CRITICAL INFRASTRUCTURES: THREATS, VULNERABILITIES AND PROTECTION

Danijela D. Protić
General Staff of Serbian Army, Department for Telecommunication and Informatics (J-6), Centre for Applied Mathematics and Electronics, Belgrade, Republic of Serbia
e-mail: adanijela@ptt.rs,
ORCID iD: http://orcid.org/0000-0003-0827-2863

DOI: 10.5937/vojtehg64-9986

FIELD: Electronics, Telecommunication, Security, Transportation
ARTICLE TYPE: Review Paper
ARTICLE LANGUAGE: English

Abstract:

This paper presents six critical infrastructure sectors: electric power systems, energy sources and supply, manufacturing, transport and storage of hazardous substances, traffic and transportation, information-telecommunication infrastructure, and supply with basic viands. The sources of adverse unwanted events due to accidents, technical faults, natural disasters, and human error are presented. Prediction and prevention of these events are explained in details.

Key words: *transportation, protection, vulnerabilities, threat, critical infrastructure, hazards.*

Introduction

Critical infrastructures are important infrastructures the destruction or incapacity of which can have tremendous consequences for national security, economy, environment and people. Critical infrastructure relates to assets, physical facilities, systems, communication networks, processes and supply chains which, if destroyed or degraded, would significantly affect the well-being of the nation. Disruption of critical infrastructure can result in catastrophic loss of life, adverse economic effects, etc.

Critical infrastructure protection involves programs and activities implemented by government, regulatory bodies, research institutions, users and owners, in order to reduce vulnerability in case of an unwanted

event. It also includes crisis management in order to strengthen resilience of critical infrastructure (Lewis, 2006). The European Union (EU) (2006) has adopted the action plan for the protection based on the prevention of incidents which may disrupt critical infrastructure security. The plan relates to detection and response to security breaches, recovery from accidents, and international cooperation. According to this plan, critical infrastructure consists of activities, networks, services, material goods and information technology that, if destructed, can have significant impact on health, safety and economic prosperity of the citizens and/or the economy of the member-states. Also, national critical infrastructures of member-states are defined as systems, networks and facilities of national importance whose disruption may have serious impacts to national security, health, property, environment, security, economic stability and governments (Protić, 2012, pp.82-101). In Great Britain, Sweden, Netherlands and Switzerland, the most common critical infrastructure is telecommunications. In Germany, one of the most important critical infrastructure sectors is also communication infrastructure, (O`Neil, Dempsey, 2000, p.12), Canada and Australia also included mass media. In the United States of America (US) critical infrastructure sectors are agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemical industry, postal and shipping (Kljajić et al., 2010, pp.75-78). Considering that disasters and adverse unwanted events most often occur locally, national strategies ensure that the first response to emergencies is local. On the other hand, federal authorities have responsibilities to manage emergencies at the national and global level (Službeni glasnik, 86/2011). Also, their jurisdictions are laws and regulations in this field, as well as strategy for increasing resilience of critical infrastructures. In 2012, Gospić et al. summarized critical infrastructures in information and communications, electric power, transportation, oil & gas, banking and finance, water & emergency services, and government (Gospić et al., 2012, pp.51-59). Moreover, the authors refer to the standards in risk management which are also the scope of this work.

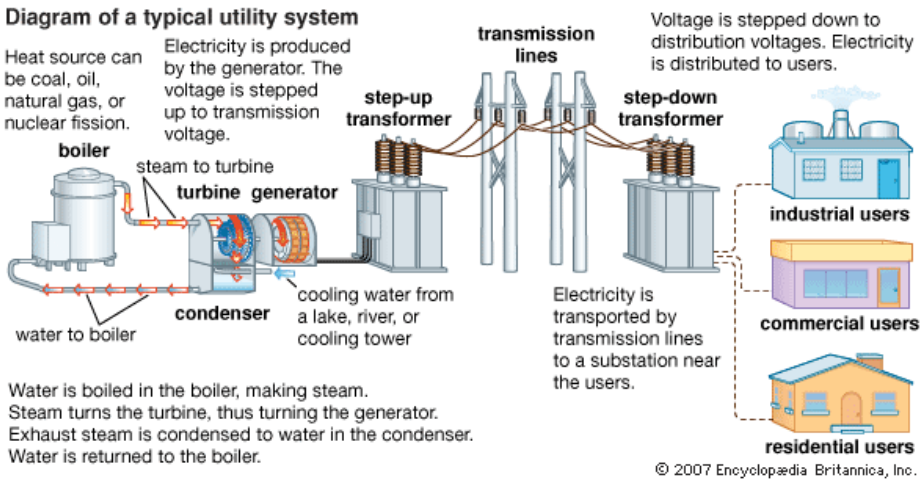
In accordance with the literature rewiev and the good practice, six critical infrastructure sectors are presented here, respectively: (1) electric power systems, (2) energy sources and supply, (3) manufacturing, transport and storage of hazardous substances, (4) traffic and transportation, (5) information-telecommunications infrastructure, and (6) supply with basic viands (NIPP, 2013). Threats, vulnerabilities and protection of these infrastructure sectors are shown in the following text, respectively. The last chapter concludes the paper.

Electric power systems

Electric power systems belong to the world's most complex man-made systems. Power generation, long-distance transmission lines and local distribution systems must all work together to deliver electricity to a range of users (https://mitei.mit.edu/). Electrical power outages significantly affect society and economy, causing cascading effects. Protecting this critical infrastructure implies the preservation of its basic functions in a way that is consistent with appropriate risk assessments, which are carried out in several phases. First, the sources of risks are examined. They may be technical or mechanical, natural disasters, human errors, and the like. Then, the following impacts of accident are estimated: 1) rapidity (constant, slow, fast speed), 2) duration (intermittent, continuous), 3) spread effects (local, national, global), 4) frequency (event happens frequently, sometimes, again), 5) reliability (deterministic, heuristic, unknown), etc. The protection is carried out at power sources, generators, transmission lines, distribution systems, information and communication systems, etc. Protective equipment is used, as well as mechanisms for switching electrical circuits, protective relays, protective chambers and SCADA (Supervisory Control and Data Acquisition) systems, for generator monitoring, whereas consoles which monitor production no longer have to be in the vicinity of the manufacturing plant (Inductive automation, 2016). The problem that arises is a cyber-attack.

Production and distribution of electrical energy

Electrical energy is generated by production plants where the primary source of energy is converted into electrical energy. Conventional power plants can be hydro, thermal and nuclear power plants (Rajković, Kukulj, 2011). Hydroelectric energy is converted by hydraulic turbine coupled with a generator. In a thermal power plant, fuel is burned in steam boilers in which high-pressure steam is produced. A steam turbine converts steam into mechanical energy. A nuclear power plant consists of a nuclear reactor which generates heat by nuclear fission of uranium. Heat passes to liquid carbon dioxide, water or sodium. Processes that follow are similar to those in thermal power plants. Figure 1 gives a diagram of a typical system for the generation, transmission and distribution of electrical energy from power plants to industrial, commercial and residential users, i.e. consumers (www.kids.eb.com).



Picture 1 – Production and distribution of electrical energy
Рис. 1 – Производство и распределение электрической энергии
Slika 1 – Proizvodnja i distribucija električne energije

Electric power networks consist of a distribution system that includes low-, medium-, and high-voltage networks, substations, information and telecommunication systems, and other energy facilities for maintenance and management of the network and equipment.

