Security Assessment for Communication Networks of Power Control Systems Using Attack Graph and MCDM

Nian Liu, Jianhua Zhang, *Member, IEEE*, Hao Zhang, and Wenxia Liu

***Abstract*—The security assessment is a key function that should be performed in advance of any security deployment. Since experiences of cyber attack in power control systems are still limited, a complete methodology of security assessment for communication networks of power control systems is needed. According to past research, the difficulties of security assessment include the security analysis of power control process, and the security degree of each control step. Therefore, the attack graph and multiple criteria decision-making (MCDM) are introduced to deal with these difficulties. The overall security assessment is decomposed into two parts. One is the security analysis model for power control systems using attack graph, includes the basic concepts definition, construction algorithm, vulnerability function of each control step, and connection model-based system vulnerability calculation. Another one is focused on the quantification of the security degree in each control step—a hybrid MCDM approach integrated with an analytic hierarchy process (AHP) and a technique for order preference by similarity to ideal solution (TOPSIS) are proposed to value the vulnerability factors derived by the security analysis model. Finally, an instance communication network of power control system is modeling to test the validity of security assessment. The result supports the usefulness of the security assessment.**

***Index Terms*—Attack graph, communication network, multiple criteria decision-making, power control system, security assessment.**

I. Introduction

MODERN power systems have become highly integrated hybrid systems with the information and communication systems. The use of information technologies provides the benefits for power system control and operation, but also introduces the potential for cyber security vulnerabilities. Consequently, the security of information and communication systems has gradually become one of the main factors that affect power system security [1], [2].

The needs and requirements related to the cyber security of power utilities and control systems have been widely discussed, and some practical methods are reported [3]–[9]. At the same time, the IEC 62351 series standards were published, these technical specifications focused on the data and communications security of power systems management and associated information exchange [10]. According to the IEC 62351–1, the security assessment is an issue typically the most daunting, is how to decide what needs to be secured and to what degree it needs to be secured. Therefore, the security assessment is a key function that should be performed in advance of any security deployment [10].

There have been several studies focused on the security assessment of power control systems. Vulnerability assessment methods based on the Probabilistic Risk Assessment (PRA) for power control systems are proposed in [11], [12]. The security levels are calculated by the probabilities of occurrence of cyber security events, the probabilities of incidents caused by the events, and the related power loss. The probabilities are frequently calculated from statistical sampling, historical records or experimentation. Although there has been many cyber security events that result in damage occurring in the power systems [2], it is still difficult to identify these probabilities for the lack of history database of cyber security incidents [13], and it is also unavailable to do experiment on power control systems for the reasons of critical and real-time operation. The concept of a device visibility path based on graph theory is introduced in [14], and a small Prolog application is developed to calculate a device vulnerability level for a target device within a hypothetical substation. This method is a practical way to identify the vulnerabilities of remotely accessible devices in a complex control system, but how to assign values to the vulnerability level matrix of the Prolog application is not solved. An evaluation framework described in [15] provides a simple and intuitive method based on evidential reasoning for assessing the heterogeneous property of information security in a power communications system. The method incorporates the many insecure facts and incomplete data that are inherent in large-scale systems. The overall result is a set of indicators including the software, hardware, information and communication, which highlight the level of information security within a studied communication system. However, the assessment do not take the effects of network topologies into consideration, which are always introduce global security holes by the interaction of local vulnerabilities in communication networks [16]. Therefore, to estimate the cyber risk is a delicate task, since experiences of cyber risk assessment in process control systems are still limited. A complete methodology supporting the security analysis of power control system is needed [5].

Manuscript received September 28, 2008. Current version published June 23, 2010. Paper no. TPWRD-00745-2008.

N. Liu, J. Zhang and W. Liu are with the Key Laboratory of Power System Protection and Dynamic Security Monitoring and Control Under Ministry of Education, North China Electric Power University, Beijing 102206, China (e-mail: nian_liu@163.com).

H. Zhang is with the North China Power Dispatching Communication Center, North China Grid Company, Beijing 100053, China (e-mail: outstandinghao@163.com).

This work was supported by the National Natural Science Foundation of China (No. 50877026).

Digital Object Identifier 10.1109/TPWRD.2009.2033930

0885-8977/$26.00 © 2010 IEEE

Authorized licensed use limited to: Kansas State University. Downloaded on January 21,2021 at 17:06:23 UTC from IEEE Xplore. Restrictions apply.

To support the security analysis of power control process, and quantify the security degree of each control step systematically, a security assessment method for the communication networks of power control systems using the attack graph [16] and multiple criteria decision-making (MCDM) is proposed. The content of the paper is organized as follows. Section II briefly analyzes the difficulties and possible solutions. In Section III, the security analysis model for power control systems is defined based on the attack graph. Section IV introduces an approach to quantify the vulnerability factors obtained from security analysis model. Section V, the overall procedure for the security assessment is illustrated. In Section VI, an instance communication system is used for case study. Finally, the conclusions are given in Section VII.

II. Difficulties and Possible Solutions

A. Difficulties of Security Assessment for Power Control Systems

In aforementioned methods, the difficulties of security assessment for power control systems can be concluded as follows.

1) The vulnerabilities introduced by interconnection of devices in power control systems are difficult to identify. When evaluating the security of a power control network, it is rarely enough to consider the presence or absence of isolated vulnerabilities (e.g., local vulnerability of an isolated device). Large networks typically contain multiple platforms and software packages and employ several modes of connectivity. Inevitably, such networks have security holes that introduced by interconnections of local vulnerability [16].
2) The quantification of security degree is a complex task due to two factors. One is the existence of various security properties. The security degree of specified communication networks are determined by a number of properties, such as platforms, software, communication protocols, and security countermeasures, etc. It is important to take the effects of these properties into consideration. Another one is the lack of historical data of cyber security incidents. This creates problems for researchers that are trying to assess the security level of power control systems. Reasons for electric power utilities resistance to the disclosure of security incidents include fear of liability, loss of reputation and competition issues [13].

