Annals of Spiru Haret University.
Economic Series
Since 2000
ISSN:2393-1795 ISSN-L:2068-6900
EDITURA FUNDAȚIEI ROMÂNIA DE MÂINE

Issue 2/2018

THE ROLE OF INTERDEPENDENCES BETWEEN CRITICAL INFRASTRUCTURES FOR SUSTAINABLE DEVELOPMENT

Laurențiu ASIMOPOLOS[1], Adrian-Aristide ASIMOPOLOS[2], Natalia-Silvia ASIMOPOLOS[1]

[1] Geological Institute of Romania, Caransebes Street, 1, Bucharest, 012271, Romania, Tel: +40751550941, +40740315186, Fax: + 40314033499, Email: laurentiu.asimopolos@igr.ro, natalia.asimopolos@igr.ro

[2] University Politehnica of Bucharest, Faculty of Transportation, Splaiul Independentei 313, Corp JA 003, Sector 6, Bucharest, 060032, Romania, Tel: +40727345113, Fax:+40213181012, Email: adrian.asimopololos@gmail.com

How to cite: ASIMOPOLOS, L., ASIMOPOLOS, A.A., ASIMOPOLOS, N.S., (2018). The Role of Interdependences between Critical Infrastructures for Sustainable Development. *Annals of Spiru Haret University. Economic Series, 18*(2), 63-81. doi: https://doi.org/10.26458/1823

Abstract

Critical Infrastructure Systems must provide and guarantee a good basis for people, goods, services and information on which the health, safety, comfort and economic activity of a society depends.

The phenomenon of globalization causes an increase in risks to critical infrastructures. For mitigation of these, the criteria of dependence and interdependence between them are imposed.

The security risks increasing related with interdependences between critical infrastructures that are not readily identifiable by traditional risk identification processes. A systematic analysis of the interdependences between critical infrastructures, using five dimensions (physical, cyber, geographic,

Annals of Spiru Haret University.
Economic Series
Since 2000
ISSN:2393-1795 ISSN-L:2068-6900
EDITURA FUNDAȚIEI *ROMÂNIA DE MÂINE*

Issue 2/2018

logical and social) is necessary. The relationships between Critical Infrastructure (CI) failure and their resilience are in function with interdependences between subsystems of each CI.

In this paper we show some considerations on the dimensionality of interdependences between critical infrastructures from the energy sector and Information and Communication Technology (ICT). After a breakdown of SCADA systems, we presented few examples of cybernetic attack against ICT and energy infrastructures. Main technological, economic, and regulatory changes have modified the relationships among infrastructures, and the information technology revolution has led to substantially more interconnected and complex infrastructures with generally greater centralization of control.

Keywords: *threats; vulnerabilities; risks; critical infrastructure; interdependences.*

JEL Classification: O_{33}

Introduction

Regionalization and polarization, the two contradictory dimensions of globalization, reveal the essential importance of interconnections and interactions between different components and elements of human spaces, from localities to economic sectors, from interest groups to cultural associations, from local structure to institutions, from companies to individuals, etc. Globalization requires a vision of the world, human space, a vision that seems to be more appropriate to man's existential relating.

The network calls for decentralization and deconcentration, specialization and cooperation, autonomy and convergence, emphasizing synergy and entropy, highlighting the importance of rules and institutions.

Sustainable rural development implies building a complex of activities legislative, organizational, economic, financial, social and cultural ones to ensure the improvement of the material and spiritual situation of the rural population through the non-destructive valorisation of the rural space resources.

The complexity and diversity of risks and threats, interconnected and characterized by multiple determinations, calls for an integrated, systemic and comprehensive approach to security objectives, with a focus on protecting those

Annals of Spiru Haret University.
Economic Series
Since 2000
ISSN:2393-1795 ISSN-L:2068-6900
EDITURA FUNDAȚIEI ROMÂNIA DE MÂINE

vital components for the safety and well-being of socio-economic life. Critical Infrastructure Protection (CIP) activity involves common efforts to identify and evaluate any vulnerabilities, threats and risks. As such, the protection of critical infrastructures – a determinant element for maintaining stability and security – requires developing and harmonizing strategies in the field. They must allow the identification and early warning of risks while at the same time adopting and timely initiating preventive and counter-interventions decisions / approaches.

The analysis of social vulnerability towards critical infrastructure failure has the potential to inform a population about planning and design of schemes.

The vast issue of CIP and the interdependencies between them has been dealt with in many papers, of which I recall [Leaua & Ardeleanu, 2012; Badea *et al.*, 2012; Setola & Porcellinis, 2007] and in many normative acts (Directive 2008/114/EC, etc.).

Concerning critical infrastructures from different fields of society, as subsystems within a global system, it is necessary to analyze the connections (unidirectional dependencies or bidirectional interdependencies) that exist between them.

