empirical studies have been made and published focusing on building databases of different kinds and/or to obtain findings for decision making.

For example, the database in (Luiijf et al. 2009) was built from public reports of disruptions of CIs from open sources like newspapers and Internet news outlets. The following results were derived from a subset of 1,749 failure incidents in 29 European countries (95% occurred after 2000) with noticeable effect to society (e.g., at least 100,000 electric power customers affected). Events have been classified as “cascade initiating”, “cascade resulting,” and “independent” (see previous section). The results disclose that:

– “Cascades resulting” events are more frequent than anecdotally thought, i.e., almost 30% (501 out of 1,749) of the reported incidents result from incidents in other services, and that “cascade initiators” are about half as frequent (268 out of 1,749, see Table 2.5).
– The dependency matrix is sparsely populated and cascades are highly asymmetrical; the dependencies are more focused and directional than often thought.
– Energy and telecommunication are the main cascading initiating sectors, energy is the only sector which initiates more cascades than it ends up receiving (146 versus 76, see Table 2.5).

Table 2.5 Categorization of number of CI disruption events (Luiijf et al. 2009)

CI sector	Cascade initiating	Cascade resulting	Interdependent	Total	Sample size
Education	0	3	1	4	4
Energy	146	76	388	609	590
Financial Services	1	26	33	60	60
Food	0	4	3	8	8
Government	2	40	26	68	67
Health	1	16	22	39	39
Industry	5	15	7	27	27
Internet	15	51	95	161	160
Postal Services	1	0	0	1	1
Telecom	69	125	114	308	295
Transport	19	128	276	423	433
Water	9	18	51	78	76
Total	268	501	1,017	1,786	1,749

Table 2.6 Events categorized by initiating and affected sector (number of events) (Luiijf et al. 2009)

	Initiating sector											
CI Sector	No sector	Energy	Financial services	Government	Health	Industry	Internet	Postal services	Telecom	Transport	Water	Grand total
Education	1	1									2	4
Energy	515	65				4			2	1	3	589
Financial Services	34	5	3				3		15			60
Food	4	3								1		
Government	27	17		1	1	1	4		14	1	1	67
Health	23	11			2				2		1	39
Industry	12	12				1				1	1	27
Internet	109	14					10		27			160
Postal Services	1											1
Telecom	170	62					1		57	5		295
Transport	294	98		1		3		1	5	15	5	422
Water	58	14				2					2	76
Total	1,248	302	3	2	3	11	18	1	122	24	15	1,749

Table 2.7 Elements for criticality definition

Conditions for a critical situation	Criticality criteria
“If disrupted or destroyed”	Serious “debilitation and impact on”, “would incapacitate”, “so vital to”, “essential to”:
“The incapacity of destruction of such systems and assets”	The “entire system”
“If degraded or rendered unavailable for an extended period”	The “national public health”, “safety”
“Disabling any of them”	“National security”
(Non)“continuous, reliable operation”	“National defense”
“Disturbance, functional deficiency or destruction”	“National economic security”
	“Minimum operations of the economy and the effective functioning government”
	“Social or economic well-being of citizens or of the nation”
	“Quality of life”
	“Or any combination of those matters”

– Within the energy sector 61 (out of 65) dependencies exist between the electrical power subsector services, and within telecommunication services disruptions of telecom backbones most seriously affect Internet services (see Table 2.6).

With regard to escalation of cascades, the analysis shows that a cascade initiating event in the energy sector triggers 2.06 disruptions of other services, but taking all events into account (including independent) only one out of two events triggers a disruption of another CI. For the telecommunication sector the respective numbers are 1.86 disruptions and two out of five. Interestingly, 421 events (out of 501 resulting in cascades) are first level, 76 are second level, and 4 are third level cascades; no deeper cascades have been found. This contradicts the results of the evaluation of selected experienced events (Table 2.4) and may be due to a bias of the open source media information consulted.

