International Scientific Conference

National Critical Infrastructure Protection
Regional Perspective

October 24th, 2013

УНИВЕРЗИТЕТ У БЕОГРАДУ
ФАКУЛТЕТ БЕЗБЕДНОСТИ
UNIVERSITY OF BELGRADE
FACULTY OF SECURITY STUDIES

Belgrade, 2013

UDC 338.45:351.78
316.472:351.78

Ozren Džigurski, Goran Mandić, Mladen Milošević

University of Belgrade, Faculty of Security Studies
odzigurski@gmail.com
gmg381@yahoo.com
mladen.milosevic@gmail.com

CRITICAL INFRASTRUCTURE SECURITY AND SOCIAL NETWORKS

(extended version)

Abstract: The systems of Critical Infrastructure (CI) belong to the category of socio-technical systems. Generally, the CI of one state includes the following business and industrial sectors, such as energy systems, transport and distribution networks, telecommunication and information systems, chemical industry and technological systems, agriculture and food industry, banking and financial management systems, public health systems, public administration, etc. Given the significance of the CI systems for the functioning of the state and its business entities, the CI system is very susceptible to various eminent threats imposed by both external and internal factors. Knowing the operational and functional characteristics, as well as their complex functional interdependence, these infrastructure systems require a special approach in defining and implementing their safety and protection.

This paper addresses three aspects of security of CI: the security of SCADA systems as key technology components for the management of CI, social engineering as an important component of security threats to CI and the influence of social networks on the safety of CI, as a higher level of threat and protection of the CI.

Key words: *critical infrastructure, SCADA security, social engineering, social networks*

1. SCADA SYSTEMS AND CRITICAL INFRASTRUCTURE

Industrial Control Systems (ICS) are devices, systems, networks, and controls used to operate and/or automate industrial processes. These devices are commonly found and used in nearly every industry sector, transportation systems, output and transmission of energy, as in many other areas of critical infrastructure systems.

SCADA (Supervisory Control and Data Acquisition) represent systems and/or networks that communicate with the ICS for the purpose of the collection of the necessary data for process monitoring and control units that control processes. As automation continues to evolve and becomes more and more important in the world, the use of ICS/SCADA systems becomes widespread. ICS/SCADA systems are particularly applied in all areas of CI containing process control, such as energy and transportation systems, production and distribution of food and water, chemical industry, etc.

In the domain of CI system, in terms of safety performance, ICS/SCADA systems represent a major problem. Because of the way they are implemented, ICS/SCADA systems are very susceptible to various kinds of physical and logical attacks, that is, the attacks such as unauthorized access to the data and devices in these systems. The reason for this is that the ICS/SCADA systems are usually implemented with a very large number of components that can be distributed over a large area, connected by wires or wirelessly. Within this framework, the SCADA systems are practically the Achilles heel of these categories of CI systems given that they are located in the appropriate places for the purpose of direct collection of data necessary for process control, and can carry out the direct management of individual executive procedural devices. Because of their spatial distribution, these places may be insufficiently secured by various types of unauthorized access and criminal attacks. The Central Control System ICS is

usually physically secured enough; however, it is mainly because of the control system that it is endangered by the attacks on unauthorized access to process data for the purpose of process control.

The issues of security and the protection of the SCADA systems, as critical components are investigated for a long time in a period of time, and even though almost all the problems are known and all the best practical solutions in this area have been applied, it is still not possible to achieve the maximum safety of the operation of these systems. One of the crucial reasons for this is the architecture of these systems and their spatial distribution (Krutz, 2006, pp. 7-10).