Dependency between two critical infrastructures is a one-way connection, whereby the operation of one of the infrastructures directly influences the operating state of the other.

Unlike dependence, interdependence is a bidirectional connection between two or more infrastructures, through which the operation of each influences the state of others, i.e. two infrastructures are interdependent when each is dependent on the other.

In practice, interdependences between infrastructures lead to a more complexity of 'systems and subsystems' assemblies, which are characterized by multiple connections between feedback and feedforward infrastructures and implicitly between related domains. In view of this, the analysis of the behaviour of an infrastructure viewed in isolation from the general environment is a wrong or at least incomplete approach.

A correct approach should take into account the analysis of bi-directional interdependences between infrastructures.

According to this approach, in this paper we present the role of interdependences between critical infrastructures in development of society, with particular reference at two infrastructures (energy and information and communications technology – ICT), as well as Supervisory Control and Data Acquisition – SCADA systems.

Annals of Spiru Haret University.
Economic Series
Since 2000
ISSN:2393-1795 ISSN-L:2068-6900
EDITURA FUNDAȚIEI ROMÂNIA DE MÂINE
Issue 2/2018

General considerations on the dimensionality of interdependences between critical infrastructures

In the literature [Leaua & Ardeleanu, 2012] five categories of interdependencies are identified: physical, cyber, geographic, logical and social. Although each has distinct features, these categories are not mutually exclusive.

• "physical" interdependencies;

Two infrastructures are physically interdependent if the capacity of one depends on the material performance of the other.

For example, ICT infrastructure ensures data monitoring, control and adjustment for an energy infrastructure, while electricity generated by the generator provides the energy required to operate SCADA, ICT facilities for energy infrastructure.

• "cyber" interdependencies;

Two infrastructures have "cyber" interdependence if the state of one depends on the information provided by the other data transmission system. In this case, information products resulting from the operation of an infrastructure constitute "raw material" for the operation of the other infrastructure.

For example, the state of the operation of an ICT infrastructure has an overwhelming impact, through the information transmitted, on energy infrastructure. Conversely, the informational results transmitted from the energy infrastructure can be used by the ICT infrastructure to make adjustments, operational safety measures, stopping subsystems to avoid damage, etc.

• "geographic" interdependencies;

Infrastructures are geographically interdependent if the occurrence of a local event can create disturbances in the state of operation of those other infrastructures. Geographic type interdependence occurs when elements of two or more infrastructures are in spatial proximity. Because of this proximity, events such as an explosion or a fire can cause disturbances or damage to these spatially interdependent infrastructures. Such related disturbances are not caused by "physical" or "cyber" connections, but rather because of the influence that the event exerts simultaneously on all infrastructures.

For example, a gas pipe or an energy line that has telecommunication lines in the vicinity.

• "logical" interdependencies;

This type of interdependence is determined by control systems linking a component from an infrastructure to another component of another infrastructure

Annals of Spiru Haret University.
Economic Series
Since 2000
ISSN:2393-1795 ISSN-L:2068-6900
EDITURA FUNDAȚIEI ROMÂNIA DE MÂINE

without a direct physical, cyber or geographic connection. An example of this may be interdependence between electricity generation and transport infrastructure, energy market regulations and existing investments in this area. The "logic" interdependence between infrastructures is due to human decisions and activities and not as a result of a direct physical interaction.

Research, analysis, evaluation of results and decision-making in the fields of energy and ICT are logically interdependent.

• "social" interdependencies

Represents the influence that an event associated with a component of an infrastructure may have on social factors (for example, public opinion, population confidence, fear or cultural issues). Even if there is no physical or direct relationship, the manifestation of the event has consequences on other infrastructures. This influence can be distinguished over time by the initial causes. For example, a major damage to the energy system would substantially reduce ICT outcomes at society and vice versa.

While it is generally accepted that interdependences are critical when jeopardizing the normal functioning of the economy and society in general, a deeper assessment of the impact on national economy and security has only developed over the last decade. That is why the key aspects of knowing the effects of interdependences are their chaining across multiple critical infrastructure sectors and the possibility of unforeseen effects.

The study of interdependences can be used to qualitatively assess the vulnerability of industry sectors to infrastructure disruption and can support the estimation of potential impacts induced by infrastructure service outages, at organization and industry sector level. This can inform and foster public and private sector investments to enhance infrastructure resilience [Giovinazzi *et al.*, 2016].

Rinaldi *et al.* (2001) provides a clear and exhaustive elicitation of infrastructure interdependencies that can be used to identify security risks. The framework (figure no. 1) is a conceptual high-level model that presents six dimensions of interdependency that are subsequently explored, analyzed, and dissected. Though the framework does not explicitly attempt to model and analyze security threats that arise from the interdependencies, it does however bring together in a very neat abstract level the factors (technical, legal, economic, business, social/political, legal/regulatory, public policy, health and safety) that

Annals of Spiru Haret University.
Economic Series
Since 2000
ISSN:2393-1795 ISSN-L:2068-6900
EDITURA FUNDAȚIEI ROMÂNIA DE MÂINE

influence the operation of critical infrastructures and drive the complexities of the interdependencies observed [Rinaldi, Peerenboom, Kelly, 2001].

