INTERNATIONAL JOURNAL OF APPLIED MATHEMATICS AND INFORMATICS
DOI: 10.46300/91014.2021.15.8 Volume 15, 2021

Analysis of Cyber Networks in a System Concept

Dana Prochazkova, Jaroslav Srp, Jan Prochazka
Faculty of Transport Science
Czech Technical University
Konviktska 20, 110 00 Praha 1
Czech Republic
dr.prochazkova.dana@seznam.cz http://www.fd.cvut.cz

Received: March 12, 2019. Revised: April 28, 2021. Accepted: October 17, 2021. Published: November 16, 2021.

Abstract: - The aim of the paper is to show that all cyber networks (such as telecommunication, IT or ICT networks) are systemically identical or very similar, although each of them is applied in another industry or economy field or includes other added functional elements. The effort is to show that systemic identity (similarity) of the mentioned networks identifies the same set of network security threats that can be solved using the same approaches and techniques. The integrative approach based on the systematic approach enables to effectively use the efforts of professionals and all means target to the actual problem solving. The mentioned networks classification to the cyber critical infrastructures is also made based on this concept. Cyber system and cyber networks are threatened by both, the internal system deficits (technical and organisational nature) and the wide range of disasters: natural disasters - impacts primarily on the technical resources; intentional events caused by human vandalism, theft, terrorist attacks; technological accidents; and failure of electricity supply; etc. They threaten individual humans, human groups and states by their technical and organisational deficits and by the IT disuse.

Key-Words: - Cyber networks, Failures, Management, Security, Safety.

I. INTRODUCTION TO PROBLEM

The cyber infrastructure belongs to the critical infrastructure that is fundamental territorial system that ensures daily needs of humans and at critical situations is important for response, stabilisation of situation and for start of renovation and development [1-3]. As each other infrastructure it consists of objects and networks. It is basic for collection, analysis and spreading the information across the users of different nature. The structure of whole cyber system, i.e. interconnected information and communication systems has three basic parts: procedural structure; technical structure (hardware); and program structure (software). The individual parts are mutually interfaced, i.e. mutually dependent. Each section then has its function and its structure [4]. The performed inventory showed that for cyber network safety the following critical items must be followed: processes; data sets; software; hardware; operators; and documentation [4].

The disasters that caused damages in cyber system and its infrastructure have an origin in: technology and infrastructure of system itself (construction, reliability, function and operation, material, organisation etc.); external disasters (natural disasters, technological disasters as fire, explosion, contamination by hazardous substances, failure of other infrastructures as electrical networks, control of territory etc.); human factor (human failure / error); and in human intent (viruses, hacking, terrorist attacks etc.) [1,4,5]. Because the cyber system and cyber infrastructure are relatively new aspects, so for their safety there have not been unified system of norms and standards yet. According to good engineering practice principles each problem should be solved on several levels, Figure 1 [6,7].

The cyber networks create at present the basic functional pillar of majority of systems in different branches of national and international economy, Figure 2. They are not only the tool for communication and exchange of structured information but also the means with help of which there is realised governance of vitally important infrastructures, e.g. remote control of transformers, dams etc. It is the reality that through them there are realised mutual interactions of networks that can lead to cascade failures of critical infrastructure [3], Figure 3.

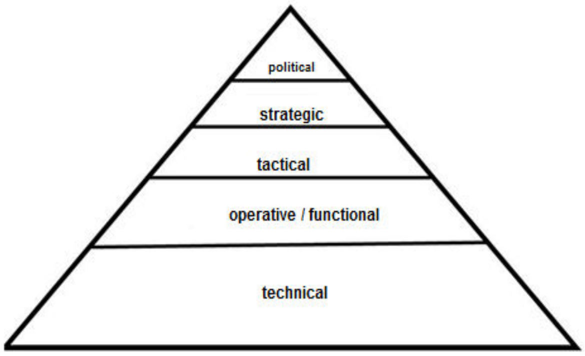

Figure 1: Levels on which security problems should be addressed [6,7]