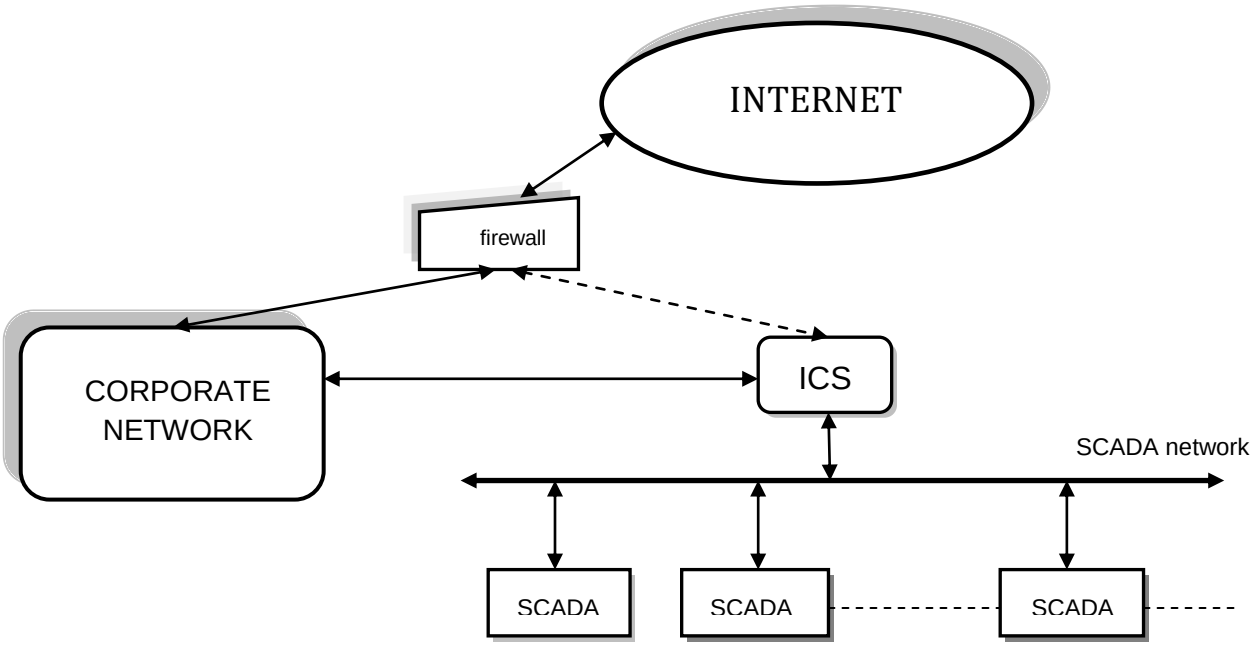

Figure 1- The architecture of the ICS/SCADA system.

The paper further presents possible solutions and recommendations for achieving a high level of security of SCADA systems, as well as the possibility to analyze the achieved level of security and the protection of ICS/SCADA system.

The following specific actions should be taken to increase the security of SCADA networks:

1. Identify all external connections to the SCADA networks;
2. Turn off the unnecessary ties to the SCADA network;
3. Assess and improve the safety of all remaining connections to the SCADA network;
4. Improve the operation of SCADA networks by removing or disabling the unnecessary operational service;
5. Do not use standard protocols for data transfer in order to protect the ICS/SCADA system;
6. Implement the security features that are enabled by the devices recommended by the manufacturer;
7. Establish firm control over all media used for a systematic approach to SCADA networks;
8. Establish a system for the detection of internal and external intrusion in the ICS/SCADA system and establish a continuous monitoring of incidents;
9. Perform technical review of SCADA devices and networks, as well as any other associated networks to identify security problems;
10. Establish physical and technical (FT) control and perform security assessments for all remote devices and systems connected to the SCADA network;

11. Establish SCADA expert teams to identify and evaluate possible attack scenarios on the ICS/SCADA system.

The following steps focus on management actions to establish an effective cyber security program of ICS/SCADA system:

1. Clearly define cyber security roles, responsibilities, and authorities for managers, system administrators, and users.
2. Document network architecture and identify systems that serve critical functions or contain sensitive information that require additional levels of protection.
3. Establish a rigorous, ongoing risk management process.
4. Establish a network protection strategy based on the principle of defense-in-depth.
5. Clearly identify cyber security requirements.
6. Establish effective configuration management processes.
7. Conduct routine self-assessments.
8. Establish system backups and disaster recovery plans.
9. Senior organizational leadership should establish expectations for cyber security performance and hold individuals accountable for their performance.
10. Establish policies and conduct training to minimize the likelihood that organizational personnel will inadvertently disclose sensitive information regarding SCADA system design, operations, or security controls.

As can be inferred, a high level of ICS/SCADA systems can be achieved by applying complex activities, systems and security measures and protection. These activities include organizational measures, the implementation of measures to protect access to data via the appropriate logical protection measures, and establishing a system of physical and technical security with multiple levels of protection. In addition, a continuous monitoring of security and functioning of the ICS/SCADA system is necessary. For the analysis of the achieved level of protection of ICS/SCADA system, the penetration test (pen-test) is used. Penetration tests are an integral part of the complete audit (auditing) security system.