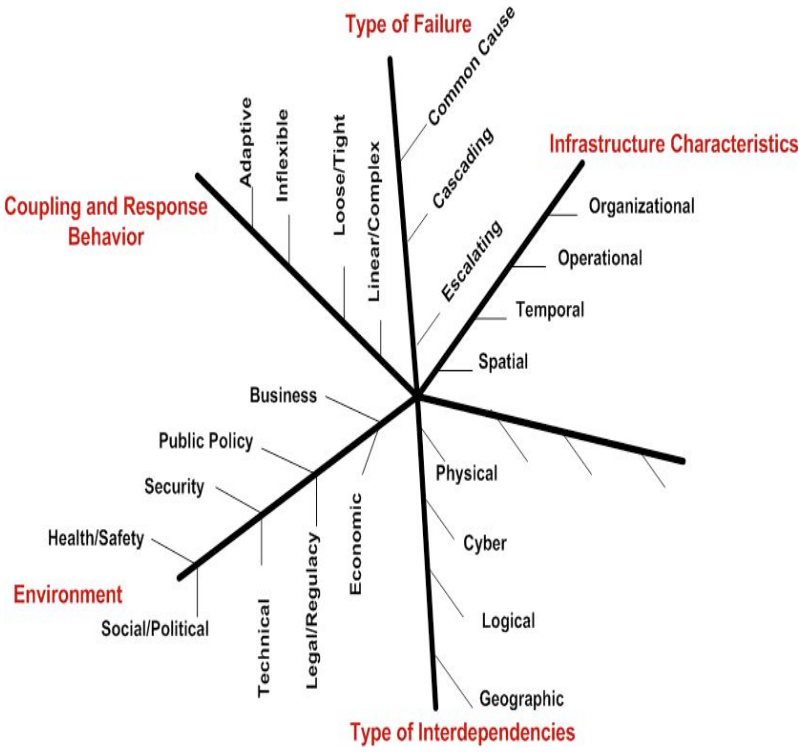

Figure no. 1. Six dimensions of interdependency that are subsequently explored, analyzed, and dissected
(after Rinaldi, Peerenboom, Kelly, 2001)

Disruptions to critical infrastructure systems such as electric power or transportation frequently cause major social and economic loss in disasters, both directly and through failures in one system leading to or compounding disruptions

Annals of Spiru Haret University.
Economic Series
Since 2000
ISSN:2393-1795 ISSN-L:2068-6900
EDITURA FUNDAȚIEI ROMÂNIA DE MÂINE

in another. Strategic approaches regarding infrastructure failures are needed to guide community mitigation and preparedness efforts [Chang *et al.*, 2007].

In the following figures are presented the vital systems and their essential components in the form of graph (nodes and connections) of all the relationships that exist between different systems and their effects (figure no. 2, figure no. 3).

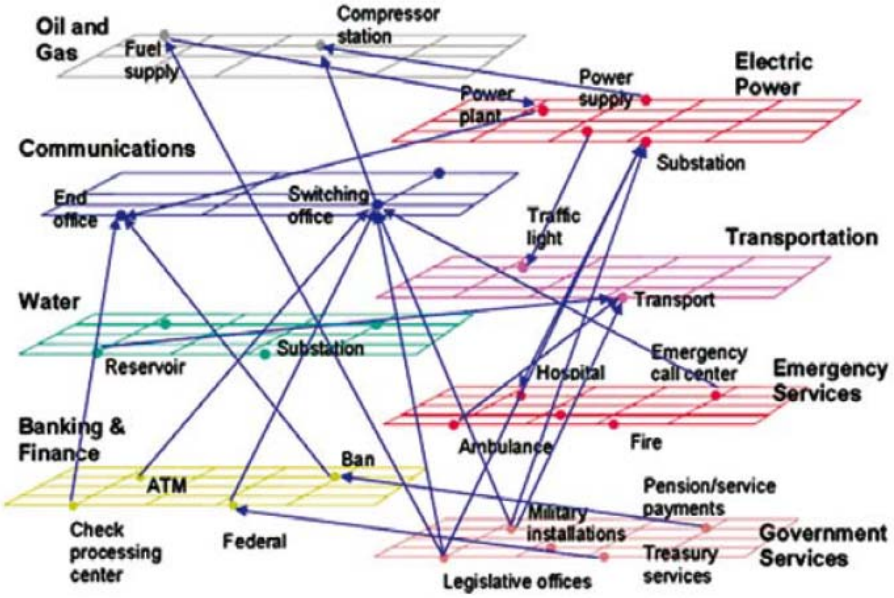

Figure no. 2. The interdependence graph and the propagation of effects between critical systems
(after Steven Rinaldi in Liviu Dumitrache, 2011)

In order to quantify the dependence and interdependence of critical infrastructures, the following parameters were introduced: the dependency index (a measure of robustness relative to inoperability transmitted) and the influence of gain (a measure of the influence that a specific infrastructure transmits on the overall level of the system).

