

An Integrated Approach to Survivability Analysis of Large Complex Critical Infrastructures⁶

Sandro Bologna
ENEA– Casaccia
Via Anguillarese 301
00060 Rome – Italy
bologna@casaccia.enea.it

Thomas Beer
IABG
Einsteinstrasse 20
85521 Ottobrunn
beer@iabg.de

Abstract: The integrated approach for analysis of Large Complex Critical Infrastructures (LCCIs) to afford survivability aimed at preparing a Roadmap for Research and Development for critical infrastructure protection. Modelling and analysis of these large and complex systems is a challenge because of their non-linear and time-dependent behaviour. Existing models are inadequate, lacking necessary methodologies and therefore cannot protect infrastructures against a variety of blackouts. This article explores possible complications and relates them to four, prior identified, layers of network operation. Methods are required to help design new networks and support analysis of currently employed systems. Main needs for the design task will be elaborated and necessary development like the establishment of a general approach to the problem of modelling and analysis of LCCI's are covered. In presenting an analytical approach to develop an exhaustive methodology for survivability analysis a step-by-step procedure should lead to a scenario set which is capable to identify a set of high-risk hazardous paths. The analytical approach will be supplemented with a complex system as well as a simulation approach. Integrating these three approaches in a coherent framework should gain deeper insights in necessary and reasonable avenues to break new ground.

1 Background

The increasing complexity and interconnectedness of Large Complex Critical Infrastructures (LCCIs) and their supporting Networked Information Intensive Systems (NIISs) pose new challenges for modelling and analysis of the survivability of the systems. Newly emerging properties have to be understood, represented and analysed. While important steps have been taken on individual infrastructures, issues like interdependence and cascading effects among infrastructures have received much less attention. Not even is an exhaustive classification of possible types of failures available or in development. This situation calls for concerted efforts for an exploration of new methods and tools.

The various aspects of interactive infrastructure networks present numerous theoretical and practical challenges in modelling, simulation, prediction, and analysis in coupled and uncoupled systems. These systems comprise a heterogeneous mixture of dynamic,

⁶ This work was partially supported from European Commission under the EU-IST Framework

interactive, and often non-linear entities, unscheduled discontinuities, and numerous other significant effects. Existing mathematical models of such systems are vague and no methodologies for the understanding of the behaviour of these complex systems exist. The science of complex systems as well as chaos theory with attributes like entropy and complexity is considered particularly relevant to the study of topological properties and emerging behaviour of such interactive infrastructures. One of the problems we are facing in this domain is similar to those of fractals. Partitioning them into even smaller parts does not simplify the problem. Take, e.g., a power grid with a variety of production, switching, and transmission stations. A compartmentalisation of these stations or even a break down on a lower level does not lead to a better understanding or ability to protect anything. Additionally, in many complex networks, the human participants are both the most susceptible to failure and the most adaptable in management and recovery. Thus, modelling these networks will need to include the bounded rationality of actual human thinking. Furthermore, modelling will need to be carried out at a range of different resolutions, to achieve the overall objective of survivability analyses.

The following list of complications illustrates that networks representing LCCIs are inherently difficult to understand [St01]

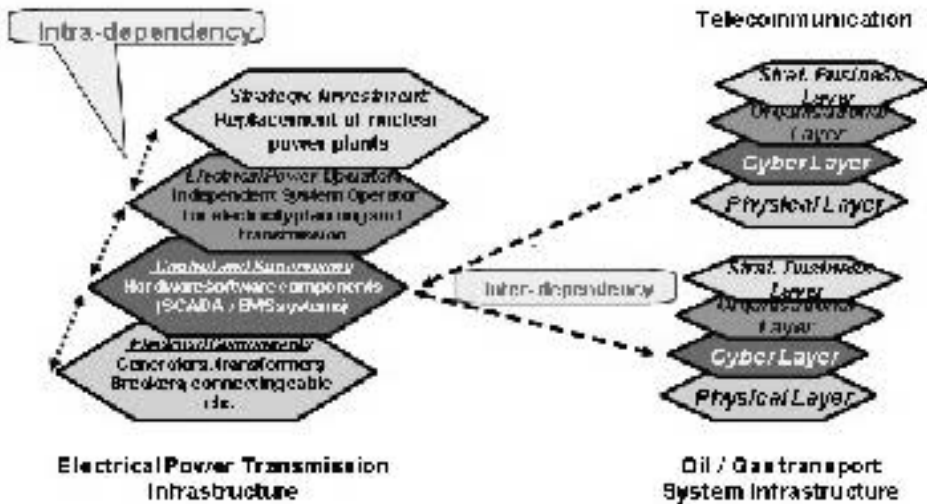
- Structural complexity: increasing number of nodes and links between nodes.
- Network evolution: the link between nodes could change dynamically over time.
- Connection diversity: the links between nodes could have different weights, directions and signs.
- Dynamical complexity: the nodes could be non-linear dynamical systems. In a network the state of each node can vary in time in complicated ways.
- Node diversity: there could be many different kinds of nodes in distributed, open systems.
- Meta-complication: the various possible complications can influence each other. For example, the present layout of a power grid depends on how it has grown over the years – here network evolution affects topology.