Penetration testing belongs to a domain of ethical hacking where appropriate information security experts are hired to perform security attacks to various levels of ICS/SCADA systems, with the aim of discovering all vulnerabilities and gaps in the protection of these systems.

Penetration test is a method of evaluation of computer and network security by simulating an attack on a computer system or network from external and internal threats. The process involves an active analysis of the system for any potential vulnerabilities that may result from insufficient or improper system configuration, known and unknown hardware, software or operational failures, shortcomings in the application of technical and safety protection. This analysis is done from a position of a potential attacker and can involve active exploitation of security vulnerabilities.

The level of protection and all discovered security weaknesses are then recorded and submitted to those responsible for the security of ICS/SCADA system. Effective penetration tests will incorporate the information obtained from the tests with the assessment of potential safety threats to ICS/SCADA system, to carry out a series of technical and procedural countermeasures to reduce security risks.

Penetration tests are important for several reasons, in order to:

- Determine the feasibility of a set of attack vectors.
- Identification of higher risk vulnerabilities that are due to a combination of lower risk vulnerabilities exploited in a specific order.
- Identify vulnerabilities that are difficult or impossible to detect by standard network or application software for vulnerability scanning.

- Estimates of the size of the possible impact on the business and operational activities for successfully executed attacks.
- Testing the network protection capability to successfully detect and respond to attacks.
- Providing evidence for increased investments in security personnel and technology

Despite the intensive application of these recommendations and technical means for the protection of ICS/SCADA systems, there is very little evidence showing the insecurity of ICS/SCADA systems and devices. More important, this trend of uncertainty continues to grow as more and more of these systems and devices are connected to the Internet. Using the internet, you can easily search and find the built-in ICS/SCADA systems that are exposed to the Internet. In addition to Google and other search engines, the attackers can use other websites for this purpose. All this is especially true for ICS/SCADA systems implemented in the past that were and are exposed to the Internet, and did not have any built-in security mechanisms. In addition, these systems, which are numerous, especially in critical infrastructures, are usually not later upgraded in terms of security and protection against unauthorized access, so they become an easy target for the attackers.

For the analysis of vulnerability of ICS/SCADA systems, an IT trap can be applied - *a honeypot* to detect the attacks on the system. In computer terminology, a honeypot is a trap to detect, deter, or otherwise oppose the attempts of unauthorized use of information systems. Generally, it consists of a computer, data and networks that look like they are part of the core network, but in fact represent their imitation and are monitored in isolation, and seem to contain information or resources of value to the attackers. Honeypot works like intrusion to detection systems (IDS), which are implemented in each instance of ICS/SCADA systems, but in this case virtual and not actual address is used. Honeypot architecture is implemented to fully emulate the real ICS/SCADA system and is used to collect the data on who, when and for what purpose attacks the real ICS/SCADA systems.

