Interdisciplinary Description of Complex Systems 13(1), 48-56, 2015

REQUIREMENTS OF THE INSTALLATION OF THE CRITICAL INFORMATIONAL INFRASTRUCTURE AND ITS MANAGEMENT

Béla Puskas[1] and Zoltán Rajnai[2,] *

[1]c/o Obuda University
Budapest, Hungary

[2]Doctoral School on Safety and Security Sciences – Obuda University
Budapest, Hungary

DOI: 10.7906/indecs.13.1.7
Regular article

Received: 1 December 2014.
Accepted: 5 January 2015.

ABSTRACT

The segments of the network can be paralysed by a series of chance events or a well-organized, targeted attack. If we know our system and lead a safety-conscious life we can avoid unpleasant events, system down. The Critical Information Infrastructures has become a complex network. Consequently the items of the system, their mutual effects and links and the map of the network have to be known properly. We have to realize that everything is linked with each other and the physical and logistical networks have mutual effects on each other as well. It is obvious, that the problem of mapping the complexity is very important. One of the most important part of the cognition is the obtainment and sorting of information.

KEY WORDS

network, structure of networks, critical infrastructures, critical information infrastructures

CLASSIFICATION

JEL: L86, M15
PACS: 89.70.Hj

*Corresponding author, η: rajnai.zoltan@bgk.uni-obuda.hu; +36 30 445 1103;
Óbudai Egyetem, Biztonságtudományi Doktori Iskola, 1034 Budapest, Bécsi út 96/b, Hungary

INTRODUCTION

The main goal of my essay is to highlight the importance of system thinking and the complexity of the critical informational infrastructure. In the followings we introduce the complex structure of a datacentre, its aspects, and the highly combined system of its elements.

Among the system elements the essay is introducing the sophisticated structure of a datacentre in details, while outlining the informatics hardware, software and other technologies. Relating regulations, financial and human resources factors, as important substances, are also mentioned.

According to the basic principle of the system thinking the certain system cannot be examined as an independent unit. Each individual system consists of different networks, while the systems are creating other networks with each other as well. The elements of the networks are permanently influencing each other and continuously altering themselves. The critical informational infrastructure can be considered such a system as well, which is continuously changing from its development till its shutdown. The IT systems are not developed exclusively for their own sole purposes, but they are based on the strategy of the organisation created in line with the main goals of the business venture/organisation. The informatics strategy is usually created simultaneously with the other strategies of the organisation and it supports the critical informational infrastructure. Any other course of development can result in unexpected and serious errors. The hierarchical structure and system thinking are inevitable factors of the critical informational infrastructure management. The IT systems can be influenced by different stochastic impacts. If the management is not concentrated in one hand only "symptomatic treatment" can be applied, which similarly to the medical disciplines cannot solve the problem. Moreover the intervention to unknown system elements can cause damages as well. The IT system is composed by the relating processes and the network structure of different stages and their modifications monitored in various time spans of its running [1].

The critical informational infrastructure can be described by the following five criterions:

- main management procedures (central management and coordination),
- information security,
- domino theory[1],
- the principles of the weakest chain-link and the particle-whole,
- interdependency[2] [2].

The democracy approaching to anarchy, the network of Internet, the connection of cells is all scale free networks, which can withstand the random attacks. Nevertheless they do not satisfy the demands of the critical informational infrastructures, because they are quite unprotected against targeted attacks. The structure of armies has also not evolved accidentally on a way as we know it today. Nowadays all armies based on hierarchical, centralised authoritarian systems, which include not only the human resources but the technical regulations and their relations composing the structure as a whole. Business ventures often outsource their management, which can be motivated by economic reasons emerging during financial crisis situations. However certain outsourced functions or the concentration of same working phases in one country can pose serious threats on a long term. They can be advantageous from financial aspects but in case of social or national security viewpoints they can be very harmful. Is it satisfactory if all client databases of a business venture active in different countries are stored in one state, or our bank saves certain data or business procedures in cloud applications? The answer is obviously: no. An integrated IT system developed in line with the principles of system thinking is essential in the life of a country or an organisation.

The requirements regarding the availability, level of data management, archives and savings etc. have to be determined by the management of the organisation. Following this phase the conditions of development and running have to be set up. These conditions are as follows:

- financial resources (during the whole life cycle);
- human resources (skilled experts, logically organized hierarchical structure of personnel);
- legislation and the determination of working procedures;
- timing (technological sequence and time factors).

The efficiency of the system will be defined by the weakest of the aforementioned factors. The conditions, environment and impacts are altering dynamically. The failing of certain elements can be balanced moderately by the enhancement of the others but the safety of the system can be ensured by the homogeneity.

