Chapter 13
Addressing Interdependencies of Complex Technical Networks

Wolfgang Kröger and Cen Nan

13.1 Introduction

This chapter deals with large-scale technical systems, i.e., a wide-area network of physical-engineered infrastructures that function synergistically to provide a continuous flow of essential goods and services, groups within our societies or societies as a whole (increasingly) depend on. The most vital ones, such as the electric power and water supply system, information and communication technology (ICT), transport systems, are called **critical infrastructures**. They are subject to rapid technological and organizational changes (e.g., from monopoly to open competitive markets) and face multiple threats (e.g., technical-human, natural, physical, cyber, financial, contextual; either unintended or malicious); they may pose risk themselves (e.g., high-voltage lines or gas pipelines). In general, those systems have become more tightly integrated as well as more interdependent, also due to cyber-based host technologies for communication and control (SCADA[1] systems) moving from closed and dedicated to open and commercialized structures (see Sect. 13.2.2). As demonstrated by experience disruptions may start slowly, accelerate and cascade within and among infrastructure systems [1]. The "2003 Italian blackout" may serve as an illustrating example.

Those critical infrastructure systems have always been "complicated" but in recent years they have witnessed growing interconnectedness and interdependencies, have turned into **complex systems** (see Table 13.1 for contrasting juxtaposition).

[1] Supervisory Control and Data Acquisition.

W. Kröger (✉)
ETH Risk Center, ETH Zurich, Scheuchzerstrasse 7, 8092 Zurich, Switzerland
e-mail: kroeger@ethz.ch

C. Nan
Land Using Engineering Group, ETH Zurich, Universitätstrasse 16, 8092 Zurich, Switzerland
e-mail: cen.nan@usys.ethz.ch

G. D'Agostino and A. Scala (eds.), *Networks of Networks: The Last Frontier of Complexity*,
Understanding Complex Systems, DOI: 10.1007/978-3-319-03518-5_13,

Table 13.1 Contrasting complicated with complex systems (Acc. to [2])

Complicated systems (mechanical watches, commercial aircraft, nuclear power plants, etc.)	Complex systems (stock market, power grids, transport networks, www, social networks, etc.)
• Large number of highly connected components; frequency-consequence curves tend to follow a normal distribution	• Large number of highly connected components; frequency-consequence curves tend to show “fat tails” and follow power law distributions
• Components have well-defined rules and are governed by prescribed interactions	• Rules of interaction between the components may change over time and may not be well understood
	• Connectivity of the components may be quite plastic and roles may be fluid; interactions are not obvious
• Structure remains closed and stable over the time; limited range of responses to changes in their environment	• Systems are more open, respond to external conditions and evolve; interact with their environment
• Low dynamic, mostly linear behavior	• High dynamic and non-linear behavior; sudden regime shifts possible
• No adaptation; one key defect may bring the system to a halt	• Display organization without a central organizing principle (self-organization/emergence)
	• Inadequate information about the state of the influencing variables; probabilistic rather than deterministic behavior
• Decomposing the system and analyzing sub-parts can give an understanding of the behavior of the whole, i.e. the whole can be reassembled from its parts (“deductionism”)	• The overall behavior cannot be described simply in terms of their building blocks; the whole is much more than the sum of its parts (“systems approach”)

13.2 Understanding Complex Systems by Means of Exemplary Systems

13.2.1 Electricity Power Supply System

The electric power supply system (EPSS), consisting of power generators, high-voltage transmission and low-voltage local distribution grids, with transformers/substations in between, has become one of the most important critical infrastructures that modern societies and other infrastructures depend on. However, electricity is seen as common good; security of supply is a key issue but public lacks awareness of major blackouts. In Europe, while originally designed to serve a region and to allow for trans-boundary assistance in case of need, the EPSS has turned into an open system with given energy flux boundary conditions crossing neighboring countries without centralized control. Regional and vertically integrated monopolies are being

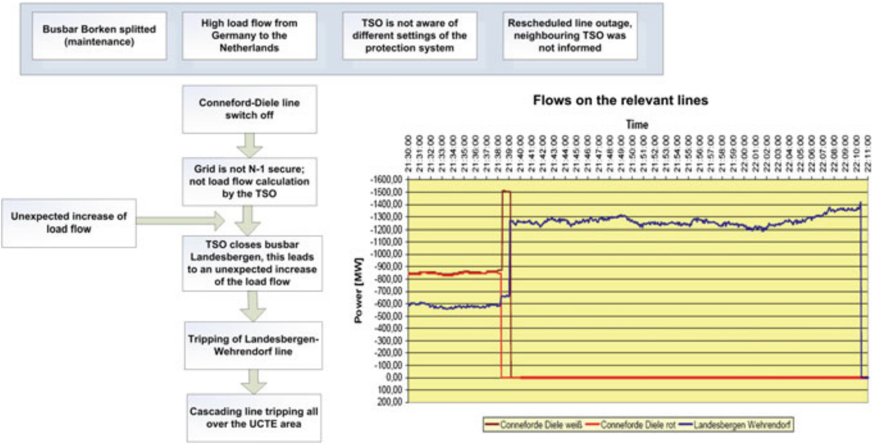


Fig. 13.1 Initial conditions and failure mechanisms leading to splitting of the ENTSO-E grid on 4 November 2006 (formation of areas at 22:20; re-synchronization of area 1 and 2 at 23:24, of area 3 at 23:57 h) [3]

replaced by an intricate market structure and stressing operation modes, closer to security margins. The risk of power outages spreading over wide geographic areas has increased. Furthermore, the integration of large shares of intermittent energy sources (wind and solar, increasingly at most suitable sites far away from consumer centers) has also made the power grid more vulnerable, often going along with lack of awareness and underestimation of complexity. As evidenced by the disruptive event of 4 November 2006, triggered by a planned, re-scheduled line cutoff (to let a new built vessel pass), the initial conditions can be manifold and of different types and the failure and spreading mechanisms are often hard to foresee and control (see Fig. 13.1). Finally the ENTSO-E[2] grid split into three areas of under (two)—and over (one)—frequency.

Table 13.2 depicts information about most recent major blackouts that happened in various regions of the world due to different reasons. Root cause analyses of them have revealed the following patterns:

- Operation of systems beyond original design parameters (high trans-border flows, integration of wind power, etc.).
- Malfunction of critical equipment and adverse behavior of protective devices; insufficient system automation in some cases (lack of investment).
- Lack of situational awareness and short-term emergency preparedness.
- Limited real time system monitoring beyond TSO (Transmission System Operator) control area and weak cross-border coordination in case of preparedness.
- Inadequacy of N-1 security criterion, of its implementation/evaluation.

[2] European Network Transmission System Operator-Electricity.

Table 13.2 Major blackouts of highly reliable bulk power systems

	Blackout	Loss [GW]	Duration [h]	People affected	Main causes
Aug. 14, 2003	Great Lakes, NYC	~60	~16	50 Mio	Inadequate right-of-Way maintenance, EMS failure, poor coordinadintion among neighbouring 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 Mio	Two independent component failures (not covered by N-1 rule)
Sept. 28, 2003	ltaly	~ 30	up to 18	56 Mio	High load flow CH-l, line flashovers, poor coordination among neighbouring TSOs
July 12, 2004	Athens	~ 9	~3	5 Mio	Voltage collapse
May 25, 2005	Moscow	2, 5	~4	4 Mio	Transformer fire, high demand leading to overload conditions
June 22, 2005	Switzerland (railway supply)	0, 2	~ 3	200'000 passengers	Non-fulfilment of the N-1 rule, wrong documentation of line protection settings, inadequate alarm processing
Aug. 14, 2006	Tokyo	?	~5	0.8 Mio households	Damage of a main line due to construction work
Nov. 4, 2006	Western Europe (planned line cut off)	~14	~2	15 Mio households	High load flow D-NL, violation of the N-1 rule, poor inter-TSO coordination
Nov. 10, 2009	Brazil, Paraguay	~14	~4	60 Mio	Short circuit on key power line due to bad weather, ltaipu hydro (18 GW) shutdown
March 11, 2011	Northern Honshu	41	days		Grid destruction by earthquake and tsunami
July 30–31, 2011	India	~32	~2 days	620 Mio	High power demand due to extreme weather (heat) situation, weak inter-regional power transmission corridors

As “soft” (organizational, human) factors often dominate they cannot be ignored when analyzing the EPSS.

Due to pervasive use of cyber-based technology, partially unsecured like the internet, the risk of cyber attacks on the EPSS, and on the SCADA system and EMS (Emergency Management System) in particular, has increased but does not manifest as a trigger for blackouts yet. Parts of the EPSS spread over wide geographic and socio-political areas and are easily accessible, making them highly vulnerable to terrorist attacks; investigations have shown that “brute force attacks” (on more than single elements) are necessary to imperil the stability of a large-scale grid [4].

The tendency to growing instabilities may also be amplified by future trends within the EPSS:

- Future power system requires significant changes in the transmission and distribution system (“smartgrid”/“super grid”) including RES-generation at most suitable sites and long-distance transport to consumer hubs.
- Means to better balance demand and supply will be given to “households”; the current generation of “smart meters” is unsecured introducing the risk of manipulation and cyber attacks (“worst scenarios” show grid collapse).
- Development of future market-oriented power supply systems are driven by political targets and demonstration of feasibility; vulnerability and security issues are often not sufficiently included.

Given the complexity and complex behaviors following disruptive events of the systems such as the EPSS it has been argued that reliability and vulnerability analysis have to go beyond the conventional approach of decomposition (e.g., fault tree analysis) or cause-and-effect/causal chain development (e.g., event tree analysis) to be able to capture emergent behavior and failure cascades, especially when strong interdependencies exist (see [5]). The behavior of the whole system can hardly be understood/described as the sum of the behaviors of its elements. Furthermore, the operational contexts including organizational factors, safety culture, coexistence of different technologies, etc, need to be adequately accounted for.