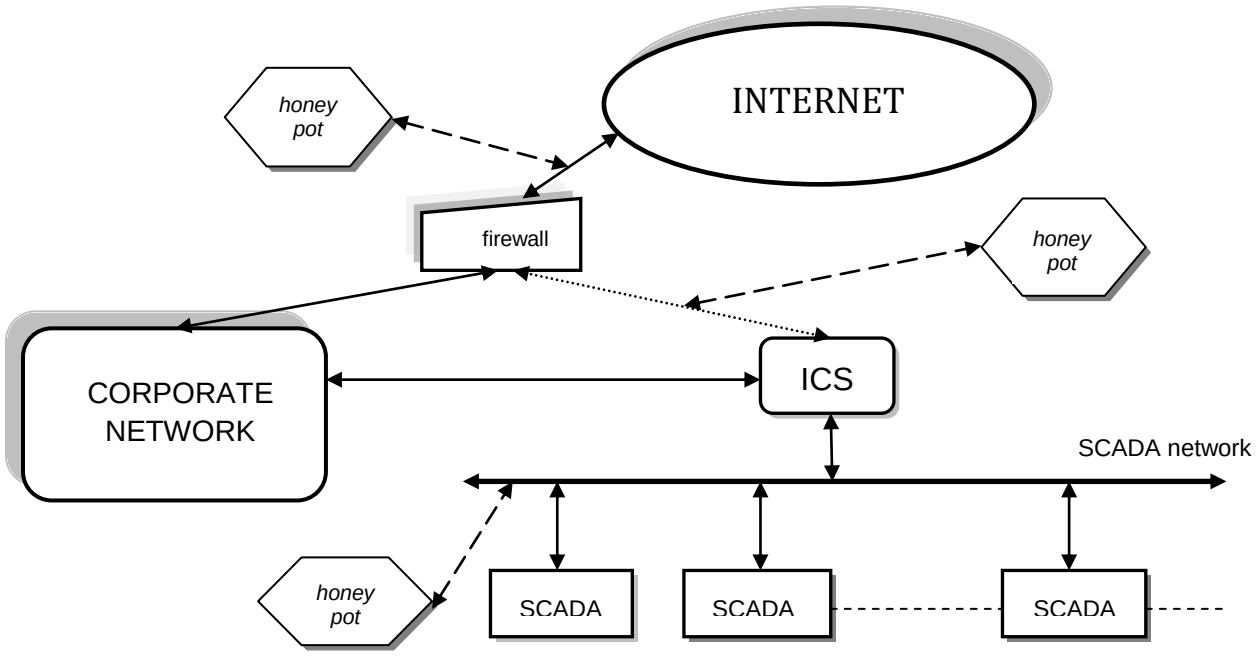

Figure 2 - *Honeypot* architecture

A research example that can show the effectiveness of this architecture, realized on the Amazon EC2 cloud web service with three instances (Wilhoit, 2013). These instances are replicating the work of real

SCADA and PLC devices in the system that control the water pressure in the water system and were used to collect statistical data about the attacks on them. In addition, *the honeypot* instances are displayed as part of a real project within the water system and are optimized for search engines and launched on Google, to attract attention and allow attackers to easily find them.

After only a 18 hours of its launch on the internet, found the first signs of an attack on one of the honeypot instances. During the time that the honeypot instances continued to collect statistical information about the attacks, the results obtained by statistical analysis proved to be alarming. Statistics from this report contains data for 28 days with a total of 39 attacks from 14 different countries, which of these attacks, 12 were unique, and can be classified as a "target", while 13 attacks are repeated of the same actors, for a period of several days and can be considered or the "target" and / or "automatic". All in all, China has accounted for most of the attacks, the attempts of 35% of the total number of attacks, followed by the U.S. with 19%, and Lao by 12%. Other attempts to attack, with a percentage of less than 10%, came from the following countries: United Kingdom, Netherlands, Japan, Brazil, Poland, Vietnam, Russia, Palestine, Chile, Croatia, and North Korea.

As implied, the ICS/SCADA systems exposed to the Internet are relatively an easy target for the attackers. Until adequate security of these systems is implemented, these types of attacks are likely to become very common and destructive in the years to come. However, the origin of the attack and the attacker motivations are not questionable. Continued research must be focused on the motives, the sources of the attacks, the improvement of security techniques and the increasing sophistication of ICS/SCADA system. It is expected that the trend will continue in the area of the attacks on ICS/SCADA system, with possible far-reaching consequences. With continuous efforts and the use of computer-security techniques, the ability to defend from these attacks will help increase the safety of all organizations in the field of critical infrastructure.

2. SOCIAL ENGINEERING AND CRITICAL INFRASTRUCTURE SYSTEMS

Critical infrastructure systems belong to the category of socio-technical systems that can be classified into two main categories. One category is based on the operation using the ICS/SCADA control and process systems. This group contains all the CI systems whose many components are distributed over a large area in order to manage and control. It primarily relates to energy, transport, industrial and similar systems. The second category of CI systems includes other CI systems whose functioning is not based on the principles of process control, i.e. without the use of ICS/SCADA system. This group is made out of financial systems, medical systems, public administration, etc.

Common to both categories of the CI systems is that they do their operation based mainly on the use of information - communication technologies. Therefore, the security of both categories of the CI system is primarily based and depends on the implementation of the principle of security of information - communication technologies. In terms of protection from security threats in these systems complex physical-technical (FT) protection devices, networks and systems are applied, as well as sophisticated logical protection against unauthorized access to data and all the components of the CI system. However, despite the establishment of a high level of quality, the application of modern FT and logical protection still has certain shortcomings, which leads to the fact that the absolute safety of the CI system cannot be achieved.