B. Attack Graph

Attack graphs depict way in which an adversary exploits system vulnerabilities to achieve a desired state. System administrators use attack graphs to determine how vulnerable their systems are and to determine what security measures to deploy to defend their systems. Attack graphs of a specified network represent a collection of possible scenarios in a computer network. Each penetration scenario is a sequence of actions taken by the intruder, typically culminating in a particular goal—administrative access on a particular host, access to a database, service disruption, etc. For appropriately constructed network models, attack graphs give bird's-eye view of every scenario that can lead to a serious security breach [16].

Attack graphs can serve as a useful tool in several areas of network security, including intrusion detection, defense, and forensic analysis. The benefits of the attack graph are taking the effects of interactions of local vulnerabilities into account and finding global security holes introduced by interconnection. According to the benefits, it is a possible solution for security analysis of power control systems.

C. Multiple Criteria Decision-Making

The MCDM methods deal with the process of making decision in the presence of multiple criteria or objectives. For example, the analytic hierarchy process (AHP) is such a methodology used widely to solve problems having multiple criteria [17]. The AHP actually forces the user to evaluate the importance of each criterion in relation to the others systematically and carefully in a hierarchical manner. The security degree of specified communication networks are determined by various security properties. The AHP could be a practical method to evaluate the importance of these security properties as multiple criteria.

Lack of historical data of cyber security incidents is another barrier for security assessment. In case where these "objective" sources are sparse, "subjective" sources are often used in the form of expert opinion [13]. The AHP is designed to handle the decision environments in which subjective judgments are inherent in the decision making process. Moreover, inherent in the AHP is the ability to handle input from multiple decision makers.

Furthermore, the security properties may be competitive benchmarking for AHP. For example, the security holes and the cryptography strength are competitive benchmarking, the security degree of target system are reduced with the increasing of security holes, but enhanced with the increasing of cryptography strength. Competitive benchmarking led to the introduction of the technique for order preference by similarity to ideal solution (TOPSIS) [18]. TOPSIS is widely accepted due to its sound logic, simultaneous consideration of the ideal and the anti-ideal solutions, and easily programmable computation procedure.

Therefore, the objective of this study is to integrate the AHP and TOPSIS method for the quantification of security degree.

D. Structure of the Security Assessment

Based on the analysis of study difficulties and possible solutions, the structure of security assessment for communication networks of power control systems is illustrated in Fig. 1.

III. Security Analysis Model Based on Attack Graph

A. Basic Concepts

Power control systems are distributed systems connected through multi-level network. Attack is the process to use the vulnerability of the system to achieve a series of transfers of state control. When attacking action is actualized, certain

Authorized licensed use limited to: Kansas State University. Downloaded on January 21,2021 at 17:06:23 UTC from IEEE Xplore. Restrictions apply.

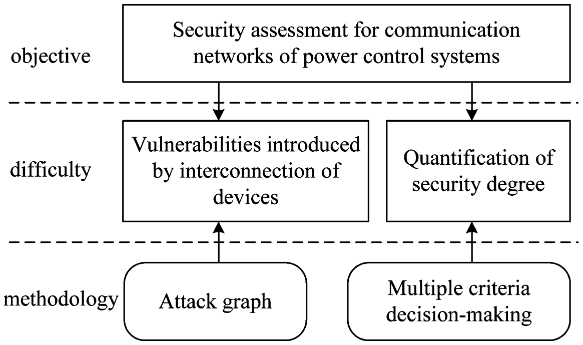

objective
Security assessment for communication networks of power control systems
difficulty
Vulnerabilities introduced by interconnection of devices
Quantification of security degree
methodology
Attack graph
Multiple criteria decision-making

Fig. 1. Structure of the security assessment.

conditions must be satisfied. The basic concepts are defined as follows.

Definition 1: Subject (S). The Subject is the initiator of operations. In power control systems, $s \in S$ can be users or equipment.

Definition 2: Node (N). The Device in power control systems is a node, using a triple $n = (i, u, f)$, $n \in N$ to denote. In this triple, i is the only identifier of the node, and it could be set as an equipment name or network address; u is the authentication method used on the node, such as passwords and certificates; f is the access control method applied in software of n.

Definition 3: Privilege (V). It is used to describe the operating privilege of a subject in a node. When $s \in S$ and $n \in N$, the function $v(s,n) \rightarrow \{0,1,2\}$ expresses the privilege level of s in n. The concrete privilege levels and types can be setup according to the actual situations.

Definition 4: Relation (R). The Relation refers to connections between nodes, using a quadruplet $r = (n_1, n_2, o, t)$, $r \in R, n_1, n_2 \in N$ to denote. Where o represents the communication port, and t represents the message type. For example, $r(n_1, n_2, o_1, t_2) \in R$ means that node n_1 is able to visit n_2 through the port o_1 by the medium-speed message t_2 [19].

Definition 5: State (Z). The State is the available operation states of devices in power control systems. Each state is a triple $z = (s, n, v(s,n))$, $z \in Z$, $s \in S$, $n \in N$, $v(s,n) \in V$. The state of a device is the prerequisite of the next action to be implemented.

Definition 6: Action (A). The Action represents aggregate of all the possible actions for devices in power control systems. The Action is a quadruplet $a = (m, z_s, z_d, \lambda)$, $a \in A, z_s, z_d \in Z$. Where m is the name of the action; z_s and z_d represent the initial state and final state of the action a; λ is a vulnerability factor, which is a parameter to measure the difficult level of action a.

B. Construction of the Security Analysis Model

Attack graph describes all the possible paths to insecurity state of a target node. Using attack graph, the construction algorithm of security analysis model for a communication network of power control system is described as follows.

1) Input: S, N, V, R; Target node n_d.
2) Output: Z, A, Attack graph AG_{n_d}.
3) Algorithm:

Step 1) According to N and R, construct a directed graph (N, R), the vertex is $n \in N$ and the edge is $r \in R$.