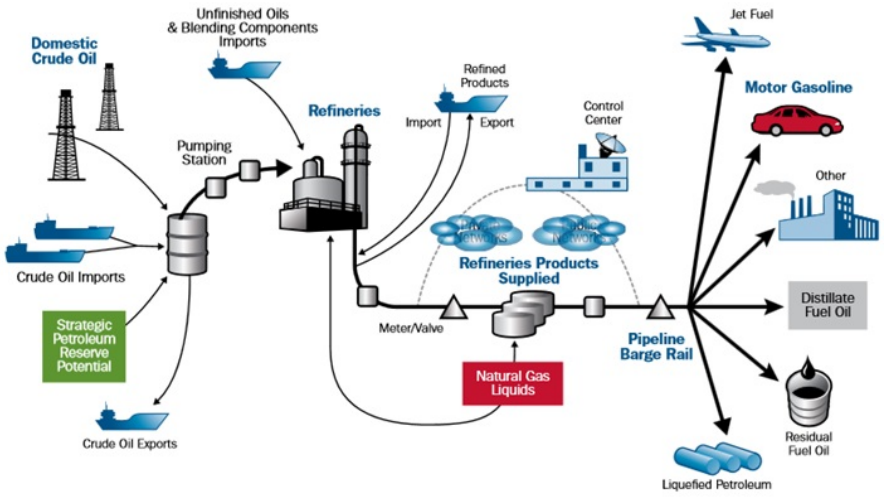
Safety in the production and distribution of electrical energy is based on the resilient system and surveillance, guard, duplication of the most important equipment, because the outage of any part of the system may cause long-term losses and consequences on health and environment. Losses can be (1) related to the IT sector, (2) material (3) destruction of equipment, (4) various damage in urban areas, etc.

Renewable energy

Hydropower, wind, solar energy, biomass energy and geothermal energy are all renewable energy sources (Jovanović, 2013). In contrast to energy sources such as coal, oil, or gas that pollute environment and cause the greenhouse effect, renewable energy sources are inexhaustible and do not pollute the environment. Protection of renewable sources is identical to the principles of the protection of other energy power systems (physical security, monitoring, SCADA). Special attention is paid to possible damage of pipelines for hot water in urban areas.

Energy sources and supply

Energetic stability is a subject of growing global concern because a large number of countries do not have their own sources to ensure energy independence (Kolev, 2013, pp.31). Instead, they often rely on energy sources located in other countries, which are often away and sometimes unstable. Today, considering complicated modern energy security challenges, decision-makers of every state should first learn scientific approaches to the new field of protection in energy policies in order to be able to deeply understand the national-level cooperation on economic, political, infrastructure and military aspects. In this regard, energy planners are responsible for critical energy infrastructures regarding the protection of energy facilities and infrastructures in state territories (see Figure 2), involving measures oriented to prevent damage and restore safe and reliable energy supply sources under the best conditions. (Hazard strateji enstitutsu, 2014).



Picture 2 – Energy sources and supply chains
Рис. 2 – Энергоисточники и сети истемы снабжения
Slika 2 – Izvori energije i lanci snabdevanja

Measures and actions taken in order to achieve a reliable and safe energy supply, qualitative distribution of electricity, environment projects, cooperation with other countries, market development, etc. represent the energy policy of any state and are preventive measures for protection. Three paragraphs that follow describe the protection of gas supply, oil and petroleum product supply and supply of solid fuels, respectively.

Gas supply

From an economic and ecological point of view - gas is the most acceptable energy source. It is produced by dry distillation of coal, by-products of agricultural waste or by gaseous fuel from other gases by purification, or blending. Gas supply is a chain that consists of natural or synthetic gas production, pipelines and distribution network. In this chain, a big role is also given to dealers who organize the sale of gas through the distribution network to customers. Gas supply does not include the extraction of natural gas, coke ovens operation, manufacturing petroleum derivatives and technical fuel, and distribution of gaseous fuels through transport pipelines. Customers of natural gas, the facilities of which are connected to the distribution system and customers who buy small quantities of gas are entitled to public supply, and the rest of the customers buy gas from the licensed supplier (Agencija za energetiku RS, 2015).

To connect to a pipeline, one should have a house connector, a control/measurement set, gas installation and a consumption counter. Communal inspectorate, sanitary inspectorate and fire police are responsible for safety of gas distribution and gas supply. The very fact that these inspectorates exist clearly indicates the system with a high risk. The prevention measures needed for this system are the following: employees have to be familiar (or educated) with technical regulations, connectors and distribution network, they need to know protective measures against fire, first aid, etc.

Oil and petroleum products supply

In accordance with the objectives of energy policy, it is necessity to increase supply of oil and petroleum products and thus facilitate development of a competitive market, which encourage the development of economy and at the same time retain economic control in the transport via pipelines, and transport of derivatives through product pipelines. The overall structure of petroleum products is dominated by motor fuels (gasoline, diesel, jet fuel, liquid petroleum gas), fuel oil, etc. (Komisija za zaštitu konkurencije RS, 2012).

Facilities for oil and petroleum derivatives must be constructed to follow technical rules for manufacturing space, equipment, devices, storage, and sale. Protection is performed as follows: the fuel pump must have indoor and outdoor space, the surface must be built on solid materials (concrete, stone, asphalt), the space should be illuminated, and the pumping machine must be marked clearly and connected to the tanks for dispensing. Facilities for wholesale trade of oil must be fenced having tanks whose volume depends on the derivative.

Protić, D., Critical infrastructures: Threats, vulnerabilities and protection, pp. 812–837

Storage of oil, petroleum products and biofuels are in a direct relation with trade so economic entities engaged in this activity must have appropriate permissions to trade (Službeni glasnik RS, 57/2011). However, since the requirements for obtaining such licenses are rigorous in terms of security measures, this is the first line of defense against accidents, errors or malicious attacks on supply and storage.

Solid fuels supply

Solid fuels are used for electricity generation in thermal power plants, in agriculture, industry, heating plants, and in households as firewood (Marković, 2011). The combustion of solid fuels has one of the largest impacts on health and the environment. Solid fuels are a complex combination of chemical and biological substances so their combusting result in the emission of sulfur oxides, carbon monoxide, nitrogen oxide, flying particles of ashes, organic materials, gases, microelements, and halogens (fluorine and chlorine).

Large-scale fires are rare in solid fuels supply chain. Nevertheless, industry has to apply the prevention measures by training personal for fire protection, the first aid, handling combustible materials, maintenance of storages, and similar.

Manufacturing, transport and storage of hazardous substances

Critical infrastructure that consists of manufacturing, transportation and storage of dangerous, hazardous materials, is one of critical infrastructures that influence economy and relate to other critical infrastructures. One of the reasons is that hazardous materials, during manufacturing, transportation, storage or handling, can be extremely dangerous to the health and environment. On the other hand, hazardous substances are important and used on a daily basis in households, agriculture and industry. Depending on their chemical characteristics, their aggregate state, and a degree of hazard, dangerous substances are classified in 13 classes as follows: (1) Class 1 – explosives and objects with explosive materials, (2) Class 2 - gases, (3) Class 3 – flammable liquids, (4) Class 4.1 – flammable solids, self-reactive substances and de-sensitivity explosives, (5) Class 4.2 – substances liable to spontaneous combustion, (6) Class 4.3 – substances that emit flammable gases in contact with water, (7) Class 5.1 – oxidizing materials, (8) Class 5.2 – organic peroxides, (9) Class 6.1 – Toxic

materials, (10) Class 6.2 – infectious substances, (11) Class 7 – radioactive substances, (12) Class 8 - corrosive substances and (13) Class 9 – other dangerous substances (Zakon o prevozu opasnih materija, 2002). Chemicals are classified as elementary, special, agricultural, pharmaceutical and those for consumer usage (Službeni glasnik RS, 36/2009, 88/2010 and 92/2011).