The next level and one of the sophisticated ways of security threats of the CI system is the use of social engineering.

Social engineering is based on the application of appropriate procedures that mislead people who are somehow involved in the functioning of the CI system to collect data and information that enable attackers to the system, input and access data and information-communication components of the CI

system. In short, social engineering is a form of manipulation of individuals in order to indicate that they do something they normally would not do, and refers to the fulfilment of certain requirements set by the attacker.

Critical infrastructures are vulnerable to the attacks from many angles, including the physical access attacks and attacks carried out over the network. Co-dependence between the infrastructures puts all at risk, so that a successful attack on one part of the system is likely to affect the other parts of the system that are not directly attacked, but are mutually connected (Parker et al., 2004, p. 229).

The attacks of social engineering use human interactive communication, where communication skills are used so that the victim is cheated into doing a compromising thing, such as the disclosure of personal information, or opening e-mail messages that contain malware. Social engineering can be combined with many other methods in order to compromise the security of computer systems. While social engineering attacks are simple and low-tech, they can be surprisingly effective if performed well (Kanellis et al., 2006, p. 16).

The ways of conducting social engineering can methodologically be divided in relation to the presence or absence of communication and contact between the attacker and the attack on:

- The execution by contact;
- The execution without contact, and
- The combined method of execution.

Each mode of execution of social engineering has its advantages and limitations, and a person who successfully uses social engineering achieves their goal by using different methods and procedures. If he feels that his victims are becoming suspicious about testing and access, the person who uses social engineering methods also changes the attack. In the attack of social engineering, the techniques are often combined (Janczewski et al., 2008, p. 183).

The common techniques (methods) of misleading by Mitnick are:

- Impersonating a colleague;
- Posing as an employee in a service provider company, partner companies or Enforcement Section;
- Posing as someone who is in a higher position;
- Impersonating a new employee who needs help;
- Offers help if it comes to a problem, then causes the problem, which leads to the victim asking help from the attacker;
- Sending the victim a free software or upgrades to install;
- Sending viruses or Trojan horses attached to an e-mail;
- Recording the victim's typing on the keyboard using the computer system or program;
- Leaving the diskettes or compact discs with malicious software at the workplace;
- Use of internal terminology of a specific internal organizational unit in order to gain the person's trust, and ... (Mitnick et al., 2003, p. 334).

All of these techniques can be classified into three main groups:

- False impersonation technique;
- A technique of exploiting negligence, carelessness and ignorance of targets, and
- Technique of reverse social engineering.

It should be noted that the techniques are rarely used alone and that it is usually a combination of two or more techniques. When it comes to CI systems, the use of social engineering is not simple because the CI

system structure is usually very complex and the operation is based on expert knowledge and high technology (Gonzalezet al., 2006, pp. 79-90).

Today, after the 11th of September 2001, social engineering is a part of a well organized cyber attack aimed to cause panic with physical attacks on critical infrastructure and facilities, such as companies, water and energy systems (Janczewski et al., 2008, p. 183).

An interesting classification was implemented in the U.S., where they studied and analyzed specific types of groups or organizations that could possibly attack the critical infrastructure of the state or government computer networks. It was found that at the national level, over 100 countries have technology and information prerequisites for this type of attack. At least 20 countries have targeted the United States in the past, and some of them have the same features of information technology and knowledge as the United States (Parker et al., 2004, p. 220).

According to this classification, the following groups are identified as threatening:

- National governments (the rarest threat, but in the case of an attack the biggest damage can be made);
- Terrorists;
- Spies, including corporate espionage;
- Organized Crime;
- Insiders, and
- Hackers (the most common threat, but the slightest possibility of damage).

According to this classification, an insider is a person who is not necessarily employed in the legal entity that is under attack. In the context of these threats, insiders are those who have access to computers and computer networks, and have knowledge of the value of the information contained in the legal entity. This group comprises a majority of the employees, but may also include the family members of employees, business partners, customers, suppliers, and, in rare cases competitors.

In terms of threats made to CI with this method, apart from the usual methods and techniques of social engineering, it is necessary for these attackers to have highly professional and practical knowledge of the corresponding domain of critical infrastructure (electronics, IT, telecommunications, technology, energy, etc.). For this reason, this threat is most effectively carried out by a combined approach in the form of synergies of external and internal sources of danger, that is, the employees and the attackers who have no employment relationship with the target of attacks.