Step 2) Determine the operational state of n_d after being attacked, formulated as follows.

$$z_d = (s_i, n_d, v(s_i, n_d) \geq 1)$$

where s_i represents the intruding subject; $v(s_i, n_d) \geq 1$ represents the accepted privilege of s_i to control node n_d.

Step 3) Using n_d as the initial vertex, and the inedges of nodes as the search direction, traverse the directed graph (N, R). When visit a node n_i, determine the current state z_i by last state z_{i-1} of upper node n_{i-1}.

Step 4) Extract the action $a_i = (m_i, z_i, z_{i-1}, \lambda_i)$, which determined by the transfer of two states.

Step 5) Establish the attack graph $AG_{n_d} = (Z, A)$ of the target node n_d.

C. Vulnerability Function of a Control Step

The control step in attack graph is a state transfer, which is motivated by an action. The vulnerability of a state transfer represents the difficult to execute an action. The vulnerability function can be defined based on the theory of reliability [20].

Definition 7: For any actions $a \in A$, vulnerability of state transfer $P_v(c)$ is defined as the success probability of the state S_s transfer to the state S_d.

$$P_v(c) = P(C \leq c) = 1 - e^{-\lambda c} \tag{1}$$

where c is the equivalent cost of attacks; C is equivalent cost of attacks after achieving the object; λ is Vulnerability factor, expressing the difficulty level of a successful action. State transfer becomes more difficult when λ becomes smaller.

The vulnerability of state transfer is the probability of successful actions in given conditions and time. If the value of $P_v(c)$ becomes bigger, the vulnerability of the target system becomes bigger, and the probability of a success attack becomes higher. Exponential distributed function is used to define the vulnerability function, and the reasons are following:

1) If there is an available path to the target node, and the attacker paid sufficient cost to infinite, which is $c \rightarrow \infty$, then $P_v(c)|_{c\rightarrow\infty} = 1$, so that the attacking purpose finally could be achieved;
2) When $c = 0$, then $P_v(c)|_{c=0} = 0$, means attackers do not carry out any attacks, and they are unable to realize any attack purpose.
3) If a single action does not successful, the nodes will still maintaining a normal state, which has the same characteristic of "no memory" as the exponential distribution.

Equivalent attack cost depends on the level of knowledge, computing resources, action time and tools when attacking is carried out. Similar to the concept of time in reliability calculations, the life cycle of objects is concerned in reliability calculation, while the attack cost after achieving the object is concerned in the vulnerability assessment.

Authorized licensed use limited to: Kansas State University. Downloaded on January 21,2021 at 17:06:23 UTC from IEEE Xplore. Restrictions apply.

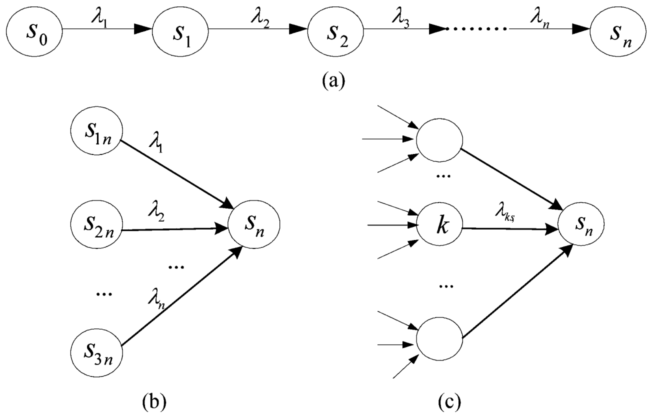


Fig. 2. Connection model of the attack graph. (a) Serial model. (b) Parallel model. (c) Series-parallel complex model.

D. Calculation of System Vulnerabilities Based on the Connection Model

The connection model of attack graph includes serial, parallel, and series-parallel complex (see Fig. 2). Based on the vulnerability function of state transfer, C_i and λ_i are respectively setting as the equivalent cost and vulnerability factor when the $i\text{th}$ action is successful, and the mathematic algorithms of vulnerabilities are defined as follows.

1) Serial model

$$\begin{aligned} P_s(c) &= P(C_1 + C_2 + \cdots + C_n \leq c) \\ &= 1 - \sum_{i=1}^{n} \frac{\prod\limits_{\substack{j=1 \\ j\neq i}}^{n} \lambda_j e^{-\lambda_j c}}{\prod\limits_{\substack{j=1 \\ j\neq i}}^{n} (\lambda_j - \lambda_i)} \end{aligned} \tag{2}$$

where $\forall i \neq j \rightarrow \lambda_i \neq \lambda_j, n \geq 2.$.

2) Parallel model

$$\begin{aligned} P_s(c) &= P(\min(C_1, C_2, \ldots C_n) \leq c) \\ &= 1 - e^{-\sum_{i=1}^{n} \lambda_i c}. \end{aligned} \tag{3}$$

3) Series-parallel complex model: traversing all of the paths from the target state to initial state, every feasible path is a serial model, and the calculations between each feasible path are treated as parallel model.

IV. Quantification of Vulnerabilities

The vulnerability of each control step is determined by vulnerability factor λ. The quantification of vulnerabilities is the process to value λ of actions in attack graph. The AHP is used to determine the weight of various security properties, and the TOPSIS is used to standardize value of the vulnerability factors due to some competitive benchmarking.

A. Hierarchical Structure of Security Properties

The construction of hierarchical structure according to different security properties is the basis for quantification. The hierarchical structure in this study is divided into four different layers. The first layer is the target layer, which is used to determine the value of vulnerability factor λ. The second layer is the criteria layer, including the main types of security property. The third layer is the indicator layer, which subdivide the criteria layer into smaller types of criteria. The forth layer is the action layer, including actions involved in the process of state transfer.