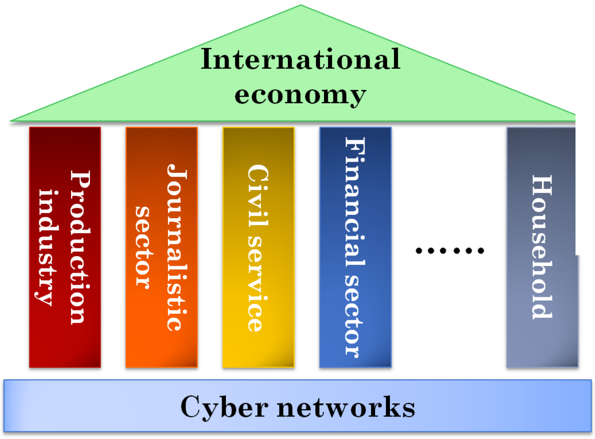

Figure 2: Cyber network value

In different economic sectors regarding to various use of appropriate cyber nets the followed networks have a different designation / label, as cyber networks, telecommunication networks, IT networks, ICT networks etc.

For cyber system safety the most important system properties are: vulnerability; resilience; adaptability to changes induced by internal and external disasters [7]. In management and engineering disciplines there are special tools by which we identify, analyse, asses, manage and trade of with risks of various kinds including cross-sectional ones. The paper tries to compile general cyber network by help of which we can govern risks of all kinds for goal that is cyber systems´ safety, i.e. to ensure the safe cyber systems´ themselves and their safe vicinity; at present we mostly concentrate to cyber system security (the assets outside of cyber systems are only marginally solved [4].

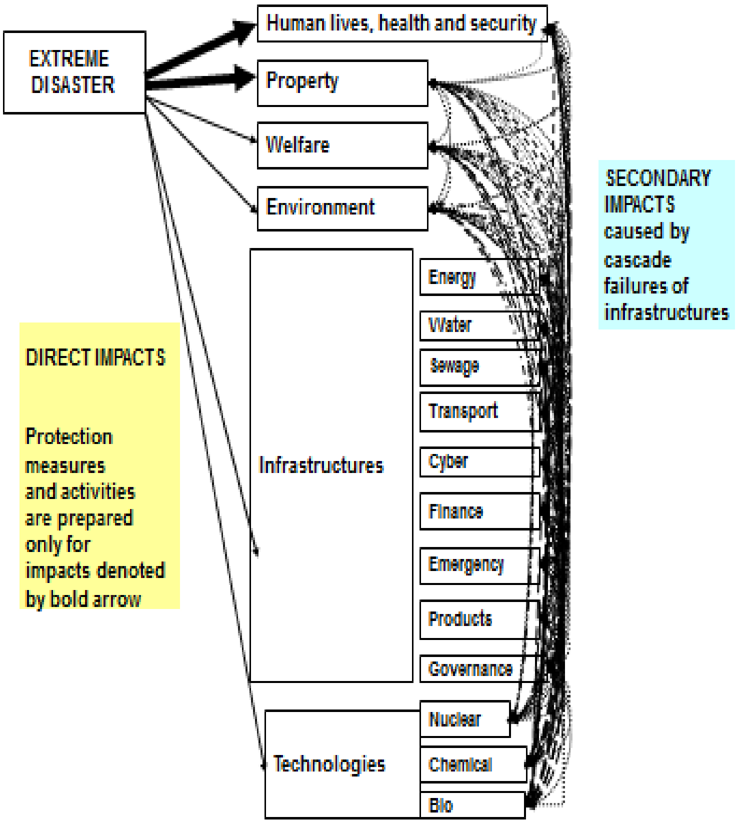
EXTREME DISASTER
Human lives, health and security
Property
Welfare
Environment
Infrastructures
Energy
Water
Sewage
Transport
Cyber
Finance
Emergency
Products
Governance
Technologies
Nuclear
Chemical
Bio
DIRECT IMPACTS
Protection measures and activities are prepared only for impacts denoted by bold arrow
SECONDARY IMPACTS caused by cascade failures of infrastructures

Figure 3: Impacts of extreme disaster on territory and infrastructures [4]

For cyber system safety the most important system properties are: vulnerability; resilience; adaptability to changes induced by internal and external disasters [7]. In management and engineering disciplines there are special tools by which we identify, analyse, asses, manage and trade of with risks of various kinds including cross-sectional ones. The paper tries to compile general cyber network by help of which we can govern risks of all kinds for goal that is cyber systems´ safety, i.e. to ensure the safe cyber systems´ themselves and their safe vicinity; at present we mostly concentrate to cyber system security (the assets outside of cyber systems are only marginally solved [4].