However, the attackers first need to learn this expert knowledge, and then to gather further information about the components and entities, which are necessary for the implementation of social engineering. All this requires a very large amount of time, measured in months and years, or requires a serious commitment of teamwork.

In what way is it possible to speed up the preparatory work for the implementation of social engineering? One way is to attempt to insert malicious software, and if it is accepted and activated, it provides the access to CI. Here the technique of exploiting the negligence is used, carelessness and ignorance of targets as well, including: eavesdropping in public places, looking over the shoulder, examining the offices, reviewing the contents of a computer, monitoring an employee entering in the restricted-protected area, looking at waste, installation of malicious programs , phishing…

In addition to phishing, a new term appears, that represents the combined performance of social engineering - Vishing. English title is the abbreviation of Voice (voice) and phishing (phishing). Vishing indicates a criminal activity that uses a combination of voice (actual social engineering contacts) and phishing (the execution of social engineering without contact), where the use of voice makes the targets go to a fake web address (Humphreys, 2008, p. 253).

Because of the complexity of these attacks all the above is usually not enough to speed up the intrusion.

Another way to help speed up these procedures is hiring an insider, someone who works within the CI system and is in some way familiar with the information and operating of the CI system. This person, who has access to system components, may install the malicious software that allows an attacker to enter the system. In case they do not have access, or enough privileges to install the software, an insider can attempt to use social engineering to obtain confidential information for that purpose, an approach to familiar faces from the surroundings is used if those familiar faces are in charge of the operation of the CI systems and in some way can carelessly provide the necessary information about the system.

If an insider does not have access to familiar faces, he/they may try, together with the external source of danger to bring the technique of reverse social engineering.

It is believed that a reverse social engineering attack is the most complicated of them all because it takes a lot of preparation and skills in order to be successfully performed (Gregg, 2006, e-book). Reflected in the fact that the person who carries out social engineering is in their views, knowledge and action, according to the targets, a positive and legitimate person, someone they are looking for information from (Granger, 2001). This technique is the most difficult to detect because the target is contacted by the attacker without doubting his identity as an expert in a particular area (Kee, 2008).

The premise of this technique is in a nutshell reflected on the creation of a problem with the targets by the person who carries out the social engineering or by an insider that is later on invited by the target to resolve the troubleshooting. Of course, in addition to solving the problem the attacker uses the position in which he found himself, moving to locate and retrieve information that were the main target of the attack.

The attack involving these techniques must be well planned and consists of the following three phases:

- Sabotage,
- Promoting of the attacker, and
- Assistance (Nelson, 2001).

Sabotage can be a real problem that exists or suspicion of the targets that there really is a problem. The real problem and the doubt are created by the attackers using other techniques.

Promoting essentially means that the attacker in the first place has the knowledge and skills to solve the problem. For targets that belief can be achieved by previous contacts with the attacker when he assured the target that he was well suited to address these problems, therefore, the targets would address the attackers for help. An attacker can call the target presenting as an employee of the company that supplied hardware or software in question, and give their phone to contact him in case of any problems. Another way of promoting is to make a false report for the target to see on their monitor, saying that an error in the system occurred and to contact the persons who is suitable for the problem solving.

And finally, help providing, when the person who executes the social engineering, in order to solve this problem asks for information from the employee. Since the problem is resolved quickly and professionally, everyone is generally satisfied that the attacker got the information he needed.

Given that there are many examples of successful attacks on CI systems through social engineering, the basic protection from the attacks is by a method of staff training and learning about the methods and techniques of social engineering. This is especially significant for the CI systems implemented in the past, with older generations of technology and the application of simpler safety and protection measures. A particular problem represents the fact that people who now manage the CI systems are not sufficiently familiar with the way of functioning of these systems in the past.

3. SOCIAL NETWORKS AND SYSTEMS OF CRITICAL INFRASTRUCTURE

Another way to speed up the process of coming to confidential information about the CI system is by collecting and analyzing the information from the relevant social networks using the methods of social engineering by contact through social networks and internet chat rooms. Certain people carelessly put confidential information on social networks about themselves, their business, and even about some functional characteristics of ICS/SCADA and other technical systems.