B. Compose the Pair-Wise Comparison Decision Matrix

The pair-wise comparison matrices of the criteria and indicator layers are composed separately. As for measurement scale, this study uses numerical values 1–9 and their reciprocals. The values of 1,3,5,7, and 9 represent equal importance, weak importance, essential importance, demonstrated importance, and extreme importance of security properties, respectively; while the values of 2,4,6, and 8 represent the intermediate values of adjoining scales. Let $\boldsymbol{A}$ represent a $n \times n$ pair-wise comparison matrix

$$\boldsymbol{A} = (a_{ij})_{n\times n} = \begin{bmatrix} 1 & a_{12} & \cdots & a_{1n} \\ a_{21} & 1 & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & 1 \end{bmatrix}. \tag{4}$$

The diagonal element a_{ij} represents the strength of importance degree of the $i\text{th}$ element compared to the $j\text{th}$ element, and thus $a_{ij} = 1/a_{ji}$, where $a_{ij} > 0$.

C. Calculate the Indicator Weight and the Consistency Test

The largest eigenvalue $\lambda_{\max}$ and relevant normalization eigenvector $\boldsymbol{W} = (w_1, w_2, \ldots, w_n)$ of the matrix $\boldsymbol{A}$ are calculated. Then get the combinatorial weight of each layer by the following formula:

$$\boldsymbol{W}^{(i)} = \left(\boldsymbol{W}_1^{(ip)}, \boldsymbol{W}_2^{(ip)}, \ldots, \boldsymbol{W}_n^{(ip)}\right) \boldsymbol{W}^{(p)} \tag{5}$$

where $\boldsymbol{W}^{(p)}$ is the combinational weight vector of criteria layer elements compared to target layer element, and $\left(\boldsymbol{W}_1^{(ip)}, \boldsymbol{W}_2^{(ip)}, \ldots, \boldsymbol{W}_n^{(ip)}\right)$ is the weight matrix of the indicator layer elements compared to criteria layer elements.

In order to guarantee the consistency of the matrices, checkout is necessary, and the methods can refer to [17].

D. Standardize the Index Value of Evaluation

Construct the decision matrix of m actions compared to n indicators.

$$\boldsymbol{B} = (b_{ij})_{m\times n} \quad i = 1, 2, \ldots, m,\ j = 1, 2, \ldots, n$$

where b_{ij} is the $j\text{th}$ indicator value of the ith action.

Establish a normalized decision matrix $\boldsymbol{Z}$

$$\boldsymbol{Z} = (Z_{ij})_{m\times n} \tag{6}$$

where $z_{ij} = a_{ij}/\sqrt{\sum_{j=1}^{n} a_{ij}^2}$.

Authorized licensed use limited to: Kansas State University. Downloaded on January 21,2021 at 17:06:23 UTC from IEEE Xplore. Restrictions apply.

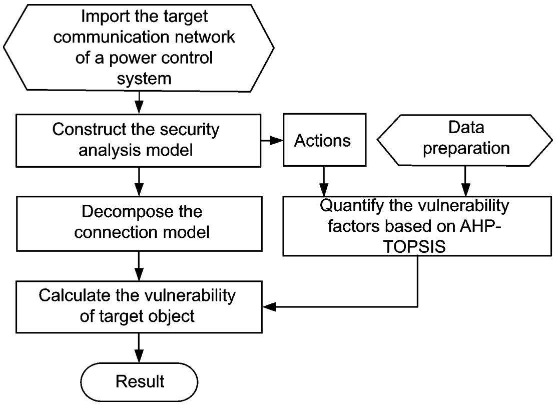

Import the target communication network of a power control system
Construct the security analysis model
Actions
Data preparation
Decompose the connection model
Quantify the vulnerability factors based on AHP-TOPSIS
Calculate the vulnerability of target object
Result

Fig. 3. Overall procedure of the security assessment.

Calculate the weighted decision matrix

$$\boldsymbol{Y} = \boldsymbol{Z}\boldsymbol{W}$$

where $\boldsymbol{W}$ is a diagonal matrix composed by the combinatorial weight of each layer in $\boldsymbol{W}^{(i)}$.

E. Calculate the Vulnerability Factor of Actions

Determine the positive ideal and negative ideal solution

$$\boldsymbol{X}^{+} = \left(x_1^{+}, x_2^{+}, \ldots, x_n^{+}\right), \quad \boldsymbol{X}^{-} = \left(x_1^{-}, x_2^{-}, \ldots, x_n^{-}\right).$$

If y_j is the efficiency indicator,

$$x_j^{+} = \max\left\{y_{ij}\right\}, \quad x_j^{-} = \min\left\{y_{ij}\right\}.$$

If y_j is the cost indicator

$$x_j^{+} = \min\left\{y_{ij}\right\}, \quad x_j^{-} = \max\left\{y_{ij}\right\}.$$

Calculate the separation measures, using the n-dimensional Euclidean distance. The separation of each alternative from the positive ideal solution and negative ideal solution are given as follows, respectively.

$$di^{+} = \sqrt{\sum_{j=1}^{n}\left(x_{ij} - x_j^{+}\right)^2}, \quad di^{-} = \sqrt{\sum_{j=1}^{n}\left(x_{ij} - x_j^{-}\right)^2}. \tag{7}$$

Calculate the vulnerability factors of actions, defined as the relative closeness to the ideal solution

$$\lambda_i = \frac{di^{+}}{\left(di^{-} + di^{+}\right)}, \quad i = 1, 2, \ldots, m. \tag{8}$$

V. Procedure of the Security Assessment

The overall procedure of the security assessment is illustrated in Fig. 3.