Annals of Spiru Haret University.
Economic Series
Since 2000
ISSN:2393-1795 ISSN-L:2068-6900
EDITURA FUNDAȚIEI ROMÂNIA DE MÂINE

Issue 2/2018

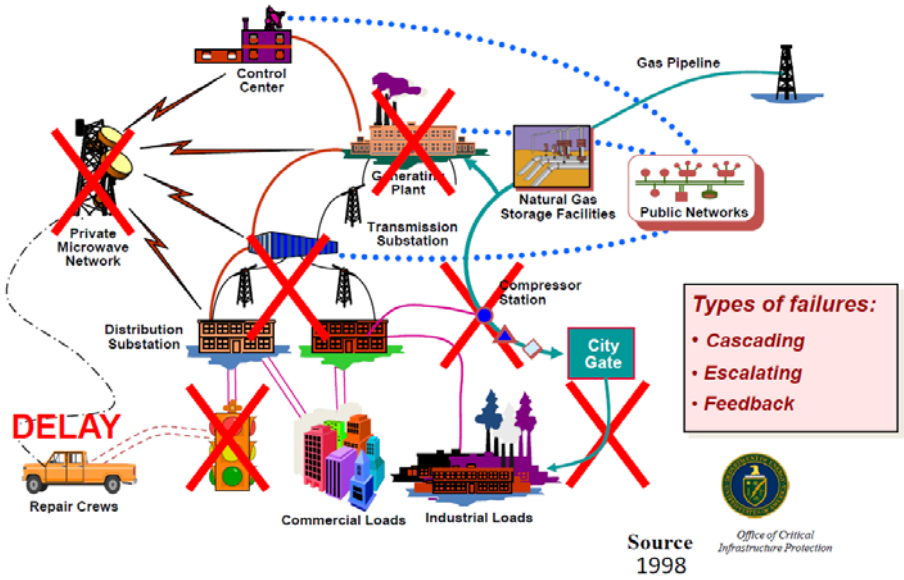

Figure no. 3. Example of interdependence in the energy industry
(after Roberto Setola, 2013)

Inoperability is the incapacity of an infrastructure to perform specific operations. Coefficients of inoperability can be quantified using the Leontief matrix, of which there are many scientific articles in specialized literature. The development of input-output models using matrix computational theory, simplex problem solving, stochastic processes theory and other methods of operational research, numerical analysis and statistical analysis are not the subject of the present paper (due to the large expansion of each methodology). The common point of each method is to determine the inoperability coefficients of the critical infrastructure subsystems that is dependent on the operation of other infrastructures and their subsystems. For any method chosen, however, the entry data in the model should be identified as accurately as possible. This is very laborious due to the lack of properly spent and monitored events, and in places where we have unknown input data, we have to estimate them based on scenarios.

Annals of Spiru Haret University.
Economic Series
Since 2000
ISSN:2393-1795 ISSN-L:2068-6900
EDITURA FUNDAȚIEI ROMÂNIA DE MÂINE

Interdependence between critical infrastructures from the energy sector and Information and Communication Technology (ICT); SCADA systems

Within the energy sector, at the convergence of communications and information technologies has developed a complex technology that is specializes on tasks related to the management of transmission and distribution networks. These networks with many variables, complex interactions and branches are of a very long length and can cross different areas [Hildick-Smith, 2005]. SCADA systems have been designed to address complex issues within the energy sector's objectives.

Transport and distribution networks are extremely difficult to administer. This was done (prior to SCADA systems) by placing measuring tools and training ground teams at key points of the network. Field teams were meant to read the values of networking tools or make measurements, communicate the readings to those responsible for network management, and perform the operations required by them. The communication of the readings to the network administrators, as well as in the opposite direction, was done either by telephone or by transmitting stations. The process was very tedious and even inefficient. In order to make the values read and perform remote operations more efficient, the telemetry and remote command methodologies have been introduced. This has become possible thanks to the development of modern means of communication.

On the other hand, the computing equipment became more and more advance.

Once a SCADA system has been implemented, operations can be monitored and controlled, and the system produces profit maximization information. Since SCADA is the centre of triggering, transmission, and distribution of operations, anyone who uses the system information can benefit from an overview of the site, installation, and operation of the system.