Generically, we may represent the domain of interest in four layers (see Figure 1)[Ba02, SA02, AC02]:

1. The physical infrastructure;
2. Automation and control;
3. Supervision, management and response;
4. Strategic and Company policy.

Layers 2 and 3 correspond to the management and control sections. They also form part of the NIIS supporting the physical infrastructure.

Different types of simplifications, according to the kind of property we want to study, for example static vs. dynamics properties, will be necessary. Assuming that we have methods and tools to study different properties of an available network, the follow-on question arises: If we couple many such systems, what can be said about their collective behaviour? The answer we could provide is: not much. It will be a function of different complications that will characterise the single system network.



Four Layers LCCI Model

To progress on this issue the European Commission launched a one year project named ACIP, with the purpose to prepare a Roadmap for Research and Development on the subject of “Analysis and Assessment of Critical Infrastructure Protection” for the next five to ten years. The ACIP Roadmap addresses research needed for the thorough understanding of problems of survivability analysis in the context of a highly distributed network of nodes. The proposed Roadmap focuses on groundbreaking concepts to understand the dynamics and behaviour of complex systems and networks.

Methods are required for

- analysing networks and systems for survivability, based on aspects such as the properties of individual nodes, the overall system, interconnections between nodes, as well as faults and intrusions to which the system is susceptible, and
- designing new networks (regularly incorporating parts of existing networks) to ensure survivability, resilience, security and similar properties.

2 Main Needs

To understand and characterise the problems posed by LCCIs with respect to survivability of the underlying NIISs, analytical skills should be focused on interconnection, composition and complexity of systems, the impact of faults, intrusions and any resulting cascading, escalating and not classified effect. Aim is a thorough understanding what to model, how to model it, and how to define properties for survivability.

To develop approaches to modelling and simulation of systems that are capable representing different levels of interdependencies among critical infrastructures, the underlying NIISs as well as all types of attacks, failures, and accidents which are detrimental to the survivability of critical infrastructures.

To develop techniques and simulation tools that help to build a basic understanding of the dynamics of complex infrastructures.

To develop methods for predictive survivability analysis, aimed at acquiring and processing information related to potential survivability threats and how these are handled.

To investigate the possibility using recent advances in the field of complex networks, focusing on statistical mechanics, to evaluate properties of the network topology and emerging behaviours.

To investigate possibilities of formal techniques combined with different symbolic and probabilistic techniques, with different levels of modelling power and analytical tractability. These techniques should be selected according to the properties to be evaluated, the complexity of each subsystem and its level of interaction within the NIIS at which it belongs.

To implement prototype versions of computerised tools to support the methodology.

To validate the developed methodology and tools in the application to different interdependent LCCIs.

3 Main Developments Necessary

Provide an overview of the phenomenology of networks with new findings from different fields and draw a state-of-the-art picture of theoretical methods and approaches. One important goal of the Roadmap is also to initiate interdisciplinary exchange between researchers in different fields, with a cross-fertilizations of ideas, for the purpose to bring the IT community out of stagnation.

Establishment of a general approach to the problem of modelling and analysing the LCCIs based on the latest progresses on the field of Complex Networks modelling and analysis.

Development of a system modelling approach incorporating the critical infrastructure, and the supporting NIIS. The model will have to represent all known types of attacks, failures, and accidents that are detrimental to the survivability of the critical infrastructure. This encompasses failures and faults in the system components, environment-related events, as well as human errors and intrusions. Due to the need for a consistent, complete, and unambiguous model, it is considered important that the network and the survivability properties are represented in a formal notation and is also necessary to facilitate automated analysis of these properties.