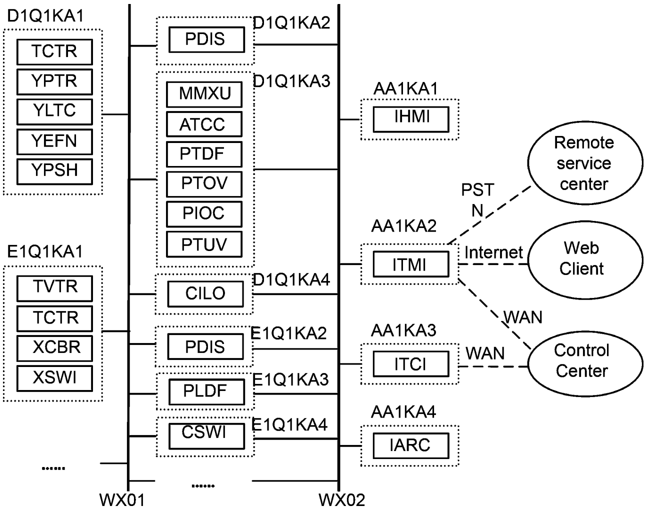


Fig. 4. Instance communication network.

VI. Case Study

A. Instance Communication Network

Take the T1–1 transmission substation that illustrated in IEC 61850 as the example for vulnerability assessment. The internal communication network of the substation is connected use Mode 3 [21]. The external communication network of the substation referred to the structure described in [2]. Considering the essential protection and control equipment, the logic devices (LD) and logic nodes (LN) of two bays are modeling, as shown in Fig. 4. The meanings of the LNs can be found in IEC 61850 7–2 [22].

According to the conventional configurations described in [2] and the IEC 61850, the security countermeasures of initial scheme are described as follows. 1) a firewall is setup on external communication gateway of substation; 2) the internal communication protocols completely adopts IEC 61850 8–1 9–1 [23], [24]; 3) The password authentication is setup on LNs of the bay level, and simple access control is implemented by virtual access view [22]; 4) The networks of control center are protected using firewall and antivirus software, and isolated from external business networks; 5) The firewall and antivirus software are installed in web client; and 6) the remote connection implements SSL authentication and cryptographic algorithms use the opened international standards of cryptography (for example, RSA, AES, etc.).

Based on the initial scheme, extended security countermeasures include C1 to C6 (see Table I). Three different schemes are setup to analysis the impact of different security countermeasures. Scheme 1 mainly concerns the security of information exchange, including C1, C2 and C4; scheme 2 mainly concerns the node security, including C3, C5, and C6; scheme 3 integrates the strengths of the scheme 1 and 2, including C1 to C6.

B. Construct the Security Analysis Model

Take circuit breaker E1Q1KA1XCBR as a target node, and then construct the security analysis model. The directed graph

Authorized licensed use limited to: Kansas State University. Downloaded on January 21,2021 at 17:06:23 UTC from IEEE Xplore. Restrictions apply.

TABLE I
SECURITY COUNTERMEASURES

Number	Security countermeasure
C1	Setup intrusion detection system on communication network of the substation layer
C2	Use the security expansion defined in IEC 62351 for internal communication networks
C3	Use PKI certificate and mandatory access control for devices
C4	The remote connections from the control center to substation are established based on VPN
C5	Scan the software holes of computers on the network of substation layer, and setup the related patches
C6	Scan the holes for web clients, setup the related patches, and use the certificate authentication when log on.

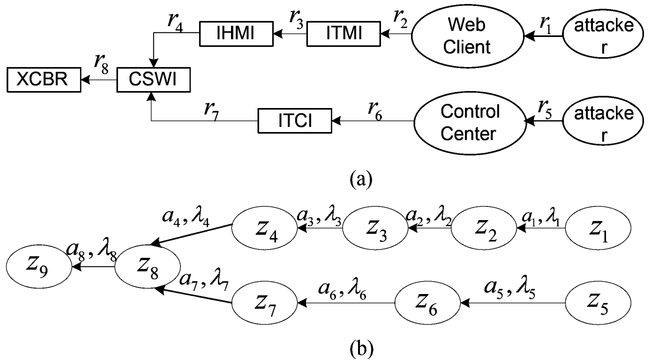


Fig. 5. Directed graph and attack graph for E1Q1KA1XCBR. (a) Directed graph (b) Attack graph.

TABLE II
RESULT OF SECURITY ANALYSIS

State	Action	Vulnerability factor
$z_1 = att, ip_{att}, v(att, i_a) \geq user$	a_1	λ_1
$z_2 = att, ip_{wc}, v(att, ip_{wc}) \geq admin$	a_2	λ_2
$z_3 = att / tech, ip_{itmi}, v(att, ip_{itmi}) \geq tech$	a_3	λ_3
$z_4 = att, ip_{ihmi}, v(att, ip_{ihmi}) \geq oper$	a_4	λ_4
$z_5 = att, ip_{att}, v(att, ip_a) \geq user$	a_5	λ_5
$z_6 = att, ip_{cc}, v(att, ip_{cc}) \geq oper$	a_6	λ_6
$z_7 = att / oper, ip_{itci}, v(att, ip_{itci}) \geq oper$	a_7	λ_7
$z_8 = oper, ip_{cswi}, v(att, ip_{cswi}) \geq oper$	a_8	λ_8
$z_9 = cswi, mac_{xcbr}, v(cswi, mac_{xcbr}) \geq admin$	—	—

and the attack graph are shown in Fig. 5. The results of the security analysis include states and actions, are listed in Table II.

C. Quantify the Vulnerability Factors

The first step of quantification is to establish the hierarchy structure of security properties for AHP. The target layer is used to determine the value of vulnerability factor λ. The criteria layer includes communication protocols, node security, cryptography, network monitoring, and attacker knowledge, etc. The indicator layer includes 14 kinds of evaluation criteria subdivided from the criteria layer (see Fig. 6). Note that the hierarchy structure established in Fig. 6 is only an instance for case study, and the concrete elements should be selected according to applications.

The second step is to collect data for pair-wise comparison matrices of criteria and indicator layers, and decision matrix of actions compared to indicators. In this study, the sample data of the pair-wise comparison matrices are listed in Tables III–VIII, using numerical values 1–9 and their reciprocals. For example, the value 1/3 in row 01 line 02 of Table III represents the importance of criteria 01 compared to criteria 03. The decision matrix of actions compared to indicators is listed in Table IX. In the initial scheme, the difficulties of action 1 to 8 on the indicator 021 are respectively 3, 4, 3, 3, 4, 6, 3 and 3, but in scheme 3, the difficulties are respectively 3, 7, 7, 7, 4, 7, 7 and 4. In practice, the data should be collected by studying documentation, interviewing staffs and experts.