13.2.2 Industrial Control System

The growth of the worldwide interconnectivities of computing devices provides users new means to share and distribute information and data. In industry, this results in the adoption of modern ICTs and, subsequently, in an increasing integration of various facilities, i.e., industrial control system (ICS). In general, ICS is a term that encompasses several types of control systems, e.g., DCS (Distributed Control System), PLC (Programmable Logic Controller), SCADA, etc. ICS is typically used in modern critical infrastructure systems to enable the operators to continuously monitor and control them for the purpose of ensuring their proper operation [6]. Compared to other ICSs, SCADA system is normally used to monitor and control very large industrial process facilities such as electricity transmission facilities and oil

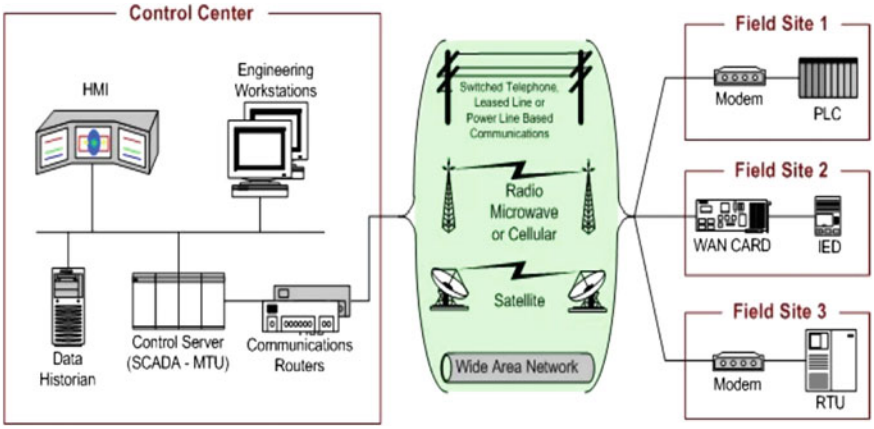


Fig. 13.2 General structure of a SCADA system [8]

and gas production facilities [7]. Its fundamental purpose is to allow a user (operator) to collect data from one or more remote facilities and send control instructions back to those facilities. For instance, voltage, frequency and phase angle are all important parameters in an EPSS and need to be continuously monitored for maintaining a normal operation environment.

Figure 13.2 shows the general structure of a SCADA system. There are four levels in a standard SCADA system hierarchy mainly based on the functionalities of devices. Level 1, the lowest level in the standard hierarchy, includes Field Level Instrumentation and Control Devices (FIDs and FCDs), e.g., sensors and actuators. Remote Terminal Unit (RTU), the level 2 in the standard hierarchy, is a rugged industrial common system providing intelligence in the field. It is a standard stand-alone data acquisition and control unit with the capabilities of acquiring data from monitored processes, transferring data back to the control center, and controlling locally installed equipments. Communication Unit (CU), the level 3 in the standard hierarchy, provides a pathway for communications between a control center and RTUs. Different protocols (e.g., Modbus and Profibus) and mediums are adopted by the CU. Most devices in the scope of the first three levels of the SCADA system hierarchy are installed (hardwired) in a substation. Master Terminal Unit (MTU), the level 4 in the standard hierarchy, can be regarded as a "host computer" issuing commands, collecting data, storing information, and interacting with SCADA operator who can communicate with substation level devices. Compared to the RTU, the MTU is a "master machine", which is able to initiate the communication either automatically by its installed programs or manually by an operator. Generally, three devices are included in a MTU: HMII (Human Machine Interface), control server, and engineering working station. The hardware configuration varies depending on the type and size of the system, while general functionalities are similar (see [9] for more information).

The trend from proprietary technologies to more standardized and open solutions together with the increased number of connections among ICSs and LAN/WAN

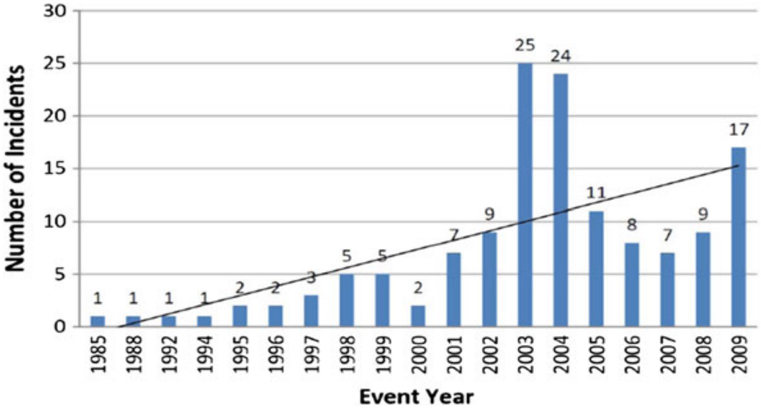


Fig. 13.3 Distribution of annual industrial security incident rates [17]

(Local/Wide Area Network) poses a significant threat. Originally, a SCADA system was designed as a point-to-point system connecting a monitoring or command device to remotely located sensors or actuators. By now, it has evolved into a complex network that supports the communication between a central control unit and multiple remote units using advanced ICT [10]. Having said this, extensive uses of them introduce new types of security threats to SCADA systems [11, 12]. For example, Stuxnet, a self-replicating computer worm, has recently challenged the securities of infrastructure systems for its capability of modifying the control logic of field level control systems through SCADA systems. This sophisticated "superworm" is a Windows-specific computer work, specifically written to attack SCADA systems, and was first discovered in June 2010. It should be noted that the only target of Stuxnet was Simatic WinCC, a Windows-based SCADA system developed by SIEMENS. Once inside the system, it uses certain exploits to infect other WinCC computers within the local network. According to [13], this computer worm infected Iran's nuclear enrichment facilities at Natanz, and other sites, and destroyed 30 % of its centrifuges by a self-destruct mechanism.

Recent surveys show that a number of attacks against ICSs, especially SCADA systems, have been reported over the years, e.g., the prominent Maroochy Shire accident in Australia (2000), the Florida power outage in USA (2008), etc [14, 15]. There are also numerous unreported incidents by asset owners and operators related to security issues in ICSs [16]. As seen from these incidents, threats to ICSs come from numerous sources, e.g., hostile governments, disgruntled employees, malicious intruders, human errors, technical failures, natural disasters, etc. Figure 13.3 shows annual industrial security incident rates from 1985 to 2009 based on records from RISI (Repository of Industrial Security Incidents).[3] As shown in Fig. 13.3, the annual incident rate gradually increased in the late 90's and peaked around 2003. It then

[3] RISI is a database including a number of technical incidents in which process control, industrial automation or SCADA systems were affected.

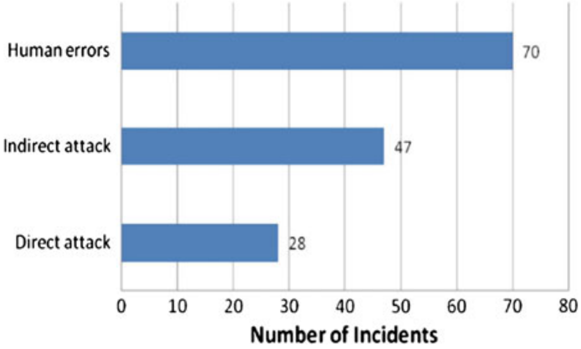


Fig. 13.4 Comparison of different types of industrial security incidents (1985–2009) [17]

declined sharply in the mid 2000's (2005–2007) and appeared to rise again in the late 2000's; a linear interpolation shows that its trend is increasing at probably 20–25 % per year over the last decade [17]. These incidents can be also grouped into direct attacks, indirect attacks (e.g., worms and virus), and human errors (Fig. 13.4). It should be noted that an incident can be classified into more one category. For example, an incident might may be caused by direct attacks and human errors. Unintentional incidents, e.g., equipment failures and malware attacks, also account for a significant number of incidents.

13.2.3 Railway System

Railway systems provide transportation services for passengers and goods in almost all countries and across borders. It is a large-scale infrastructure system that, if degraded, disrupted or destroyed, has serious impacts on the health, safety, security and well-being of citizens and on the effective function of the society. The 2009 Viareggio incident may serve as an example. On June 29, a freight train from Trecate, hauled by a locomotive with 14 bogie tank wagons derailed at Viareggio, Italy at 23:48 local time. The first wagon hit the platform of the station and overturned to the left, the next four wagons also overturned and the two following derailed but remained upright, the last seven did not derail, remaining intact on the track. The derailed wagons crashed into houses alongside the railway line causing a massive explosion that destroyed two blocks of flats, killing 22 people, injuring more than 40 and forcing around 1000 people to evacuate their homes (see [18] for this and other incidents).

In general, a railway system can be broken down to the following subsystems:

- **Infrastructure**: tracks, on-track equipment including switches, engineering structures (tunnels, bridges, etc.), associated station infrastructure (platforms, zones of access, etc.), safety and protective devices.

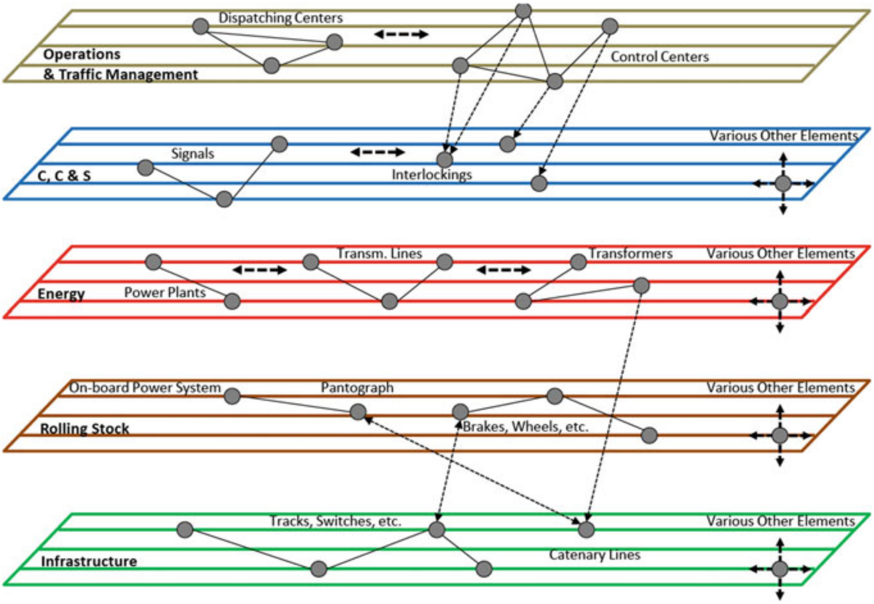


Fig. 13.5 Multilayer representation of the railway system [18]

- **Energy**: electrification system, including its own power plants, transmission systems, substations, transformers, overhead contact lines, etc.
- **Control, Command and Signaling**: all the equipments necessary to ensure safety and to command and control movements of authorized trains including track-side equipments such as radio block centers, interlockings, base transmission units.
- **Rolling Stock**: locomotives and wagons including all the various on-board equipment, named accordingly control equipment, structural components (brakes, wheels, car body, bogies, axles, etc.) and the power equipment (motors, main transformer, battery system, pantograph, etc.).
- **Operation and Traffic Management**: operation and control centers including the technical equipment and personnel at all levels of organization and operation.