SCADA systems are made up of components of a different nature, which are connected to each other. The master schema of a SCADA system includes the following main components [Badea *et al*., 2012]:

– measuring components;

– actuating and automation components for electrical networks: switches, circuit breakers, etc.;

– hardware devices and computers, printers, plotters, monitors, synoptic displays, intelligent process control modules, programmed logic control modules, storage units;

– software components, operating systems (in real time or not), data collection systems, database management systems, simulation programs, communication programs, data archiving / restoration programs;

Annals of Spiru Haret University.
Economic Series
Since 2000
ISSN:2393-1795 ISSN-L:2068-6900
EDITURA FUNDAȚIEI ROMÂNIA DE MÂINE

– communications components (LANs, network cables, network cards, telephone lines, modems, terrestrial radio communications, broadcasting stations, transmission relays, satellite communications, satellite broadcasting stations, etc.).

To provide decision support, SCADA systems must offer a wide variety of services. Exhaustive enumeration of all services may be even impossible, so I will only call the most representative ones: the communications service, the data acquisition service and the remote-control service, the display of the most important states, the data logging and the interface operating, trend tracking and analysis services, remote order launch services, tracking and checking data, etc. If one of the exceptional conditions has occurred, the alarm service is triggered.

An important goal is to verify access to the system, this is done by the security service, which allows access to passwords. At each computer or terminal access is protected and has a certain level of access. Also, system operators have a password that gives a certain level of access (from their own computer or terminal). An operator's access to a system at a particular terminal is based on his / her own password, the access privileges granted by the system being the minimum of the implicit rights of the terminal and the operator.

One of the analysis tools of a SCADA system is a special place for the simulation service. This allows simulation of the network, which offers, among other things, the advantage that fewer measuring elements can be mounted, because the simulation will allow the interpolation of the values and at some points where such instruments are not mounted. On the other hand, the entire simulation system allows the analysis of some scenarios (the impact of some developments, network expansions, the effect of parameter changes due to damage, the fall of a transformer station in the case of an electrical network, etc.).

The requirements for the SCADA system and its components are multiple, the most important of which is the opening and observance of standards. The purpose of the opening is the possibility of working with other systems such as enterprise information system, design software system, consumption billing system, LAN / WAN workstations, distributed control systems, manufacturing management systems, modelling systems processes, optimization systems, etc.

Opening must be present both in terms of hardware (different hardware platforms), software (different operating systems and portable code), communications (international and de facto standards) and data management (such as SAG-SQL Access

Annals of Spiru Haret University.
Economic Series
Since 2000
ISSN:2393-1795 ISSN-L:2068-6900
EDITURA FUNDAȚIEI ROMÂNIA DE MÂINE

Group) and applications (interfaces and support offered for other programs). In most cases, in order to meet this requirement open-ended client-server architecture was chosen.

The second important requirement is adaptability: the ability to configure the components according to the concrete requirements, even if these requirements change over the life of the system; the ability to connect new equipment or programs to the existing system.

Making available timely data is another very important goal, so useful and timely action can be taken that could cause accidents.

Data security is also very important, the intrusion into the system can lead to disclosure of confidential information, which can cause serious malfunctions in the system. It is also necessary to set up an archiving system, once recorded data can be consulted and then for analysis. The system must provide the ability to quickly detect network failures and locate them as accurately as possible. It should also be able to provide all the data regarding the possible elements involved in the repair of the fault.

Since the implementation of a large-scale SCADA system involves very large investments, the problem of implementing such a system needs to be conceived gradually. Also, since the design phase, it has to be taken into account the possibility of extending the system, both in terms of increasing the number of measuring points and extending the functionality of the system.

The management of the firm must be convinced of the usefulness of introducing such a system by demonstrating the material advantages and the possibility of gradual implementation. Users are likely to show reluctance to a completely new system that they have not used to working on, so they need to be educated in advance with the system being put into service. Also, with the introduction of new elements, users need to know what they are and what their role is. For the implementation, operation and maintenance of the system, the goals pursued need to be clearly defined, the tasks to be performed and the persons who will deal with these issues must be determined. The access rights of these people must also be delimited very strictly and clearly. In order to assist the SCADA system, an intervention team will be set up, which in case of exceptional events can carry out the necessary repairs and will periodically carry out the maintenance of the equipment.

An energy system can be functionally found in one of the following states: normal operation, alarm, incident-failure and restoration.

Annals of Spiru Haret University.
Economic Series
Since 2000
ISSN:2393-1795 ISSN-L:2068-6900
EDITURA FUNDAȚIEI *ROMÂNIA DE MÂINE*

In the vast majority of time, the energy system is capable of operating under normal conditions (stable mode). In this operation, attention is given to economic functioning as well as functioning to successfully deal with small-scale incidents.