II. CYBER NETWORKS

ICT network includes three basic professional parts: information, communication and technological. Under the term "ICT" is real technological network solution to which it belongs both, the computer network realisation and the telecommunication technology in dependence of actual solved problem [8].

The typical representant of IT networks is the worldside Internet, the architecture of which is in

Figure 4. The Internet network architectute is on the top subsystems [10]: the subsystem of base stations (BSS) with base stations (BTS) to which there are level created by national providers of internet services (NAP) that have their routers interconnected by high speed links either through network access points (NAP) or directly, i.e. peer-to-peer connections. On regional and local level the internet services providers are individual ISP who for data transfers uses data networks of national providers. The end users are connected to Internet network interface on local levels (ISP).

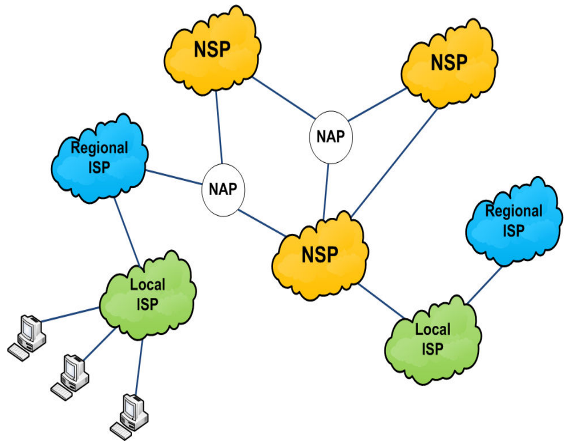

Figure 4: IT networks´ architecture [9]

The model of telecommunication networks could be the classic GMS network with localisation system, the scheme of which is in Figure 5 [10]. Generally, it is possible to note that telecommunication networks (GMS, GPRS, UMTS and others) are in principle created by two basic subsystems [10]: the subsystem of base stations (BSS) with base stations (BTS) to which there are interfaced the mobile devices and their control (BSC – Base Station Controller); and network subsytem - the basis of which is created by mobile switching centre of appropriate operator (MSC – Mobile services Switching Centre) with register of all participants of mobile operator (HLR) and on participants being just in the vicinity of a given switching centre (VLR) and with authenticity centre (AuC) and a register of mobile devices (EIR). The other components are real network solution specific.

The CESNET network is a national high speed computer network intended for science, research and education in the Czech Republic. Technological basis comes from the IT networks but it has its own infrastructure interconnecting the university cities with high speed connections.

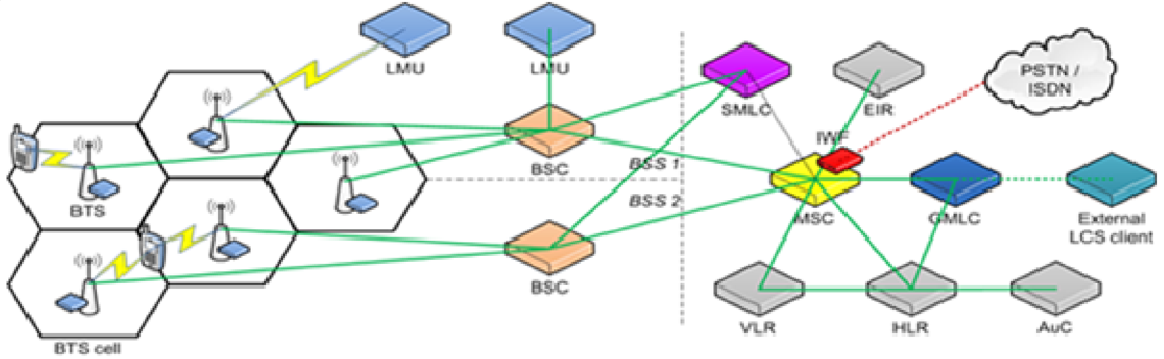

Figure 5: GMS model [10]

