http://dx.doi.org/10.5755/j01.eee.20.7.8027

An Improved Risk Assessment Method for SCADA Information Security

J. D. Markovic-Petrovic[1], M. D. Stojanovic[2]
[1]*CE Djerdap Hydroelectric Power Plants Ltd., HPP Djerdap 2,*
Kraljevica Marka 2, 19300 Negotin, Serbia
[2]*University of Belgrade, Faculty of Transport and Traffic Engineering,*
Vojvode Stepe 305, 11000 Belgrade, Serbia
jasna.markovic@djerdap.rs

***Abstract*—In this paper, we address information security risk analysis in SCADA systems and propose an improved security risk assessment method in the case of attacks on the SCADA information and communication infrastructure. The assumption is that intrusion prevention/detection systems are implemented as security mechanisms. The proposed method has been demonstrated on an example of the SCADA system in a hydropower plant. Cost-benefit analysis has been performed on the basis of the Return on Security Investment.**

***Index Terms*—Cyber-attack, information security, return on security investment, risk assessment, SCADA.**

I. Introduction

Evolution of the Supervisory Control and Data Acquisition (SCADA) systems has in the previous decade created a substantial problem pertaining to their security. Reasons for their vulnerabilities to different forms of cyber-attacks include the following: (1) implementation of open communication standards, (2) connectivity of the control systems with other networks, (3) limitations in the existing security technologies, (4) remote access, and (5) availability of technical information on control systems. Because the security of SCADA systems is of high importance due to their indispensable role in the industry, this is a current field of research with the expectation of specific solutions for security and information security risk management.

A secure ICT system should, in general, provide the following, by order of priority: confidentiality, integrity and availability. Industrial remote monitoring and control systems have the same security requirements, however in a reversed order. The pathway towards the fulfilment of the security requirements dictates the adoption of a security policy that clearly defines regulations, business process protocols, staff roles, permissible activities, actions and processes [1], [2]. Regulations define methods for protecting the integrity of the information, determine the confidentiality of information, data availability, as well as the access control of resources and applications.

ICT systems in the electric power utilities are required to meet high standards in terms of reliability, availability and transfer of correct and timely information for the purposes of production planning, efficient utilization of the energy potential, remote management in production, transmission and distribution areas, reporting and successful business management of the system in general. From the remote management aspect, measuring, control and management of the electric energy production in hydroelectric power plants, SCADA has a central role. Fig. 1 shows a block diagram of SCADA implementation based on stand-alone concepts. Such concepts enable the highest reliability level of the production cycle because in the instance of an outage of any of the production-transfer units, generator-transformer, other areas and all other production-transfer units remain in the production cycle undeterred. The ICT structure of such units is enjoined into one synergy at the level of SCADA systems.

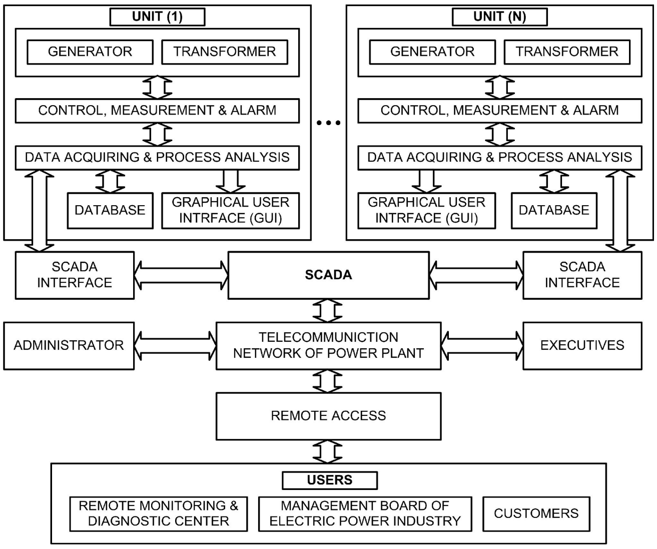
UNIT (1)
GENERATOR
TRANSFORMER
CONTROL, MEASUREMENT & ALARM
DATA ACQUIRING & PROCESS ANALYSIS
DATABASE
GRAPHICAL USER INTRFACE (GUI)
...
UNIT (N)
GENERATOR
TRANSFORMER
CONTROL, MEASUREMENT & ALARM
DATA ACQUIRING & PROCESS ANALYSIS
GRAPHICAL USER INTRFACE (GUI)
DATABASE
SCADA INTERFACE
SCADA
SCADA INTERFACE
ADMINISTRATOR
TELECOMMUNICTION NETWORK OF POWER PLANT
EXECUTIVES
REMOTE ACCESS
USERS
REMOTE MONITORING & DIAGNOSTIC CENTER
MANAGEMENT BOARD OF ELECTRIC POWER INDUSTRY
CUSTOMERS

Fig. 1. An example of SCADA system in a hydroelectric power plant.