Figure 13.5 shows a multi-layer representation of the railway system with various interacting hetero-geneous subsystems and associated components: parallel planes represent different subsystems while nodes represent various elements together with some of interconnections between them (arrows). The elements of the various layers depend on each other, depicted by various horizontal (inside a layer) and vertical (between layers) links. These links introduce direct and indirect (inter) dependencies and a failure of an element of the lower layers can cause cascading failures up to the top layers that could affect the function of infrastructure systems. For example, one plane represents the rolling stock subsystem whereas the parallel lines consist of the on-board power system (with nodes on this line being for the pantograph and various other elements), the on-board control system and so on.

Maintaining daily normal operation of railway systems is a highly challenging task and involves multi-dimensional, highly complex collections of technologies, processes and people and as such, the railway system is vulnerable to potentially catastrophic failures on many levels. In general, railway systems are subject to various hazards and threats:

- Sudden interruption of services due to loss of energy supply or communication and control.
- Operation of the system close to its limits (e.g., tight operational schedule).
- Malicious cyber-attacks on control systems.
- Accidents with injuries, fatalities or release of dangerous goods (e.g., derailment and/or collision) due to technical and/or human failures.
- Natural forces and environmental factors (e.g., landslides, extreme weather conditions) with consequences on operational availability and safety.

13.3 Interdependencies

13.3.1 Illustrating Evidence

Critical infrastructure (CI) systems have been continuously exposed to multiple threats and hazards. A single failure within any infrastructure system or even loss of its continuous service may be damaging enough to our society and economy while cascading failures crossing subsystems and/or even boundaries have the potential for multi-infrastructural collapses and unprecedented consequences. The importance of preventing or at least minimizing negative impact of cascading failures due to interdependencies among these systems has been recognized, not only by governments but also by the public, as a topic of CI Protection (CIP). The purpose of the protection is not just to identify the cause of failures and prevent them but also to halt ongoing cascading or escalating events before affecting other infrastructures. Therefore, it is vital to get a clear understanding of these often hidden interdependency issues and potential failure cascades, and to tackle them with advanced modeling and simulation techniques. In general, addressing the significance of interdependencies among infrastructure systems and uncertainties of their interactions is a challenge due to the complexity and perpetual nature of those systems, the lack of sufficient information clearly characterizing failure propagations, and the lack of modelling/simulation tools, by which system interactions can be comprehensively analyzed.

Nevertheless, it is still possible to find some evidences from many documented incidents through qualitative analysis of available information, which can help us to shed some lights on the understanding the characteristics of interdependencies [19]. The 2001 Baltimore tunnel fire may serve as an example: On July 18, a freight train with 31 loaded and 29 empty cars passed through the Howard Street Tunnel in Baltimore, USA. At 3:08 p.m., 11 cars derailed while the lead locomotive was about 1,850 feet from the east portal. Four of them were tank cars and one contained tripropylene. The derailment caused the puncturing (2-inch-diameter hole near the

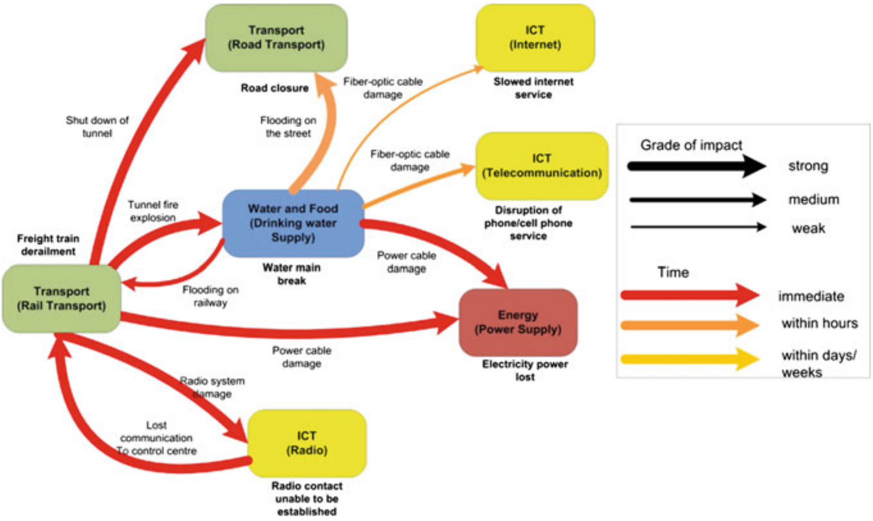


Fig. 13.6 Interdependency graph of 2001 Baltimore tunnel fire [19]

bottom of the tank) of the car carrying tripropylene and the subsequent ignition of this flammable liquid. The fire spread the contents of several adjacent cars, creating the heat, smoke, and fume that blocked the access of the tunnel for five days and eventually shut down the down-town area. As shown in Fig. 13.6, a technical failure (freight train derailment) occurring in the railway system continued to propagate into other infrastructure systems due to interdependencies. For instance, the break of the water mains (a failure within drinking water supply system) due to the tunnel fire/ explosion flooded the tunnel and damaged power cables and fiber-optic cables. The radio system was also damaged due to the derailment and therefore, the radio contact between train crewmembers and corresponding control center could not be established. About 1,200 Baltimore buildings lost electricity and both internet and telephone services were interrupted [20].

The 2012 India power blackout, occurred on July 30 and followed by another power outage on July 31, can serve as another example. The incident is the largest blackout in history, affecting 620 million people. It started from a tripped transmission line, which caused the failure of a substation. The cascade then spread further beyond this substation and led to a massive power outage throughout 22 states of India. Vital infrastructure systems were affected: railways and airports were shut down; health services provided by several hospitals were interrupted; drinking water services were interrupted due to the failure of electric pumps. This incident also demonstrates that the breakdown of such a complex infrastructure system is often the result of a relatively slow system degradation escalating into a fast avalanche of component failures, which finally lead to failures of directly or indirectly coupled systems.

These two incidents, as well as others such as the 2003 North America power blackout, 2004 Rome telecommunication node failure, 2005 Hurricane Katrina, etc, are regarded to be rare. It can be argued that the probability of future occurrence of similar events could be relatively low. However, negative consequences of events, triggered by one single event, developing into fast cascades crossing system boundaries, can be worsened significantly due to interdependencies among systems. Analysis of those "low frequency, high consequences" disruptive events can help us to understand what can be expected due to interdependencies, even if in different contexts and scales. For example, cascades are directional in both cases, the 2003 North America and the 2012 India blackout, meaning that most of affected infrastructure systems have unidirectional relationships (dependencies) with power infrastructure systems.

13.3.2 Definition and Dimensions

From a technical perspective, the term *dependency* depicts a linkage between two systems through which the state of one system influences the state of the other, whereas *interdependency* is a bidirectional relationship through which the state of each system is correlated to the state of the other [21]. Interdependency can be of six different types: the first of three types can be referred as *direct* while the last three can be referred as *indirect interdependencies,* see below for a brief definition based on work done by Rinaldi et al. [21] and modified by the authors:

(i) **Physical**—the state of one system depends on the material output(s)/flows(s) of the other, e.g., a pipeline network provides gas to fuel a power station while the electricity generated is used to power compressors and controls of the gas supply network;
(ii) **Geospatial**—components of multiple infrastructure systems are in close spatial proximity and a local event is able to affect all these components, e.g., earthquake, flooding or a fire;
(iii) **Informational**—infrastructure systems are interconnected via electronic, informational links, e.g., a 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;
(iv) **Socio**—an infrastructure system affects another one via socio factors such as public confidence, trusts, culture issues, etc;
(v) **Policy/procedure**—an infrastructure system affects another one due to factors such as market structure, organizational change, etc;
(vi) **Finance**—an infrastructure system affects another one due to factors such as market condition, finance crisis, etc.