III. SYSTEM NETWORK MODEL

On the basis of present knowledge the infrastructures´ models are represented by model “System of Systems (SoS)” [7]. The SoS model allows to consider cross-sectional risks and internal dependencies and to understand the causes of domino effects, acceleration or synergis events etc.

Based on Bayessian theory the complex systems with executive and control part communicating one another by help of real communication channels there is possible according to work [12] to use the model of linkages in cyber system that is given in Figure 6.

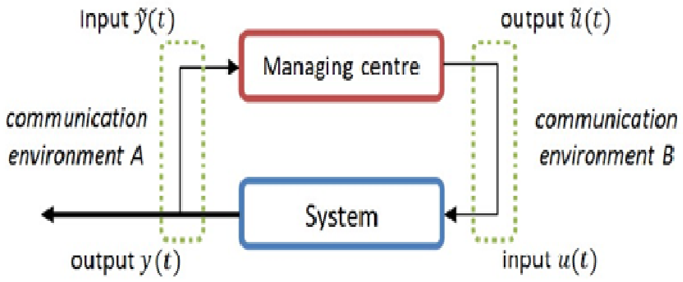

Figure 6: Relations in the cyber system [12]

The given model expresses in cyber network functionality the typical process in which the control $\widetilde{u}(t)$ influences the system functionality and at the same time, the outputs from the given system $y(t)$ retrospectively influence the given control. At the same time we consider an opportunity of modification (intentional or non-intentional) damage of transferred data when control $\widetilde{u}(t)$ is by transfer modified to control $u(t)$ and the system output $y(t)$ is modified to the system output $\widetilde{y}(t)$. From the model it follows that whole cyber system functionality is influenced by two main factors:

- correct behaviour of system, i.e. demanded system outputs in each time point of its operation, and corresponding system control, i.e. operating / control instructions that lead to correct system behaviour,
- correct transfer of data among cyber system components.

In next we concentrate to the transfer infrastructure of cyber systems, i.e. to the second mentioned item and the first one we assume as fulfilled.

The cyber networks are systems of organize set of bundles that create their logical elements that are mutually interfaced in compliance with a given order by selected physical layer. The suitable model is the Gauss transfer channel with one data input $x(t)$ and one output $y(t)$, Figure 7 [13].

$x(t)$
Transfer medium
$y(t)$

Figure 7: Gauss transfer channel[13]

The Bayesian theory (conditional probability density) is then to use for exact mathematical description of both, the individual communication channels and the whole cyber system [12,13], i.e. for:

- communication channel without memory (without regard to outputs in time smaller that point *t*) it is valid: $p(y(t)\,|\,x(t))$,
- communication channel with memory (e.g. for channel with backward control) it is valid: $p(y(t)\,|\,y(t-1), y(t-2),..., y(t-M), x(t))$ for data up to time point M round,
- cyber system described in Figure 6 with parameters $\Theta = \{\theta_1, \theta_2,..., \theta_N\}$ it is possible to derive the following relations:

- cyber system: $p(y(t)\,|\,y(t-1),..., y(t-M), u(t),..., u(t-M), \Theta)$
- control centre: $p(\widetilde{u}(t)\,|\,\widetilde{y}(t-1),..., \widetilde{y}(t-M), \widetilde{u}(t-1),..., \widetilde{u}(t-M))$
- communication medium A: $p(\widetilde{y}(t)\,|\,y(t)), p(y(t)\,|\,\widetilde{y}(t))$,
- communication medium B: $p(u(t)\,|\,\widetilde{u}(t)), p(\widetilde{u}(t)\,|\,u(t))$.