The alarm operation mode is characterized by the fact that for any incidents or damages that are detected (accidental shutdown of a large power energy group, the start of a transmission line, etc.), preventive measures are taken by starting from the reserve of groups, change of the electrical network configuration, etc. The emergency operation mode is characterized by the occurrence of a primary incident or an emergency (the triggering of a transmission line which leads to important moments in the power circulation and the voltage values), in such situations the energy system must have the necessary reserves (group starts from the reserve – hydropower and hydroelectric power plants – changes in the system's electrical network configuration) to successfully deal with these phenomena (static and dynamic stability reserves). As a rule, the major incident is followed by associated incidents (firing of electric lines and energy groups, power pervasions on power lines and energy groups), resulting in the energy system being required to the maximum from the point of view of static or dynamic stability.

There is a state of restoration in which, when the energy system has successfully dealt with the demands, the triggered lines and energy groups are started in which no failures occurred, and when the energy system has ceased to function, it first restores the connection between the important parts of the power system, parallel to the power plants and the important arteries, then all the networks and plants are put into operation (parallel), supplying to consumers alimentation with energy.

The safety of the functioning of the energy systems, in a scientific approach to problems, regarding the energy supply of the society, led to the establishment of a conception of this field, and to the use of a probabilistic method of analysis logically framed in an independent discipline, called Reliability. Reliability is concerned with the study of the functioning of technical systems in order to meet the objectives for which they are achieved. Reliability, as defined by the International Electronic Committee, is characteristic of a device that expresses the likelihood that the device will perform a precise function, under determined and time-bound conditions. In the most general form, the safety of a system can be defined as its ability, within a given time frame, to operate under well-specified conditions. The energy system consists of all the installations and equipment's that produce, transport, distribute and use the

Annals of Spiru Haret University.
Economic Series
Since 2000
ISSN:2393-1795 ISSN-L:2068-6900
EDITURA FUNDAȚIEI ROMÂNIA DE MÂINE

electric and thermal energy produced in district heating, intended to supply these forms of energy to all sectors of economic and social cultural activity. The main objective of our country's energy system (SEN) is to ensure that consumers supply electricity and heat produced safely, economically and at established parameters.

The study of the reliability of the energy systems is based on statistical and probabilistic methods, on economic models for optimization of technical solutions and is complemented by a set of technical and organizational measures applied in the phases of conception, execution and exploitation of the installations. Thus, the safety of an energy system implies a succession of operating, intermediate conditions, stops for planned repairs, etc., characterized by the state of the installations for the production, transport, distribution and use of electric and thermal energy. The operation of an energy system can, however, be influenced by the fuel supply, by the existing reserves in the fuel supply. Faults in the operation of the energy system and its component parts (transport networks, transformers, control equipment and information technology, telecommunication equipment, etc.) are defined and grouped conventionally into several categories.

Current malfunctions are deviations from the normal state or deficiency of equipment and installations or their component parts that do not require them to be shut down or decommissioned and can be remedied during operation or at planned stops.

Disturbances are failures in the electrical networks that lead to the interruption in power supply of consumers in the low-voltage grid in the thermoelectric power stations leading to forced triggers or forced stops of equipment or installations which do not directly affect the production of electric or thermal energy, such as, as a rule, equipment and installations in annexed households, or in hydroelectric plants.

Incidents are defects caused by an event or a sequence of events that change the previous state of operation of an installation or its element with consequences either of immediate or future reduction of power produced in the energy system or of interruption in electricity or heat supply to consumers. An isolated incident is one that occurs at a given time in an installation or an element thereof and does not cause other incidents and does not affect the operating state of other installations or elements but only as a result of the current operation of protection and automation with which they are provided. Associated incident is the operating incident occurring in an installation or its element at the time of the primary incident. The failure is an incident of a certain complexity or succession of incidents occurring at a given time in an installation, system area, or overall energy system resulting in

Annals of Spiru Haret University.
Economic Series
Since 2000
ISSN:2393-1795 ISSN-L:2068-6900
EDITURA FUNDAȚIEI ROMÂNIA DE MÂINE

significant equipment damage or power outages or heat, or both of these forms of energy, of particular industrial consumers or consumer areas.

The management of the activities of an owner / administrator / operator in the energy field should mainly cover the following areas:

– technical, commercial and economic, corresponding to the MIS (Management Information System), GIS (Geographic Information System), etc.;

– the operation of electrical installations in low, medium and high voltage networks which correspond to the SCADA / DMS systems [System Control and Data Acquisition / Distribution Management System];

– the measurement of the electrical energy corresponding to the AMR (Automatic Meter Reading) type subsystems.

Strategic Objectives in MIS domain:

• Provide integrated information from all operational / specialized IT systems / subsystems (ERP, GIS, SCADA, etc.) to all users, including subsidiaries, to support strategic and operational decisions.

• Ensuring transparency to customers and partners by providing interactive, online information using INTERNET / INTRANET specific technologies.

• Optimal use of development and production funds for the development of the national integrated IT system through the preservation / development of branch-level investments and / or the acquisition of outsourcing software provider at central level and subsidiaries.