Finally, by using the AHP-TOPSIS integrated method, the value of vulnerability factors can be calculated. As shown in Fig. 7, the values of action 2, 3, 4, 6, and 7 in the scheme 1 is lower than that in the initial scheme, but the differential is not much. The action 1, 2, 3, 4, 6, and 7 in scheme 2 is different from that in the initial scheme. In particular, the effect of the reduction on action 1, 2, and 6 is more obvious. Scheme 3 is the integration of scheme 1 and 2, and the effect of reduction is the best.

D. Calculate the System Vulnerability

According to the connection model of the attack graph in Fig. 5, the instance is a series-parallel complex model, which can be divided into two series model. The two groups of vulnerability factors are presented as follows:

$$\boldsymbol{\lambda}^a = [\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_8], \quad \boldsymbol{\lambda}^b = [\lambda_5, \lambda_6, \lambda_7, \lambda_8].$$

Then, calculate the system vulnerability

$$P_s(c) = \max \begin{pmatrix} P(C_1 + C_2 + C_3 + C_4 + C_8 \leq c), \\ P(C_5 + C_6 + C_7 + C_8 \leq c) \end{pmatrix} = 1 - \sum_{i=1}^{n} \frac{\prod\limits_{\substack{j=1 \\ j \neq i}}^{n} \lambda_j^a e^{-\lambda_j^a c}}{\prod\limits_{\substack{j=1 \\ j \neq i}}^{n} \left(\lambda_j^a - \lambda_i^a\right)}. \tag{9}$$

As shown in Fig. 8, the result of the system vulnerability is a curve changing with the equivalent attack cost. When the attack cost is the same, the system vulnerabilities decrease from the initial scheme to the scheme 3. This result is consistent with the value of λ. Compared to the scheme 2, the scheme 1 is less effective. It is mainly due to two reasons that are security degree and interconnection. First, the factors that influence the system most are the security issues of nodes, including authentication and access control. The scheme 2 contributes obvious enhancement on this issue and the system vulnerability reduces sharply. Second, the scheme 1 is only setup for communication protocols and has improvement on system security, but not deal with

Authorized licensed use limited to: Kansas State University. Downloaded on January 21,2021 at 17:06:23 UTC from IEEE Xplore. Restrictions apply.

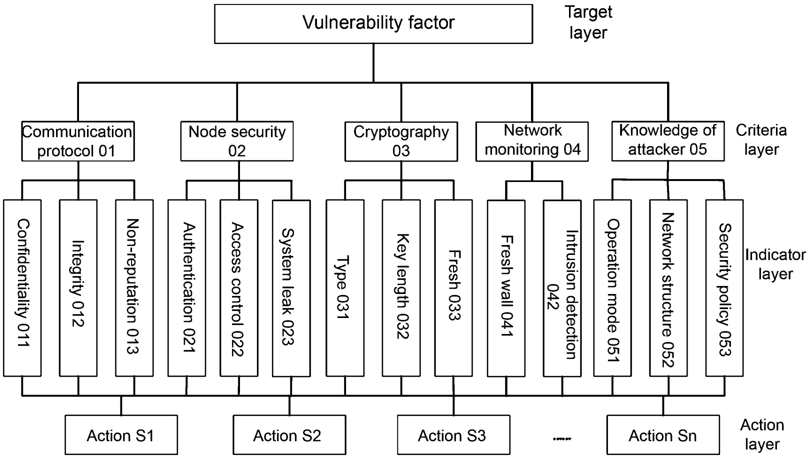


Fig. 6. Instance hierarchy structure.

TABLE III
PAIR-WISE COMPARISON MATRIX OF THE CRITERIA LAYER

	01	02	03	04	05
01	1	1/3	3	1	2
02	3	1	6	3	8
03	1/3	1/6	1	1/2	1
04	1	1/3	2	1	2
05	1/2	1/8	1	1/2	1

TABLE IV
PAIR-WISE COMPARISON MATRIX 01 OF THE INDICATOR LAYER

	011	012	013
011	1	1	1/3
012	1	1	1/2
013	3	2	1

TABLE V
PAIR-WISE COMPARISON MATRIX 02 OF THE INDICATOR LAYER

	021	022	023
021	1	2	1/2
022	1/2	1	1/3
023	2	3	1

TABLE VI
PAIR-WISE COMPARISON MATRIX 03 OF THE INDICATOR LAYER

	031	032	033
031	1	1/3	1/4
032	3	1	2
033	4	1/2	1

TABLE VII
PAIR-WISE COMPARISON MATRIX 04 OF THE INDICATOR LAYER

	041	042
041	1	2
042	1/2	1

TABLE VIII
PAIR-WISE COMPARISON MATRIX 05 OF THE INDICATOR LAYER

	051	052	053
051	1	1/2	1/3
052	2	1	1/2
053	3	2	1

the action 1 and 2, which are two important system holes introduced by interconnection, so its effect is limited.