IV. GENERAL MODEL OF CYBER NETWORKS

For the IT networks it is typical that on lower hierarchy levels the system and its control is realised on the same logical bundle of network, and therefore, in this case we separate both parts. Contrary, the IT networks of higher hierarchy level usually act as their control centres (e.g. they create logic interfaces in network framework). The non-negligible element of IT networks is the human who adjusts the functional rules of given network. From the view of system and system control, the general model of IT network is shown in Figure 8. A lot of networks overlapping are the source of interdependences, i.e. cross-sectional risks which cause failure cascades.

The telecommunication networks have generally more centralized concept (it is a consequence of different historical development of two interconnected technologies, i.e. the telecommunication one and the information one), and therefore, the composition is more simple and it is given in Figure 9.

V. METHODS FOR STUDY OF CYBER NETWORKS

As we said above the present problems of cyber networks are interdependences that are connected with system architecture and the real impacts of various disasters on cyber networks and on other public assets [11]. The first task means usually the solution of non-structure problems, i.e. determination of critical items of cyber networks. For such case it is suitable the Analytical hierarchy process (AHP) method [14] by which we can solve tasks as: determination of cyber network structure; results for individual levels of network problem in selected hierarchy; and aggregate results for the whole. The other suitable methods are benchmarking, Ishikawa diagram, criticality matrix, responsibility matrix, the Delphi method, case study method, panel discussion, Petri nets, Bayesians

´nets, SWOT analysis, checklist analysis, FTA etc.

[5].