According to this statement and the COBIT[3], our system can be ranked into four evolvement level. The highlighted characteristics of the primary and service continuity model are as follows (the list is not exhaustive):

0 Non-existing – There are no recognizable processes at all. By the general consideration, the management does not have to deal with the continuity of service.

1 Initial/Ad Hoc – There are signs of the recognition of an activity, which has to be coped with. However there are no standardized processes but ad hoc actions are applied in case of individual incidents. The procedures of general management are irregular, the responsibilities for the continuous service are informal and the authorizations for the tasks to be carried out are restricted. The management gradually recognizes the risks threatening the continuous services and the need of it. The IT responses to significant shutdowns are slow and unprepared.

2 Periodic, but instinctive – The processes reach the level of similar actions carried out by different employees involved in similar processes. The responsibility for the continuous service is determined. The inventory of critical systems and elements exists but it can be unreliable. The evolvement of the procedure of continuous service in in progress but its success depends on the individuals.

3 Regulated process – The basic processes are standardized and documented and they are introduced in trainings. The programme of the training is formulated but the implementation of it is initiated by individually. The responsibilities for planning and testing of the continuous service are determined and assigned to certain persons. Based on individual initiations the regulations are followed and trainings are implemented in order to manage serious extraordinary situations or catastrophes. In case of highly available components and systems redundancy measures are applied. The inventory of critical systems and components is updated.

4 Controlled and measurable – The management monitors and measures the appropriateness to procedures and intervenes in case of improper running. The leader informational and decision making support systems utilize the provided information. The regulations and responsibilities regarding the continuous service are forced to be carried out. The extraordinary events disrupting the continuous service are classified and all relating chains of reporting are known by all concerned persons.

5 Optimized – The informatics system is used for the automatization of working processes on an integrated way and other tools are provided in order to improve the quality and efficiency. The informatics and continuous operation plans are integrated into the business activity plans and they are regularly updated. The procedures of availability and the planning of continuous service are completely in harmony. The management excludes any sources of catastrophes or serious emergency situations. The goals achieved by the continuous service are regularly measured and its metrics are calibrated [3, 4].

Nowadays that facility or service, which despite of its importance in case of its malfunction, disturbance, failing or destruction do not cause direct, serious damages to the economic, social, healthcare, public or national security situation of the population or the working of public administration, is also called critical infrastructure [5]. Actually the real grave problem is not the false declaration of a non-essential system as an essential one, but the neglect of the real primary systems to another less important resources.

The development of the IT system suitable for the goals of the business venture or the critical infrastructure can be initiated if the four basic principles and the commitment of the management are provided. The main element of the system is the central database, which can be handled as an integrated system virtually, but according to the principles of geo-redundancy must be established in at least two or more locations. If the whole infrastructure is considered as one system, the database is one of the system elements and the part of the complex network. In the following part only this element is going to be examined by its connections and non-exclusive nature in the system.

The geographical location of the system elements cannot be neglected. The climate, structure of the soil, geographical location also can influence the operation of our system. Besides of them the economic, political and security aspects have to be objectively determined as well. Prior to the establishment of the facility the distance of its location from any settlement, the density of population, the standard of living and the traffic conditions have to be well considered. The typical statistical information such as the probability of earthquakes, floods, fires, storms (tornados, hurricanes), temperature, number of sunny hours, snow, height above the sea or ground level etc. regarding the particular area are also very important. The geographical environment has also its impact on the organization of the physical, electronic and human protection of the facility. The stability and reliability of the means of communication, the capability and the possibility of separated operation of other public services (water, electricity, gas and other services) have to be examined as well. The conditions of the lines of communication (logistic), their load-bearing capacities and the risks of extreme weather conditions are also very important. At last but not least the relating environmental protection aspects have also to be considered.

Following the obtainment of the aforementioned information the main characteristics of the datacentre have to be determined. According to the TIER recommendations of the UPtime Institute the datacentres can be ranked into four groups in which the weakest chain-link has to be examined, Table 1.

The datacentre's main parts are the informatics and communication infrastructures, which include the server and machine halls (server rooms), encrypting rooms, incoming communication room (receiver), info-communication halls, technical (they can be separated, e.g. UPS[4], air conditioning, firefighter etc.) rooms, stores, workshops, control rooms, aisles and other premises. During the construction the materials and thickness of the walls, the weight-carrying capacities of the roofing and flooring, the waterproofing, sizes and security characteristics of the doors and windows, the EMC[5] characteristics of electromagnetic protection, the foundations of the houses have to be planned properly. The ground-plan of the premises, structure of the soil, the underground water sources, the orientation of the building, its distance from other constructions, the condition of roads, the possible environmental effects, the names of rooms surrounding the main functional halls, the overall condition of the building have to be documented.

