ACTA TEHNICA CORVINIENSIS – Bulletin of Engineering
Tome VIII [2015] Fascicule 4 [October – December]
ISSN: 2067 – 3809

[1.] Zoltan RAJNAI, [2.] Béla PUSKAS

DECISION-MAKING SUPPORT SOFTWARE APPLICATION OPTION FOR CRITICAL INFORMATIONAL INFRASTRUCTURES

[1-2.] Óbuda University, Doctoral School on Safety and Security Sciences, Budapest, HUNGARY

Abstract: There can be practical question in connection with the networks: Do the malfunctions of devices, eruptions of social conflicts, devastations of biological or chemical disasters happen accidentally? 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.

Keywords: network, future IT warfare, structure of networks, Critical Infrastructures, Critical Information Infrastructures

INTRODUCTION

We can ask a practical question regarding the networks: does the malfunctioning of technical devices, eruption of social conflicts, biological or chemical disasters happen accidentally?

Segments of the networks could be disabled by incidental events or well-organized and planned interventions as well. In 2013 the 91 % of business ventures suffered from cyber-attacks from which 9% were targeted. Considering the permanently increasing numbers and threat of these attacks and the growing tendency of cyber espionage backed by professional organizations, the situation is graver than ever. However from the point of view of network theory it is worth mentioning that the 13 % of business espionage was committed by humans and not technical devices.[1]

The goal of present essay is to emphasize the importance of system thinking and the complexity of informatics systems. I also intend to introduce briefly the elements of the IT systems and highlight the lack of software supporting the monitoring of the complex systems and decision making processes and the deficiency of the relating legislation and standards.

A research of Symantec – conducted between the July of 2012 and the June of 2013 – has been already dealt with the energy sector as one of the fields of the Critical Infrastructure. During the aforementioned timespan the average number of detected daily attacks was 74, of which 9 were launched against the energy sector. The vitally critical systems were attacked by 16 % of all targeted attempts, which made them the second most endangered networks. Fortunately the attacks did not cause serious loss of data (at least the researchers did not know about them) but by the continuously increasing number of them the attacks could exceed the statistical limit of harmful attempts.[2] The analysis of the attacks revealed the growing number of weaknesses as well by which the threats arriving from external sources mean greater risks. Nowadays the 10 % of the business ventures are under permanent attacks and pressure.

The success of the dangerous targeted attacks is enhanced by the significant sources provided by different organizations, business ventures, even public administrations. Generally the victim does not even notice the attack and the detection of weaknesses and their solutions could take years. The recognition of the violation is even more difficult in the lack of information on its source, the main client, the coder, the attacker and so an. The malicious codes usually exploits the unique human and technical weaknesses of the systems and these sophisticated "tools" can cause more damage to a country or a facility of vital importance than a traditional military strike. For example the IT warfare and its new field, the IT operations can ruin the financial sector or political structure of a certain country, which could influence the course of events in the affected area on a long term and relatively on a low cost.

Other risk endangering the IT infrastructure is the inner threat originating from the planning and coordination faults of working processes or other procedures and the drawbacks of the human nature, which could pose the greatest threat by the misconduct of IT systems, data and information. Many times CEOs working in different fields propose different solutions in connection with the same IT matter, which should be avoided by exact regulations, audited organizations, education and training, safety-conscious working attitude, sufficient human and financial resources.

The third aspect of the subject is the availability of the system, which includes the failed setting up, risks of operation, amortization, *technological or operational defect of technical devices. A sustainable and highly available system can be provided by reliable producers, proper technology and redundancy and operational environment satisfying the goals of the system.*

The critical infrastructure, which includes the critical informational infrastructure, has to be operated within the framework of the aforementioned environment.

Our system must be run by the common interpretation of the three fields (external effects, internal effects, structure of the system). In my opinion the existing defence mechanism is not sufficient and other mechanisms should be invented. From this aspect the setting up of the multilevel protection is inevitable and a particular software capable to map up the different networks, find their inherency and draw up the necessary conclusions is highly needed. If we know our system and run it on a safety-conscious way, we may not encounter with service interruptions or loss of data. So, it is important to know the items of our system, their effects on each other, their links with each other and the map of the network properly. We also have to be aware of the fact that everything relates with each other such like the physical and logical networks. That is obvious that extremely important to map up their complexity, which – as the most important step of it - must include the gathering of data and organizing it into databases.