Another fairly simple measure of (inter)dependency was proposed by Zimmermann (2004) which compares the duration of outages in the initial system disruption, e.g., power outage, with the duration of outages of specific public services and businesses affected. The investigations based on power outage data from North America from 1990 through 2004. Results showed that the duration of outages linked to the electricity outage for affected public services exceeded the duration of the initial power outage itself pointing to the fact that cascading events did escalate.

2.5 Degree of Criticality

The definition(s) of CI (this chapter) focus on systems and assets which are considered critical with regards to some criteria, possibly varying from one country/region specific definition and associated perspective to another. These

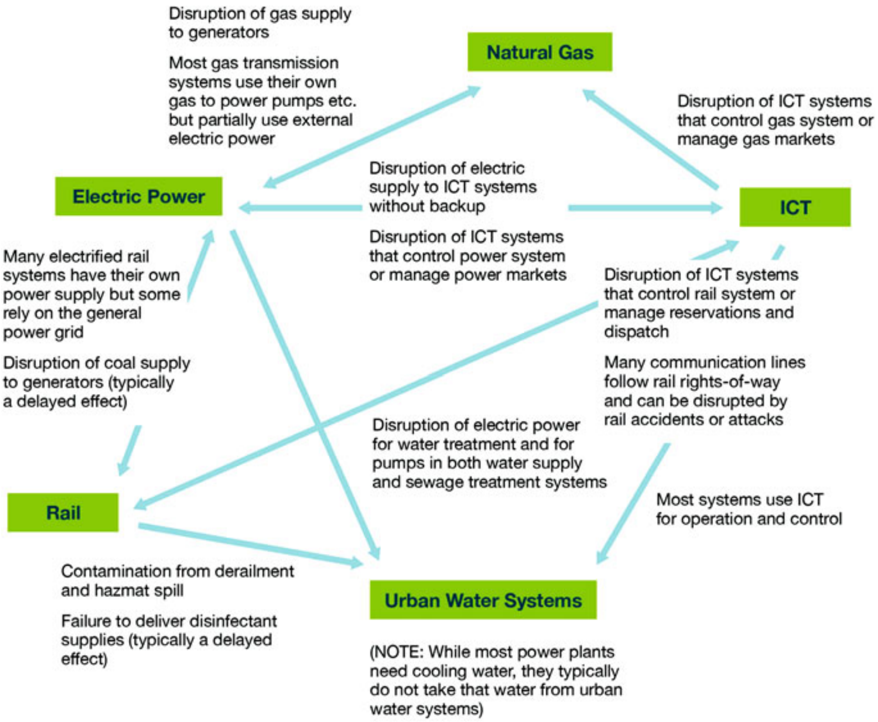

Natural Gas
Electric Power
ICT
Rail
Urban Water Systems
Disruption of gas supply to generators
Most gas transmission systems use their own gas to power pumps etc. but partially use external electric power
Disruption of ICT systems that control gas system or manage gas markets
Disruption of electric supply to ICT systems without backup
Disruption of ICT systems that control power system or manage power markets
Many electrified rail systems have their own power supply but some rely on the general power grid
Disruption of coal supply to generators (typically a delayed effect)
Disruption of ICT systems that control rail system or manage reservations and dispatch
Many communication lines follow rail rights-of-way and can be disrupted by rail accidents or attacks
Disruption of electric power for water treatment and for pumps in both water supply and sewage treatment systems
Most systems use ICT for operation and control
Contamination from derailment and hazmat spill
Failure to deliver disinfectant supplies (typically a delayed effect)
(NOTE: While most power plants need cooling water, they typically do not take that water from urban water systems)

Fig. 2.6 Example for the evaluation of the degree of criticality (IRGC 2006)

definitions (Table 2.7) are descriptive rather than a precise yardstick to objectively assess criticality and its degree. There is no standardized usage and broad-based mutual understanding of what criticality is and how to measure it (see also Bouchon 2006). Nevertheless, the description of conditions for a critical situation focuses on a disturbance or loss of continuous (reliable) service and places the analysis of CIs in the realm of the analysis of reliability (systems view) or availability (users view), of risks for the owner/operator and/or the public due to adverse events, and of vulnerability of the system and/or the society.