During the construction the regarding standards, legislation, security regulations of operation and utilization, work and healthcare rules have to be followed strictly, besides the suitability

Table 1. TIER recommendation of UPtime. TIER I – basic infrastructure, one way energy supply without redundancy, TIER II – certain elements of the infrastructure have reserves, TIER III – the infrastructure can be maintained without shutdown, and TIER IV – fault-tolerant infrastructure [6].

Characteristics	TIER I	TIER II	TIER III	TIER IV
Active support elements	N	$N + 1$	$N + 1$	$2(N + 1)$
Supply route	only 1	only 1	1 active, 1 reserve	2 active
Maintained without service	no	no	yes	yes
Fault-tolerant	no	no	no	yes
Independent supply routes	no	no	no	yes
Permanent cooling	Depending on workload	Depending on workload	Depending on workload	Provided
Nominal capacity, W/m^2	210 - 320	430 - 540	1070 - 1610	> 1610
Duration of construction, month	3	6	10 - 20	15 - 20
Annual shutdown, h	28,8	22	1,6	0,4
Availability of machine room, %	99,671	99,749	99,982	99,995

of construction jobs and utilization as a computer centre. The different execution plans cannot contradict to each other, which can be achieved by the means of continuous communication and cooperation. The cooperation of different professions is very important in the planning phase as well, because only this kind of joint activity can guarantee the high quality outputs in the fields of the construction of premises, cooling, mechanical engineering and informatics systems. Similarly to any other fields, the documentation of every phase of the construction is very important. According to this principle, apart from the basic documentation of the datacentre, the other descriptions of the water, sewer, air conditioning, fire protection and security systems have to be prepared. In order to satisfy the regulations and for the better guidance and crisis management the elements of the system have to have clear inscriptions on them.

In case of the installed hardware and software elements the compatibility must be fully proper. During the installation period the subcontractors have to certify that the selected equipment fulfils the relating demands and standards. Beneath the antistatic (10^{-9} - 10^{-12} Ω surface conductivity) flooring, the separated strong- and light-current, cooling and fire protection cables have to be placed and the floor covering has to satisfy the electric shock protection regulations (10^{-6} - 10^{-9} Ω surface conductivity). The static capacity of the foundation has to bear the weight of all the installations. The flooring cannot slope at all, except the logistic supply routes in which case a maximum 10 % slope angle is allowed by the correction of ramps. The load-bearing capacity of the logistic supply routes have to be adjusted to the heaviest installation to be carried on them.

The technological area, which is above the suspended ceiling, has to accommodate the cables of the sensors, fire protection and air conditioning devices. The floor, ceiling and walls have to be covered with dustproof, non-mouldering and fire resistant materials. The distance between the floor and ceiling must be minimum 2,5 m. The walls, floor and roof of the server hall must be equal to the load-bearing capacity of a 30 cm thick, solid brick wall. Because of security and heat protection reasons the installation of windows is not recommended. The size of the main doors must fit to the specified dimensions of the logistical supply routes and they have to withstand to any breakthrough attempts for minimum 15 min. The building structure has to satisfy the demands of waterproofing properly. The datacentre, including the structures of the public services, has to be protected against the dampness of the soil. In the

different rooms only the essential public service networks can be installed. In the walls, floor and ceiling of the datacentre no cables can be installed. If the aforementioned cables are installed above the protected rooms they must be divided and equipped with pressure sensors and automatic closing valves. The protected rooms must be equipped with dampness sensors and they must be protected against external water floods (e.g. fire extinguishing).