Classification of threats to the survivability of infrastructures and contribution to survivability related to these threats. In order to focus on survivability issues relevant to the application area, the identification of survivability properties will be done in exchange with stakeholders and end users.

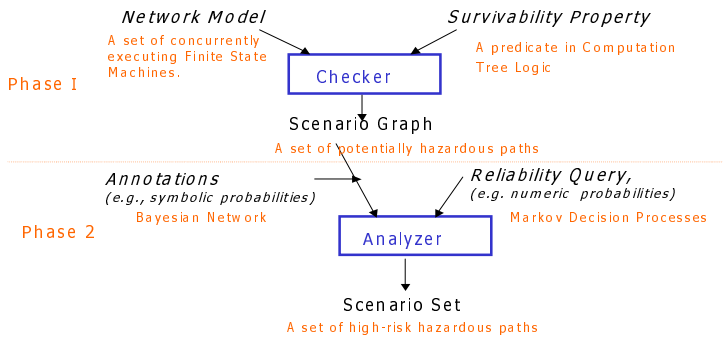
Methodological support for the identification of high-risk scenarios, including attack scenarios. This can be utilised by decision makers, system developers, and others to make well-informed decisions concerning survivability measures and policies, and their implementation in the NIIS.

A toolset supporting the methodology.

4 The Analytical Approach

One of the innovative aspect of ACIP is the attempt to provide criteria for the development of an exhaustive methodology for survivability analysis. The main components of the methodology are a combination of formal and “classical” techniques.

Figure 2 sketches the main steps of this approach [Jh00, Wi00]:



Overview of the proposed integration of formal and probabilistic techniques

Modeling the Network. In this step, the network will be modelled as a set of concurrently executing finite state machines and can be described as a set of nodes and interconnections.

Expressing the Survivability Properties. In this step the class of survivability properties of interest for and in cooperation with end users will be defined. System properties can be defined in various ways. Computation Tree Logic (CTL), besides other approaches, has been extensively used for this purpose.

Generating Scenario Graph. In this step model checking will be used to verify network properties. A scenario graph is a compact representation of all counterexamples to a given property. A counterexample is a system trace starting from an initial state and leading to a state that violates the given property. Scenario graphs have been implemented within SMV, however they could be built for other model checkers as well.

Symbolic Probability Analysis. In this step the user, together with the designer, assigns symbolic probabilities to events of interests. This provides a rough indication of the relevance of the potentially hazardous paths to the most relevant incidents.

Numerical Probability Analysis. In this step the user, together with the designer, provides numeric probabilities to events of interests, which will enable measurement and classification of each individual event in a scalar leading to a topology of most relevant incidents.

The formal approach will be based on formulating the network model in terms of concurrently executing finite state machines, and the survivability properties in terms of predicates in CTL. By employing a model checker, the result of this phase of the analysis is a scenario graph, representing a set of potentially hazardous paths. Each path

in the graph will represent a sequence of events potentially leading to a situation detrimental to the survivability of the critical infrastructure.

The output of the methodology in phase one is a set of possible scenarios that can lead to detrimental situations. Traditionally, the consequence tree method has been the most frequently used approach to identify these scenarios. In phase two the set of potentially hazardous paths is used as a basis for identification of the set of high-risk paths.

The branch “Bayesian Methods” deals with the problem of assessing the probabilities of sequences/chains of events which can cause the undesired event to occur by taking into account all the related uncertainties. In a Bayesian view, there is no separation between inference and probability assessment. All the probabilities are assessed conditional on observed data which are informative with respect to the uncertain event of interest. The branch “Markov Decision Processes” deals with the problem of assessing numerical probabilities to the sequence/chains of events which can cause the undesired event to occur.

As any other analytical approach, the main problem to face is the tractability of the problem when the complexity of the system increases. This is the case with LCCIs and their underlying NIISs. Some characteristics of their complexity are:

- strong interdependence of LCCIs: one event in one part of one LCCI can create a global effect by cascading throughout LCCIs;
- the adaptive property of reconfiguration of LCCI components, subsystems and systems to events and surroundings;
- systems belonging to LCCIs often spread across vast distances, are non linear, heterogeneous, and highly interactive.;
- in each situation LCCI's are subject to natural disasters, attacks, and unusually high demand;
- LCCI's are not born at once, but evolved over years, which causes a variety of related properties that may be detrimental.

5 The Complex Systems Approach

The world we live in could be constructed in a way that any complex system in nature can be modelled as a network, where vertices are elements of the system and edges represent the interactions between them.