Products of chemical industry are used as fertilizers, chlorine for water treatment, polymers for oil derivatives manufacturing, product for households, industry and many more. Considering the diversity of industry, it is very difficult to determine the profile of protection in general. Instead, risks are assessed for each production-consumption chain, due to the variety in manufacturing technology, design of products and relevant manufacturing processes. Vulnerabilities are related to: 1) terrorist attacks and the release of dangerous chemicals that could potentially endanger human lives, 2) chemical weapons or products that can be used as weapons, and 3) psychological effects of the consequences of accidents on the population. Threats can be natural disasters, caused by human factors, technical threats or malfunctions, disruption of electricity, and similar. Natural disasters can be earthquakes, eruptions, windstorms and hurricanes. Human accidental or intentional errors can be terrorism, cyber attacks, explosions, bombing, as well as traffic accidents, breakdowns, etc. Law, rules and standards regulate safety of manufacturing, usage and storage of hazardous materials in order to reduce the probability of accidents. Attacks on critical infrastructure, technical errors and malfunctions result in large pollution so it is extremely important to ensure all processes from manufacturing to consumption. Numerous raw materials, by-products and final products are carriers of risks in the manufacturing and handling hazardous substances. Accidents concerned with them cannot be predicted. For that reason, the necessity is education in areas related to a specific vulnerable system, hazardous substances, policies, standards and regulations. Additional education of personnel should be performed periodically during their professional engagement.

Production of hazardous substances

A large number of manufacturing plants which use various raw materials and products based on highly toxic chemicals are a serious threat to a broad territory, with unforeseeable consequences for people, environment and the economy, if an accident happens (Gaćeša, 2012, pp.312-315). For these reasons, production of hazardous substances has to be ensured from any occurrence of incidents. That is why manufacturing processes are separated one from another. (To prevent a

possible cascade effect that could affect other parts of the industry process.) For this purpose, a control system for monitoring and alerting can be very useful and important. Also, a major role in a crisis that arises from an unwanted event such as malfunction, technical errors, human error, or similar, is played by staff trained to react quickly to accidents (calling emergency services, fire fighting, first aid, etc). Panic in working with hazardous substances must be reduced to a minimum.

Transport of hazardous substances

One of the risks of handling hazardous substances is moving them from one place to another. Hazardous substances are transferred by roads, railways, waterways and through the air, in accordance with internationally agreed rules, recommendations and predefined procedures for carrying out safe transport (Služben glasnik SRJ, 15/1995, 28/1996 and 37/2002). Senders, carriers and recipients participate in the transport of hazardous materials and follow several steps: senders determine whether the substances are classified in accordance with standards and give information about them to carriers. Carriers must have permission to transport goods. In addition, they are obliged to use appropriate packaging for the transport and to ensure that empty packages are cleaned and properly marked. Carriers note that hazardous materials fulfill legislations, provide transport documents, visually inspect and check that everything is according to standard, note if all permits are valid, verifiy that a vehicle is not overloaded, etc. Recipients shall not postpone the receipt of goods without any particular reason and must confirm receipt of hazardous substances. They examine goods and documentation and provide unloading only if there were not failures in transport. Finally, they clean and decontaminate vehicles or containers. If there are changes in goods, the recipient can refuse reception.

Storage of hazardous substances

Warehousing of hazardous substances ensures maximum protection and minimum risks of serious injuries and damage to the environment (Službeni glasnik RS, 92/2010). Storage of hazardous materials is performed by qualified personnel, responsible and licensed for handling dangerous substances. The warehouse must be built in accordance with regulations, standards, technical requirements, government planning, and construction of warehouses. Access to the warehouse must be protected from accidents. The space for storage must meet requirements for humidity, temperature, air pressure and lighting. The warehouse must

be cleaned, while explosive and flammable materials must be arranged by type and kept at distance. Empty containers must be stacked according to the type and packed to be sealed with the proper lids, and resistant to the chemicals inside.

Traffic and transportation

Economy and quality of life depend on traffic and transportation systems that function well. Traffic and transportation connect people to jobs, family, medical care, education, and goods needed for everyday life. As with other major critical infrastructures such as water or electricity supply, the importance of traffic and transportation systems become apparent only when problems arise (Transportation Research Board, 2005). Maintenance and protection of this critical infrastructure is one of the key prerequisites for achieving sustainable economic and social development.

Although the terms traffic and transportation are often used interchangeably, in essence they do not have the same meaning. Transportation is a commercial service activity were goods, passengers or energy are moved, conveyed or carried from one place to another. On the other hand, traffic is organized passage of people and vehicles along routes of transportation, which is the result of applied technology and transportation needs. It is a public service, which is tasked to meet the needs of society, i.e. traffic is broader term than transportation.

Traffic and transportation belong to critical infrastructure because of the function of connecting points/destinations, in order to transport people, goods, products, semi-products and derivatives, in a variety of transportation means. Roads, ports, railways, airports, power systems and telecommunications in traffic and transport are most vulnerable to physical damage. A significant part of this infrastructure is an information system for accessing and processing information, maintaining communication during transportation, accessing databases, positioning and other services vulnerable to cyber attacks.

Traffic and transportation networks

Traffic covers provision of transportation services of passengers and freight via roads and railways, waterways and air, as well as services on terminals, parking lots, covering storage and handling cargo. Transport refers to the land infrastructure (highways, bridges, tunnels, and viaducts), aviation (planes and other aircraft, air traffic control, airports, heliports, runaways), waterway infrastructure (coast, ports, waterways, intermodal terminals) and rail transport (highways, secondary active rails,

freight wagons, locomotives). In addition, postal transport is one of the essential parts of the transport system.

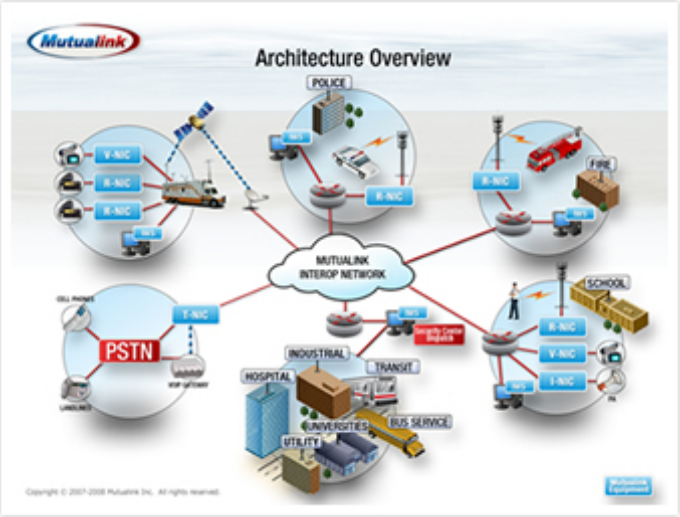
Bridges, viaducts and tunnels are assessed as high-risk infrastructure for transport. The protection is performed by building flexible bridges with embedded systems for flood and fire protection, help-lines, etc. Modern bridges are equipped with sensors for monitoring the structure to avoid a crisis if the sensors detect the vibrations of the cables, for example. Detectors can be accelerometers, strain gauges, anemometers, temperature sensors, etc. The same principles of protection apply to viaducts since they are bridges over the ground. Tunnel protection is mainly carried out in the process of planning, in accordance with standards for constructions and materials.