Infrastructures are considered highly critical because of being both a trigger of a potential crisis and a means to resolve a crisis/emergency situation; the telecommunication systems may illustrate this. Therefore, criticality objectives are primarily related to strategic objectives of a state entity although other subjective standpoints, i.e., of owners/operators, insurers, other stakeholders and the general public, are worth mentioning and may lead to other criticality criteria. Referring to the Swiss Federal program for critical infrastructure protection (CIP) as an example, the “criticality of an infrastructure” denotes its relative importance regarding the potential consequences of a disturbance, functional deficiency, or destruction for the public and its vital resources” (Federal Office of Civil Protection 2009). The probability of such an event is deliberately not regarded as important.

Attempts have been made to further specify criticality and to distinguish degrees of criticality. The European Commission—EC (EC 2004) has proposed to distinguish three criteria—within its concept of CIP focused on the fight against terrorism:

- *Scope*: The loss of a critical infrastructure element is rated by the extent of the geographic area which could be affected by its loss or unavailability, i.e., international, national, provincial/territorial, or local.
- *Magnitude*: The degree of the impact of loss can be assessed as none, minimal, moderate, or major. Among the criteria which could be used to assess potential magnitude are:

  (a) Public impact (amount of population affected, loss of life, medical illness, serious injury, evacuation)
  (b) Economic (GDP effect, significance of economic loss and/or degradation of products or services)
  (c) Environmental (impact on the public and surrounding location)
  (d) Interdependency (among other critical infrastructure elements)
  (e) Political (confidence in the ability of government)

- *Effects of time*: This criteria ascertains at what point in time the loss of an element could have a serious impact (i.e., immediate, 24–28 h, 1 week, other).

This has been taken up by the International Risk Governance Council (IRGC) to assess the degree of criticality of five coupled physical-engineered infrastructures. This was done semi-quantitatively, based on expert judgment and screening analysis applying the so called traffic light model (IRGC 2006); see Fig. 2.6 for a snapshot of the results. Sometimes it might be of interest to distinguish between objectives, e.g., economy/economic security, public health and safety, and to address interdependencies separately.

Taking again the Swiss CIP program as the example, it was proposed to assess the criticality at the level of 31 subsectors[4] 'according to their "relative importance" (see definition above). The main purpose is to give steer to more detailed analyses aiming at the identification of critical elements in prioritized infrastructures (called vertical criticality) and to strategic planning (BABS 2008). Three criteria are distinguished:

- Effect on other subsectors (dependence)
- Effect on the public
- Effect on the economy

Four categories have been established to specify the effect (consequences)—from none (0), small (1), median (2) to large (3). It is assumed that the "loss of continuous service" will take place without pre-warning, will last approximately 3 weeks, and will affect the whole country. A spider diagram is used to illustrate

[4] The sector energy, for instance, is divided into the subsectors electric power, oil, and gas supply.