The rooms must be heated with water-free devices, for example with hot air. The air conditioning must be provided by industrial precision equipment, which is capable to run 7×24 h. Due to the high demands the air conditioning equipment must be calibrated by $2N$ cooling availability. In case of the failing of an element the system has to cool down the heat produced by the critical overload without the assistance of the air conditioning control system. For the operation of the equipment (22 ± 1) °C temperature has to be provided by uninterrupted and filtered air and draught-free airflow, which also makes the room suitable for permanent working. The best way to achieve the goal and most effective work is to build a closed, cold corridor between the rack boots. The cold and warm conveying pipes of the corridors cannot hinder the operation of the systems and they cannot produce condensing water. In the cold corridor the temperature must be (22 ± 1) °C, the level of relative humidity must be (50 ± 10) % during peak hours as well. Based on the gathered statistical information the environmental and climate effects of the last 100 years can be determined by which, together with the characteristic data of the planned equipment and the given cubic metre of air, the cooling parameters can be planned. The unexpected breakdown of air conditioning has to be detected in real time and an alert message should be sent simultaneously. The noise pollution cannot exceed the standards. The deleterious effects of the mechanical equipment (e. g. diesel generator, air conditioning etc.) placed in the server room has to be reduced by isolations absorbing or reflecting the electronic radiation, while the vibration has to be handled by damping solutions. Due to the high level availability, similarly to the other redundant supply systems, the electrical systems need to have two separated supply tracks in cases of the external service provider and the datacentre as well. Both supply tracks must be controlled by an automatic switch and the power supply cannot be interrupted by and unexpected malfunction or planned maintenance. To ensure the permanent and independent power supply a diesel-electronic equipment must be installed, which automatically starts and provides electricity in case of unexpected interruption. During the bridging period a high availability $2N$ UPS has to be used. The power supply systems have to satisfy all power demands of all equipment responsible for the continuous service of the datacentre. The independent power supply of the critical equipment placed in the server room has to be provided through separated tracks and circuit breakers, while the power is received by the redundant power supply units of the certain equipment. The whole electrical power network has to comply with the regarding standards and legislation.

The entrance and the exit of the building must be secured by automatic security system using electronic card, PIN code or biometric identification. All entry and exit must be unavoidably documented, which is provided by such technical solutions like one-man barriers, gates supervised by security guards. If the datacentre is unmanned the alert system has to go live automatically. All moving have to be monitored by CCTV systems. The electronic security systems can be substituted by human guard personnel, who register all movements at the entry points. The job of the security guard is supported by the CCTV system by which the guard can check the alert messages and monitor and control the security zones, fences, corridors and service rooms and other external areas. With the CCTV system, security lighting must be used as well, which can serve as the lighting of the emergency routes and exits, too.

The electronic signal system, monitoring the security areas, service rooms, doors and windows, wall, floors and roofs, is also an important part of the security measures. The

protection must include the elements of the supporting infrastructure as well and the local alerts must directly notify the security guard. The alert systems must react to the intrusion attempts, smoke, fire, water and the alteration of the humidity level [7].

Since the server rooms and the other service rooms must be handled as separated fire protection zones. They must be equipped by separated alert and automatic fire extinguisher systems. The fire alert system must be a VESDA[6] or an equal aspirant equipment.

In case of fire the security system must alert the employees locally, notify the reaction force, provide ventilation and close the fire clack-valves of the air condition system, however the automatic fire extinguishing has to be controlled by humans. In case of a fire nearby the server room the structure of the walls has to prevent the increase of heat – during the cooling period as well – which must stay below 50 °C in the server room. The fire extinguisher cannot damage the informatics systems. Prior to the fire extinguishing the servers have to save automatically and shut down. The cables of the electric power supply system must be fire resistant.

For the management of the datacentre all documents needed for the safe and continuous operation must be prepared. The documentation must include all preventive, detecting, improving measures, which should be taken in order to ensure the long term and safe operation. The regarding, updated and detailed technical documentation of the whole system including the instructions concerning the operation and crisis management must be available by every concerned specialists. By the means of different trainings the quality level of the management can be increased. The equipment and its technical characteristics of the informatics system are very important part of the datacentre. Since the infrastructural network is built from these elements and they continuously influence each other, they have to be operated in a complex homogeneous system. This equipment include the support devices, client stations, data storages, saving systems, the network active devices, the rack boots, data storage medias, uninterruptible power supplies, generators, air conditioning and ventilation, public service networks, the noise and vibration characteristics of the devices, thunder protection, controlling, security and fire alert systems and their characteristics. Indirectly this category includes the tools of maintenance, spare parts and the documentation (instructions of operation and safety measures, guaranties, licenses, contracts etc.), which can be hard-copy versions or stored digitally. Besides the hardware the software needed for the operation of the system and business procedures is also has to be mentioned. This category includes operation systems, saving, communication (mail clients), antivirus software, firewall systems, endpoint protection, supervising, log gathering and analysing, cyphering and office applications or other business support products such as web applications, databases, teamwork and process support, administrator software. In order to follow the modification of these applications the number of versions and the updates must be documented properly. In case of unique software development, the project has to be documented from its initiation till its end. The completed software has to be audited as well. The developed software cannot be tested on the live system because it violates the aforementioned demands [8].