Modern telecommunication systems supporting SCADA rely on the Internet protocol (IP) and Ethernet technologies. SCADA-specific protocols are being developed at the application layer (including data models and presentation) and use the IP protocol stack. SCADA systems are typically integrated into a common IP-based network, together with the other operational and corporate telecommunication services. Networks thus designed have certain weaknesses

Manuscript received January 21, 2014; accepted May 26, 2014.
This research was funded by a grant (No. TR 32025) from the Ministry of Education, Science and Technological Development of Serbia.

and vulnerabilities that malicious users are familiar with.

It is particularly difficult to detect and prevent distributed attacks where several attackers simultaneously attack a target (i.e. a vital network server). This type of an attack is known as distributed Denial of Service (DDoS) and can be launched at any layer of the protocol stack. Research shows that such attacks on industrial control systems are quite frequent and may have severe consequences [3], [4].

Design of security system assumes a detailed risk analysis, which should be periodically repeated (in parts or entirely) during system exploitation and upgrade. The main objective of this work is to propose a risk assessment method suitable for industrial SCADA systems that will allow the determination of the optimum level of security investment and definition of different levels of acceptable risk.

II. Information Security Risk Management

The sum of system vulnerabilities, threats to the system and impacts makes up the risk. Risk is a function of the probability that a particular source of threat will use a potential vulnerability, resulting in detrimental and unwanted impact on the business. In order to undertake risk analysis, the following factors must be recognized, assessed and defined: (1) asset; (2) vulnerability; (2) threat; (4) impact and (5) controls.

There are no risk-free systems, and the costs of such a solution would surpass the asset value to be protected or the value of the losses caused by the risk. Therefore, the focus is directed from avoiding to managing the risk, with pre-defining the acceptable risk level. Risk management includes several steps: (1) identification of the system and system components; (2) identification of asset and its value; (3) establishing of the security objectives; (4) risk analysis through identification of vulnerabilities and threats; (5) risk assessment; (6) making decisions on acceptable risk; (7) selection and implementation of measures to decrease the level of risk. Risk management is a continuing process and all steps are cyclically repeated in order to improve the security system and decrease the level of risk.

In discussing ICT security, risk pertaining to a particular resource is assessed on the basis of the asset value, resource vulnerabilities, threats that might abuse those vulnerabilities, probability that the threat will be realized and impact caused if the threat is realized [5]. Risk management includes identification, selection and implementation of controls that will decrease the assessed risk to the acceptable level.

The most important part of the risk management process is risk assessment, which is also the area most susceptible to errors. Literature lists different approaches, methods and tools for the information security risk assessment. Qualitative assessment proposes methods that interpret loss as a subjective measure, i.e. risk level is assessed as low, middle or high. Quantitative assessment is based on a mathematical approach (numerical analysis, statistical methods) that interprets risk in numerical values of appropriate units. These can include economic values such as the expected annual loss, investment return, etc. A comparative analysis of the different approaches to risk assessment can be found in [6].

Information Security Risk Analysis Method (ISRAM) [7] is a quantitative method that allows effective participation of managers and staff into the process. Structured in seven steps, ISRAM provides a guideline for risk assessment that considers the probability of occurrence as well as the consequences of occurrence of security breaches. A risk management framework using Bayesian networks has been proposed in [8], with the objective to determine the network compromise probability under different levels of attack. Iheagwara [9] represents a model that introduces the Cascading Threat Multiplier (CTM), multiplying factor that will be included into expanded definition of Single Loss Expectancy (SLE). CTM is somewhat subjective and is introduced mainly for the purpose to think in broader terms and look at the bigger picture when considering the risks associated to the compromise of a given asset. In the method proposed by Suh and Han [10] the significance of various business functions of the business model and the necessity of various IS assets are determined. Considering that the available risk assessment methods and tools are expensive and designed for large enterprises, a simplified risk assessment algorithm that is tailored for the small and medium enterprises has been proposed in [5].