According to the definition the IT system or facility of vital importance (known also as critical informational infrastructure) is: "the network-like physical or virtual systems of the society, which by the necessity of providing continuously information or the availability of the informatics environment are vital items of the system or they are essential for the running of other identified vital system elements."[3]

From the viewpoint of the critical informational systems the system thinking approach is very important. It is supported by the proper knowledge of our system, the preparation of an exact data asset inventory, which includes the working processes, system elements, their links, environment variables and many other things. After the survey and the accurate documentation, the system can be modelled by certain aspects. The next step of modelling is the systematization of data and the demonstration of elements and their links by graphs. Then the graphs are organized in matrixes, which can be processed by computers more easily.

For the sufficient operation the system should have a well-prepared programme plan including the whole life cycle of the system. This programme plan can be controlled by a software application, which has to be able to permanently receive inputs and send signals and alerts regarding dangerous events occurring during the operation. Based on the stored data it has to be able to recognise such kind of relations, which can't be found out of the knowledge of subsystems exclusively or they are originating from the complexity of the system. Using artificial intelligence the software has to continuously develop its knowledge base on the relations and links of the system's items and it has to propose in connection with the necessary maintenances and upgrades. Initially the modular software has to support the risk analysis and risk management as well. The risk analysis must be carried out with respect of confidentiality, integrity and availability. The system may not affect processes in case of temporarily working or shutting down for a longer time, but confidentiality has to be considered as an important demand in these cases as well.

The examination of a system of complex network elements can be carried out by the assistance of network theory, or from another approach using the graph theory. The graphs are the mathematical descriptions of networks by which the interactions, navigations and behaviours can be introduced on a mathematical way. The "models" of different systems can be similar to each other, which can indicate the existence of rules. Following the preparation of graphs simplifications can be carried out and on other way unseen but harmful relations can be identified in the network. In case of more loops or surplus redundancies the normal operation of the system could switch to emergency status quite soon. Apart from the known events introduced in the risk analysis many tiny irrelevant events can also alter the system. Moreover, according to my approach, the different networks can be considered as one dimension of IT, human, infrastructural, traffic etc. Networks, which are not independent from each other but they are linked and form up a complex system of a multidimensional network. In these networks two points or two separated IT systems may not have relations with each other but there could be other edges or network nodes, which link them up. The graphs can be converted into matrixes by a method introduced later on and by the matrixes the calculations, revealing the relations, can be done more easily.

The simplest matrix calculations to analyse the links are as follows: The method of matrix creation is based on the number taking place in the columns' and rows' cross section. In this case the columns and rows mean the nodes of the network.

i row; j column

NEIGHBOURHOOD MATRIX

The neighbourhood matrix indicates the number of edges between two nodes.

It can be interesting from more points of view. On one hand the redundancy can be planned by them, while the surplus links, causing incalculableness and instability in our network, can also be found.

a_{ij} *indicates the number of edges linking* p_i *and* p_j *nodes*

$$\boldsymbol{A} = [\boldsymbol{a_{ij}}]$$

In case of undirected graphs:

$$a_{ij} = \begin{cases} 1, & \text{if } p_i \text{ and } p_j \text{ are linked directly, edge} \\ 0, & \text{in every other case} \end{cases}$$

In case of directed graphs:

$$a_{ij} = \begin{cases} 1, \text{if there is an edge from } p_i \text{ to } p_j \\ 0, \text{in every other case} \end{cases}$$

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix};$$

for instance: $A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 2 \\ 0 & 3 & 0 \end{bmatrix}$

Edge matrix

Edge matrixes indicate the links between edges and vertices.