Characterising the structural properties of the networks is of fundamental importance for an understanding of the complex dynamics of those systems. Networks provide graphic images of populations forming connections among individuals. Web-like structure describe a large variety of systems in many fields of science which could also be utilised for CSA. Recently, the growing interest in complex systems has prompted the study of real networks with novel and previously uncharacterised topological properties. What we need to define is a unifying framework, which can be fundamental in order to develop a solid theoretical understanding of physical processes underlying the formation of

complex networks. Methods which come to mind are biological, social, and physical system theory. Fortunately have all disciplines mature programmes of system theory and cross-connections are well established. One example may be the application of Maturanas' and Varelas' (biological) theory applied to social science where autopoietic systems are employed in the theory of social systems.

Traditionally has the study of complex networks been the territory of graph theory. While graph theory initially focused on regular graphs, since the 1950's large-scale networks with no apparent design principles were described as random graphs, proposed as the simplest and most straightforward realisation of complex networks. Make some dots on a page and start drawing lines between them at random. You end up with a network in which, on average, all the dots – or nodes – have the same number of links. Now count the number of nodes with one link, two links and so on, and plot these numbers on a graph. You end up with a well-known distribution, the Poisson distribution. This model has guided our thinking about complex networks for decades since its introduction. But the growing interest in complex systems prompted many scientists to reconsider this modelling paradigm and ask a simple question: are real networks behind such diverse complex systems as the cell or the Internet fundamentally random? Our intuition clearly indicates that complex systems must display some organising principles which should be at some level encoded in their topology as well. The intuition is now also supported from empirical data coming from different databases of complex systems networks. They have a lot of nodes with a few links, a few nodes with a medium number of links and very few nodes with lots of connections. If you plot these numbers on a graph, you end up with an ever-decreasing curve characteristic of what physicist call a power law. A new term has been invented to distinguish this type of networks from random graphs; they are normally reported as scale-free network. But if the topology of these networks indeed deviates from random graph, we need to develop tools and measures to capture in quantitative terms the underlying organising principles. [Re02]

6 The Simulation Approach: Modelling LCCI's Interdependencies like a population of Interacting Agents

All critical infrastructures have one property in common – they are all complex collections of interacting components in which change often occurs as a result of learning processes; that is, they are Complex Adaptive Systems (CAS). [Ri01] Seen from this perspective each component of an infrastructure constitutes a small part of the intricate web that forms the overall infrastructure. From a CAS perspective, infrastructures are more than just an aggregation of their components. Typically, as large sets of components are brought together and interact with one another, synergies emerge. This additional complexity exhibited by a system as a whole, beyond the simple sum of its parts, is called emergent behavior and is a hallmark of CAS. CAS do not require strong central control for emergent behaviours to arise.

One effective way to investigate CAS is to view them as populations of interacting agents, where an agent is an entity with a location, capabilities, and memory. Agents communicate with one another as they operate in a particular environment. Each agent receives inputs from other agents and sends outputs to them. One powerful computational approach to understanding CAS is agent-based modelling and simulation (ABMS). An ABMS consists of a set of agents and a framework for simulating their decisions and interactions. [Br02, Ma01]

When examining the more general case of multiple infrastructures connected as “system of systems”, we must consider interdependencies. Infrastructures are frequently connected at multiple points through a wide variety of mechanisms, such that bidirectional relationship exists between the states of any given pair of infrastructures; that is, infrastructure i depends on j through some links, and j likewise depends on i through other links. It means to consider connections among agents in different infrastructures, with a dramatically increase of the overall complexity. [Am00]

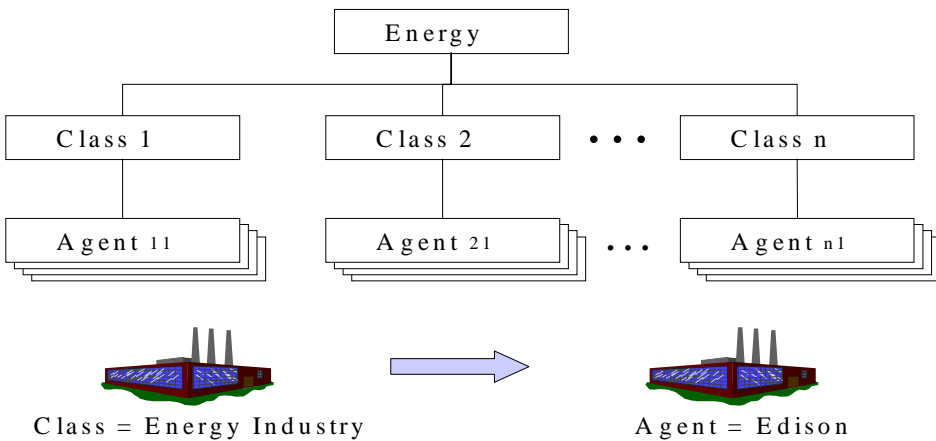
Unfortunately, the science of infrastructure interdependencies is relatively immature. Developing a comprehensive architecture or framework for interdependency modelling and simulation is a major challenge. Many models and computer simulations exist for aspects of individual infrastructures, but simulation frameworks that allow the coupling of multiple interdependent infrastructures are only to be considered.