• Computer administration of the archive of physical documents, transposed in electronic format, according to the legislation in force.

• Managing the information within the national integrated IT system to be done under Confidentiality, Integrity and Availability according to the ISO 27000 security standard and based on IT best practices in accordance with ITIL (Information Technology Infrastructure Library) standards.

• Basic infrastructure: Data area equipment – LAN (Local Area Network) – Storage Area Network (SAN) Storage Devices – Servers, Operating Systems, Databases for all information systems / subsystems (MIS, GIS, SCADA, etc.).

• Uniformity of computer systems / subsystems in relation to the information technologies used by similar electricity companies within the European Union.

• Reduction of operating costs of the National Integrated Information System.

• Reducing power consumption at the main CPCD and Disaster Recovery [DR] Reserve Centres.

Annals of Spiru Haret University.
Economic Series
Since 2000
ISSN:2393-1795 ISSN-L:2068-6900
EDITURA FUNDAȚIEI ROMÂNIA DE MÂINE

• Ensure technology independence (servers and operating systems) at the level of software applications, programming languages, and databases.

• Increase the integration of information systems (MIS, SCADA, GIS, etc.) using a single integration technology.

Another example of the interdependence between ICT infrastructures and oil and gas transport infrastructure through air surveillance, the installation of warning markers, advanced video surveillance systems, telecommunication and intrusion detection (conducted by HELINICK). The system is based on Distributed Acoustic Sensing (DAS) technology that prevents incidents that can affect transport pipelines, primarily by providing information before events that can lead to an incident. The principle is based on the optical fibre cable capture technology installed along the pipeline and uses advanced software algorithms to provide real-time pipeline status information. With this technology, sounds and images in real time are obtained from areas where burglary or incidental attempts are detected. The telecommunication system is based on optical transmission to the control centre and monitoring stations. Telecommunication networks use VSAT technology as a back-up solution and if the optical transmissions are interrupted, telephone, SCADA and security services are automatically taken over to the VSAT system to ensure continuous operation.

Cybernetic attack through energy infrastructures

The National Centre of Cyber Security Incident Response – CERT-RO is a national contact point for cyber security incidents and has as main activity the realization of general views on the nature and dynamics of these types of events / incidents, relevant for assessing cyber security risks for IT infrastructures and electronic communications on the national territory of Romania, within the competence of CERT-RO.

Computer threats to the national cyber space have diversified, both from a quantitative perspective and from the point of view of technical complexity. Some examples of this type:

• Botnet drone – Network of computer systems compromised, controlled remotely by other people / organizations than their owners.

• Microsoft Security & Security Centre: Attackers use botnet to send spam, spread computer viruses, attack other computers and servers, or commit other types

Annals of Spiru Haret University.
Economic Series
Since 2000
ISSN:2393-1795 ISSN-L:2068-6900
EDITURA FUNDAȚIEI ROMÂNIA DE MÂINE
Issue 2/2018

of fraud or crime. If your computer becomes part of a botnet you could involuntarily become an accomplice to the attacker.

• Industrial Control Systems (ICS) – control and control computer systems used in industrial processes.

• SCADA (Supervisory Control and Data Acquisition) – ICS's largest subgroup.

• Smart Grids – a modern electrical network with bidirectional communication capability between customer and supplier, as well as complex measurement and monitoring systems.

Examples of cyber-attacks on energy infrastructures:

STUXNET – 2010

– it was identified at the Iranian nuclear plant at Natanz;

– views 4 zero-day vulnerabilities;

– the worms used a series of default passwords of some Siemens (WinCC, PCS7) applications to access Windows operating systems;

– it succeeded in changing the rotation speed of the centrifuges used to determine uranium concentrations.

DUQU – 2011

– uses identical techniques to those of Stuxnet;

– it seems to have been created only for recognition actions on industrial control systems.

FLAME – 2012

– apparently developed by DUQU creators;

– specialized on stealing information through various methods in computer systems;

– discovered in computer systems running in SCADA from Iran, Lebanon, Syria and Sudan.

Conclusions

The economic and social development stimulated by the accelerated technological progress and the phenomenon of globalization has strengthened the strong interdependence and interaction of the systems that ensure the security and welfare of human society. The need to interconnect systems against the background of the trend towards the removal of administrative barriers, together with the

Annals of Spiru Haret University.
Economic Series
Since 2000
ISSN:2393-1795 ISSN-L:2068-6900
EDITURA FUNDAȚIEI ROMÂNIA DE MÂINE

integration of infrastructure networks, drives global security and stability developments.

The transnational interconnections of infrastructures and the sphere of risk manifestation, which have borrowed the elements of representation and evolution that are shaped by the globalization process, prefigure the perpetuation of the critical infrastructure risks and allow the extension of the "cascade system" on other countries, the effects of aggression on systems or processes.