TABLE IX
DECISION MATRIX OF ACTIONS COMPARED TO INDICATORS

Indicator	Initial scheme	Scheme 3
011	1 3 1 1 3 5 1 1	1 5 5 5 3 9 5 5
012	1 3 2 2 3 5 2 2	1 5 6 6 3 9 6 6
013	1 3 2 2 4 6 2 2	1 5 6 6 4 9 6 6
021	3 4 3 3 4 6 3 3	3 7 7 7 4 7 7 4
022	3 3 4 4 3 6 4 3	3 7 7 7 3 7 7 3
023	8 7 5 1 5 5 1 1	8 2 5 1 5 2 1 1
031	3 6 3 4 6 8 4 1	4 7 4 5 7 9 5 2
032	3 6 3 4 6 8 4 1	3 6 3 4 6 8 4 1
033	2 5 1 3 5 6 3 1	5 8 5 6 8 9 6 2
041	5 9 1 1 9 9 1 1	5 9 1 1 9 9 1 1
042	1 1 1 1 7 1 1 1	1 1 7 7 7 1 7 1
051	7 3 5 5 6 3 5 3	7 3 5 5 6 3 5 3
052	7 5 7 7 6 5 7 3	7 5 7 7 6 5 7 3
053	7 5 5 5 6 5 5 3	7 5 5 5 6 5 5 3

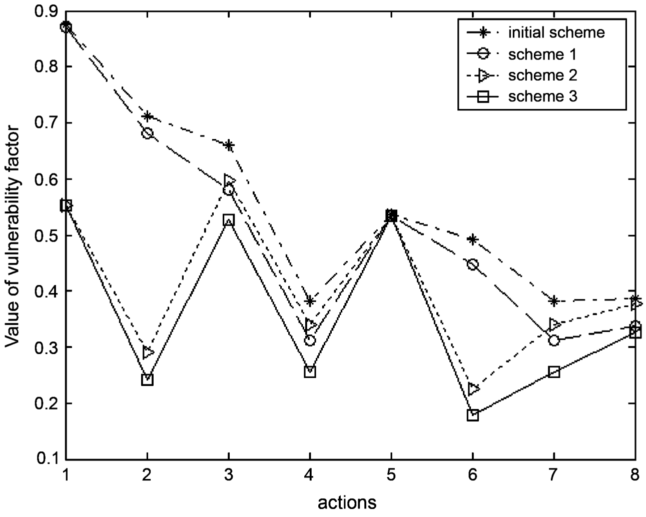


Fig. 7. Vulnerability factor value of actions.

VII. CONCLUSION

This paper proposed a security assessment method for communication networks of power control systems. The attack graph and MCDM are introduced to deal with the current difficulties in security assessment procedure. The result of security assessment is a dynamic system vulnerability changed with the equivalent attack cost. Comparing the results of different

Authorized licensed use limited to: Kansas State University. Downloaded on January 21,2021 at 17:06:23 UTC from IEEE Xplore. Restrictions apply.

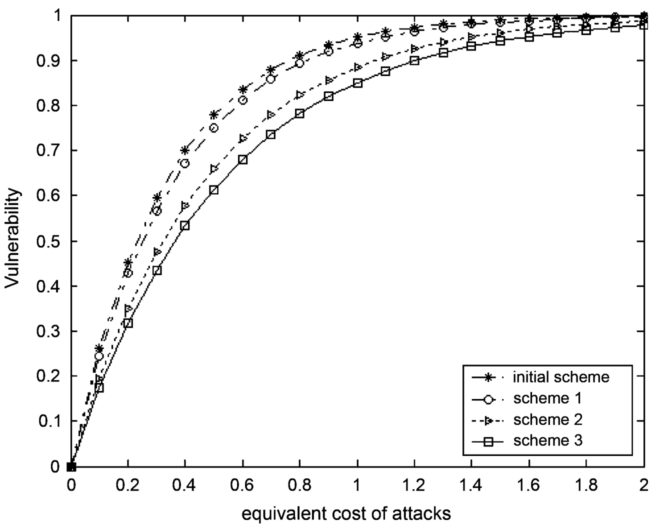


Fig. 8. System vulnerabilities according to different schemes.

schemes, the value is affected by the interconnection issues and security degree of countermeasures.

In general, it is often inclined to set an acceptable benchmark value, and the security of the system depends on the comparison between assessment results and the benchmark value. However, the selection of this benchmark is a complex task. It is often depends on the comparison of the benefit E_t received from attack with the cost E_c of attack. If $E_t/E_c \leq 1$, the system is considered safe, else if $E_t/E_c > 1$, the security degree of system becomes weaker with the increase of ratio E_t/E_c. Therefore, the setting of benchmark values still needs to consider the consequence of incidents. Recently, in a study of risk assessment for power systems, the economical efficiency, power loss, and severity are commonly used to quantity the consequence of accidents. To establish a unified scale or equivalent method compatible with the attack cost is a problem to be further studied.

REFERENCES

[1] *CLEVELAND F. IEC TC57 Security Standards for the Power System's Information Infrastructure— Beyond Simple Encryption. // IEEE Power Eng. Soc. Transm. Distrib. 2005/2006*, , May 21–24, 2006.

[2] D. Dzung, M. Naedele, T. V. hoff, and M. Crevatin, "Security for industrial communication systems," *Proc. IEEE*, vol. 93, no. 6, pp. 1152–1177, Jun. 2005.

[3] S. Sheng, W. Chan, K. Li, D. Xianzhong, and Z. Xiangjun, "Context information-based cyber security defense of protection system," *IEEE Trans. Power Del.*, vol. 22, no. 3, pp. 1477–1481, Jul. 2007.

[4] G. Ericsson and A. Torkilseng, "Management of information security for an electric power utility—on security domains and use of ISO/IEC 17799 standard," *IEEE Trans. Power Del.*, vol. 20, no. 2, pp. 683–690, Apr. 2005.

[5] G. Ericsson, "Toward a framework for managing information security for an electric power utility—CIGRE experiences," *IEEE Trans. Power Del.*, vol. 22, no. 3, pp. 1461–1469, Jul. 2007.

[6] N. Liu, B. Duan, J. Wang, and S. Huang, "Study on PMI based access control of substation automation system," in *Proc. IEEE Power Eng. Soc. General Meeting*, Montreal, QC, Canada, Jun. 18–22, 2006.

[7] L. Wang, T. Mander, H. Cheung, F. Nabhani, and R. Cheung, "Security operation modes for enhancement of utility computer network cybersecurity," presented at the IEEE Power Eng. Soc. General Meeting, Tampa, FL, Jun. 24–28, 2007.