Although quantitative approaches enable precise risk assessment, methods which propose expressing ICT resources value only by their book value are inadequate for SCADA systems. Security risk assessment in such systems assumes definition of risk metrics based on the probability of attacks occurrence and their impact to the continuity and performance of the industrial process [11], [12]. Loss assessment pertaining to a realized risk is complex and there is no reliable methodology to enable forecasting loss with high precision. For better results, more parameters should be included in the analysis. The main novelty of this work is the proposal of an improved risk assessment method, which calculates loss expectancy taking into account the impact of attack strength to SCADA system’s performance and the set of different conditions that may increase indirect losses.

III. The Proposed SCADA Risk Assessment Method

The objective of investing in ICT security is increasing the security of information assets from all types of threats. Investments in ICT security can be financially represented, which is not the case with their benefits in terms of decreased potential losses. The questions that need to be answered are: (1) when is a system secure enough and (2) what is the price of such a protection, because a greater investment in security does not necessarily ensure a higher level of security.

An expected result of the information security risk management process is a quantitative value assigned to each risk that can be used for ranking all risks, complete with defining of critical levels and priorities, measures to ensure feasibility of investing in security and preparations for unexpected costs.

Traditional risk assessment assumes calculation of the *SLE* as a function of two variables: Asset Value (*AV*) and Exposure Factor (*EF*). Variable *EF* denotes the ratio of lost assets in a particular incident. On the basis of Annual Rate of Occurrence (*ARO*) the value of the Annual Loss Expectancy (*ALE*) can be determined, as follows

$$ALE = SLE \times ARO = AV \times EF \times ARO. \tag{1}$$

The indicator of cost effectiveness of investing in ICT security is Return on Security Investment (*ROSI*), calculated as investment return ratio within the stipulated period and represents the balance of *ALE* reduced by the ratio of prevented attacks and capital invested in security mechanisms (C_S) [13], i.e.

$$ROSI = \left(ALE \times \%RiskMitigated - C_S\right)/C_S. \tag{2}$$

We further propose a modification of the traditional method for risk assessment in calculating the efficiency of the Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) for protection against a particular class of attacks (e.g., DDoS) on the infrastructure of the SCADA systems. SCADA systems use specific IDS/IPS equipment due to dedicated application layer protocols [12], [14]. To calculate *ROSI*, it is necessary to estimate the value of the investment in security mechanisms, costs created by occurred attacks and the ratio of prevented attacks.

Investing in a security system can incorporate a single investment into the implementation of a security system (C_I) and annual maintenance that includes system updates and technical support (C_M). Because the initial investment is substantial, an average costing over a number of years (*Y*) needs to be factored, beginning with the first year of the implementation of security, as follows

$$C_S = \left(C_I + \sum_{i=1}^{Y} C_{Mi}\right)/Y. \tag{3}$$

Costs caused by attacks can be divided into: (1) direct, that come as a consequence of the disruption of the production process, and (2) indirect, that include system recovery costs and numerous additional costs, i.e. penalties for failing to meet obligations, irrecoverable loss in natural resources, damage to the environment, etc. To determine the costs created as a consequence of a realized attack, the basic *ALE* formula is used whereby the sum of all maximum direct losses (*DL*) during an attack is multiplied by the number of potential attacks during a year. The formula is then modified by the weighting factors that quantify indirect costs (*W*) and weighting factor W_A which role is to scale the proposed maximum direct losses as a function of strength of attack. In general, the assumption is that there are *M* types of direct losses and *N* different conditions that can contribute to indirect losses. This way we obtain the following expression for the *ALE*

$$ALE = W_A \prod_{i=1}^{N} W_i\Big(\sum_{j=1}^{M} DL_j\Big) \times ARO. \tag{4}$$

Selection of weighting factors might be a delicate process, which depends on a number of techno-economic conditions and is, certainly, company-specific. The first prerequisite is to carry out the analysis of historical data in order to obtain statistical values. Second, the probability of the attack(s) occurrence should be determined. Relying on those results, the attacks' effects on the overall costs (direct and indirect) should be predicted. Finally, in order to measure the attacks' impact on the performance, it is desirable that a company defines its key performance indicators (KPIs). KPIs are defined according to company's key performance objectives (productivity, availability, reliability, security, network outage impact reduction, integrity, downtime, etc.) that should support fulfilment of business objectives [15].

Figure 2 illustrates the calculation defined by (4).