Figure 13.7 shows six dimensions for describing interdependencies including the six types. The "coupling and response behavior" of interdependent systems deserves special attention, as it directly influences whether the infrastructures are adaptive or inflexible when perturbed or stressed. As shown in this figure, the degree of coupling can be tight or loose, which addresses the nature of correlation of a disturbance in one system to those in another. The coupling order is either directly connected (first-order-effect) or indirectly through one or more intervening infrastructures

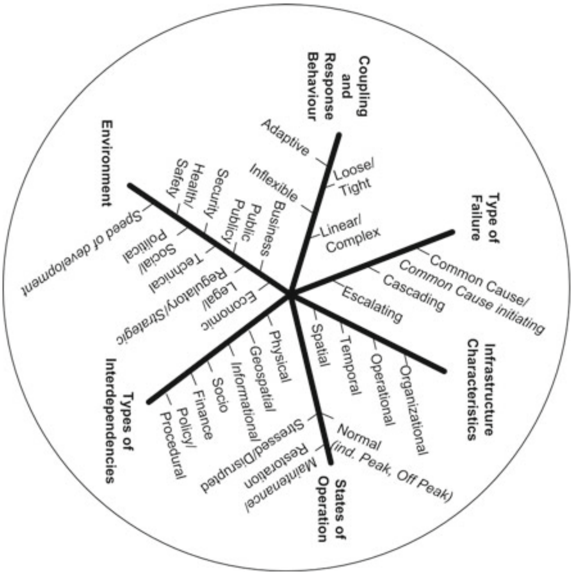


Fig. 13.7 Six dimensions for describing interdependencies (according to [21], modified by the authors)

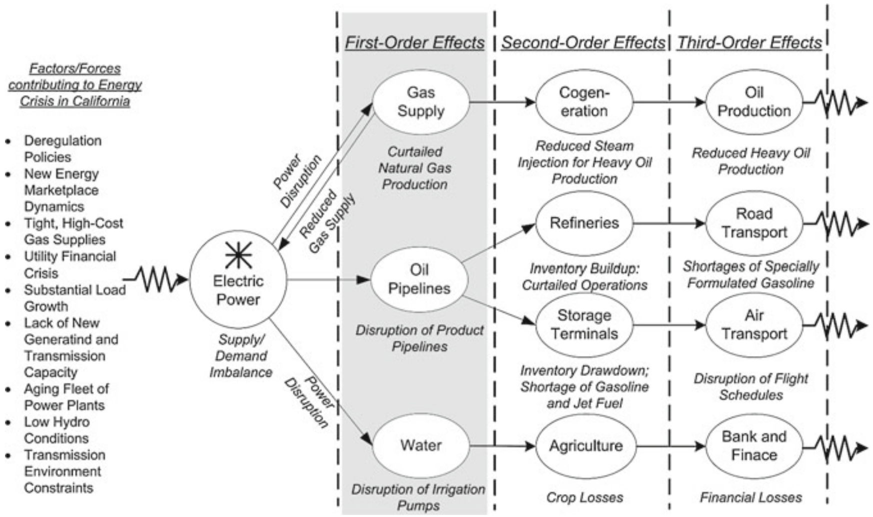

Factors/Forces contributing to Energy Crisis in California
• Deregulation Policies
• New Energy Marketplace Dynamics
• Tight, High-Cost Gas Supplies
• Utility Financial Crisis
• Substantial Load Growth
• Lack of New Generatind and Transmission Capacity
• Aging Fleet of Power Plants
• Low Hydro Conditions
• Transmission Environment Constraints
Electric Power
Supply/ Demand Imbalance
Power Disruption
Reduced Gas Supply
Power Disruption
First-Order Effects
Second-Order Effects
Third-Order Effects
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. 13.8 Examples of nth-order interdependencies and effects taking Energy Crisis in California as a basis [21]

(second-order up to n-order effects, see Fig. 13.8 for illustration). The linearity or non-linearity/complexity of the interaction, i.e., whether or not systems can interact with others outside the normal scheme or operational sequence, not intended by design being subtle and difficult to detect, shows unfamiliar feedback loops.

Interconnectedness and interdependencies may have a positive or negative impact on the complex system behaviors indicating the need to find the right balance. Failures (negative impact) that arise from strong interdependencies (and coupling) can be classified as follows:

- **Common cause initiating events:** one event causing failure or loss of service of more than one infrastructure, e.g., areal external events such as earthquakes, floods, or extreme weather conditions, due to spatial proximity.
- **Cascade initiating events:** failure of one infrastructure causing failure or loss of service of at least another infrastructure, e.g., ruptures of mains of the water supply system.
- **Cascade resulting events:** 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 electrically driven.
- **Escalating events:** failure or loss of service of one infrastructure escalating 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.

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

13.4 Analyses of Interdependencies

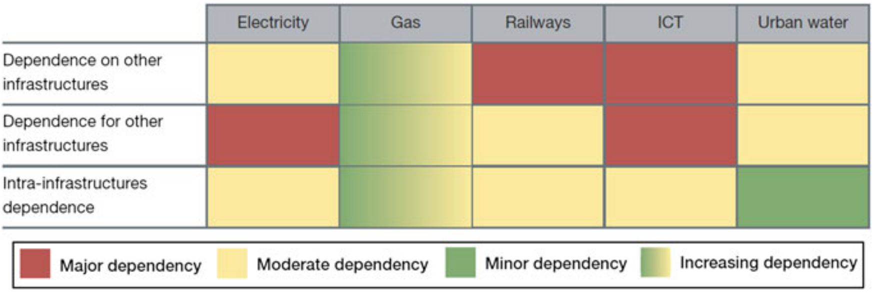
The challenges regarding understanding, characterizing, and investigating interdependencies among infrastructure systems are immense and research in this area is still at an early stage [22, 23]. In recent years a great deal of effort has been devoted by researchers and two main directions can be distinguished, i.e., **knowledge-based** and **model-based** approaches.

13.4.1 Knowledge-Based Approaches

Knowledge-based approaches, e.g., empirical investigations or brainstorming, intend to use data collected by interviewing experts and/or analyzing past events to acquire information and improve the understanding of the dimensions and types of interdependencies. In order to address the question whether certain combination of infrastructure failures are more common than others, one of the early empirical investigation studies built a database using the collected information from a number of maintenance or operation accidents, reports of the US National Transportation

Table 13.3 Effect ratios [24]

Type of infrastructure systems	No. of times infrastructure systems caused failure of other infrastructure systems	No. of times infrastructure systems was affected by other infrastructure failures	Ratio of causing versus affected by failure
Water mains	34	10	3.4
Roads	25	18	1.4
Gas lines	19	36	0.5
Electric lines	12	14	0.9
Cyber/fiber/optic/telephone	8	15	0.5
Sewers/Sewage treatment	8	16	1.3



	Electricity	Gas	Railways	ICT	Urban water
Dependence on other infrastructures	🟨	▨	🟥	🟥	🟨
Dependence for other infrastructures	🟥	▨	🟨	🟥	🟨
Intra-infrastructures dependence	🟨	▨	🟨	🟨	🟩

🟥 Major dependency 🟨 Moderate dependency 🟩 Minor dependency ▨ Increasing dependency

Fig. 13.9 Dependencies between critical infrastructures, according to Ref. [25]

Safety Board and news media searches [24]. The database mainly includes accidents that occurred from 1990 through 2004 in connection with failures during construction, maintenance or operation, or due to facility condition related to age of structures. Table 13.3 depicts the ratio of causing failure of another type of infrastructure versus being affected by failure of another type of infrastructure according to the database. As shown, water mains cause failures of other infrastructures more frequently while gas lines and telecommunication lines are more likely to be damaged by other infrastructures.

A policy brief of the International Risk Governance Council [25] also introduces an assessment based on brainstorming sessions among experts around the world and categorizes how dependent each infrastructure is on the others, how dependent the others are on it, and also how strong the intra-infrastructure dependencies are (Fig. 13.9). According to this report, among five reference infrastructures, electricity, railways and ICT are most important ones. Most infrastructures have a major dependency on the electricity infrastructure, while the railway infrastructure has a major dependency on other infrastructures. The ICT has a major dependency on others, as well as major dependence for other infrastructures.

The knowledge-based approach is straightforward and easy to understand. It is capable of providing a qualitative assessment on the severity of interdependencies and can be considered as an efficient screening method. However, it is a purely data-driven approach, meaning that the accuracy of results depends on the quality and the interpretation of the collected information.

13.4.2 Model-Based Approaches

Model-based approaches aim to analyze interdependent infrastructure systems comprehensively by using advanced modeling/simulation techniques, capable of providing both quantitative and qualitative information. Even modeling single infrastructure systems is a challenging task because of their inherent characteristics such as dynamic/nonlinear behaviors and intricate rules of interaction with their environment due to their openness and high degree of interconnectedness. This task could become even more challenging when more than one infrastructure systems must be considered and interdependencies among them need to be tackled. Traditional approaches and methods based on decomposition and cause-consequence-relations such as fault and event trees reach the limit of their capacity [26, 27]. In recent years, a variety of advanced modeling approaches have been developed and applied, e.g., Input-output Inoperability Modeling (IIM), Complex Network (CN) Theory, PetriNet (PN)-based modeling, Agent-based Modeling (ABM), etc.

The **IIM approach** is an example of capturing interdependencies among infrastructure systems via the development of mathematical models. This approach is originally a framework for studying the equilibrium behaviour of an economy by describing the degree of interconnectedness among various economic sectors [28]. It assumes that each system can be modelled as an atomic entity whose level of operability depends on other systems and propagation between them can be described mathematically based on the basic Leontief high order mathematical model [29]. The IIM approach is capable of analyzing cascading failures and providing a mechanism for dependency measurement. In [30, 31], Haimes et al. applied this approach to study impacts of high-altitude electromagnetic pulse on electric power infrastructure. The great advantage of this type of mathematical model is its preciseness. However, deriving an appropriate representation of multiple infrastructure systems is not easy due to their inherent complexities. To overcome this difficulty, the task of analysing behaviours of interdependent infrastructure systems as a whole can be turned into the analysis of the aggregate behaviours of many smaller interacting entities.