Airport operations rely on complex, bounded and stacked infrastructures. An airport is a part of aviation that includes aircraft, air-traffic control, commercial airports, additional airports, heliports, and landing strips. Aviation also includes civil and joint use military airports, heliports, short takeoff and landing ports and seaplane bases (Homeland Security). Four types of events are closely associated with the airport infrastructure: (1) a planned event, (2) an incident, (3) a disaster that causes a lot of damage, but can be managed with an appropriate assistance and (4) a large-scale disaster (catastrophe) that completely disables communities or regions in which it has appeared. Catastrophes can be caused by natural disasters (gale-force winds, floods, earthquakes, landslides, eruptions, wild fires, ice storms), accidents (falls, industrial accidents, infrastructure failures, mechanical failures, human errors), pandemics (SARS, biological weapons), unrests (riots, strikes, demonstrations, boycotts, sabotage), terrorism (explosives, hostages, kidnapping, cyber-crime), and the like. What is most important in protecting airports is to ensure continuity of operations in urgent situations (prevention, preparedness, mitigation, response to crisis, recovery from crisis and reconstruction). A quick reaction is the task of response teams; however, the structure of the airport, organization, management policies and defense must ensure normal functioning in an emergency as well.

Information and telecommunication infrastructure

Communications, energy, transportation, water supply and other critical infrastructures largely depend on computer networks whose functions of generation, processing, storage and data transmission are very vulnerable to malicious attacks that can extremely destabilize the

economy, jeopardize national security and disrupt the quality of daily life. Generating, processing, and exchanging information are now fast and efficient, which significantly reflects modern business and life in general. At the same time, all the benefits provided by development and implementation of new technologies have become a source of potential attacks on sensitive information that can be available to unauthorized users, modified, or destroyed. Figure 3 presents the architecture overview of the interoperable communications platform that links together police, fire, hospitals, schools, mails, and other community assets (www.mutualink.net, 2009). This platform is one of various tools for improving community safety and readiness.



Picture 3 – Mutualink platform
Рис. 3 – Мутуалинк платформа
Slika 3 – Mutualink platforma

The Mutualink is a comunity wide inter-operable multimedia platform which links together two-way radios, telephones, and public address systems is such a way that video and data files can be shared among parties on a real-time incident basis, which enhances preparedness and effectiveness in an emergency.

Telecommunications network

A telecommunications network is a structure of computing telecommunication resources for communication and information between distant locations. Telecommunications networks include

terminals (for accessing the network), computers (that process information and are interconnected by the network), links (that form a channel through which information is transmitted from a sending device to a receiving device), telecommunications equipment (that facilitates the transmission of information), and telecommunications software (that controls message transmission over the network) (http://www.umsl.edu/).

Two principal types of telecommunications networks can be distinguished from the point of view of their geographical scope: Local Area Network (LAN) and Wide Area Network (WAN), each of them containing active equipment (switches, routers, PBX equipment, wireless communications, optical converters), and passive equipment (optical and copper cables, antennas, sockets). Telecommunications networks can be public, mobile, cable, hybrid, optical access networks, low voltage networks, etc (Vujić, Dukić, 2015). The first one is used between stationary terminal points. In a mobile network, terminal points are not at specific locations and the terminal-points connections are carried out via the radio. Cable networks are primarily designed for TV signals transmission to the terrain where the classic reception is not possible (a large number of users receive the same content). In the hybrid network, the access network is realized with coaxial cables, while fiber optic cables are used to connect the central hub and peripheral hubs. The optical network provides a broad access solution with transmission based on multiplexing. A low-voltage power network can be used as a telecommunications network in suburbs or villages, with approximately equal distribution of housing facilities throughout the territory, where substations must be close to each other. A low-voltage network is a poor transmission medium, having low bandwidth and high interference.

Telecommunications networks connect other critical infrastructures, so that any potential vulnerability of these networks is a threat to telecommunication networks and vice versa. Vulnerabilities occur at devices, network infrastructures, data content, etc. so combating threats requires a cooperation between manufacturers, operators, providers, suppliers, users and the state, which must be focused on the prevention and awareness of threats.

Information and communication system

The information and communication system consists of personnel, hardware, software, cable connections, wireless connections, power supply, and equipment. Each of the assets plays a role in maintaining transmission between users or between other systems. For that reason, processing and distribution of information have to be carried out in real

time, thus meeting the needs of users, business and public services, whose activities are related to the online communication.

The structure of the information and communication system indicates the vulnerability of a large number of elements that can be classified into: physical threats (architecture, hardware, power supply) and cyber threats (information processing, decision-support systems, and services). The information and communication system can be impacted by natural disasters (physical destruction), industrial accidents (construction collapse, fire), product or service failures (communication failure, data centre failure), public relations (unwelcome media attention, adverse publicity of media), business and management (hostile takeover, sudden strike, competitor launches new product), etc. It is impossible to protect information and communication systems from all threats. However, prevention of some accidents (before they happen) and response to them (after they occur) can be done. There are four steps to ensure business continuum: (1) planning (getting business in the best position to react to, and recover from, an emergency), (2) incident response (processes put in place to ensure that business reacts properly and orderly to an incident as it occurs), (3) accident management (coordination of responses to an incident that threatens to harm, or has harmed, people, structures, ability to operate valuables and reputation), (4) business continuity (restore system to normal functions) (Holman, Houser, 2011).

Absolute protection of information and communication systems is impossible to achieve, but it is possible to achieve a high level of security within a network, operating systems, applications, databases and procedures. For information and communication systems, security can be achieved by the CIA Triad (Confidentiality, Integrity, and Availability). Moreover, protection are authentication, accountability, access control, non-repudiation, intrusion-detection, Denial of Service, etc. (IBM, 2005). That provides access control, identity verification, encryption, confidentiality, etc.

Attacks to the information and communication infrastructure can be diverse: passive and active, internal (insider) or external, and similar. The most known attacks are (1) Denial of Service – the legitimate users are not allowed to use the network because of overloaded network services. This attack paralyzes the functions of the server, or a web site. The attack reduces bandwidth and damages information about configuration. The protection can be carried out by turning off some network services, back upping, etc. (2) Phishing is a form of fraud in which the attacker tries to learn information such as log in credential, or accounting information, by masquering as a reputable entity or person in e-mail, instant message, and other communication channels. A gateway e-mail

filter can trap many targeted phishing e-mails. A web security gateway can also provide another security layer by preventing users from reaching the target of malicious link. (3) Botnet is a collection of compromised computers often referred as zombies infected with malware that allows an attacker to control them. Botnet owners are able to control the machines in their botnet by means of covert channels such as Internet Relay Chat, issuing commands to perform malicious activities such as sending spam mail, and information theft. (4) Spam is an electronic version of junk mail. An unsolicited e-mail involves sending unwanted messages to a large number of recipients. To-do measures against spam are installing spam filtering/blockage software, deleting e-mails suspected as spam, reading e-mails in plain text, keep software and security patches up-to-date, etc. (5) Sniffing and spoofing refer to listening to a conversation. Sniffer is an application that can capture network packets using a sniffer. Once the packet is captured, the contents of packets can be analyzed. Sniffers are used by hackers to capture sensitive information such as passwords, account information, etc. The attacker can follow the path until he finds the switch to which he is connected. From there, the attacker can enable a monitor port as the port to which he is connected. Switch security is the first line of network security from internal hacking. Switch security is the path attackers must go through to get to the rest of the network (Tetz, 2015). Spoofing refers to actively introducing network traffic pretending to be someone else. It is typically used in a scenario where one generates network packets that say they originated by computer A while they are really originated by computer B. (6) Malicious software (malwer) is any software that gives partial to full control of one's computer to do whatever malware creator wants. Malwares are categorized as viruses, worms, trojans, and backdoors. Adware and spyware seek to embed themselves to watch what the user does, and act upon that data. Root kits seek to give full access of one's machine to the attacker to do what they want (http://www.seas.ucla.edu).

Supply with basic viands

Supply with basic viands has critical dependencies with transportation systems, energy sector, water systems, chemical and dams. This critical infrastructure comprises manufacturing, processing and delivery systems,which consist of farms, restaurants, warehouses, etc. Critical infrastructure of basic viands supply consists of two sub-structures. One supplies people with water and the other one supplies them with food. These two infrastructures are described in the chapters that follow.