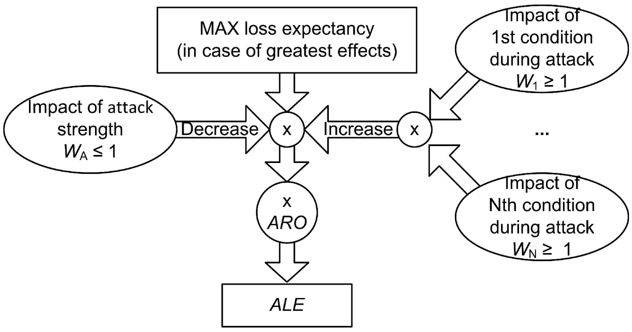
MAX loss expectancy
(in case of greatest effects)
Impact of 1st condition during attack $W_1 \geq 1$
Impact of attack strength $W_A \leq 1$
Decrease
x
Increase
x
...
Impact of Nth condition during attack $W_N \geq 1$
x *ARO*
ALE

Fig. 2. The factors of Annual Loss Expectancy in SCADA system.

IV. Case Study

We observe a run-off-river hydropower plant with the total installed power of 270 MW. The assumption is that two Network IDS/IPS are installed, the first towards the corporate network, the second towards the process network, and one Host IDS per each key server (Fig. 3).

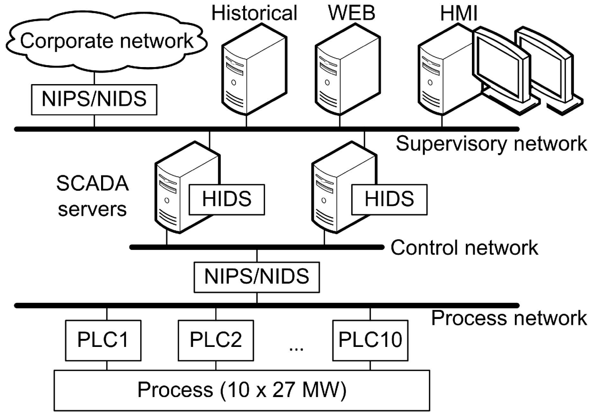

Fig. 3. Architecture of SCADA network in hydroelectric power plant.

In this scenario, the direct loss is caused by the outage in the electric energy production which can come as a consequence of the outage of the production unit, if the target of the attack was the controller of the aggregate block, or as a consequence of failure in power regulation due to the outage of the remote management system. The above costs correspond with the duration of the attack (t_A), time required for system recovery, installed power of the plant (*P*) and unit price of electric energy (c_E). The recovery time is stipulated to be proportionate to the W_A weighting factor with the recovery time after a maximum strength attack (t_{Rmax}). Consequences of the attack can be classified into several groups, i.e.: (1) control disabled without impact on the management; (2) control and management from the remote control centre disabled without impact on the local management and production; (3) control and management from the remote and local control centres disabled without production outage; (4) all control and management systems outage with minor impact on the production process; (5) all control and management systems outage with major impact on the production process. An example for the indirect costs would be the penalties paid for not delivering contracted energy (W_E) and losses created by the evacuation of excess hydro-potential (W_H), if the attack occurred during a period of high inflow, i.e.

$$ALE = W_A W_E W_H P(t_A + W_A t_{R\max}) c_E \times ARO. \qquad (5)$$

An attack can occur at any time of day or year and it is difficult to forecast potential effects. However, it is possible to assess the impact on the costs if an outage in the remote management system caused overflow of excess water. An example pertaining to the defining of weighting factors is provided in Table I. On the basis of thus defined probability functions for weighting factors, expected annual loss can be determined.

TABLE I. WEIGHTING FACTORS.

Impact		Very low	Low	Medium	High	Very high
W_A	Probability	40 %	25 %	20 %	10 %	5 %
	Value	0.01	0.2	0.25	0.5	1
W_E	Probability	5 %	20 %	50 %	20 %	5 %
	Value	1	2	3	4	5
W_H	Probability	0 %	50 %	35 %	15 %	0 %
	Value	n.a.	1	1.5	2	n.a.

Literature [9] stipulates that the probability of detected attacks on the IDS systems falls within the 61.5 % to 86.2 % band. In SCADA systems the intensity of traffic does not show substantial variation, which increases the probability of detection / prevention of attacks (the example proposes the value of 90 %). According to the research [3] the highest probability of downtime caused, for example, DDoS attacks is 30 minutes. The maximum recovery time is stipulated to be 120 minutes. The *ROSI* value depends on the predicted number of attacks on the annul level. In the provided example (Fig. 4) a positive value is achieved if $ARO \geq 3$. The same graph shows the correlation of *ROSI* with the weighting factor W_A, which varies depending on the defined probability function.