The **PN-based approach** is a mathematical modeling language for the description of distributed systems which has also been used to represent/assess interdependencies among infrastructure systems. In this approach, components (subsystems) of infrastructure systems and their states are modeled using basic PN elements such as places, transitions, etc. In [32], the Swiss railway system is modeled using the PN-based approach for the purpose of vulnerability assessment, illustrated in Fig. 13.10. Elements of various subsystems such as track lines and transformers are selected and categorized as root causes potentially leading to single and/or common cause failures of the track lines. The core of the vulnerability analysis consists of integrating vari-

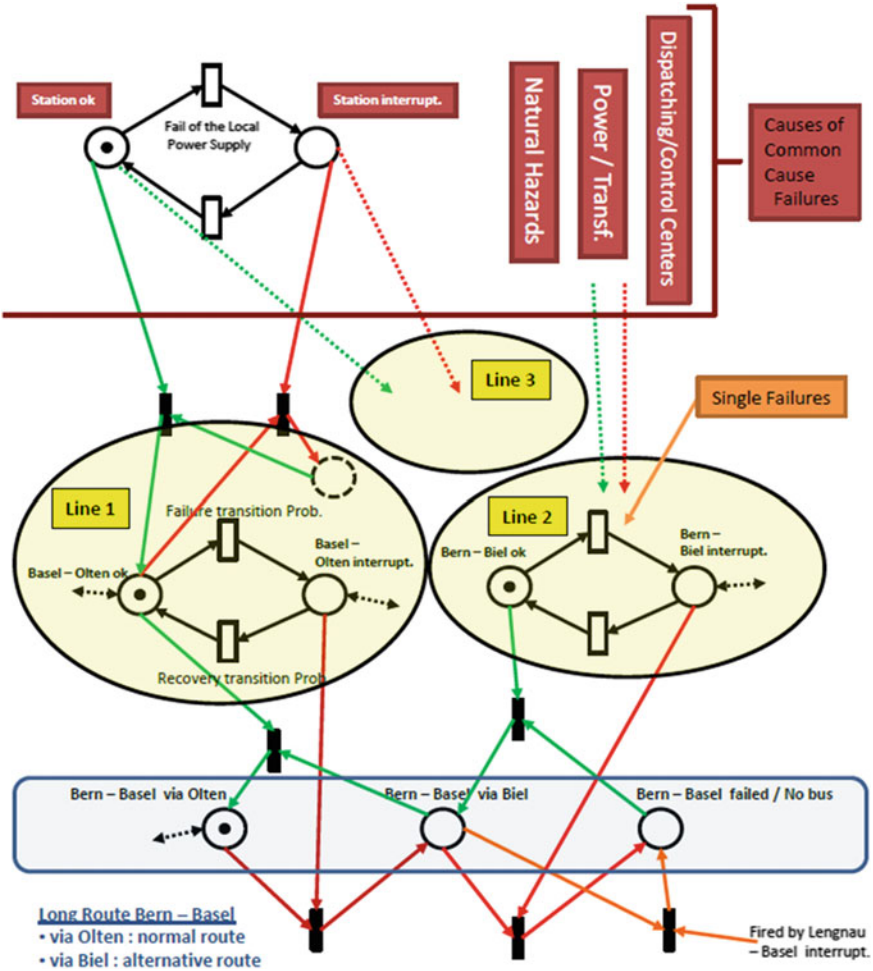


Fig. 13.10 The concept of PN-based modeling approach representing Swiss railway system [32]

ous risk factors affecting the system's operational performance in one "multi-layer" PN-based model.

This approach alone has difficulties representing infrastructure systems quantitatively and often needs to be combined with other methods. For example, in the Europe-wide project IRRIS (Integrated Risk Reduction of Information-based Infrastructure Systems), the PN-based approach is combined with the ABM approach to analyze and manage infrastructure interdependencies [33].

Fundamental elements of the **CN theory approach** are originally formed by graph theory [34]. A graph G (V, E) is composed by a set of nodes (vertices) V and the set of connections E between them. Each node (or vertex) represents an element of the system, while a link (or edge) represents the relation between corresponding

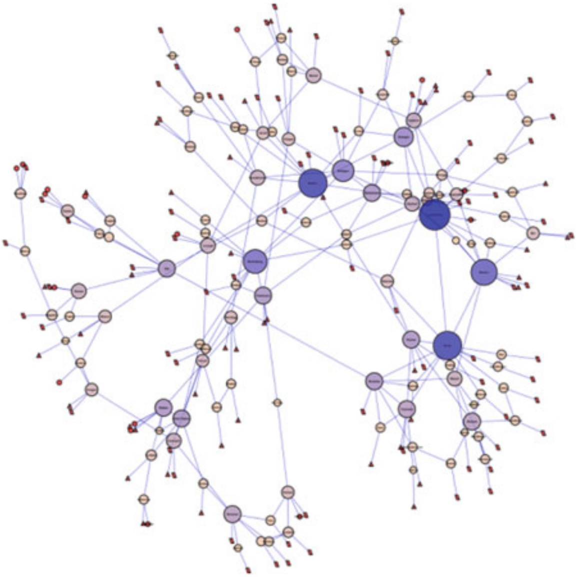


Fig. 13.11 Representation of the Swiss transmission grid using CN theory [4]

elements. A graph can then be drawn by plotting nodes as points and edges as lines between them. In general, a graph can be analyzed by well-developed parameters, e.g., the order/size of a graph, the weight/strength of a link, the degree/degree distribution/betweenness of nodes, etc. A complex network can be regarded as a graph with non-trivial topological features that do not occur in simple networks such as lattices or random graphs but often occur in real graphs. The CN theory is an approach capturing the coupling phenomenon as a set of nodes connected by a set of links and by this characterizing their topology. A number of modelling efforts have been made to adopt this approach for the development of infrastructure system models and interdependency-related assessments, demonstrating its capability of representing relationships established through connections among system components [35, 36]. In [4], the Swiss transmission grid is modelled and analyzed using the centrality analysis of this approach in order to perform heuristic investigations of potential malicious attacks (Fig. 13.11). In total, 242 nodes are developed to represent substations, loads, and power generating stations and 310 links to represent transmission lines.

The CN theory approach is based on the network model mapping physical configuration of the components (elements) of studied infrastructure systems and their (physical or logical) interconnections. The analysis of the topological properties of the network is able to reveal useful information about the structural properties, topological vulnerability, and the level of functionality demanded for its components. However, this approach lacks the ability to capture uncertain and dynamic characteristics of

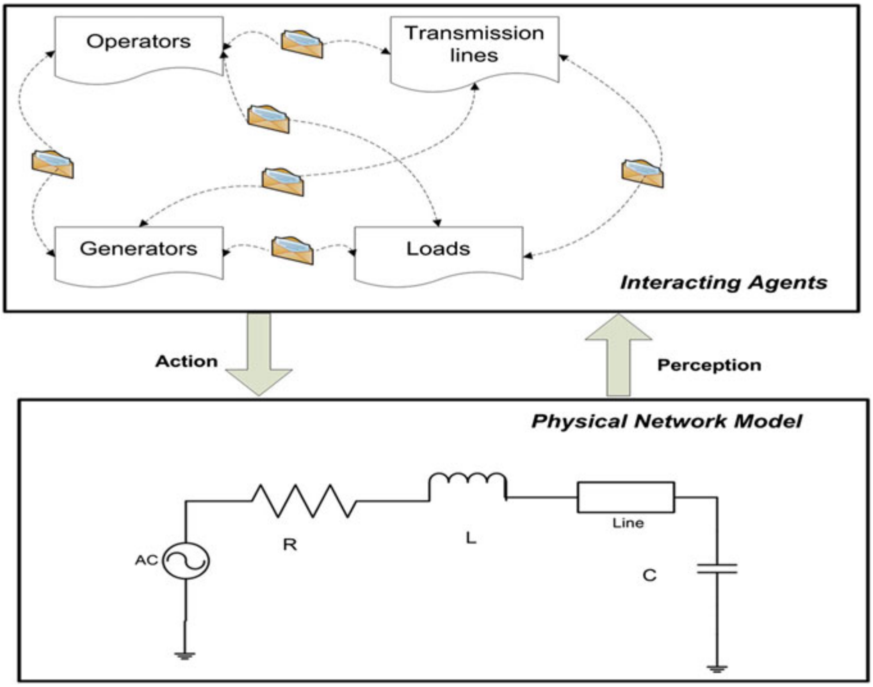


Fig. 13.12 Two-layer modeling concept (using application to the electric power supply system as an example)

infrastructure systems and system properties when dynamical processes, acting on the network, occur.

Using the **ABM approach**, each agent is capable of modifying its own internal data, its behaviours, its environments and even adapting itself to environmental changes. An agent can be used to model both a technical component (e.g., a transmission line), and a non-technical component (e.g., a human operator), while different agents interact with each other directly or indirectly. This approach is able to provide an integrated environment where a more comprehensive analysis of dynamic system behaviours can be performed by “looking-into” the component level of studied system(s) [37]. In [38], the Swiss transmission grid is modeled/simulated using the ABM approach for the purpose of system reliability analysis. Instead of only using nodes and links to represent substations and transmission lines respectively (recall CN theory modeling approach), agents are created to model various components of the system such as generators, busbars/substations, transmission lines, operators, and loads. The rules of behaviors of each agent are represented by using Finite State Machines (FSMs) and include both deterministic and stochastic time-dependent, discrete events. The model is developed using a two-layer modeling concept, illustrated by Fig. 13.12. Within this concept, the lower layer represents the separate modeling of the physical components by means of conventional, deterministic techniques such as power flow calculations, whereas the upper layer represents the abstraction of the whole system (in this case, electric power system) with all its technical and non-technical components as individual agents. Overall, the ABM approach achieves a closer representation of system behaviors by integrating the spectrum of different phenomena that may occur, e.g., generating a multitude of representative stochastic, time-dependent event chains. However, this approach demands a large number of parameters defined for each agent, requiring thorough knowledge of the studied system(s).

It should be noted that other model-based approaches, which have also been applied by researchers but not discussed in this chapter, include **System Dynamic** [39], **Bayesian Network** [40, 41], **Dynamic Control System Theory** [42–44].

13.4.3 Comparison of Approaches

It is difficult to compare these (knowledge-based and model-based) approaches since all of these approaches have their own advantages and disadvantages. The knowledge-based approaches are straightforward and easy to understand, while the model-based approaches are more comprehensive and promise to gain a deeper understanding of behaviors of studied system(s). The level of this "deeper understanding" also varies: Some approaches are only capable of analyzing studied system(s) at the structure/topology level, which can be considered as appropriate approaches for the screening analysis, e.g., CN theory and PN-based modeling approaches, while some approaches are capable of capturing and analyzing dynamic behaviors of studied systems, e.g., ABM and IIM approach. Among all these, the ABM approach seems more promising than others, not just due to its capability for representing the complexity of any infrastructure systems, but also its modeling flexibility and adaptability. For example, the ABM approach can be integrated with many other modeling/simulation techniques and even be used to implement other models mentioned above.