Water supply

Water supply and quality of drinking water are indicators of population's health, thus confirming their important role in daily life. Changes in water supply cause discomfort and anxiety in people, reduce hygiene and affect life and economy in general. Consequently, water supply is a critical infrastructure. The sector of water supply is sensitive to a number of possible attacks including contaminations, physical attacks, or release of toxic gases. The results of attacks are sick or dead people, and disabled services such as fire fighting, working of hospitals, storage of meat products, etc.

Water supply is a complex system that consists of hydraulic structures, i.e. (1) wells (water supply systems that have water reservoir and water distribution and fountains), (2) systems for raw water transportation, (3) water treatment plants, and (4) distribution networks consisting of tunnels for primary transport, water supply networks, pumping stations and reservoirs.

The protection is carried out through prevention, control and maintenance. Water used for public supply must be safe to drink, according to the predescribed standards, recommendations and directives, which are mandatory in the country. Water quality is determined by inspection of physical, chemical and microbiological parameters. During each inspection, data is taken from (1) sources (2) reservoirs, and (3) distribution networks. Principles of risk assessment are monitoring and reporting on water pollution indicators. Pollution is a chemical, physical or biological change in water that has a negative impact on people and/or environment. Water pollutants can be concentrated facilities such as urban areas, industrial facilities, landfills, or can be spread out such as land with pesticides and fertilizers, or dumps.

Food suply

Production, distribution, storage, and supply with food is one of the most critical infrastructures that depends on many other critical infrastructures, such as production and distribution of water, transportation, energy, chemicals' supply and others. Bases of this critical infrastructure are (1) acquisition of raw materials, cultivation of crops and livestock (2) manufacturing, processing and packaging of food, (3) storage, and (4) transportation and distribution of products.

The protection is implemented in the food supply chains for livestock and livestock food, in vegetable production chains (seeds, fertilizers), and in other parts of infrastructure for manufacturing, storage and distribution of

food. The focus of food safety is to protect the food supply from chemical, biological, radiological and other contamination. Deliberated actions on the food supply chain are unpredictable but accidental contamination can be prevented or early detected to minimize the consequences of an accident.

Conclusion

Critical infrastructures have a significant role in national strategies of many countries, which increasingly intensifies efforts in protection of these vulnerable systems. Strategies for the protection of critical infrastructures have become strategies of sustainability of government, economic stability, prosperity, industry, public health and environment. In the last two decades, the most important critical infrastructures were electric power systems, transportation, water and food supply, agriculture, and vital industrial plants. In the modern world, information and telecommunications technology, mass media, banking and finance, and the environment have also become critical infrastructures.

Each state determines its own critical infrastructures in accordance with the requirements of its national policy. Unions, such as the EU, have certain criteria for the Union, while each state is free to estimate their critical infrastructures. Results from practice show that the most known critical infrastructures are electric power systems, energy supply, manufacturing, transport and storage of hazardous substances, traffic and transport, information and telecommunication infrastructure and the supply of basic viands, described in this paper.

Depending on the type of infrastructure, threats to critical infrastructures can be classified into two groups: physical threats, and cyber attacks. Pipelines, substations, warehouses, communications infrastructure and industrial plants are mostly exposed to physical threats. Cyber threats jeopardize systems for monitoring and control, databases, operating systems, software, automated production facilities, and the like.

Vulnerabilities of critical infrastructures are determined by their functions. Generators, distribution networks and information and telecommunication networks are vulnerabilities of electrical power systems. In energy sources and distribution networks, these are gas and oil pipelines, manufacturing and warehouses. In the production and treatment of hazardous substances, vulnerabilities are products as well as transportation and storage of substances. In traffic and transportation, the most vulnerable structures are airports, bridges and tunnels. Physical infrastructure is one of the two vulnerabilities in the information and telecommunication systems. The other one is related to the communications. Manufacturing, supply and storage of food and water are vulnerabilities of viands.

Protection of critical infrastructures has to be carried out for each infrastructure depending on its threats and vulnerabilities. It is necessary to protect all parts of the critical infrastructure considering various functions and physical infrastructure. It is essential that a risk is assessed and that all employees are well trained. Physical protection of systems is performed by fencing, guarding, blockades, or separation of production processes because of the domino effect. Protection against cyber attacks is important in infrastructure components which are controlled by computer networks, connected to the Internet, or based on automated production processes.

References

Agencija za energetiku Republike Srbije. . *Tržište energije. Prirodni gas*. Retrieved from http://www.aers.rs/Index.asp?l=1&a=42&tp=TEG 2016 Jan 5.

Commission of the European communities. 2006. *Communications from the Commission on a Europe Programme for Critical Infrastructure Protection*.Brussels: Commission of the European communities.

Gaćeša, N. 2012. Prikaz monografije "Opasne materije" autora Vlade Radića. *Vojnotehnički glasnik/Military Technical Courier,* 60(1), pp.312-315.

Gospić, N., Murić, G., & Bogojević, D. 2012. Managing critical infrastructure for sustainable development in the telecommunications sector in the Republic of Serbia. *E-society Journal,* 51.

Holman, E., & Houser, K. 2011. *Managing a Disaster: Getting Started with IT Crisis Management and Emergency Response Teams, IBM, SHARE in Orlando*. Session 10388..

Introduction to z/OS Security 2005. IBM Corporation.

Jovanović, B.. *Obnovljivi izvori energije*. Retrieved from http://www.raris.org/download/Prezentacija_Okrugli%20sto_%20Obnovljivi%20izvori%20energije.pdf 2016 Jan 4.

Kljajić, Z., Mandžuka, S., & Škorput, P. 2010. Primjena ICT-a u upravljanju kritičnom infrastrukturom u tranzicijskom zemljama. *Telekomunikacioni forum TELFOR,* 18, pp.75-78.

Kolev, D. 2013. Globalni aspekt energetske bezbednosti. *SVAROG,* 6, pp.18-31. DOI 107251/SVR1306018K.

Komisija za zaštitu konkurencije Republike Srbije. . *Izveštaj o sektorskoj analizi tržišta trgovine na veliko i trgovine na malo derivatima nafte u 2011. godini*. Retrieved from http://www.kzk.org.rs/kzk/wp-content/uploads/2013/02/Sektorska-analiza-trziste-nafte_2011-godina_ZA-SAJT.pdf 2016 Jan 5.

Lewis, G. 2006. *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*.New Jersey: John Wiley & Sons Inc..

Marković, D. 2011. *Procesna i energetska efikasnost*.Beograd: Univerzitet Singidunum.

NIPP. . *Partnering for Critical Infrastructure Security and Resilience*. Retrieved from http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf 2015 Dec 15.

Official web site of the Department of Homeland Security, Transportation System Sector. Retrieved from http://www.dhs.gov/transportation-systems-sector 2016 Jan 5.

Official web site of the Department of Homeland Security, Food and Agriculture Sector. Retrieved from http://www.dhs.gov/food-and-agriculture-sector 2016 Jan 8.

O'Neil, M.J., & Dempsey, J.X. 2000. Critical infrastructure protection: Threats to privacy and other civil liberties and concerns with government mandates or industry. *Depaul Business Law Journal,* 12, pp.97.

Protić, D. 2012. Strategija razvoja informacionog društva u Republici Srbiji do 2020. godine - bezbednost i kritična infrastruktura. *Vojnotehnički glasnik/Military Technical Courier,* 60(4), pp.82-101.

Rajković, D., & Kukulj, N. 2011. *Proizvodnja i pretvorba energije*.Rudarsko-geološki-naftni fakultet, Sveučilište Zagreb.

