SIE 2015
6th International Symposium on Industrial Engineering
24th-25th September 2015
FACULTY OF MECHANICAL ENGINEERING
STEINBEIS ADVANCED RISK TECHNOLOGIES
INNOVATION CENTER FME

A HYBRID SECURITY RISK ASSESSMENT METHOD FOR SCADA NETWORKS

Jasna Markovic-Petrovic[1], Mirjana Stojanovic[2]
[1]CE Djerdap Hydroelectric Power Plants Ltd., HPP Djerdap 2, Negotin, Serbia
[2]University of Belgrade, Faculty of Transport and Traffic Engineering, Belgrade, Serbia

Abstract. *This paper deals with the issue of security risk in Supervisory Control And Data Acquisition (SCADA) systems. We propose an advanced risk assessment method tailored for SCADA systems by a suitable algorithm for determining weighting factors that quantify cyber attack conditions. We introduce a subjective component of the weighting factor based on the system experts' responses to a specific questionnaire. Results of the cost-benefit analysis indicate that return on security investment can be increased with the proposed method.*
Key words: *Information security, Infrastructure attacks, Risk assessment, SCADA, Weighting factor.*

1. INTRODUCTION

SCADA systems monitor and control geographically dispersed process equipment on multiple sites in power grids, water plants, oil refineries and natural gas distribution, and other critical infrastructures. Due to standardization and connectivity to the Internet, modern SCADA systems face with the increased risk of cyber attacks and failures that are inherent to enterprise IT systems [1]. Risk management has been recognized as an integral part of SCADA information security management. It comprises risk analysis, risk assessment methodology, selection of security mechanisms and making a decision on the implementation of appropriate mechanisms.

There are many security risk assessment methods and tools based on recommendations and standards [2]. The methods have been developed to be used mostly in business information systems, and their use for security risk assessment of control information systems in the industry is not straightforward.

This paper proposes an improvement of security risk assessment method for specific SCADA systems described in [3] by introducing a new component, the personal attitude of employees who have work experience in the respective industrial process, control system, IT system, etc. This approach can be justified by the fact that good knowledge of a process along with actual values acquired from statistical analyses should generate a more comprehensive view of potential risks. Consequently, the advanced, hybrid method should provide a more precise risk assessment.

The rest of the paper is organized as follows. Section 2 surveys the related work. The novel hybrid risk assessment method is explained in Section 3. In Section 4, we evaluate the proposed method, and compare it with the reference method [3] on the example of SCADA system in a hydropower plant. Section 5 concludes the paper.

2. RELATED WORK

Literature describes different security risk assessment approaches, methods and tools that can be categorized as qualitative and quantitative. Qualitative risk assessment methods interpret losses as a subjective measure, e.g. the risk level is assessed as low, medium or high. Methods from this category are simple, but they do not provide the possibility of a cost-benefit analysis. In contrast, the quantitative risk assessment is based on mathematical approach (numeric analysis, statistical methods) that interprets the risk in numeric values of appropriate units. Combination of qualitative and quantitative methods is suggested for the information security risk assessment.

One of the methods created for business information systems is CRAMM (CCTA Risk Analysis and Management Method). It is a qualitative method supported with appropriate tools. An integral part of the tools is a rich library of potential vulnerabilities, threats and security measures [4]. Experiences in the application of this tool show that it is not

appropriate for use in SCADA systems due to complex mapping of information assets.

Reference [5] describes methods and procedures that provide a framework for a continuous process of security risk assessment within the electrical power remote control system. The authors have pointed out the necessity of perceiving the consequences which the realization of risks would have on the whole electric power system. Based on the risk index, security measures are proposed and the risk assessment procedure is repeated after the security measures have been implemented.

The risk model based on Bayesian network determines the network compromise probability under different levels of attack. Bayesian network model, used in security risk assessment in SCADA systems [6], identifies four risk sources: human factor, environmental factor, equipment failure and management process failure. The proposed model provides a more objective risk assessment comparing to traditional models.

In the absence of the reference method for security risk assessment in SCADA systems there is a need to define the methodology which would integrate the risk management and security risk assessment for both operational and business infrastructures [7]. In the previous research [3], we have proposed a security risk assessment method in the case of Distributed Denial of Service (DDoS) attack on SCADA system infrastructure. In a DDoS attack, each individual attacker can generate traffic similar to the legitimate one, but the attack strength is increasing by using multiple coordinated sources. This property makes intrusion detection and prevention (IDPS) rather difficult. In [8] we have presented an in-depth analysis of performance degradation and service disruption under DDoS attacks, carried out by simulations of typical SCADA system in a hydropower plant.