13.4.4 Hybrid Modeling/Simulation Approach

13.4.4.1 Challenges and Basic Concept

Some of the model-based approaches which have been introduced and discussed in the previous section can be used to model interdependencies among infrastructure systems as well as single systems and interdependencies within, e.g., CN theory, PN-based and ABM approach. Some of them can only be used to model interdependencies, e.g. IIM. Due to inherent complexity of interdependencies among infrastructure systems, in practice, there is still no "silver bullet approach". Instead, it has proven necessary to integrate different types of modeling approaches into one simulation tool in order to fully utilize benefits/advantages of each approach and to optimize the efficiency of the overall simulation. One of the key challenges for developing

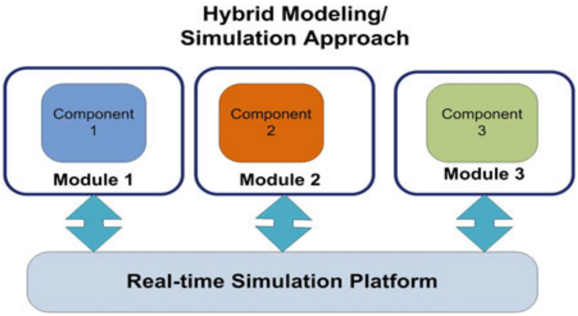


Fig. 13.13 Architecture of the hybrid modeling/simulation approach

such type of simulation tool is the required ability to create multiple-domain models, e.g., discrete and continuous time models, time-based and frequency-based models, and to effectively exchange data among them [45]. One solution for meeting these challenges and handling these technical difficulties is to distribute different simulation components by adopting the concept of modular design. The overall simulation platform can be divided into different simulation modules at first, which could be domain-specific or sector-specific simulation components, so as to make the best use of computational resources, and then distribute them across one simulation platform.

This so-called hybrid modeling/simulation approach, illustrated in Fig. 13.13, intends to integrate different modeling and simulation techniques, and can be considered as a successor of the traditional simulation approach in case multiple systems need to be simulated. It changes the way to design and develop simulation tools: Instead of building a "heavy weight" simulation component, a number of "light weight" components are developed interacting with each other over a real-time simulation platform, which not just potentially improves the efficiency and flexibility of the developed simulation tool but also decreases its overall complexity. Each distributed "light weight" simulation component is developed to represent its own system characteristics using appropriate modeling approaches. The information and control commands exchanged among simulation components are interpreted and processed over the network connection, allowing quick assembly of independently developed components without full knowledge of their peer simulation components.

13.4.4.2 High Level Architecture (HLA)

While several simulation standards do exist for supporting the distribution simulation components, the most widely implemented and applicable one is the HLA simulation standard [46], which is a general purpose high-level simulation architecture/framework to facilitate the interoperability of multiple-types models and simulations. In 1998, the first complete HLA interface specification was released to the public [47]. In 2000, HLA was approved as an open standard by the organization of the Institute of Electrical and Electronic Engineers: IEEE Standard 1516–2000 [48]. Since then, the HLA standard has been revised and improved; the most current one is HLA-Evolved.

As an open IEEE standard, HLA has been widely adopted across various fields of simulation industries during the last decade. The EPOCHS (Electric Power and Communication Synchronizing Simulator) is an early attempt to distribute several individual simulators by adopting the HLA standard, which utilizes multiple research and commercial systems from various domains [49, 50]. Computer experiments show that "*the overall simulations have been sped up after distributing simulation components based on the standard of HLA*" [51]. Similar results are also observed while working on an agent-based framework for controlling activity flows between the ISS (Interactive Simulation Systems) components [52]. Furthermore, HLA has been applied to other industry fields such as the US border operation study [53], rail traffic safety system simulation [54], and many others [55–57]. Although, this standard has been questioned regarding its feasibility in the research field of interdependency study, it is still the most applicable and feasible one if compared to other similar simulation standards such as Distributed Interactive Simulation (DIS) and Aggregate Level Simulation Protocol (ALSP). One distinguished advantage of this standard is its support of live participants, meaning that the representation of the live world such as a human being, a real process instrumentation device and a field controller can be integrated into the simulation world. More details about the HLA standard can be found in [58]. While HLA is the architecture, a simulation standard, Run Time Infrastructure (RTI) is the software, the core element of the HLA standard, which provides common services to all participating federates.

13.4.4.3 Structure of the Experimental Simulation Platform

An experimental simulation platform has been developed to assess interdependency-related vulnerabilities between SUC (System Under Control) and its SCADA system by adopting the hybrid modeling/simulation approach (implemented using the HLA standard). The platform consists of four major components: SUC model, SCADA model, RTI server, and simulation monitor, all connected over a LAN (see Fig. 13.14).

The SCADA model is a discrete-event and agent-based model, developed by a failure-oriented modeling approach (Fig. 13.15). In this approach, the "agent state" is defined as a location of control with a particular set of reactions to conditions and/or events of its related agent. For example, open and close are two states defined for an agent representing a circuit break device. The "device mode" including both operational mode and failure mode is defined as the hardware status of corresponding simulated hardware devices. For example, failure-to-open and failure-to-close are two device modes defined for a field control device. The transition of various device modes can affect corresponding agent states. With the help of this modeling approach, technical failures of simulated devices of a SCADA system can be easily determined and corresponding failure propagations can be visualized/studied. The core of the device mode model is given by the state diagrams illustrated in Fig. 13.16, which

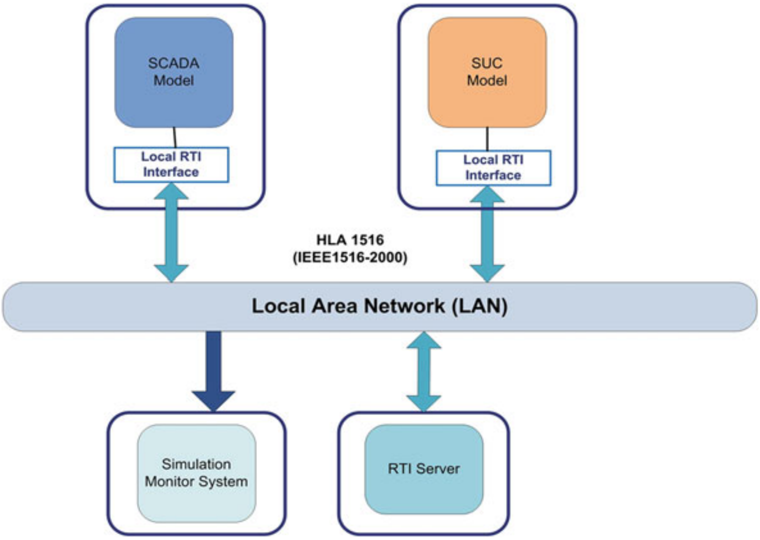


Fig. 13.14 Architecture of the experimental simulation platform

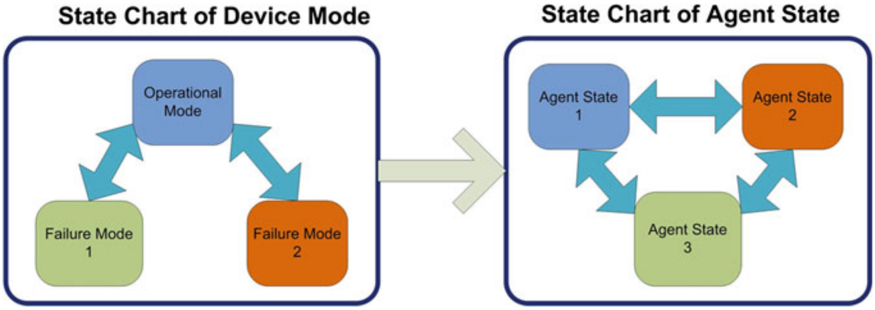


Fig. 13.15 Failure-oriented modeling approach

reflects a continuous-time, discrete-state Markov model describing failure behaviors of a studied device with one operation mode (left) and two failure modes (right) (see [59] for more details).

The SUC model is a continuous-time and agent-based model. The aim of this model is to investigate various system operating situations which could potentially result in a blackout of the Swiss electric power transmission network [5]. The SUC model simulates scenarios in a continuous time by means of conventional techniques such as power flow calculations. Since it was previously designed as a stand-alone model, no inputs from external models had been specified. To include this model in the experimental platform, a Java-based independent HLA-compliant interface is developed, which is responsible to process all inputs (outputs) to (from) the model (see [38] for further details).

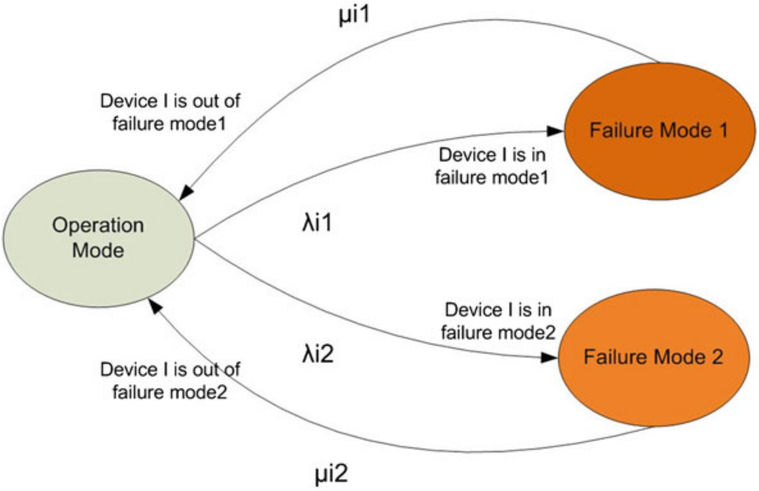

μi1
Device I is out of failure mode1
Failure Mode 1
Device I is in failure mode1
Operation Mode
λi1
Device I is in failure mode2
λi2
Failure Mode 2
Device I is out of failure mode2
μi2

Fig. 13.16 State diagram of the device mode model (λ constant failure rate; μ repair rate)

The RTI server acts as the center of the experimental platform and is responsible for simulation synchronization and communication routing between all components, through the local RTI interface of each model. Each federate communicates with this server via its own local RTI interface and starts to follow central federation management. The simulation monitor system is a real-time tool, through which the simulation of two models can be observed.