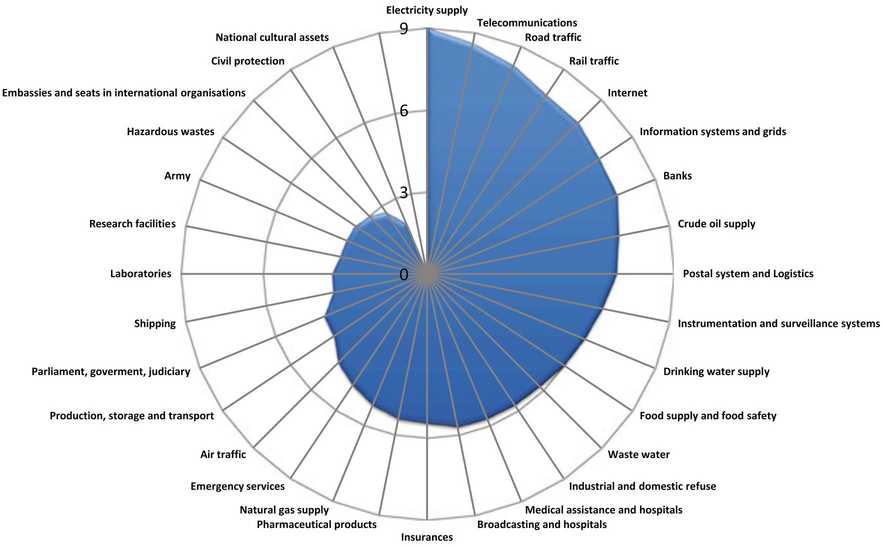


Fig. 2.7 Criticality of subsectors (Federal Office of Civil Protection 2008)

the results (Fig. 2.7): electric power supply and telecommunication are highest ranked.

Activities are undergoing at the level of the European Union aimed at identifying “European critical infrastructures” (EC 2008) by taking three aspects into account:

- Risk of casualties (number of fatalities and/or injuries)
- Economic loss (percentage of GDP)
- Public effect (number of people affected)

To be regarded “critical” for the European Union at least two Member States must be significantly affected by a loss of service of the infrastructures under consideration (currently the energy [electric power, oil and gas supply] and transport sectors). As in all other cases known to the authors, definition and assessment of criticality focus on loss of service; misuse of infrastructure to intentionally cause harm to the public, economy, and government (“weaponizing”) is not taken into consideration; penetration into unmonitored parts of the urban drinking water system and dumping of hazardous substances may serve as fictitious example for illustration.

References

Bouchon S (2006) The vulnerability of interdependent critical infrastructures systems: epistemological and conceptual state-of-the-art (EU report). EU Commission, Joint Research Centre, Ispra, Italy

Dueňas-Osorio L, Vemuru SM (2009) Cascading failures in complex infrastructure systems. Struct Saf 31:157–167

Dueňas-Osorio L, Vemuru SM (2009) Cascading failures in complex infrastructure systems. Struct Saf 31:157–167

ETH–Laboratory for Safety Analysis (2008) Interdependencies. Report for FOCP, 2009

European Commission (2004) Critical infrastructure protection in the fight against terrorism, COM (2004) 702 final, Brussels, 20 October 2004

European Commission (2008) Directive on the identification and designation of European critical infrastructure and the assessment of the need to improve their protection. Council of the European Union, Brussels

Federal Office of Civil Protection (2008) Schlussbericht horizontale Kritikalität (final report on horizontal criticality), Berne, 10/2008 (for internal use).

Federal Office of Civil Protection (2009) The Federal Council's basic strategy for critical infrastructure protection, Berne, 5/2009

Guckenheimer J, Ottino JM (2008) Foundations for complex systems research in the physical sciences and engineering. Report from an NSF Workshop in September 2008

IRGC (2006) Managing and reducing social vulnerabilities from coupled critical infrastructures, White Paper No. 3, International Risk Governance Council, Geneva, p 68

Luiijf E, Nieuwenhuijs A, Klaver M, van Eeten M, Cruz E (2009) Empirical findings on critical infrastructure dependencies in Europe. In: Proceedings of CRITIS 2008, Rome, Italy, 13–15 October 2008, pp 302–310

Pederson P, Dudenhoeffer D, Hartley S, Permann M (2006) Critical infrastructure interdependency modeling: a survey of US and international research. Technical report INL/EXT-06-11464. Idaho National Laboratory, Idaho, USA

Rinaldi SM, Peerenboom JP, Kelly TK (2001) Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Contr Syst Mag 21(6):11–25

Union for the Coordination of Transmission of Electricity (2008) Operational handbook. www.ucte.org. Accessed date/month/2008

Zimmermann R (2004) Decision-making and the vulnerability of interdependent critical infrastructure. In: Proceedings of the IEEE international conference on systems, man, and cybernetics, the Hague, Netherlands