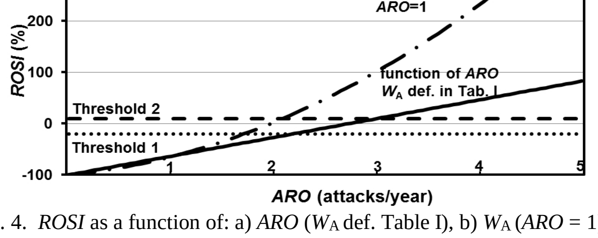

Fig. 4. *ROSI* as a function of: a) *ARO* (W_A def. Table I), b) W_A (ARO = 1).

In making decisions regarding the cost effectiveness of investing in security mechanisms it is important to set a threshold which considers the importance of SCADA systems in the industrial systems and the consequences that a denial of remote management service will have on the society (the graph shows a definition of threshold 1 that accepts the investment for the predicted number of 2 attacks per year, notwithstanding the negative value of *ROSI*).

V. CONCLUSIONS

The paper proposes and investigates an improved method for information security risk assessment, which is suitable for industrial SCADA systems. The method introduces weighting factors that quantify losses in accordance with the attack conditions and its strength. We also discuss the prerequisites for determining the values of weighting factors, according to company-specific needs. The case study refers to security risk assessment of the SCADA system in a hydropower plant. Applying the proposed method in a real system enables the assessment of potential loss expenses and cost-benefit analysis of the stipulated security mechanism. Establishment of a predefined threshold for *ROSI* should contribute to determining the optimal level of investment in security.

REFERENCES

[1] CIGRÉ Technical Brochure TB 317: "Security for Information Systems and Intranets in Electric Power Systems", JWGD2/B2/C2.01, 2007.

[2] CIGRÉ Technical Brochure TB 419: "Treatment of Information Security for Electric Power Utilities (EPUs)", WGD2.22, June, 2010.

[3] Ponemon Institute: "Cyber Security on the Offense: A Study of IT Security Experts", November 2012.

[4] J. Markovic–Petrovic, M. Stojanovic, "Analysis of SCADA System Vulnerabilities to DDoS Attacks", in *Proc. of the 11th Int. Conf. TELSIKS 2013*, Nis, Serbia, 2013, vol. 2, pp. 591–594.

[5] S. Japertas, G. Cincikas, R. Sestaviskas, "Company's Information and Telecommunication Networks Security Risk Assessment Algorithm", *Elektronika ir Elektrotechnika*, no. 5, pp. 33–36, 2012.

[6] T. Tsiakis, "Information Security Expenditures: a Techno-Economic Analysis", *Int. Journal of Computer Science and Network Security*, vol. 10, no. 4, pp. 7–11, 2010.

[7] B. Karabacak, I. Sogukpinar, "ISRAM: information security risk analysis method", *Computers & Security*, vol. 24, no. 2, pp. 147–159, 2005. [Online]. Available: http://dx.doi.org/10.1016/j.cose.2004.07.004

[8] N. Poolsappasit, R. Dewri, I. Ray, "Dynamic Security Risk Management Using Bayesian Attack Graphs", *IEEE Trans. Dependable and Secure Computing*, vol. 9, no. 1, pp. 61–74, 2012. [Online]. Available: http://dx.doi.org/10.1109/TDSC.2011.34

[9] C. Iheagwara, A. Blyth, M. Singhal, "Cost effective management frameworks for intrusion detection systems", *Journal of Computer Security*, vol. 12, no. 5, pp. 777–798, 2004.

[10] B. Suh, I. Han, "The IS risk analysis based on a business model", *Information & Management*, vol. 41, pp. 149–158, 2003. [Online]. Available: http://dx.doi.org/10.1016/S0378-7206(03)00044-2

[11] S. Papa, W. Casper, S. Nair, "Availability-based risk analysis for SCADA embedded computer systems", *Proc. World Congress in Computer Science, Computer Engineering and Applied Computing*, pp. 541–547, 2011.

[12] G. Dondossola, F. Garrone, J. Szanto, "Cyber Risk Assessment of Power Control Systems - A Metrics weighed by Attack Experiments", *IEEE Power and Energy Society General Meeting*, pp. 1-9, San Diego, CA, 2011.

[13] W. Sonnenreich, J. Albanese, B. Stout, "Return on Security Investment (ROSI) - A Practical Quantitative Model", *Journal of Research and Practice in Information Technology*, vol. 38, no. 1, pp. 45-56, 2006.

[14] B. Zhu, S. Shankar, "SCADA-specific Intrusion Detection/Prevention Systems: A Survey and Taxonomy", in *Proc. of the 1st Workshop on Secure Control Systems (SCS)*, 2010.

[15] ITU-T Recommendation E.419: "Business oriented key performance indicators for management of networks and services", 2006.