13.4.4.4 Validation the Hybrid Modeling/Simulation Approach

To demonstrate the capabilities of the hybrid modeling/simulation approach, as well as of the simulation platform, for representing interdependencies among infrastructure systems, several experiments have been designed including feasibility and failure propagation experiments.

The purpose of the **feasibility experiment** is to study whether the HLA-compliant distributed simulation environment is capable to simulate interdependencies. In order to visualize the interdependency phenomena between SCADA and SUC, the scenarios that will trigger power line overload alarm are generated manually during the simulation. Generally, the maximum load each power transmission line can carry has been previously determined by its operator and is called *overload threshold*. If the real power flowing through a transmission line exceeds its overload threshold, this line is considered to become overloaded. An accidentally overloaded transmission line could cause a system collapse. Therefore, suitable corrective actions should be taken in order to alleviate the overloaded transmission lines. Normally, whenever a monitored transmission line is overloaded, an alarm will be generated and sent to the operator in the control center by the RTU of the SCADA system. If, after a certain period, the operator fails to react to the overload alarm, then the protection devices such as disconnectors will automatically isolate the overloaded transmission line to minimize negative consequences. It should be noted that the procedure for handling a power line overload alarm is complicated and other factors should also be considered. In order to simplify this problem, it is assumed that the overload alarm failed to be handled correctly only if the operator fails to react to the alarm in time and the protection device fails to trigger. Three case study scenarios are developed by modifying parameters of corresponding agents in order to observe three different outcomes after the occurrence of the transmission line overload: (1) neither operator nor protection device react the alarm, (2) operator reacts alarm, (3) protection device is triggered after operator fails to react.

The observed simulation results from three case studies show that the propagation of cascading failures between infrastructure systems due to interdependencies can be simulated and visualized with the help of the experimental platform. Although the models are distributed, overall simulation performance is not affected and interconnections between models can still be efficiently handled (see [58] for more information).

To investigate the phenomenon of failure propagation and related issues, another experiment has been developed and conducted. In this so called **failure propagation experiment**, a number of tests are conducted by triggering single or even multiple technical failures in order to observe and study sequent events due to the failure propagation. For example, in a single technical failure test, which is mainly related to the investigation of the physical interdependency, the FID agent[4] is developed to represent a power flow transducer (PTi) measuring power flow (in unit of MW) transmitted in a selected transmission line that is included in the SUC model. It is assumed that the PTi is calibrated incorrectly due to the aging. A list of sequential events after the incorrect modification of the PTi's calibration value is recorded using a database during the simulation. As learned by studying these records, at certain time, the PTi's calibration value is modified incorrectly. As a consequence, the output of the PTi is more than its measured variable value should be. According to this wrong value, the RTU generates a wrong overloading alarm and sends it to the MTU causing the operator in the control room to make a wrong decision, i.e., to redistribute the power flow of a transmission line. As the result, the amount of power transmitted in this line decreases, although it should not. The measured variable from PTi, as part of the SUC, acts as physical input into the SCADA system. This relationship can be considered as the **physical interdependency**, which causes the failure of PTi to propagate from the SUC to the SCADA system and go back to the SUC (see [27] for more information).

[4] FID agent is an agent representing a field instrumentation device such as a sensor or transducer.

According to investigation results, analyzed based on both feasibility and failure propagation experiments, it can be concluded that three types of interdependencies can be simulated using the current experimental simulation platform: physical, cyber, and geographical interdependency.[5]

13.4.4.5 Brief Introduction of "In-Depth" Experiments

In order to investigate and identify interdependency-related (often hidden) vulnerabilities between the SCADA system and the SUC, three "in-depth" experiments are also developed and conducted.

The first experiment is the **substation level single failure mode experiment**, in which different failure modes of each substation level component (i.e., FID, FCD, and RTU) are evaluated by performing a number of tests related to each failure mode. In total 8 failure modes are defined for these substation level components such as FID FRH (Failure to Run (too high)), FCD FO (Failure to Open), RTU FRF (Failure to Run with Field Device), etc (see [59] for more information). One substation from the reference SCADA system including two transmission lines is randomly selected. During each test, the scenarios that will trigger power line overload alarm are loaded at the beginning of the simulation. Each test starts in the operation mode (a device mode) and one of the agent states. Within a given time period, the device mode of a respective component will go to one failure mode for which the transition time from is assumed to be exponentially distributed. After a given time period, the device mode will go back to operation mode for which the transition time is also assumed to be exponentially distributed. The transitions between different device modes have influences on corresponding agent states resulting in the change of behaviors of the SCADA system and SUC. According to the conclusion of this experiment, among all the simulated SCADA-related devices, negative effects caused by failures of the RTU device seem more significant on its interconnected SUC (see [59] for more information).

The second experiment, the **small network single failure mode experiment**, extends the scope of the first experiment to a small network including more components from the SCADA system and the SUC (40 substations and 50 transmission lines). In this experiment, one key substation[6] from the SUC model is selected for triggering the failure modes of substation level components during the simulation. For each single failure mode, two types of tests are implemented: normal and worse-case test. The modeling scenarios of normal case test are similar to of the tests in the first experiment. The worse-case test represents the worse-case situation when the operator is unable to handle any alarm received by the control center due to natural or technical failures (hazards), e.g., the failure of the control panel, flooding/fire in the control center, etc. The purpose of performing experimental tests under this situation

[5] Indirect interdependencies are not considered during these experiments.

[6] In this experiment, it is assumed that substations connecting more than 6 transmission lines are considered as key substations.

is to observe corresponding consequences if the SCADA system fails to monitor and control the SUC through the MTU. According to the conclusion of this experiment, on average, negative effects due to interdependencies are aggravated during worse-case tests, which have been demonstrated during FID FRH worse-case tests (see [60] for more information).

The third experiment, **whole network worse-case failure modes experiment**, extends the scope to the whole network including all simulated components of the SCADA system and the SUC, by which negative consequences caused by interdependencies can be observed and analyzed. In this experiment, instead of just considering single failures, double failures occurring simultaneously at different substations are also included. The same modeling scenarios defined in the worse-case tests of the previous experiment are applied, but in addition, two key substations and non-key substations are selected as exemplary substations. According to the conclusion of this experiment, failures of FIDs in both single and double failure tests show very strong degree of impacts. It is also observed in this experiment that the increase of the number of key substations could also lead to more significant negative consequences (see [60] for more information).

Based on the results from these experiments, vulnerabilities of the studied SCADA system due to its interdependencies with the SUC have been identified, which can hardly be obtained without an appropriate simulation tool due to the complexity of real systems. Furthermore, suggestions for potential technical improvements are proposed, which could be useful to minimize the negative effects and improve the coping capacity of both systems (see [60] for more information).

13.5 Conclusions

Large-scale/wide-area technical networks, such as critical infrastructures, have become increasingly interdependent going along with operational modes closer to their limits, thus stressing the systems. These tendencies and interdependencies, in particular, have dramatically increased the overall complexity of related infrastructure systems, turning them to “system-of-systems” and causing the emergence of unpredictable behaviors and negative impacts. Therefore, these systems become more vulnerable to cascading failures with widespread consequences. These interdependency-related issues should not only remain as a subject of theoretical research. The practical importance has been evidenced and highlighted by numerous major disruptive events (2001–2012) such as bulk electric blackouts and should not be underestimated.

These technical networks even continue to become more integrated and their behaviors may tend to become more complex. Understanding and characterizing them is a real challenge; research in this area is still at an early stage. It is essential to get a clearer understanding of their cascading behaviors by applying appropriate techniques. Consequently, modeling/simulating those systems will remain as a field of active research. Although progress has been made in advanced modeling and simulation, more efforts are needed to further improve the methods/tools, to validate them and to scale them up to the level of "system-of-systems" and of the systemic nature of related risks.

In practice, there is still no "silver bullet" solution. Several approaches have been introduced and discussed in this chapter. Among these approaches, the CN theory is one of most frequently used techniques for topological analysis, while the ABM can be combined with other techniques such as the Monte Carlo simulation and offers the possibilities to include physical laws into the simulation and emulate the behavior of the infrastructure as it emerges from the behavior of the individual agents and their interactions. Combining different approaches and utilizing their strengths within one simulation tool by adopting the technique of distributed simulation using appropriate standards seem promising. This so called hybrid modelling and simulation approach has already proved its feasibility and applicability in recent research study and different types of experiments. Hopefully this approach will be adopted by researchers and practitioners in the field of risk analysis. With the help of this approach, traditional approaches such as the logic trees with limitations to capture the behaviour of those systems alone can also be combined with more advanced ones such as the ABM approach and used for more comprehensive system reliability/vulnerability analysis.