SUMMARY AND CONCLUSIONS

Is it worth constructing and operating a server room? The question is at least as complex as the construction of it. Considering the aforementioned four factors the answer of a leader would be definitely no. But if we ask whether to entrust the precious business information to the care of somebody else only lead by our trust, and we even have to pay for it, then a responsible leader would most probably decide in the favour of the construction of an own datacentre. But as it has been introduced in the present essay the construction of a modern critical information infrastructure must be carried out on a very careful and well planned way.

According to the results of the network theory the construction and management of the infrastructure must be handled as a complex system. If this principle is not followed the weakest chain-link will ruin the effort in spite of the vast amount of money spent on the project. In the best cast scenario only its effectiveness will decrease but if it turns worse the interdependency will activate the domino theory, which will cause continuous malfunctions, decrease its effectiveness considerably [9, 10]. Consequently the maintenance of homogeneity is very important, but besides the developed infrastructure, the human resources, financing, training all have to be operated in a well-structured, centralized operational environment as well.

REMARKS

[1]chain reaction like damage
[2]dependency on each other
[3]Control Objectives for Information and Related Technology
[4]Uninterruptible Power Supplies
[5]ElectroMagnetic Compatibility
[6]Very Early Smoke Detection Apparatus

REFERENCES

[1] –: *Critical Infrastructure*. In Hungarian.
http://www.katasztrofavedelem.hu/index2.php?pageid=lrl_index, accessed 20th November 2014,

[2] Nyíry G.; Borda J. and Horváth Gergely K., eds.: COBIT 4.1.
IT Governance Institute, Budapest, 2007,
http://www.mtaita.hu/hu/Publikaciok/ISACA_HU_COBIT_41_HUN_v13.pdf, accessed 12th November 2014,

[3] Pokorádi, L.: *Graph-Modeling of Operating Processes*. In Hungarian.
Repülőstudományi kőzlemények **XXVI**(2), 224-231, 2014,
http://www.repulestudomany.hu/kulonszamok/2014_cikkek/2014-2-19-0114_Pokoradi_Laszlo.pdf, accessed 20th November 2014,

[4] Beinschróth, J.: *Managing IT Crises*. In Hungarian
Óbuda University, 2013,
http://uni-obuda.hu/users/beinschrothj/Kriziskezeles/Kriziskezeles_c.pdf, accessed 2nd November 2014,

[5] –: *Green Paper for Government Decision of the National Programme for Critical Infrastructure Protection*. In Hungarian.
Polgári Veszélyhelyzeti Információs Rendszer, 2008,

[6] –: *Data Center Solutions*. In Hungarian.
http://www.persecutor.hu/megoldasok/adatkozpont_megoldasok/general_kivitelezes, accessed 10th November 2014,

[7] –: *The National security authority operations and procedures of handling of such data*. In Hungarian.
Government Decree 90/2010. (III. 26.), Hungary, 2010,

[8] ISO/IEC JTC 1/SC 27: ISO/IEC 27005:2011 *Information technology – Security techniques – Information security risk management*.
ISO, 2011,

[9] Fregan, B. and Fábián, É.: *The special relationship for European integration*.
Kommunikáció, Fekete Károly, 2010,

[10] Mester, G.: *Modeling of the Control Strategies of Wheeled Mobile Robots*.
XXIII. International Conference "In Memoriam Kandó Kálmán". Kandó Kálmán Faculty of Electrical Engineering, Budapest, pp.1-4, 2006.

ZAHTJEVI NA POSTAVLJANJE I UPRAVLJANJE KRITIČNOM INFORMACIJSKOM INFRASTRUKTUROM

B. Puskas[1] i Z. Rajnai[2]

[1]c/o Sveučilište Obuda
Budimpešta, Madžarska

[2]Sveučilište Obuda – doktorska škola sigurnosnih znanosti
Budimpešta, Madžarska

SAŽETAK

Dijelovi mreže mogu biti paralizirani serijom nasumičnih događaja ili dobro organiziranim ciljanim napadom. Ako znamo naš sustav i radimo uzimajući u obzir sigurnost, možemo izbjeći neugodne događaje poput pada sustava. Kritična informacijska infrastruktura postala je kompleksna mreža. Slijedom navedenoga, elementi sustava, njihove relacije i mapa mreže moraju biti poznati. Moramo prihvatiti kako je sve međusobno povezano ta kako fizičke i logističke mreže utječu jedne na druge. Očigledno je problem mapiranja kompleksnosti vrlo značajan. Pritom među najznačajnije dijelove ulaze prikupljanje i sortiranje informacije.

KLJUČNE RIJEČI

mreža, struktura mreže, kritična infrastruktura, kritička struktura informacija