Based on the proposed security risk assessment, the cost-benefit analysis is performed for the recommended application of IDPS. Method [3] combines the quantitative and qualitative approaches. The security risk assessment is based on the mathematical approach and economic parameters using Annualized Loss Expectancy (*ALE*) and Return on Security Investment (*ROSI*) calculations. The qualitative methodology is characterized with the defining of weighting factors that quantify the conditions under which the attack has occurred. The method defines prerequisites for determination of these factors, namely statistical data analysis and Key Performance Indicator (KPI) definition in accordance with required performances necessary for the realization of business objectives. Establishment of a predefined threshold for *ROSI* should contribute to determining the optimal level of investment in security.

Weighting factors, which quantify indirect costs, are determined according to statistical analysis of the archived relevant values. The motivation for this work comes from the fact that employees' experiences are relevant for the analysis of a process. Hence, we extend the method proposed in [3] by the adjustment of the weighting factors with introduction of the subjective component, aiming at a more precise quantification of indirect costs. The novelty in this paper is the improvement of the method by an algorithm for determination of weighting factors that quantify indirect costs resulting from the conditions under which the successful infrastructural attack occurred.

3. THE PROPOSED HYBRID METHOD

The method starts from an attitude that the costs incurred by the realized attack originate from: (1) direct costs, resulting from the interrupted production process and (2) indirect costs, including the costs of the system recovery and other costs, such as penalties due to non-fulfillment of contractual obligations, unrecoverable losses of resources and environmental damage [3]. The basic formula for *ALE* includes the sum of maximum direct losses (*DL*) and Annualized Rate of Occurrence (*ARO*). The formula is modified with weighting factors that quantify indirect costs (W_k) and a weighting factor W_A whose purpose is to scale the maximum direct costs in the function of the attack intensity (1).

$$ALE = W_A \prod_{k=1}^{N} W_k \left(\sum_{j=1}^{M} DL_j\right) \times ARO \qquad (1)$$

Figure 1 shows the schematic overview of the calculation procedure.

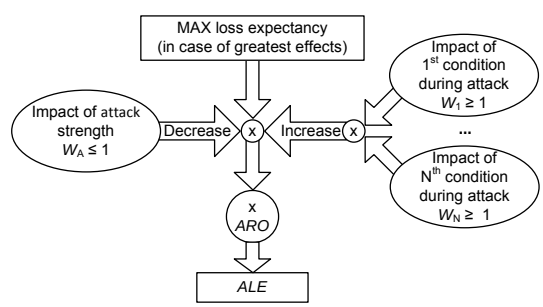

Fig. 1. The factors of *ALE* in SCADA system [3].

Selection of weighting factors is a delicate process depending on a number of techno-economic conditions within the specific SCADA system. After selection the type of weighting factors, it is necessary to determine their values. The algorithm for evaluation of weighting factors is depicted in Figure 2. The algorithm is used for each of the weighting factors in two phases. In the first phase, the experts chosen among the employees who know the process very well, IT specialists and managers are polled. The questionnaire may have one or more (*Q*) Closed-Ended Questions. The question list is

created for a specific SCADA system where a weighting factor is defined for each question (W_q) under the condition $\sum W_q=1$. The questionnaire has been designed to offer the final response categories to each of the questions (e.g. very low, low, medium, high, very high), or the response scale (e.g. 1–5, 0–100%). The quantification of obtained responses (Aj) creates one factor per each expert (Wki) (2). The questionnaires answered by all of the experts (E) serve for the creation of the weighting factors {Wki, i = 1, E}.