Službeni glasnik RS, 92/2010, Pravilnik o načinu skladištenja, pakovanja i obeležavanja opasnog otpada. JP „Službeni glasnik“, Beograd.

Službeni glasnik RS, 86/2011. Nacionalna strategija zaštite i spasavanja u vanrednim situacijama. JP „Službeni glasnik“, Beograd.

Službeni glasnik RS, 57/2011. Zakon o energetici. JP „Službeni glasnik“, Beograd.

Službeni glasnik RS, 36/2009, 88/2010, 92/2011. Zakon o hemikalijama. JP „Službeni glasnik“, Beograd.

Službeni list SRJ, 15/95, 28/96, 37/2002. Zakon o proizvodnji i prometu opasnih materija. JP „Službeni glasnik“, Beograd.

Tetz, E.. *Common Network Attack Strategies: Packet Sniffing*. Retrieved from http: //www. dummies. com/how-to/content/common-network-attack-strategies-packet-sniffing.html 2016 Jan 11.

Transportation Research Board. 2005. *Critical Issues in Transportation*. Retrieved from http://onlinepubs.trb.org/onlinepubs/general/CriticalIssues06.pdf 2016 Jan 11.

Vujić, D., & Dukić, M. 2015. *Telekomunikacione pristupne mreže*. Retrieved from http://www.telfor.rs/telfor2002/radovi/2-7.pdf

Zakon o prevozu opasnih materija 2002. Retrieved from http://www.mup.gov.rs/domino/zakoni.nsf/Zakon%20o%20prevozu%20opasnih%20materija.pdf 2016 Jan 5.

Retrieved from https://mitei.mit.edu/research/innovations/electric-power-systems-policy 2016 Jan 11.

Retrieved from www.umsl.edu/~joshik/msis480/chapt07.htm 2016 Jan 6.

Retrieved from http://www.seas.ucla.edu 2016 Jan 11.

Retrieved from https://inductiveautomation.com/what-is-scada 2016 Jan 4. *What is SCADA* . Inductive automation.

КРИТИЧЕСКАЯ ИНФРАСТРУКТУРА:
УГРОЗЫ, УЯЗВИМОСТЬ И ЗАЩИТА

Даниела Д. Протич
Генеральный штаб Вооруженных сил Республики Сербия,
Управление информатики и телекоммуникаций (J-6),
Центр прикладной математики и электроники, Белград

ОБЛАСТЬ: электроника, телекоммуникации,
безопасность, транспорт
ТИП СТАТЬИ: обзорная статья
ЯЗЫК СТАТЬИ: английский

Резюме:

В данной работе приведены шесть видов критической инфраструктуры: электроэнергетические системы, сети распределения и снабжения энергоносителей, производство, сбыт, складирование и хранение опасных материалов, первозка и транспорт, информационно-телекоммуникационные сети, снабжение продуктами питания.

В статье также представлены источники возникновения потенциальных аварий, чрезвычайных ситуаций, несчастных случаев, технических ошибок, опасных природных явлений и влияние человеческого фактора. Подробно описаны мероприятия по предотвращению и профилактике приведенных рисков.

Ключевые слова: *транспорт, защита, уязвимость, угроза, критическая инфраструктура, случай, риски.*

KRITIČNE INFRASTRUKTURE: PRETNJE, RANJIVOSTI I ZAŠTITA

Danijela D. Protić
Generalštab Vojske Srbije, Uprava za telekomunikacije i informatiku (J-6),
Centar za primenjenu matematiku i elektroniku, Beograd, Republika Srbija

OBLAST: elektronika, telekomunikacije, bezbednost, saobraćaj
VRSTA ČLANKA: pregledni članak
JEZIK ČLANKA: engleski

Sažetak:

U radu je prikazano šest kritičnih infrastruktura: elektroenergetski sistemi, mreža distribucije i snabdevanje energentima, proizvodnja, promet i skladištenje opasnih materija, saobraćaj i transport; informaciono-telekomunikaciona infrastruktura i snabdevanje osnovnim životnim namirnicama. Prikazani su izvori mogućih neželjenih događaja usled nezgoda, nesreća, tehničkih grešaka, kvarova, prirodnih nepogoda i uticaja ljudskog faktora. Detaljno su objašnjene prevencija i predikcija ovih događaja.

Uvod

Kritične infrastrukture su toliko važne da njihova destrukcija ili zaustavljanje rada može imati ogromne posledice po nacionalnu bezbednost, ekonomiju, životnu sredinu i ljude. Kritična infrastruktura odnosi se na sredstva, sisteme, komunikacione mreže, procese i lance snabdevanja koji, ukoliko su uništeni ili privremeno onesposobljeni za rad, mogu znatno da utiču na dobro stanje nacije. Prekid rada kritične infrastrukture može da rezultira ogromnim gubicima života, da ima različite ekonomske efekte, itd.

Zaštita kritične infrastrukture uključuje programe i aktivnosti vlade, regulatornih tela, naučnih institucija, korisnika i vlasnika, kako bi se smanjila

Protić, D., Critical infrastructures: Threats, vulnerabilities and protection, pp. 812–837

ranjivost usled neželjenog događaja. Ona, takođe, uključuje krizni menadžment za podizanje otpornosti kritične infrastrukture. Evropska unija usvojila je akcioni plan zaštite koji je baziran na prevenciji pojave incidenata koji mogu da naruše bezbednost kritične infrastrukture, detekciji i odgovoru na krizu i međunarodnoj saradnji. Kritične infrastrukture u EU su delatnosti, mreže, usluge, materijalna dobra i informacione tehnologije čiji bi kvar ili uništenje znatno uticao na zdravlje, ekonomski prosperitet i ekonomiju vlada država članica. Nacionalne kritične infrastrukture su sistemi, mreže i objekti od nacionalnog značaja koji mogu imati uticaj i ozbiljne posledice na zdravlje i živote ljudi i ekonomsku stabilnost država članica. U Velikoj Britaniji, Švedskoj, Holandiji i Švajcarskoj primarne infrastrukture su telekomunikacije, u Nemačkoj je dodata i komunikaciona infrastruktura, koja važi i za Australiju i Kanadu koje su uključile i masmedije. Kritične infrastrukture u SAD su elektroenergetski sistemi, telekomunikacije, skladištenje nafte i gasa, bankarstvo i finansije, prevoz, sistem snabdevanja vodom, hitne službe, kontinuitet vlasti, informacije i komunikacije.

U skladu sa navedenim, kao i principima dobre prakse, u ovom radu su prikazane sledeće kritične infrastrukture: elektroenergetski sistemi, mreža distribucije i snabdevanje energentima, proizvodnja, promet i skladištenje opasnih materija, saobraćaj i transport, informaciono-telekomunikaciona infrastruktura i snabdevanje osnovnim životnim namirnicama.

Elektroenergetski sistemi

Elektroenergetski sistem jedan je od najkompleksnijih svetskih sistema. Napajanje električnom energijom utiče na društvo i ekonomiju i izaziva domino efekat, ukoliko dođe do prekida napajanja. Zaštita ove kritične infrastrukture podrazumeva zaštitu njenih funkcija od fizičkih i elektronskih pretnji, na način koji je u skladu sa odgovarajućim procenama rizika. Prvo se proveravaju izvori rizika koji mogu biti tehnički, prirodni ili izazvani ljudskim faktorom, a zatim se proverava uticaj mogućeg rizika na funkcionisanje elektroenergetskog sistema. Za zaštitu se koriste uređaji da se spreče oštećenja u slučaju kvarova, mehanizmi za prekid rada električnih kola, zaštitni releji, zaštitne komore i veliki sistemi tipa SCADA.