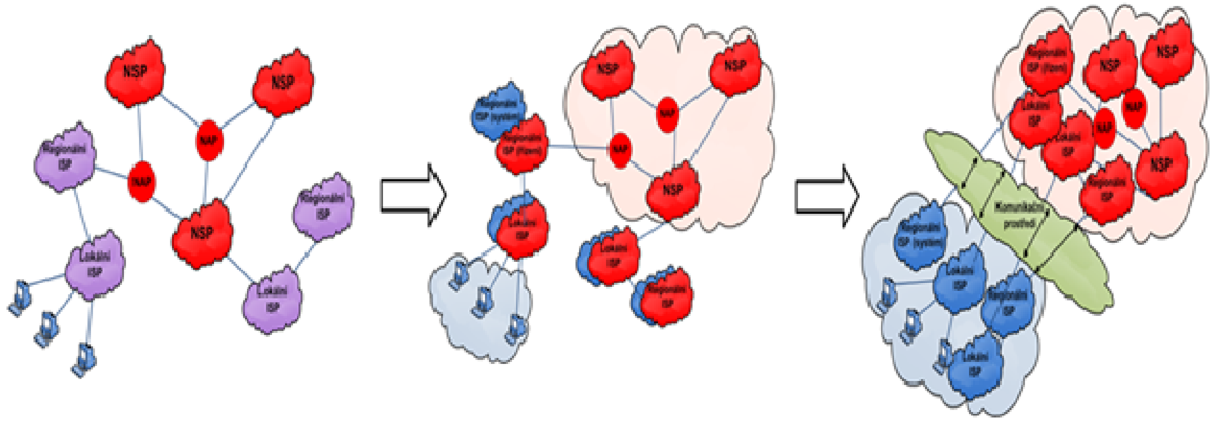

Figure 8: Composition of IT networks

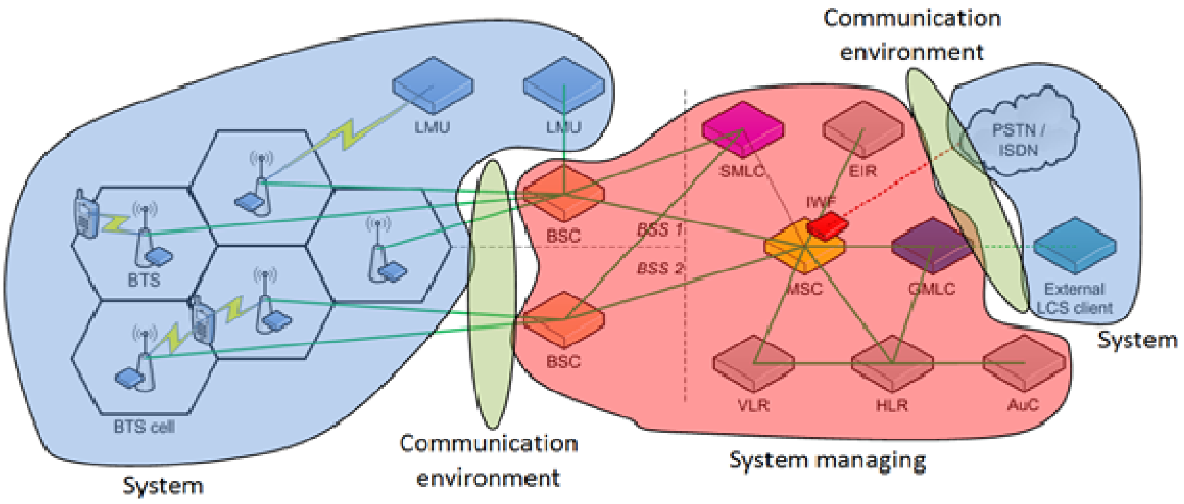

Figure 9: Composition of telecommunication networks

For the other mentioned task the standardized method What, If analysis is very suitable [14]. For determination of impacts of disasters on cyber networks and for cyber network failure on public assets we use the standardised form described in Table 1. The impacts of monitored disaster (all hazard approach [15] is used), i.e. including the cyber system failure, are followed in the territory in the disaster origin time (0h), 3h, 6h … measured from disaster origin; for times equal or higher than 3h the differentiation of primary and secondary impacts is performed - secondary ones are caused by failure of infrastructures and technologies. With regard to good engineering practice principles [14] in solution of practical problems we ddistinguish three variants: V - standard disaster size, C - critical disaster size and E - extreme disaster size. The examples of impacts are given in [4,5,7,11].

Table 1: Standardised method What, If analysis [14]

Protected interest / asset		**Impacts**
Possible impacts on lives and health of people		
Possible impacts on people security		
Potential impacts on property		
Potential impacts on public welfare		
Possible impacts on the environment		
Possible impacts on infrastructure and technology	Failure of energy supply (electricity, heat, gas)	
	Failure of water supply drinking utility	
	Failure of sewage	
	Failure of the transport	

	network	
	Failure of cyber infrastructure (communication and information networks)	
	Failure of the banking and financial sector	
	Failure of emergency services (police, fire fighters, paramedics)	
	Failure of essential services in the area (food supply, waste disposal, social services, funeral services), industry, agriculture	
	Failure of state and local government, i.e. the management of territory and human society	

The direct and indirect impacts you can see on Figures 10 and 11. By the considered method we also compiled the cyber infrastructure critical failute scenario for medium-size town and its vicinity by help of experts. The critical failure scenario of cyber infrastructure failure is in Table 2.