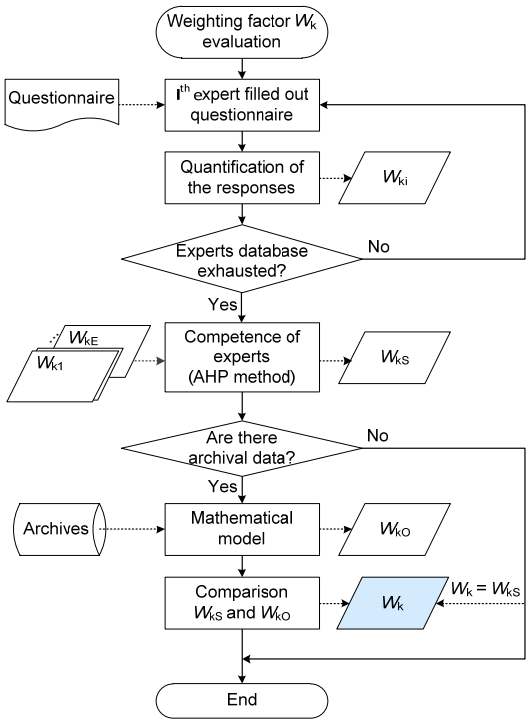

Fig. 2. The weighting factor evaluation algorithm.

The final, subjective value of the weighting factor W_{kS} is determined based on the competence of each expert C_i (3). The competence assessment is performed by Analytical Hierarchical Process (AHP) [9]. It is a multi-criteria decision-making technique that hierarchically presents criteria and performs the ranking of possible alternatives using a series of comparisons of two elements within the relationship intensity scale (up to 9 levels). The method is convenient because the final result is a numeric evaluation of the alternative (the experts, in our case). The obtained weighting factor W_{kS} contains the elements of subjectivity resulting from the choice of questions during the questionnaire design and from the experts' experience.

$$W\mathrm{ki} = \sum_{\mathrm{j}=1}^{Q} W\mathrm{qj} \times A\mathrm{j}, (\sum_{\mathrm{j}=1}^{Q} W\mathrm{qj} = 1) \quad (2)$$

$$W\mathrm{kS} = \sum_{i=1}^{E} C\mathrm{i} \times W\mathrm{ki}, (\sum_{i=1}^{E} C\mathrm{i} = 1) \quad (3)$$

In the second phase, the objective value of the W_{kO} weighting factor is determined based on the data from available archives according to the condition taken for the indirect cost. Based on the archived values, we calculate the occurrence probability of conditions under which the successful infrastructural attack would cause indirect costs. Finally, the comparison and evaluation of the factors, obtained within the two phases, is performed with determination of the final weighting factor $W_k = F(W_{kS}, W_{kO})$.

4. EVALUATION AND RESULTS

In order to evaluate the proposed hybrid method, we adopt the scenario and reference method from [3] and compare the new method with the reference one. Security risk assessment and cost-benefit analysis of IDPS implementation have been performed on an example of a run-off-river hydro power plant. The network infrastructure consists of the two parts: (1) supervisory network where the key elements are servers and human-machine interfaces and (2) process network containing controllers for supervision and control of equipment and sub-systems of the power plant. Supervisory network is connected to the corporate network with access to Internet. The implementation of four IDPSs has been anticipated: two Network IDPSs (one towards the corporate and the other towards the process network) and one Host IDPS per each key SCADA server. We have analyzed possible consequences of a DDoS attack from the aspect of supervision, control and production of electric power, and consequently, two types of costs. Direct costs are the result of the decreased production, and indirect costs are the result of: non-fulfilled obligations regarding delivery of electric power and overflow of the hydro potential if the attack occurred at the time of high inflow. Indirect costs are quantified with weighting factors W_E and W_H respectively, and they have been determined by a statistical analysis of the archived data about production, inflow and electric power delivery requests.

On the same example, we further analyze the use of the proposed algorithm for determination of the value of weighting factors W_E and W_H that quantify indirect costs resulting from DDoS attack on SCADA infrastructure. In order to determine weighting factors W_E and W_H, we have designed two questionnaires with 3 and 4 questions, respectively. We have polled: (a) the dispatcher from the Planning Department, (b) an operator from Control Centre, (c) the manager of the Exploitation Unit and (d) the top manager. The competence of each participant has been determined by AHP method based on the following criteria: (1) work experience, (2) qualification degree, (3) professional field and (4) work position. Table I shows an example of the decision-making matrix elements and the obtained values of eigenvector after the second iteration. The same principle has been used with polled

participants, for each criterion. The competence has been measured by multiplying the obtained eigenvectors. We have applied formulas (2) and (3), and obtained the subjective values for the weighting factors (W_{ES} = 1.96 and W_{HS} = 2.86).

TABLE I. PAIRWISE COMPARISON MATRIX OF THE MAIN CRITERIA.