The phenomenon of globalization, together with the positive advantages and positive transformations it brings to the international level, enables the rapid spread of direct threats to the security of all on a planetary scale. Trends in globalization of insecurity must be addressed through firm measures to block and eliminate current threats and threats, as well as the establishment of a globalization system for security.

Risks and threats to vital goals for the functioning of society and the security of citizens have gained new valences with high dynamics and increased intensity, which has led to the need for an integrated approach to the concept of critical infrastructure. Starting from the basic characteristics of critical infrastructures, the critical element of their stability, including in a cross-border context, has gained new connotations in the context of national / transnational strategies.

Priorities for the development of a strategic energy infrastructure (electricity, gas, oil) – production, transport and distribution to the final consumer requires consideration and adaptation of several sectoral measures, including protection and resilience specific to each critical infrastructure. Terrorist events, which can hardly be forgotten, require prioritization of measures to protect against terrorist acts, but other threats, vulnerabilities and risks that generate significant destructive effects and endanger the safety or security must be considered; or even people's lives.

According to this approach, Directive 2008/114/EC on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection obliges operators of critical infrastructure in the energy sector as well as operators in other infrastructures to assess all possible risk situations (all hazard approach) and to develop a Security Plan that takes into account cyber-attacks, human disasters, natural disasters and various technological threats.

In order to quantify the dependence and interdependence of critical infrastructures, will use the dependency index (a measure of robustness relative to

Annals of Spiru Haret University.
Economic Series
Since 2000
ISSN:2393-1795 ISSN-L:2068-6900
EDITURA FUNDAȚIEI ROMÂNIA DE MÂINE

inoperability transmitted) and the influence of gain (a measure of the influence that a specific infrastructure transmits on the overall level of the system).

Coefficients of inoperability, incapacity of an infrastructure to perform specific operations, can be quantified using the input-output models using matrix computational theory of Leontief. The common point of each method is to determine the inoperability coefficients of the critical infrastructure subsystems that is dependent on the operation of other infrastructures and their subsystems. For any method chosen, however, the entry data in the model should be identified as accurately as possible. This is very laborious due to the lack of properly spent and monitored events, and in places where we have unknown input data, we have to estimate them based on scenarios.

The interdependence between critical infrastructure in the energy sector and information and telecommunication technology is particularly strong, and the most obvious example is SCADA systems.

Power generation and distribution is managed by SCADA systems that depend on telecommunication services for data transmission between the systems. At the same time telecommunications rely on electricity to power communications circuitry. An interdependency exists where transport systems such as trams depend on electricity but at the same time the generation and supply of electricity may depend on the transport system, for instance to ferry in the coal, or the fuel needed to run power plants.

There are also many examples of this interdependence in the case of warning systems about the imminence of earthquakes or geomagnetic storms. Practically, the operation of the power system would be impossible without substantial input from the field of information and communication technology.

Reciprocally, information and communications technology, as well as all areas of human activities, is dependent on the use of energy in full security.

References

1. A. L. Leaua, D. Ardeleanu, “Interdependenţa infrastructurilor critice –implicaţii asupra securităţii naţionale” (*Critical Structures Interdependencies – implication for national security*), *Romanian Intelligence Studies Review* (issue: 08 / 2012): 89–100.
2. A. Badea, I. Chiuţă, A. Valciu, G. Păun, “Managementul infrastructurii critice a sistemelor electroenergetice”, *Buletinul Agir*, Supliment, 2/2012.

Annals of Spiru Haret University.
Economic Series
Since 2000
ISSN:2393-1795 ISSN-L:2068-6900
EDITURA FUNDAȚIEI ROMÂNIA DE MÂINE

3. S.E. Chang, T.L. McDaniels, J. Mikawoz, K. Peterson, "Infrastructure failure interdependencies in extreme events: Power outage consequences in the 1998 Ice Storm," *Natural Hazards*, 41 (2), (2007): 337-358.
4. L. Dumitrache, "Guvernarea riscurilor – element de cooperare între sectorul guvernamental, mediul de afaceri şi societatea civilă", *Alarma* nr. 2/2011.
5. S. Giovinazzi *et al.*, "Criticality of infrastructures for organisations," *International Journal of Critical Infrastructures,* Volume 12, Issue 4 (2016): 331-363.
6. A. Hildick-Smith, *Security for Critical Infrastructure SCADA System*, SANS Institute, 2005.
7. G. Manolescu, N. Istudor, *Logistica proiectării dezvoltării regionale* (Bucureşti: Editura Academiei de Studii Economice, 2007).
8. S.M. Rinaldi, J.P. Peerenboom, T.K. Kelly, "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies," *IEEE Control Systems Magazine*, 2001.
9. R. Setola and S. De Porcellinis, *A Methodology to Estimate Input-output Inoperability Model Parameters*, Critical Information Infrastructures Security 2007, Lecture Notes in Computer Science (Springer-Verlag, Berlin, 2008): 149–160.