References

1. Newman DE, Carreras BA, Degala NS, Dobson I. Risk Metrics for Dynamic Complex Infrastructure Systems Such as the Power Transmission Grid. Proceedings of the 45th Hawaii International Conference on System Sciences, p. 2082–2090, 2012.
2. Kröger W, Zio E. Vulnerable Systems, Springer, 2011.
3. Habenberger J, Kröger W, Probst P, Raschke M, Schläpfer M, Birchmeier J. Stromversorgungssystem Schweiz. BABS Report: ETH Zurich, 2009.
4. Bilis EI, Kröger W, Nan C. Performance of Electric Power Systems under Physical Malicious Attacks. IEEE Systems Journal. Vol. 7(4), p.854–865, 2013.
5. Eusgeld I, Kröger W, Sansavini G, Schläpfer M, Zio E. The role of network theory and object-oriented modeling within a framework for the vulnerability analysis of critical infrastructures. Reliability Engineering and System Safety. Vol. 94, p.954–963, 2009.
6. Igure VM, Laughter SA, Williams RD. Security Issues in SCADA Networks. Journal of, Computers and Security, Vol. 25, p. 498–506, 2006.
7. Boyer SA. SCADA supervisory control and data acquisition. 3rd ed. Research Triangle Park: ISA; 2004.
8. Stouffer K., Falco J., Scarfone K. Guide to Industrial Control Systems (ICS) Security. National Institute of Standards and Technology; 2008.
9. Nan C, Kröger W, Eusgeld I. Focal Report: Study of Common Cause Failures of SCADA System at Substation Level, BABS Report: ETH Zurich, 2011.
10. Balducelli C, Bologna S, Lavalle L, Vicoli G. Safeguarding information intensive critical infrastructures against novel types of emerging failures. Reliability Engineering and System Safety. Vol. 92, p. 1218–1229, 2007.
11. Nai Fovino I, Carcano A, Masera M, Trombetta A. An experimental investigation of malware attacks on SCADA systems. International Journal of Critical Infrastructure Protection. Vol. 2, p. 139–145, 2009.

12. SWISSGRID: Die Nationale Netzgesellschaft. 2007.
13. Aitel D. Cybersecurity Essentials for Electric Operators. The Electricity Journal. 2013.
14. Slay J, Miller M. Lessons learned from the Maroochy water breach. IFIP International Federation for Information Processing. Vol. 253, p. 73–82, 2008.
15. (FPL) FPaLC. FPL announces preliminary findings of outage investigation. 2008.
16. Christansson H, Luiijf E. Creating a European SCADA Security Testbed. IFIP International Federation for Information Processing. Boston: Springer; p. 237–247, 2007.
17. Zhou L. Forcal Report: Vulnerability Analysis of Industrial Control Systems - Part B: Statistics and analysis of industrial security incidents, Challenges of ICS security research. BABS Report: ETH Zurich, 2011.
18. Trantopoulos K. Focal Report: Vulnerability of Critical Infrastructrures-Rail Transport Switzerland. BABS Report: ETH Zurich, 2010.
19. Kröger W, Nan C, Trantopoulos K, Zhou L, Eusgeld I. Report: Interdependencies. BABS Report: ETH Zurich, 2009.
20. Railroad Accident Brief: Accident DCA-01-MR-004. In: Board USNTS, editor.NTSB/RAB-04/08.
21. Rinaldi SM, Peerenboom JP, Kelly TK. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. IEEE Control Systems Magazine. 2001; Vol. 21: p. 11–25.
22. Griot C. Modelling and simulation for critical infrastructure interdependency assessment: a meta-review for model characterisation. International Journal of Critical Infrastructure. Vol. 6, p. 363–379, 2010.
23. Pederson P, Dudenhoeffer D, Hartly S, Permann M. Critical Infrastructure Interdependency Modeling: A Survey of U.S and International Research. Idaho National Laboratory; 2006.
24. Zimmerman R. Decision-making and the vulnerability of interdependent critical infrastructure. IEEE International Conference on Systems, Man and Cybernetics. p. 4059–4063, 2004.
25. International Risk Governance Council. Policy Brief: Managing and reducing social vulnerabilities from coupled critical infrastructures. Geneva, Switzerland: IRGC; 2007.
26. Kröger W. Critical infrastructure at risk: A Need For A New Conceptual Approach and Extended Analytical Tools. Reliability Engineering and System Safety. Vol. 93, p. 1781–1787, 2008.
27. Eusgeld I, Nan C, Dietz S. “System-of-systems” Approach for Interdependent Critical Infrastructures. Reliability Engineering and System Safety. Vol. 96, p. 679–686, 2011.
28. Leontief WW. Input-output economics. 2nd Ed ed: Oxford University Press, New York; 1986.
29. Setola R, De Porcellinis S, Sforna M. Critical infrastructure dependency assessment using the input-output inoperability model. International Journal of Critical Infrastructure Protection. Vol. 2, p. 170–178, 2009.
30. Haimes YY, Horowitz BM, Lambert JH, Santos JR, Lian C, Crowther KG. Inoperability Input-Output Model for Interdependent Infrastructure Sectors. I: Theory and Methodology. Journal of Infrastructure Systems. Vol. 11, p. 67–79, 2005.
31. Haimes YY, Horowitz BM, Lambert JH, Santos J, Crowther K, Lian C. Inoperability Input-Output Model for Interdependent Infrastructure Sectors. II: Case Studies. Journal of Infrastructure Systems. Vol. 11, p. 80–92, 2005.
32. Trantopoulos K. Focal Report: Methods for the Vulnerability Assessment of Multi-layer Infrastructure Networks-The Swiss Rail System. BABS Report: ETH Zurich, 2011.
33. Klein R, Rome E, Beyel C, Linnemann R, Reinhardt W. Information Modelling and Simulation in large interdependent Critical Infrastructures in IRRIIS. IRRIS Report 2007.
34. Steen Mv. Graph Theory and Complex Networks: An Introduction. 1 ed: Maarten van Steen; 2010.
35. Buldyrev SV, Parshani R, Paul G, Stanley HE, Havlin S. Catastrophic cascade of failures in interdependent networks. Nature. Vol. 464, p. 1025–1028, 2010.
36. Johansson J, Hassel H. An approach for modelling interdependent infrastructures in the context of vulnerability analysis. Reliability Engineering and System Safety. Vol. 95, p. 1335–1344, 2010.

37. Eusgeld I, Nan C. Creating a simulation environment for critical infrastructure interdependencies study. IEEE International Conference on Industrial Engineering and Engineering Management, p. 2104–2108, Hong Kong, 2009.
38. Schläpfer M, Kessler T, Kröger W. Reliability Analysis of Electric Power Systems Using an Object-oriented Hybrid Modeling Approach. 16th power systems computation conference. Glasgow. 2008.
39. Min H-SJ, Beyeler W, Brown T, Son YJ, Jones AT. Toward modeling and simulation of critical national infrastructure interdependencies. IIE Transactions. Vol. 39, p. 57–71, 2007.
40. Di Giorgio A, Liberati F. Interdependency modeling and analysis of critical infrastructures based on Dynamic Bayesian Networks. 19th Mediterranean Conference on Control & Automation (MED), p. 791–797, 2011.
41. HadjSaid N, Tranchita C, Rozel B, Viziteu M, Caire R. Modeling cyber and physical interdependencies - Application in ICT and power grids. Power Systems Conference and Exposition. p. 1–6, 2009.
42. D'Agostino G, Bologna S, Fioriti V, Casalicchio E, Brasca L, Ciapessoni E, et al. Methodologies for inter-dependency assessment. 5th International Conference on Critical Infrastructure (CRIS). p. 1–7, 2010.
43. Casalicchio E, Bologna S, Brasca L, Buschi S, Ciapessoni E, D'Agostino G, et al. Interdependency Assessment in the ICT-PS Network: The MIA Project Results. In: Xenakis C, Wolthusen S, editors. Critical Information Infrastructures Security: Springer, Berlin Heidelberg; p. 1–12, 2011.
44. Fioriti V, D'Agostino G, Bologna S. On Modeling and Measuring Inter-dependencies among Critical Infrastructures. Proceedings of the 2010 Complexity in Engineering: IEEE Computer Society, p. 85–87, 2010.
45. Bloomfield R, Chozos N, Nobles P. Infrastructure interdependency analysis: Introductory research review. 2009.
46. Gorbil G, Gelenbe E. Design of a Mobile Agent-Based Adaptive Communication Middleware for Federations of Critical Infrastructure Simulations. Proceedings of CRITIS 2009. 2009.
47. DoD. Department of Defense (DOD): High Level Architecture Interface Specification. 1998.
48. IEEE. IEEE Standard for Modeling and Simulation High Level Architecture (HLA)—Framework and Rules. IEEE Std 1516–2000, 2000.
49. Hopkinson KM, Giovanini R, Wang XR. EPOCHS: Integrated Commercial Off-the-Shelf Software For Agent-based Electric Power and Communication Simulation. Proceedings of the 2003 Winter Simulation Conference. p. 1158–1166, 2003.
50. Rehtanz C. Autonomous systems and intelligent agents in power system control and operation: Springer; 2003.
51. Lees M, Logan B, Theodoropoulos G. Distributed Simulation of Agent-based Systems with HLA. ACM Transactions on Modeling and Computer, Simulation. Vol. 17(3), 2007.
52. Zhao Z, Albada DV, Sloot P. Agent-Based Flow Control for HLA Components. Simulation. Vol. 81, p. 487–501, 2005.
53. Beeker ER, Page EH. A Case Study of the Development and Use of a MANA-Based Federation for Studying U.S. Border Operations. Proceedings of the 38th Conference on Winter Simulation, p. 841–847, 2006.
54. Lieshout Fv, Cornelissen F, Neuteboom J. Simulating Rail Traffic Safety Systems using HLA 1516. Atos Origin Technical Automation; 2008.
55. Ezell BC. Infrastructure Vulnerability Assessment Model (I-VAM). Risk Analysis. Vol. 27, p. 571–583, 2007.
56. Möller B, Löfstrand B, Lindqvist J, Backlund A, Waller B, Virding R. Gaming and HLA 1516 Interoperability within the Swedish Defense. 2005 Fall Simulation Interoperability Workshop. 2005.
57. Zacharewicz G, Alix T, Vallespir B. Services Modeling and Distributed Simulation DEVS / HLA Supported. Proceedings of the 2009 Winter Simulation Conference (WSC). p. 3023–3035, 2009.

58. Nan C, Eusgeld I. Adopting HLA standard for interdependency study. Reliability Engineering and System Safety. Vol. 96, p. 149–159, 2010.
59. Nan C, Kröger W, Probst P. Exploring critical infrastructure interdependnecy by hybrid simulation approach. ESREL 2011. p. 2483–2491, Troyes, France, 2011.
60. Nan C, Eusgeld I, Kröger W. Analyzing vulnerabilities between SCADA system and SUC due to interdependencies. Reliability Engineering and System Safety. Vol. 113, p. 76–93, 2013.