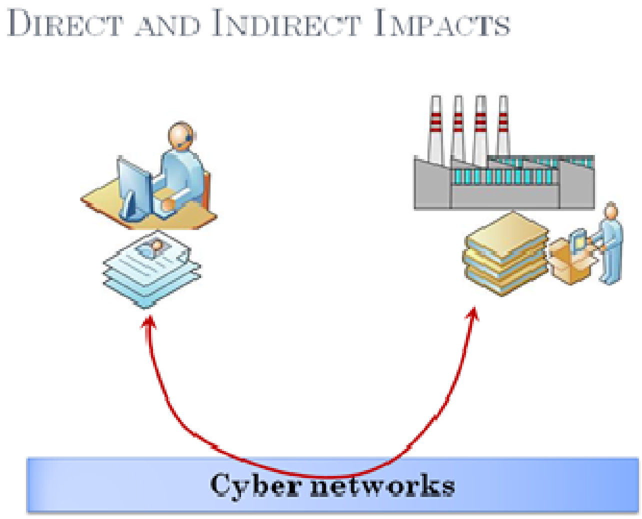

Figure 10: Direct impacts of cyber network failure

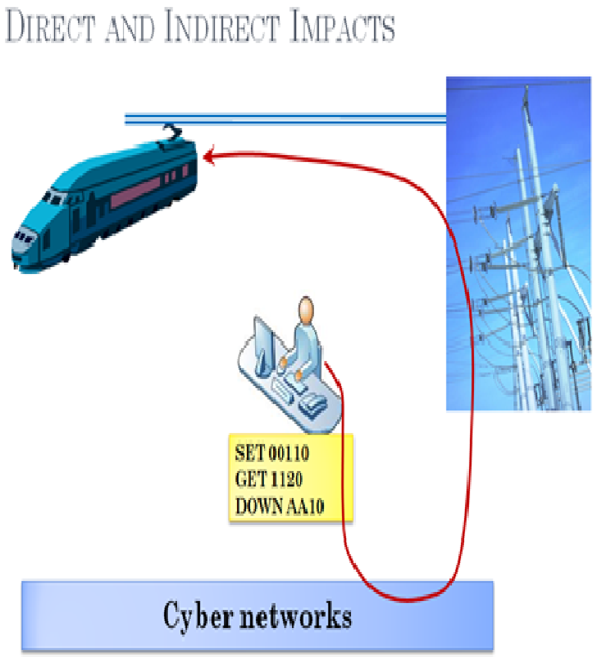

Figure 11: Indirect impact of cyber network failure

Table 2: The scenario of cyber infrastructure failure [5]

Time measure from the failure origin time	**Impacts on cyber network and other assets**
0 h	- security incidents remote reporting failure (if the communication infrastructure is based on IT infrastructure) - unavailability of web bank applications and bank services based on IT infrastructures - monitoring services failure (especially camera systems) - unavailability of certain public institutions services (central registers), limited point services
3 h	- stress from the inability to fully perform job (e.g. emails) - late or none action of the Integrated Rescue System (IRS) – by the fire detection or by the forced entry into real estate – caused due to inability to inform IRS through the automatic signaling system based on the IT infrastructure → property

	damage (fire, theft, …) - inaccessible electronic timetables (buses, trains etc.) → passengers transport limitations
6 h	- not working or unavailable internet shops, - inaccessible databases of logistic companies → loss of profit, - limited supply
14 h	- increasing stress - people cannot communicate (email, Skype, IP phones, facebook etc.) - people cannot fulfill their obligations (e.g. invoices payment) - people have no access to their finances - etc.

The expert judgement of the critical scenario of cyber infrastructure failure revealed also the impacts that threaten not only human security but also the state security, consider the following impacts: the subway emergency stop; the navigating systems collapse - connection failure with space satellites; the national defence collapse - electronically controlled military technology; police cannot use the computer databases vehicles register, human's identification and verification, comparing traces (fingerprints, ballistics); failure of security devices and systems – increased crime; inability to ensure the air transport safety; public transport collapses – no remote control; lack of information – panic, riots etc.; access to ATMs failure and thus to their own finances; failure of heat and electricity supply; troubles in building security and subsequent human checks; night street lights are not working; inability to pay pensions and social benefits; etc.

For safety of cyber networks we shall construct the the safety management system the model of which is in Figure 12 [11] that is suitable for solution of open complex systems.

VI. CONCLUSION

Cyber infrastructure is one of the critical infrastructures on the grounds of its failure has a critical impact on the protected assets. It creates with other infrastructures the open complex system denoted the critical infrastructure. Cyber infrastructures are threatening from several different sources (technology, disaster and the human factor intentional/unintentional). They are very vulnerable because no security standards and norms on technical and functional levels on sufficient level ensuring their resilience and robustness are applied. It is also true that low attention has been paid to aspects connected with safe vicinity of cyber networks. The real in-depth research should be continued in solution of problems of interdependences and their causes and in protection of public assets against to impacts of cyber system failures.