Marking:

$$B=[b_{ij}]$$

In case of undirected graphs:

$$b_{ij}=\begin{cases}1, & \text{if } e_j \text{ is not loop edge and it interlocks with } p_i\\ 0, & \text{in every other case}\end{cases}$$

$$B=\begin{bmatrix}0 & 1 & 0\\ 0 & 1 & 1\\ 0 & 1 & 0\end{bmatrix}$$

In case of directed graphs:

$$b_{ij}=\begin{cases}1, \text{if } e_j \text{ is not a loop edge and its starting point is } p_i\\ 0, \text{if } e_j \text{ is loop edge and it does not interlock with } p_i\\ -1, \text{if } e_j \text{ is not edge loop and its starting point is } p_i\end{cases}$$

$$B=\begin{bmatrix}0 & 1 & 0\\ 0 & 1 & -1\\ 0 & -1 & 0\end{bmatrix}$$

Availability matrix, power matrix

If the neighbourhood matrix is multiplied with itself the result is the availability matrix, consequently the power of the neighbourhood matrix gives the availability matrix.

This matrix determines the number of different ways leading from one point to another. The way taken is indicated by the difference of the vertices' sequence, which means that there can be only one way between two neighbouring points with disregard the real number of the linking edges.

Marking:

$$A^k = a_{ij}^{[k]};\ A^2 = a_{ij}^{[2]} = \sum_{s=1}^{m} a_{is} * a_{sj}$$

Sum matrix

The sum of the availability matrixes gives the sum matrix.

The sum matrix indicates the number of maximum k steps and other different ways, which are needed to get from one point to another.

If we would like to know whether one point can be available from another at least via one k step then the signum matrix have to be used.

Marking:

$$H_k = h_{ij}^{[k]} = \sum_{n=1}^{k} A^n$$

$$H_2 = A^1 + A^2,$$

$$H_3 = A^1 + A^2 + A^3 = H_2 + A^3$$

Signum matrix

If we want to know whether one given point can be available from another at least via one k step then the signum matrix have to be used.

Marking:

$$s_{ij}^{[k]} = \begin{cases}1, & \text{if from } p_i \text{ node we can get to } p_j \text{ via } k \text{ step}\\ 0, & \text{via } k \text{ step it can't be reached}\end{cases}$$

Availability matrix

If we only want to know whether a certain point can be reached from another one via optional number of steps, then the:

Z_(m ∗m)

availability matrix has to be used. The signum and availability matrixes can be used in many ways for IT risk analysis, but in case of risk analysis the effects of elements to each other and the reduction of them by the increase of the number of links can be also examined.

Marking:

$$Z = sign \sum_{n=1}^{m} A^n$$

During the modelling we can use deterministic, stochastic and fuzzy methods. For the development of the software different mathematical algorithms have to be used, which exist in other systems, only to mention the rapidly improving firewalls. Since the human factor is very significant regarding the behaviour of the system, a team of psychologist has to formulate the details and the know-how of the system in order to achieve success. Naturally the existing knowledge, such as standards elaborated by experts, has to be used as well.

In our opinion the accurate preparation, the careful selection of the junctions, the documentation and the reliability of the system are very important too. The planning and operation are static and dynamic at the same time. Regarding one certain process the direction and dynamics of the alteration can be also interesting. During the analysis of the systems and inputs, the systems of the multinational business ventures can cause problems as well. These problems can emerge from the affiliates, their parent companies and their other subordinations or the data centres, which are located at great distances from each other in order to establish geo-redundancy. In case of disaster prevention activity the informatics networks stretching through countries can also encounter obstacles. Due to the complexity of the environmental effects and relations, the simple running of the software can result in wrong outputs deriving from the simplification attempt of the aforementioned systems. Because of the globalisation and the improvement of IT communication systems everything is in connection with each other, which influences our system on an unpredictable way. But by the means of risk analysis, based on statistical and probability calculations, a relatively stable and reliable system can be established.

The determination of the exact amount of input needed for the modelling process is quite difficult, but it is not so much to make the necessary time boundless. The best instances of it the weather forecast, when the process of weather data can't last longer than the exact date of the forecast. On one hand, as much information has to be obtained as possible, which enables the system to make more and more accurate calculations resulting in more detailed outputs. At the same time more data can slow down the process extremely and in case of a very complex system the chance of malfunctions is more probable as well. Considering the aforementioned facts a plenty of sensors have to be used and much more calculations have to be done, while the weaknesses, threats, characteristics of assets and other basic information must be mapped up. This information can be obtained from producers or by sensors, experiences etc. but the optimization itself can't be neglected.