Modelling is necessary to understand the dynamic behaviour of LCCIs and their interdependencies. Currently, there are no mathematical models that can generate useful top-down models for these systems, that are, models that start from large-scale graphs, systematically map them into de-coupled sub-systems, and investigate the interactions between them. Because of the variety of components and potential interactions, deriving all-encompassing rules for complex infrastructures is impractical. Therefore, top-down models offer some insight but can't adequately reflect real-world situations for complex infrastructures. Traditional top-down models use algebraic/differential equations to simulate aggregate populations within complex system. Specific internal mechanisms such as adaptation and learning are ignored, as is variation that might exist among individuals.

An alternative would be to develop a bottom-up approach using autonomous adaptive agents, which allow implementation for the individual parts of a system. By concentrating on smaller parts of the system, deriving rules becomes more practical. Bottom-up models based on autonomous adaptive agents let us evaluate the local mechanisms that produce emergent patterns at system level. Emerging Agent-Based Modelling (ABM) focuses on individual parts of a system rather than the whole; focusing on smaller parts of the system makes rule derivation more practical. Finally, real-world complexity is modelled by letting the individual “agents” interact independently – which can provide a better understanding of local mechanisms that produce emergent behaviour, as opposed to the centralised control inherent in top-down models. This can be undertaken in addition to system theory. Some part of a LCCI, e.g. an ICT administered power generator, can be modelled as closed (autopoietic) system, simplifying the observation in an initial stage and leading to “simpler” rules.

Agent-based models enable the use of simulation to better understand the large-scale, non-linear behaviour of complex infrastructures in the hope of improved amelioration of disturbances and prevention of disastrous cascading effects.

For engineered systems, such simulations can be used as a tool helping to build agent-like characteristics into infrastructure components, so that they can actively respond in their real-world environment automatically, independently, and co-operatively with other components. Development of complex infrastructures that are self-optimising and self-healing through distributed management and control will come into reach. As these simulations become more detailed and physically realistic, intelligent agents will represent all the individual components of the infrastructure. These agents will evolve, gradually adapting to their changing environment and improving their performance even if conditions change.



The relationship between agent classes and agents

Complex infrastructure components, such as a generating plant or a substation, will be modelled using object-oriented methods. This allows to model them as a class of object hierarchies of simpler components, thus creating a hierarchy of adaptive agents. These agents and sub-agents, represented as autonomous “active objects”, can evolve using a combination of genetic algorithms and genetic programming. In this context, classes are treated as an analogy of biological genotypes and objects instantiated from them as an analogy of their phenotypes, see Figure 3. [Br02] When instantiating objects to form individual agents, their class attributes, which define all the potential characteristics, capabilities, limitations or strategies that these agents might possess, can be selected and recombined by the operations typical of genetic algorithms, like crossover and mutation. The physics specific to each component will determine tolerable strategies and behaviours of the object-agent representing that component.

7 Conclusion

R&D projects should be supported covering the following issues:

- Identifying and understanding of the true dynamic behaviour of the infrastructures and their interdependencies to define the requirements for simulation, analysis and modelling methods and tools.
- Develop new simulation, analysis and modelling methods and tools able to represent the true dynamic behaviour of the infrastructures and their interdependencies.
- Modelling and analysis of interdependencies between infrastructures to enhance our understanding of their behaviour.
- Validation of the developed methods and tools.

From the preliminary scouting activities conducted inside the ACIP Project the following priorities are suggested:

1. Develop methods and tools for Agent Based Modelling and Simulation applied to Large Complex Critical Infrastructures
2. Combination of formal techniques with “classical” probabilistic and stochastic techniques.
3. Support Complex Systems Approach applied to real complex networks to discover previously unknown topological properties.
4. Consider system misuse and attack modelling as one of the major challenge to develop a framework for interdependency modelling and simulation.