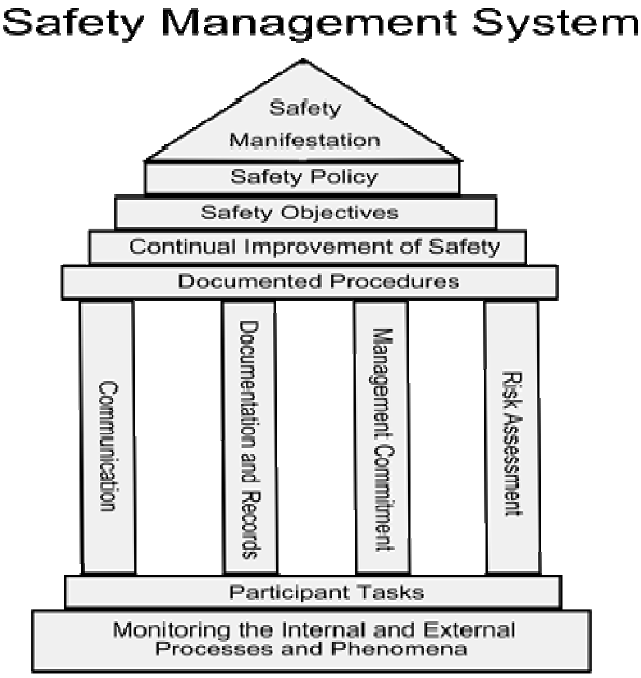

Figure 12 [11] that is suitable for solution of open complex systems.

REFERENCES

[1] S.M. Rinaldi, J.P. Peerenboom, T. K. Kelly, *Critical Infrastructure Interdependencies. (Identifying, Understanding, and Analyzing).* In: IEEE Control Systems Magazine, Vol. 21, December 2001, pp.12-25. www.ce.cmu. edu/~ hsm/im2004/readings/CII-Rinaldi.pdf

[2] Qiao Linag, Wang Xiangsui, *Unrestricted Warfare* (trans. Foreign Broadcast Information Service). Beijing, China, February 1999.

[3] D. Prochazkova, *Critical Infrastructure Safety Management.* In: Reliability, Risk and Safety. Theory and Applications. ISBN 978-0-415-55509-8, CRC Press / Balkema, Leiden 2009, 1875-1882, ISBN 978-0-203-85975-9.

[4] J. Prochazka, D. Prochazkova, *Cyber Infrastructure – Identification of Critical Spots and Impacts of Its Failure.* CYTER2012, ISBN 978-80-01-05072-9, ČVUT, Praha 2012.

[5] J. Srp, D. Prochazkova, *Analysis of Cyber Networks in System Concept.* CYTER2012, ISBN 978-80-01-05072-9, ČVUT, Praha 2012.

[6] D. Prochazkova, *Strategic Management of Safety of Territory and Organisation* [In Czech]. ISBN: 978-80-01-04844-3. ČVUT, Praha 2011, 483p.

[7] D. Prochazkova, *Analysis and Management of Risks*. ISBN 978-80-01-04841-2, ČVUT, Praha 2011, 368p.

[8] Tutor2u, *Introduction - What Is ICT?. Tutor2u* [online]. 1998. http://tutor2u.net/business/ict/intro_what_is_ict.htm

[9] G. Knight, *Internet Architecture*. University College London, 2006, 24 p.

[10] J. Srp, Geolocation and Geolocation Techniques. *Datakon 2011*: *Tutorials*. Mikulov: VUT, Brno, 2011, pp. 23-48. ISBN 978-80-214-4330-3.

[11] D. Prochazkova, *Critical Infrastructure Safety.* ISBN 978-80-01-05103-0. CVUT, Praha, 310p.

[12] V. Svoboda, M. Svitek, *Telematics Under Traffic Networks*. ISBN 80-01-03087-3. CVUT, Praha 2004, 263p.

[13] P. Moos, T. Zelinka, V. Malinovsky, *Telecommunication Services*. ISBN 978-80-01-03598-6. CVUT, Praha 2007, 176p.

[14] D. Prochazkova, *Methods, Tools and Techniques for Risk Engineering*. ISBN 978-80-01-04842-9, CVUT, Praha, 369p.

[15] FEMA, *Guide for All-Hazard Emergency Operations Planning*. State and Local Guide (SLG) 101. FEMA, Washinton 1996.