The software can be operated by a management info-communication network, which has to be independent from the "target" system, while *the operation system should be based on the RAID data storages. The system would run on three or more operation systems, which would be coordinated by a lower layer continuously monitoring its operation, alteration of the code and intervene, if it is necessary. In this case the achievements of artificial intelligence and system analysis can be installed in the software as well. Regarding the system, the existence of an unlock suitable for human intervention and the override of decisions or restoration to an earlier version is essential. Another fact is that only the systems built up by the principles of system analysis are protected against the incidental malfunctions and not the randomly created ones. In case of the scale-free networks the direct attacks are more dangerous. By the protection of the controlled and reduced edge interfaces and external connection points, the risks of attacks can be eliminated. The vast amount of data or the input of unexpected information arriving through the input points can also cause hazards endangering the running of the software. In order to minimize the impact of the butterfly effect the number of random events has to be reduced. It can be achieved by the strict regulation and maintenance of stability and the correction of abnormal processes, which can influence each other and result in chaos.*

The normal status of the system can be determined as follows:

The software can manage 7 statuses:

- *Planning phase*
- *Setting up phase*
- *Normal working phase*
- *Readiness phase*
- *Disaster phase*
- *Restoration phase*
- *System withdrawal phase*

Planning phase

The risk analysis is usually initiated in the framework of the planning phase by the input of initial values, modelling of system operation and the improvement of the final implementation plans. The software is adjusted to the environment, it is modelled, the locations of sensors are planned and the amount of the input data is optimised.

Setting Up phase

The software is adjusted to the system. Practically it is an initial, "tutorial" status, when a database of the vast amount of elementary data is created and the data links are instructing the system by the support of the artificial intelligence.

Normal working phase

The critical system element is working in a normal status, the software does not detect any unusual event and no threats, pre-identified by the risk analysis, are in effect.

Readiness phase

The software detects a pre-identified threat but it is not influencing the operation of the system. The risk is acceptable, manageable but its alteration has to be closely monitored. In case of numerous unexpected events, minor but separately manageable threats, the software sends alert messages and the restoration of normal operation has to be launched. The system can remain in this status forced by such an external impact against which we can't or don't intend to apply countermeasures. We can also anticipate regularly returning effects as well.

Disaster phase

The software detects a pre-identified serious threat, which can cause the malfunctioning or shut down of the system or other grave consequences. The software sends alert messages and attempts to maintain the reduced operation, while alarming the external cooperative organizations as well.

Restoration phase

Following the disaster phase the system is in a stable status (e.g. the default configuration of servers had been done) but its normal working status has to be restored. The external threat causing the disaster situation had been eliminated and the software supports the recovering of normal data trying to prevent the "oscillation". The restoration sequence has to be determined by priorities, which take into consideration the need of urgent recovery of the critical elements' stable status, but do not neglect the technological and logical aspects as well. Unfortunately most of the business ventures and even the critical facilities do not have incident management plan, which has to be included into the software too.

System withdrawal phase

In order to provide the permanent working of the business or fulfil the demands of legislation the withdrawal and replacement of the system must respect the principles of availability, intactness and privacy. At this stage the software does not supervise certain data, because the operation of each system elements is not assured any more but it warns if the sequence of the process could lead to disaster.[5]

The software continuously calculates the probability of switching into another status. The software also has to be prepared to isolated running, when some of the elements of the critical infrastructure has been already shut down. On one hand the software is the part of the critical informational infrastructure, because they supervise and control the critical system elements jointly, but one isolated part of it is independent and it controls the informational infrastructure. Such activities are the monitoring of the servers, the network infrastructure, the protection of the endpoints and the system against intrusions etc. and the processing of the information received from the aforementioned sources.