	(1)	(2)	(3)	(4)	Eigenvector
(1)	1	5	2	4	0,5066
(2)	1/5	1	1	1/7	0,0768
(3)	1/2	1	1	1/3	0,1235
(4)	1/4	7	3	1	0,2931

In the second phase of the algorithm, we have taken the objective values obtained in [3]. The last step is the comparison of the values from the two phases and their averaging.

At the end, we have shown the influence of the improved method on the final *ROSI* value. This indicator of effectiveness of the investment into the security mechanisms represents the relation between the savings due to prevention of a cyber attack and the cost of the implemented measure (C_S) (4) [10].

$$ROSI = (ALE \times \%RiskMitigated - C_S) / C_S \qquad (4)$$

Figure 3 shows the *ROSI* value in function of *ARO* obtained with two risk assessment methods, the reference method [3] and the proposed hybrid method. The diagram shows two values of the proposed threshold that determines the profitability of the investment in security.

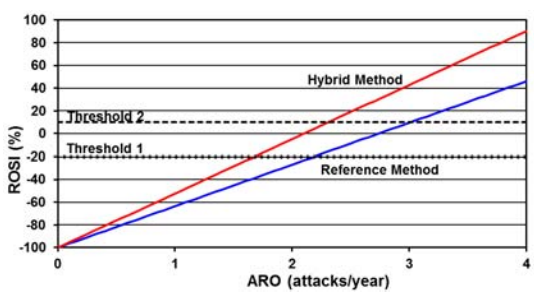

Fig. 3. *ROSI* as a function of *ARO*

Weighting factors obtained by the hybrid risk assessment method increase the *ROSI* value. The influence will be higher in the case of more frequent attacks and a higher level of the predefined threshold. The obtained result shows that the proposed quantification of the subjective risk assessment will change the final assessment of the profitability of the investment into the security mechanism.

5. CONCLUSIONS

In the paper, we have presented the improvement of the security risk assessment method in industrial SCADA systems. We have proposed an algorithm for calculation of weighting factors that quantify conditions in which an attack has been realized. Polling of experts, who know the specific process and SCADA system very well, should enable fine adjustment of weighting factors obtained by statistical analysis of archived data. Responses are then translated into a metric form, and their quantification is performed. We have also presented the results obtained with the improved hybrid method in terms of *ROSI* value that represents the relation between the savings realized by prevention of a cyber attack and the cost of the implemented security mechanism. The proposed method has advantages due to the important experts' experience, which is superimposed on the pure historical data.

REFERENCES

[1] Miller, B., Rowe, D., "A Survey of SCADA and Critical Infrastructure Incidents", in Proc. of the 1st Annual conference on Research in information technology, Calgary, AB, Canada, October 2012, pp. 51-56.

[2] Behnia, A., Rashid, R.A., Chaudhry, J.A., "A Survey of Information Security Risk Analysis Methods", Smart Computing Review Vol. 2, No. 1, 2012, pp. 79-93.

[3] Markovic-Petrovic, J.D., Stojanovic, M.D., "An Improved Risk Assessment Method for SCADA Information Security", Elektronika ir Elektrotechnika, Vol. 20, No. 7, 2014, pp.69-72.

[4] Yazar, Z., "A Qualitative Risk Analysis and Management Tool – CRAMM", SANS Institute, 2002.

[5] Dondossola, G., Lamquet, O., Torkilseng, A., "Key issues and related methodologies in the security risk analysis and evaluation of electric power control systems", CIGRÉ 2006 session, Paris, France 2006.

[6] Guo, J., Shen, X., "The Application of Bayesian Model for Power Enterprise Security Risk Management", in Proc. of the 2010 IEEE 3rd Int. Conf. on Advanced Computer Theory and Engineering (ICACTE), Chendgu, China, August 2010, Vol. 1, pp. 531-533.

[7] Sommestad, T., Ericsson, G.N., Nordlander, J., "SCADA System Cyber Security: A Comparison of Standards", IEEE Power and Energy Society General Meeting, 2010, pp. 1–8.

[8] Markovic-Petrovic, J., Stojanovic,M., "Analysis of SCADA System Vulnerabilities to DDoS Attacks", Proc. of the 11th Int. Conf. TELSIKS, Vol. 2, Nis, Serbia, October 2013, pp. 591-594.

[9] Saaty, T.L., "Decision making with the analytic hierarchy process", International journal of services sciences, Vol.1, No.1, 2008, pp. 83-98.

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