Enforcement of social engineering through social networks is a particular risk for two main reasons. The first greatest danger threatening the execution of this method of social engineering is its variety and changeability. The attacker can falsely present himself through private messages and mislead the target into giving the information he requires. If, however, the attacker estimates that this technique alone will not be effective, he may misrepresent first, then use the target's emotions such as empathy, and make him take a malicious program that will allow him access to all required information. However, if there is not enough time available, the attacker may decide not to waste time on the misrepresentation, but to send a web address with a multimedia content and by its activation the installation of malicious software is initiated. By these examples we can see that this method of execution of social engineering techniques can include all categories, individual or combined, and that all forms of its expression cannot be strictly and precisely predicted. Therefore, the mechanisms of defence (protection) must be flexible, and must include a very detailed training that provides a good understanding of all the aspects of these threats and the ability to recognize it regardless of the method the attacker uses.

Another reason that makes the execution of social engineering through social networks particularly dangerous is the characteristics of users of social networks. A large number of users of these networks present ignorance of the basic rules of personal precautions, and disregard for their own safety, and above all the neglect of the safety of the organization they work for. As a result, the users are highly prone to releasing personal information, disclosure of accurate information about the place of employment and job description, they use the same password for a social network account, as they use for their e mail accounts and work related accounts, etc. These mistakes make it so much easier for the attacker to act, as they allow him to require most of the information, or at least the information necessary for the execution of social engineering, by simple searching through some of the general search engines or social networks. These mistakes also increase the damage when it comes to the attack, because after the execution of social engineering, the attacker has a free passage to all the sites, services and applications that the user is using. Another important characteristic of the users of social networks is that they are by definition open to contact with other users. Communicating and getting to know other people is basically the purpose of social networks, which makes it easy for the attacker, as it excludes the need for finding a way for the target to accept the contact.

The advantage of this method of execution of social engineering is reflected in the minimal cost, failure to discover the identity of the attacker, a great flexibility in the choice of techniques and cooperativeness of the target.

The number of users of social networks, and the number of potential targets, is growing rapidly, which is why the enforcement of social engineering is increasing, and there is no end to it at this moment.

However, the social networks can also have a significant role in the protection of CI in crisis situations, in case of floods, nuclear accidents, epidemics, etc... The social networks and related software can further help in overcoming the major organizational deficiencies, as well as updating and replacing command and control structures, where they are vulnerable to crises.

In addition, the social networks can minimize the impact of crises and speed up the recovery of CI after accidents.

On the other hand, the social networks can be a critical part of the same infrastructure that must be protected. The social networks can be one of the good ways for sharing and gathering of information useful for the operation of CI, and for organizing various activities and engagement of resources to supplement the features of the CI (e-government can be used as an example). The new reality is that more and more connecting of physical networks of CI and social networks are realized, which can lead to security threats due to their interdependence, and due to the impact of various factors, requirements and restrictions (major energy and telecommunication systems can be used as an example).

However, the problem may appear if when the crisis occurs, the social networks which in the function of infrastructure are dangerous for the society and the economy (and dependent on each other), were attacked or disabled. The lack of information, the submission of false information and the loss of contacts from the social network may impair their ability to respond in emergency situations and lead to the delays in the operation of CI. In these situations, methodologies and techniques that have been developed for "traditional" critical infrastructure are not usually able to deal with the crisis of social networks. One reason may be that, in this case, it is not possible to organize emergency procedures for the recovery of social networks.

Particular problems when it comes to the security of the CI are anti-social networks that are created for the purpose of destabilizing the system CI (Chai et al., 2008, pp. 256-273). The founders of these networks can be a variety of criminal and terrorist groups, and even individual states that want disempowering the CI of other hostile countries, although this is usually not easily proved. Within these networks an exchange of information is performed in order to attack the CI systems, their security flaws, vulnerable targets, functioning, responsible individuals, etc. Also, the development of Cloud network infrastructure for the support of social networking has enabled the availability of command architecture and control servers that coordinate these malicious attacks. The nature of such architecture makes it more difficult to determine who owns and who controls these systems.