8 References

- [AC02] ACIP “Analysis and Assessment of Critical Infrastructure Protection”, <http://www.eu-acip.de>.
- [Am99] Amin, M., National Infrastructures as Complex Interactive Networks, Automation, Control, and Complexity: New Developments and Directions, Samad & Weyrauch (Eds.), John Wiley and Sons, 1999.
- [Am00] M. Amin, Towards Self-Healing Infrastructure Systems, Computer, August 2000.
- [Ba02] Balducelli, C., Bologna, S., Agent Based Architectures to Improve Survivability of Large Complex Critical Infrastructures, Proceedings of nine annual Conference of the International Emergency Management Society (TIEMS 2002), Waterloo, Canada, May 2002.
- [Br02] Barton, Dianne C., Analysis of Complexity in Infrastructure Systems Using Agent Based Microsimulation, Infrastructure Surety Department, Sandia National Laboratory, Albuquerque, New Mexico, USA.

- [Jh00] Jha, Somesh, Linger, Richard, Longstaff, Tom, and Wing, Jeannette M., Survivability Analysis of Network Specifications, Proceedings of the International Conference on Dependable Systems and Networks, Workshop on Dependability Despite Malicious Faults, New York City, NY, June 25-28, 2000.
- [Ma01] Macal, Charles M., North, Michael J., Simulating Energy Markets and Infrastructure Interdependencies with Agent Based Models, Decision & Information Sciences Division, Argonne National Laboratory, Argonne, IL60439, USA, <http://www.dis.anl.gov/msv/cas/Pubs/Agent2002-InfraInterdepend.PDF>.
- [Ne00] Neumann, P.G., Practical Architectures for Survivable Systems and Networks, Computer Science Laboratory, SRI International, Menlo Park CA 94025-3493, <http://www.csl.sri.com/neumann/survivability.pdf>.
- [Re02] Reka, Albert, Barabasi, Albert-Laszlo, Statistical Mechanics of Complex Networks, Review of Modern Physics, 74, 47 (2002), <http://www.nd.edu/~networks/Papers/review.pdf>.
- [Ri01] Rinaldi, S.M., Peerenboom, J. P., Kelly, T.K. 2001, Critical Infrastructure Interdependencies, IEEE Control Systems Magazine, December 2001.
- [SA02] SAFEGUARD, Intelligent Agents Organisations to Enhance Dependability and Survivability of Large Complex Critical Infrastructure, <http://www.ist-safeguard.org>.
- [St01] Strogatz, Steven H., Exploring Complex Networks, Nature, Vol. 410, 8 March 2001, http://tam.cornell.edu/SS_exploring_complex_networks.pdf.
- [Wi00] Wing, Jeannette M., Towards a Science of Survivability: A Research Agenda and a Specific Method, Proceedings of the Third Information Survivability Workshop – ISW2000, Boston, MA, October 24-26, 2000.
- [MN01] Charles M. Macal, Michael J. North, Simulating Energy Markets and Infrastructure Interdependencies with Agent Based Models, Decision & Information Sciences Division, Argonne National Laboratory, Argonne, IL60439, USA. <http://www.dis.anl.gov/msv/cas/Pubs/Agent2002-InfraInterdepend.PDF>
- [Ne00] P.G. Neumann, Practical Architectures for Survivable Systems and Networks, Computer Science Laboratory, SRI International, Menlo Park CA 94025-3493. <http://www.csl.sri.com/neumann/survivability.pdf>.
- [RPK01] S.M. Rinaldi, J. P. Peerenboom, T.K. Kelly 2001, Critical Infrastructure Interdependencies, IEEE Control Systems Magazine, December 2001
- [SG02] SAFEGUARD, Intelligent Agents Organisations to Enhance Dependability and Survivability of Large Complex Critical Infrastructure, <http://www.ist-safeguard.org>
- [St01] Steven H. Strogatz, Exploring Complex Networks, Nature, Vol. 410, 8 March 2001 (http://tam.cornell.edu/SS_exploring_complex_networks.pdf)
- [Wi00] Jeannette M. Wing, Towards a Science of Survivability: A Research Agenda and a Specific Method, Proceedings of the Third Information Survivability Workshop – ISW2000, Boston, MA, October 24-26, 2000.