Električna energija nastaje u hidroelektranama,,termoelektranama ili nuklearnim elektranama. Mreže za proizvodnju električne energije sastoje se od distributivnog sistema, podstanica, informaciono-telekomunikacionog sistema i drugih sistema i opreme potrebnih za održavanje elektroenergetskog sistema. Bezbednost u proizvodnji i distribuciji električne energije bazira se na primeni otpornog sistema, uz kombinaciju aktivnih i pasivnih mera bezbednosti.

Snaga vode, vetar, Sunčeva energija, biomasa i geotermalna energija takođe mogu da proizvedu električnu energiju, s tim što su to obnovljivi izvori energije, koji ne zagađuju okolinu i ne izazivaju efekat staklene bašte.

Izvori energije i snabdevanje

Energetski stabilnost je tema rastuće svetske zabrinutosti, jer veliki broj država nema svoje izvore energije već energetsku stabilnost obezbeđuje iz drugih država koje su često na nestabilnim područjima.

Ekonomski i ekološki najprihvatljiviji energent je gas. Gasovodi i snabdevanje gasom obuhvataju proizvodnju i distribuciju gasa distributivnom mrežom do potrošača, uključujući prodavce i posrednike, a isključujući vađenje zemnog gasa, rad koksnih peći, proizvodnju derivata nafte, itd. Za priključenje na gasovod potrebni su kućni priključak, mernoregulacioni set, instalacija u objektu, gasno trošilo i gasno brojilo. Za nadležnosti su odgovorne komunalna i sanitarna inspekcija, i protivpožarna policija. Ove službe su elementi preventivnih mera, uz striktno poštovanje tehničkih propisa za izgradnju gasovoda, razvodnih i distributivnih mreža i kućnih priključaka.

U ukupnoj strukturi proizvodnje naftnih derivata dominira proizvodnja motornih goriva, lož-ulja, i dr. U objektima za trgovinu naftom i naftnim derivatima neophodno je poštovati minimalne tehničke uslove u pogledu prostora, opreme, uređaja i načina prodaje. Zaštita se izvodi na sledeći način: stanica za snabdevanje mora imati zatvoren i otvoren deo, podloga mora da bude izgrađena od čvrstih materijala, prostor dobro osvetljen, a pumpni automati jasno obeleženi i povezani sa rezervoarima za istakanje. Skladištenje nafte, derivata i biogoriva u direktnoj je vezi sa trgovinom, pa privredni subjekti koji se bave ovom delatnošću moraju posedovati odgovarajuće licence. Uslovi za dobijanje licenci su rigorozni u pogledu mera bezbednosti.

Čvrsta goriva koriste se za proizvodnju električne energije u termoelektranama, poljoprivredi, industriji, toplanama, za grejanje i u domaćinstvima kao ogrevno gorivo. Sagorevajne čvrstih goriva ima veliki uticaj na život i zdravlje ljudi i životnu sredinu. Sagorevanjem se u atmosferu izbacuju opasne materije kao što su oksidi sumpora i azota, ugljen-monoksid, leteći pepeo, organske materije i drugi elementi koji izazivaju efekat staklene bašte. Zaštitu od požara u industriji čine poštovanje procedura i obučavanje personala koji radi na utovaru, transportu, istovaru i skladištenju čvrstih goriva.

Proizvodnja, promet i skladištenje opasnih materija

Kritična infrastruktura koju čine hemijska industrija i proizvodnja i tretman opasnih materija deo su svake nacionalne ekonomije i prožimaju druge kritične infrastrukture. Opasne materije u toku proizvodnje, transporta, skladištenja i rukovanja mogu da budu opasne po zdravlje i životnu sredinu. U zavisnosti od hemijskih osobina, agregatnog stanja i stepena opasnosti opasne materije su grupisane u devet klasa (eksplozivne materije, gasovi, zapaljive tečnosti, čvrste materije, samoreagujuće materije i čvrsti desenzitivisani eksplozivi, materije sklone samozapaljenju i one koje u dodiru sa vodom emituju zapaljive agense, oksidirajuće materije i organski peroksidi, otrovne, infektivne, radioaktivne materije, korozivne materije i ostale opasne materije i predmeti). Rezultat proizvoda hemijske industrije jeste osnov drugih privrednih grana i mogu biti đubriva, hlor, itd. Problemi u hemijskoj industriji mogu izazvati velika zagađenja životne sredine, pa je bitno osigurati svaki proces od proizvodnje opasnih materija do njihove potrošnje. Pretnje i ranjivosti ovih sistema vezani su za potencijalne terorističke napade, hemijsko oružje ili proizvode koji mogu biti korišćeni kao oružje i dr.

Jedan od segmenata rizika od neželjenih događaja pri rukovanju opasnim materijama jeste i njihov transport. Opasne materije transportuju se i prevoze drumskim, železničkim, plovnim i vazdušnim putem, a za svaki tip transporta važe pravila za sprečavanje akcidenata. Postoje regulative koje moraju da zadovolje pošiljalac, prevoznik i primalac.

Skladištenje opasnih materija vrši se na način na koji se obezbeđuje maksimalna zaštita i najmanji rizik od povreda i ugrožavanja životne sredine, u skladu sa zakonom i propisima. Obavljaju ga kvalifikovana lica odgovorna za postupanje sa opasnim materijama. Skladište mora biti izgrađeno u skladu sa planovima, a prostor za skladištenje mora da ispunjava zahteve koji se odnose na vlažnost, temperaturu, vazdušni pritisak i osvetljenje.

Saobraćaj i transport

Ekonomija i kvalitet života zavise od saobraćaja i transporta. Kao i kod drugih kritičnih infrastruktura, kao što su snabdevanje vodom ili električnom energijom, značaj saobraćaja i transporta uočljiv je tek kad do problema dođe. Održavanje i zaštita ove kritične infrastrukture jedan je od ključnih preduslova za ostvarivanje privrednog i društvenog razvoja. Saobraćaj je privredno-uslužna delatnost u okviru koje se prevoze roba, putnici ili energija, u određenom intervalu između zadatih tačaka – destinacija. Transport je, na drugoj strani, organizovano kretanje prevoznih jedinica po zadatoj ruti. To je javna služba koja ima zadatak da zadovoljava potrebe društva. Saobraćaj je širi pojam od transporta.

Saobraćaj obuhvata pružanje usluga prevoza putnika i tereta u drumskom i železničkom prevozu, u prevozu plovnim putevima i vazdušnim putem, kao i pružanje usluga na terminalima i parkinzima, kao i skladištenje i manipulisanje teretom. Transportni deo kritične infrastrukture sadrži kopnenu infrastrukturu, vazduhoplovstvo, plovnu infrastrukturu i infrastrukturu železnice. Jedan od bitnih elemenata ovog sistema je i poštanski transport.

Mostovi, vijadukti i tuneli su kritične tačke saobraćaja i transporta. Zaštita se izvodi izgradnjom elastičnih mostova, ugrađenim sigurnosnim sistemima, itd. Aerodrom je, takođe, visokorizična infrastruktura na koju mogu uticati prirodne nepogode, nesreće, pandemije, nemiri u državi, terorizam, rat i slično. Ono što je najbitnije u zaštiti aerodroma jeste da se obezbedi kontinuitet operacija u toku neželjenog događaja prevencijom, pripravnošću, odgovorom na krizu, ublažavanjem posledica krize, oporavkom i rekonstrukcijom. Brza reakcija na događaj je zadatak tima za brza dejstva koji treba da obezbedi normalno poslovanje na aerodromu.