From the viewpoint of the system management the robust systems, which change their status slowly, can be handled relatively easily. In their case the system operators have enough time to intervene, but on the other hand the shutting down of processes and the restoration can take longer time as well.[6]

SUMMARY

I am convinced that the present fast improvement of IT technology can't be sustained for so long. Such as every processes of the real human life it will also be slowed down or suddenly come to a halt by the self-regulation. This kind of development has resulted in such sudden and fundamental changes in our life that can't be compared to anything in history.

Unfortunately the dynamic improvement has been not followed by the evolution of regulations and safety properly. The main goal of my essay is the raising of awareness. The IT revolution opened up previously closed doors and the free information flow connects everything together. This vast freedom is basically welcomed but if it is leading to anarchy that could cause problems as well. There are some fields where the establishment of uncontrolled and freely established network connections can't be allowed. Apart from the concerning regulations a specific tool – a software may be – is needed, which is capable to apply the rules in practice. In fact the recent struggle (firewalls, antivirus applications etc.) is moving on a spiral way, earning a lot of money for some actors of the business segment, but it does not solve the real problem. The creation of the software supervising the critical informational infrastructure takes a long time though some elements of it already exist. As the first step a framework has to be created in which the support of decision making can be based and launched. The other parts of it will be added gradually. The input points have to be prepared to accept the devices and software already in use. As the critical system elements are working in a complex environment, which has an impact on us, we also have to invite the experts of different professional fields and integrate their achievements into the software. [7,8,9]

IT experts, mathematicians, psychologists, mechanic and electrician engineers will be highly welcomed to participate. The aforementioned idea of the software may not solve the problem and perhaps another completely different theory will be the final solution, but the processes speeding along a spiral line has to be moved anyway. Perhaps biologists, physicians or sociologists will find the answers for the questions of network analysis based on their results achieved in their unique discipline. As a matter of fact the societies and biological systems already regulate themselves and they usually encounter problems caused by the impacts of external effects.

References:

[1.] Kaspersky Lab ZAO source : http://report.Kaspersky.com/#corporate-threats [Online] 2014. [Download date: 18/10/2014]

[2.] Symantec Corporation, source: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/targeted_attacks_against_the_energy_sector.pdf [Online] 13/01/2014. [Download date: 18/10/2014]

[3.] 65/2013. (III. 8.) Korm. Rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelö-léséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról. 08/03/2013.

[4.] Pokorádi László: Rendszerek és folyamatok modellezése. Debrecen: Campus Kiadó, 2008. ISBN 978-963-9822-06-1

[5.] MAVIR Magyar Villamosenergia-ipari Átviteli Rendszerirányító Zártkörűen Működő Részvénytársaság (MAVIR ZRt.), source: http://mavir.hu/documents/10258/20774/policy5_final+version_H.pdf/8fe133d9-cda2-4581-9703-ff69226a41c2 [Online] 27/01/2012. [Download date: 18/10/2014]

[6.] F. Szlivka, I. Molnar: Measured and non-free vortex design results of axial flow fans, Journal of Mechanical Science and Technology 22:(10) pp. 1902-1907, 2008

[7.] Molnár I, Dr Szlivka F: Conclusions of the measurement data of the velocity- and pressure distribution of an axial flow fan, HUNGARIAN AGRICULTURAL ENGINEERING 19: pp. 41-42. (2006)

[8.] Rajnai Zoltán, Fregan Beatrix: Un portrait militaire au reflet de l'insurrection hongroise, ORIENTS 2013: (10) pp. 93-96.

[9.] Gyula Mester, "Sensor Based Control of Autonomous Wheeled Mobile Robots", The Ipsi BgD Transactions on Internet Research, TIR, Volume 6, Number 2, pp. 29-34, ISSN 1820-4503, New York, Frankfurt, Tokio, Belgrade, Source: http://internetjournals.net/journals/tir/2010/July/Paper%2004.pdf , 2010

[10.] Rajnai Zoltán-Bleier Attila: Technical problems in the IP comunication systems of the Hungarian Army, Academic and Applied Research in Military Science (ISSN: 1588-8789) (eISSN: 1788-0017) 9: (1) pp. 15-23. (2010)

ACTA Technica CORVINIENSIS
BULLETIN OF ENGINEERING

ISSN:2067-3809