[8] N. Liu, J. Zhang, and W. Liu, "A security mechanism of web services-based communication for wind power plants," *IEEE Trans. Power Del.*, vol. 23, no. 4, pp. 1930–1938, Oct. 2008.

[9] G. Y. Liao, Y. J. Chen, W. C. Lu, and T. C. Cheng, "Toward authenticating the master in the modbus protocol," *IEEE Trans. Power Del.*, vol. 23, no. 4, pp. 2628–2629, Oct. 2008.

[10] *IEC TS 62351-1. Power Systems Management and Associated Information Exchange—Data and Communications Security—Part 1: Communication Network and System Security—Introduction to Security Issues*, IEC TS 62351-1, May 2007.

[11] J. Yu, A. Mao, and Z. Guo, "Vulnerability assessment of cyber security in power industry," in *Proc. IEEE Power Eng. Soc. Power Systems Conf. Expo.*, Atlanta, GA, Nov. 1, 2006, pp. 2200–2205.

[12] K. Lin and K. E. Holbert, "PRA for vulnerability assessment of power system infrastructure security," in *Proc. 37th Annu. North American Power Symp.*, Oct. 23–25, 2005, pp. 43–51.

[13] C. Taylor, A. Krings, and J. Alves-Foss, "Risk analysis and probabilistic survivability assessment (RAPSA): An assessment approach for power substation hardening," presented at the ACM SACT, Washington, DC, Nov. 2002.

[14] D. Leon, J. Alves-foss, A. Krings, and P. Oman, "Modeling complex control systems to identify remotely accessible devices vulnerable to cyber attack," presented at the ACM SACT, Washington, DC, Nov. 2002.

[15] L. Nordstrom, "Assessment of information security levels in power communication systems using evidential reasoning," *IEEE Trans. Power Del.*, vol. 23, no. 3, pp. 1384–1391, Jul. 2008.

[16] O. M. Sheyner, "Scenario graphs and attack graphs," Ph.D. dissertation, Dept. Comput. Sci., Carnegie Mellon Univ., , Pittsburgh, PA, 2004.

[17] T. L. Saaty*, The Analytic Hierarchy Process*. New York, McGraw-Hill: , 1980.

[18] S. J. Chen and C. L. Hwang*, Fuzzy Multiple Attributes Decision Making: Methods and Applications*. Berlin, Germany: Springer, 1992.

[19] *IEC 61850–5, Communication Networks and Systems in Substations—Part 5: Communication Requirements for Functions and Device Models IEC*, IEC 61850–5, 2003.

[20] P. Feng, Y. Lian, and Y. Dai, "A vulnerability model of distributed systems based on reliability theory," (in Chinese) *J. Softw.*, vol. 17, no. 7, pp. 1633–1640, 2006.

[21] *IEC61850–1, Communication Network and Systems in Substations—Part 1: Introduction and Overview, IEC*, IEC61850–1, 2003.

[22] *IEC 61850–7-2, Communication Networks and Systems in Substation-Part 7–2: Basic Communication Structure for Substation and Feeder Equipment-Abstract Communication Service Interface (ACSI), IEC*, IEC 61850–7-2, 2003.

[23] *IEC 61850–8-1, Communication Networks and Systems in Substation-Part 8–1: Specific Communication Service Mapping (SCSM)—Mapping to MMS(ISO/IEC 9506–1 and ISO/IEC 9506–2) and to ISO/IEC 8802–3, IEC*, IEC 61850–8-1, 2003.

[24] *IEC 61850–9-1, Communication Networks and Systems in Substation-Part 9–1: Specific Communication Service Mapping (SCSM)–Sampled Values Over Serial Unidirectional Multidrop Point to Point Link, IEC*, IEC 61850–9-1, 2003.

Nian Liu received the B.S. and M.S. degrees in electric engineering from Xiangtan University, Hunan, China, in 2003 and 2006, respectively, and the Ph.D. degree in electrical engineering from North China Electrical Power University, Beijing, China, in 2009.

Currently, he is a Lecturer in the College of Electrical and Electronic Engineering of North China Electrical Power University, Beijing, China.

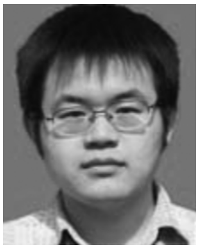
His research interests are power system management and associated information exchange, monitoring and control of new energy sources, communication systems of substation automation system, and power system security assessment.

Authorized licensed use limited to: Kansas State University. Downloaded on January 21,2021 at 17:06:23 UTC from IEEE Xplore. Restrictions apply.

Jianhua Zhang (M'04) was born in Beijing, China, in 1952. He received the M.S. degree in electrical engineering from North China Electric Power University, Beijing, China, in 1984.

He was a Visiting Scholar with the Queen's University, Belfast, U.K., from 1991 to 1992, and was a Multimedia Engineer of Electric Power Training with CORYS T.E.S.S., France, from 1997 to 1998. Currently, he is a Professor and Head of the Transmission and Distribution Research Institute, North China Electric Power University, Beijing. He is also the Consultant Expert of National "973" Planning of the Ministry of Science and Technology. His research interests are in power system security assessment, operation and planning, and emergency management.

Mr. Zhang is an Institution of Engineering Technology Fellow and a member of several technical committees.



Hao Zhang received the B.S. and M.S. degrees in electric engineering from North China Electrical Power University, Beijing, China, in 2006 and 2009, respectively.

Currently, he is an Engineer of the North China Power Dispatching Communication Center, North China Grid Company. His research interest is power system control and communication.

Wenxia Liu received the M. S. degree in electric engineering from Northeast Dianli University, Jilin, China, in 1995, and the Ph.D. degree in electrical engineering from North China Electrical Power University, Beijing, China, in 2009.

Currently, she is an Associate Professor at North China Electrical Power University, Beijing, China. Her research interests are in planning and operation of distribution system and power system communication.

Authorized licensed use limited to: Kansas State University. Downloaded on January 21,2021 at 17:06:23 UTC from IEEE Xplore. Restrictions apply.