Informaciono-telekomunikaciona infrastruktura

Komunikacije, energija, transport, vodosnabdevanje i druge kritične infrastrukture zavise od računarskih mreža koje su ranjive na maliciozne napade. Sve prednosti koje nudi savremena informaciona tehnologija istovremeno predstavljaju izvor potencijalnih napada.Telekomnikaciona mreža je skup resursa koji omogućuju prenos podataka na daljinu. Komponente telekomunikacione mreže su čvorovi, pristupna oprema i spojni

put, jezgro mreže i krajnji sistem i sistem za nadzor i upravljanje. Telekomunikacioni sistem čine hardver, softver, komunikacioni kanali i podsistemi za prenos podataka između lokacija. Sistem sadrži aktivnu opremu (svičevi, ruteri, centrale, oprema za bežičnu komunikaciju, optički konvertori) i pasivnu opremu (optički i bakarni kablovi, antene, utičnice).

Informaciono-komunikacioni sistem, koji čine personal, hardver, softver, žične i bežične mreže i prateća oprema, imaju svaki svoju ulogu u prenosu podataka i informacija između korisnika ili između drugih sistema. Struktura sistema ukazuje na dve grupe ranjivosti: fizičke pretnje po arhitekturu, hardver i napajanje i sajber ugroženost informacionih procesa i odlučivanja, sistema za podršku i usluge. Potpuna zaštita ovih sistema nije moguća, ali je dobro primeniti mere prevencije planiranjem, odgovorom na incidente, upravljanjem neželjenim događajima i kontinuitetom poslovanja. Štite se mrežni nivo, operativni sistemi, aplikacije, baze podataka i procedure. Kod komunikacije treba odrediti mere autentikacije, autorizacije, kriptozaštite, neporecivosti, itd. Napadi mogu biti pasivni ili aktivni, unutrašnji ili spoljašnji. Najpoznatiji su DoS, Phishing, Botnet, Spam, Sniffing, Spoofing i maliciozni softveri tipa virusa, crva ili trojanskog konja.

Snabdevanje stanovništva osnovnim životnim namirnicama

Snabdevanje osnovnim životnim namirnicama zavisi od transporta, energije, proizvoda hemijske industrije i slično. Čine ga proizvodnja i prerada prehrambenih proizvoda i stoke, farme, objekti za preradu i skladištenje hrane i vode.

Promena u snabdevanju stanovnika vodom izaziva prestanak rada privrede, zabrinutost građana, smanjenje higijenskih uslova i slično. Sektor vodovoda osetljiv je na niz mogućih napada kao što su kontaminacija smrtonosnim agensima, fizički napadi, ispuštanje toksičnih gasova i drugo. Rezultat napada su žrtve ili bolesni i prestanak bazičnih usluga tipa rada bolnica, pripreme i prerade hrane, itd. Vodovod je moguće zagaditi na četiri nivoa infrastrukture.To su: izvorišta, sistemi za transport sirove vode, postrojenja za prečišćavanje vode i distributivna mreža. Zaštita se izvodi prevencijom, kontrolom, održavanjem, izgradnjom nove i rekonstrukcijom postojeće distributivne mreže, održavanjem kvaliteta vode, itd. Kvalitet vode utvrđuje se pregledima inspekcije i utvrđivanjem mikrobioloških i fizičko-hemijskih faktora i pokazatelja.

Proizvodnja, distribucija, skladištenje i snabdevanje hranom je kritična infrastruktura čiju osnovu čine nabavka sirovina, gajenje poljoprivrednih kultura i stočnog fonda, proizvodnja, prerada i pakovanje, skladištenje i transport, kao i distribucija gotovih proizvoda ili poluproizvoda. Zaštita se izvodi u lancima snabdevanja hranom za životinje i proizvodima životinjskog porekla, biljnim proizvodnim lancima, i u onim komponentama infrastrukture koje podrazumevaju preradu, proizvodnju, pakovanje, skladištenje i maloprodajnu distribuciju. Fokus je u zaštiti uskladištene hrane od hemijske, biološke, radiološke ili nuklearne kontaminacije. Zaštita se izvodi analizom rizika, monitoringom i revizijom, uzorkovanjem, nadzorom nad prometom hrane, nadzorom u fazama proizvodnje, hitnim merama, itd.

Zaključak

Kritične infrastrukture imaju značajnu ulogu u nacionalnim strategijama mnogih država, pa se sve više pažnje posvećuje zaštiti ovih ranjivih sistema. Strategije zaštite kritičnih infrastruktura postale su strategije održivosti vlasti, ekonomske stabilnosti, prosperiteta, industrije, zdravlja stanovništva i zaštite životne sredine. Dve decenije najznačajnije kritične infrastrukture bile su elektroenergetski sistemi, prevoz, snabdevanje vodom i hranom, poljoprivreda i vitalna industrijska postrojenja. U savremenom svetu kritične infrastrukture su postale i informaciono-telekomunikacione tehnologije, masmediji, bankarstvo i finansije,kao i životna sredina.

Svaka država određuje svoje kritične infrastrukture u skladu sa zahtevima njene nacionalne politike. Zajednice država, kao što je EU, imaju određene kriterijume za zajednicu, dok svaka nacija može da proceni svoje kritične infrastrukture. Rezultati iz prakse pokazuju da su najčešće kritične infrastrukture elektroenergetski sistemi, izvori i snabdevanje energijom, proizvodnja, transport i skladištenje štetnih materija, saobraćaj i transport, informaciono-telekomunikaciona infrastruktura i snabdevanje osnovnim životnim namirnicama.

U zavisnosti od tipa infrastrukture, pretnje kritičnim infrastrukturama mogu se podeliti u dve grupe: fizičke pretnje i maliciozni (sajber) napadi. Fizičkim pretnjama izloženi su uglavnom cevovodi, podstanice, skladišta, komunikaciona infrastruktura i industrijska postrojenja za preradu vode. Sajber pretnjama ugroženi su sistemi za nadzor i upravljanje, baze podataka, operativni sistemi, softver, automatizovane proizvodne hale i slično.

Ranjivosti kritične infrastrukture određene su njenim funkcijama. Kod elektroenergetskog sistema ranjivi su generatori, distributivna mreža i informaciono-telekomunikacioni sistem. Kod izvora energije štite se gasovodi i naftovodi, proizvodni procesi i skladišta, a u proizvodnji i oblasti tretiranja opasnih materija štite se proizvodi, transport i skladišta. U saobraćaju i prevozu ranjivi su transportna mreža, posebno aerodromi, mostovi i tuneli. Informaciono- telekomunikacioni sistem ranjiv je na dva nivoa: fizičkom i nivou komunikacija, dok su u oblasti snabdevanja osnovnim životnim namirnicama ranjivi proizvodnja, snabdevanje i skladištenje poluproizvoda i proizvoda.

Zaštita kritičnih infrastruktura izvodi se u zavisnosti od pretnji i ranjivosti, za sve delove kritičnih infrastruktura ponaosob. Neophodno je da postoji procena rizika i da personal bude adekvatno edukovan. Fizička zaštita sistema izvodi se ograđivanjem, čuvarima, blokadama ili odvajanjem proizvodnih procesa zbog domino efekta. Zaštita od sajber napada je bitna u svim onim delovima infrastrukture koji su kontrolisani računarskom mrežom, povezani na internet ili su bazirani na automatizovanim proizvodnim procesima.

Ključne reči: *saobraćaj, zaštita, ranjivosti, pretnja, kritična infrastruktura, hazardi.*

Paper received on / Дата получения работы / Datum prijema članka: 14. 01. 2016.
Manuscript corrections submitted on / Дата получения исправленной версии работы / Datum dostavljanja ispravki rukopisa: 21. 02. 2016.
Paper accepted for publishing on / Дата окончательного согласования работы / Datum konačnog prihvatanja članka za objavljivanje: 23. 02. 2016.