Here are some of the ways that the social networks increase the safety of CI. This is primarily related to:

- Risk assessment - identify vulnerabilities of CI and categorize social networks as a new security threat;
- Monitoring - monitoring the social and anti-social networks that are potential sources of attacks on CI;
- Early warning – the use of social networks for monitoring of potential targets of CI and respond to early warnings and signs of an attack;
- Forensic analysis – the analysis and decision making in real time on recognizing the signs of a distributed attack on CI; and,
- Information sharing - sharing of information and exchange between the actors involved in functioning and safety of CI, the public and private sectors and others about previous accidents, vulnerabilities and protection options of the CI system.

Based on the previously stated possibility of threats and the protection of CI through the social networks, it can be concluded that this security aspect of co-depending of CI and social networks, has not been sufficiently studied and applied in regards of the protection of CI. For this reason, in the future research, in addition to security threats, it is necessary first of all to identify the safety measures that will minimize the threat to the future security of the system CI, and are caused by the "dark side" of the social networks. The reason for this may be a sudden development, dissemination and use of social networks in all directions and areas, and therefore, their impact on the security of the system CI is obvious.

CONCLUSIONS

Critical infrastructure systems belong to the category of socio-technical systems and in terms of security threats can be considered three aspects. The technical component of the system is based on the use of ICT and ICS / SCADA systems for process control within specific categories of CI systems. At the same time, ICS / SCADA system is a critical security component for their architecture and implementation of a large number of components and the large spatial distribution. For this reason, despite the use of appropriate organizational and technical security measures, the absolute safety of these systems can not be achieved.

All categories CI system are vulnerable also on the other no technically sophisticated ways eminent threats like social engineering or through social networks. The main activities in this case relating to the collection of all necessary information about CI systems, to allow attack and access to technical information and components in order to take control of CI systems.

Also, there is a sudden development, dissemination and use of social networks in all directions and areas, and is therefore, evident, and their impact on the functioning and security of the CI systems. For this reason, in future research, in addition to potential security threats, it is necessary first of all also to identify safety measures that will minimize future threats to the CI system, which are caused by the "dark side" of social networks.

Special security problem exists in all categories of the CI systems implemented in the past with older generations of technology and the application of simple safety measures and protection. In addition, in these systems there is a so called. generations conflict in technology and personnel, which leads that people who today manage the CI systems are not sufficiently familiar with the manner of functioning and implementation of these systems in the past. For this reason, it is urgent to perform re-engineering of these systems in order to achieve interoperability between the older and newer technology generations.

It can be concluded that the basis for achieving the safe functioning of CI systems is the application of risk management principles with the following components: implementation of organizational and technical security measures to protect the technical components of the system and training of all employees to become familiar with the techniques of application methods of threats through social engineering and social networks.

REFERENCES

1. Krutz, R. (2006). *Securing SCADA Systems*, Wiley Publishing Inc, USA
2. Wilhoit, K. (2013). *Who's Really Attacking Your ICS Equipment*?, Trend Micro Incorporated, Research Paper
3. Gonzalez, J., Sarriegi, J., Gurutxaga, A. (2006). *A Framework for Conceptualizing Social Engineering Attacks*, First International Workshop, CRITIS 2006, Samos, Greece
4. Chai, C,-L, Liu, X., Zhang, J.W., Liu, D., Dyachuk, D., Deters, R. (2008). *Social network analysis of the vulnerabilities of interdependent critical infrastructures*, International Journal of Critical Infrastructures, Vol. 4, No. 3
5. Kanellis, P., Kiountouzis, E., Kolokotronis, N., Martakos, D. (2006). *Digital crime and forensic science in cyberspace*, Idea Group Publishing (an imprint of Idea Group Inc.), Hershey – London
6. Janczewski, J. L., Colarik, M. A. (2008). *Cyber Warfare and Cyber Terrorism*, Information Science Reference, Hershey - New York
7. Mitnik, D. K., Sajmon, L. V. (2003). *Umetnost obmane*, Mikro knjiga, Beograd

8. Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management, Information Security Technical Report, Volume 13, Issue 4, November 2008.

9. Kee, J. (2008). *Social Engineering: Manipulating the Source*, April 28th 2008, http://www.sans.org/reading_room/whitepapers/engineering/social-engineering-manipulating-source_32914, Accessed on 22.07.2013.

10. Nelson, R.: *Methods of Hacking: Social Engineering*, http://sodaphish.com/files/ebks/try2innovate.com/downloads/E-books/Hacking/Methods%20of%20Hacking%20-%20Social%20Engineering.pdf, Accessed on 25.04.2012.