

Study on Model of Risk Assessment of Standard Operation in Rural Power Network

Qingji Li, Tao Yang

► **To cite this version:**

Qingji Li, Tao Yang. Study on Model of Risk Assessment of Standard Operation in Rural Power Network. 4th Conference on Computer and Computing Technologies in Agriculture (CCTA), Oct 2010, Nanchang, China. pp.440-444, 10.1007/978-3-642-18354-6_52 . hal-01563465

HAL Id: hal-01563465

<https://hal.inria.fr/hal-01563465>

Submitted on 17 Jul 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Study on Model of Risks Assessment of Standard Operation in Rural Power Network

Qingji Li¹, Tao Yang²

¹ Qingji Li, College of Information and Electrical Engineering, Shenyang Agriculture University, Shenyang 110866, China

² Tao Yang, Corresponding author, College of Information and Electrical Engineering, Shenyang Agriculture University, Shenyang 110866, China

{ Qingji Li, ximusyau@hotmail.com,
Tao Yang, yangtaosx@yahoo.com.cn }

Abstract. Operation risk is the primary risk to rural power company, and it is also an important part of security risk management. The paper establishes a model to assessed risks of standard operation in rural power network, based on Job Risk Analysis (LEC). The example and application of the model in rural power network security risk management system shows that it can realize the real-time assessment of standard operation risk, the model use is simple and the assessment result is accurate. This study has important reference value to practical application of rural power security risk assessment.

Key words: Model of risks assessment, Standard operation, Rural power network, LEC

1 Introduction

Security risk assessment management is an important part of modern business management and it also is an effective means to ensure production safety. In recent years, rural power companies are carrying out risk assessment based on its own contents and standards of risks assessment. In these standards, some are cyclical; others are real-time. But they do not give a clear and workable approach to achieve real-time assessment that combine with the standard operating. Hazard identification and control measure is the core of real-time assessment, and the model is the key to achieve real-time evaluation for standard operating. This paper proposes an assessment model that is based on method Job Risk Analysis (LEC) and has been improved and perfected, so that it can be a good combination with the risk level of security risk assessment. The model can quantify the hazard level and the effect of prevention measures, and then calculate the risk level of this operation. Based on these reminders and descriptions of various risk factors leading to the likelihood and severity of accidents, operators can effectively prevent accidents.

2 Background and platform

2.1 Background

Security risk assessment management has been widely used in finance, insurance and other industries. In November 2008, based on drawing and absorbing the international advanced management concepts and methods of security, State Grid Corporation arranged and compiled “The Security Risk Assessment Norm to Power Supply Enterprises” and “Supply Enterprise Security Risk Identification and Prevention Operations Manual”. From the standpoint of the company production safety conditions, quality of personnel, scene management, general management, the systematic assessment of enterprise security management, the norm that mainly prevents personal injury and man-made accidents evaluates enterprise security risk rating and guides enterprise to carry out security management.

The risk calculation formula of security risk assessment:

Scoring rate = Σ the actual score of items having been checked / Σ total score of all the items

Table 1. Risk rating of security risk assessment

scoring rate x	risk rating
$x \geq 0.9$	Security controlled
$0.9 > x \geq 0.75$	Low risk
$0.75 > x \geq 0.6$	Medium risk
$0.6 > x \geq 0.4$	High risk
$x < 0.4$	Out of control

2.2 Platform

In order to carry out security risk assessment management quickly, ChangChun Suburb Branch Company develop the "security risk assessment management system". The system development objective is to achieve security risk assessment scientific, convenient in the application, reliable, cost-saving effect, and provide comprehensive statistical data to decision-making to policy-makers. The system is designed and realized by ASP.NET2.0 techniques as well as the SQL 2000 back-stage database based on the higher prevalence WINDOWS platform. System assessment is divided into two parts: real-time assessment and periodic assessment. Periodic assessment is entirely based on “The Security Risk Assessment Norm to Power Supply Enterprises”; real-time assessment combining with standardized operation is a good complement to periodic assessment. Real-time assessment model based on LEC method been improved and perfected can quantify the hazard level and impact of control measures, and then calculate the risk level of this operation and effectively prevent accidents.

3. LEC Method

3.1 Introduction of LEC Method

LEC method is also named Job Risk Analysis. It's mathematic model as follow:

$$D=L*E*C. \tag{1}$$

Value of D depends on the risk possibility (L), the frequency (E) and the possible consequences (C). This assessment method is straightforward and risk level is clear. But the scores of LEC is determined based primarily on experience, so the staff who join the assessment work must have experience and can make a fair and objective evaluation of risk control measures.

3.2 LEC scores and description

Table 2 shows the possibility of an accident (L) and description.

Table 2. The possibility of an accident (L) and description

score	description
10	Entirely possible
6	Very Likely
3	Possible, but not often
1	completely unexpected
0.5	envisaged
0.2	Highly unlikely
0.1	Impossible

Table 3 shows frequency of exposure to hazardous (E) and description.

Table 3. Frequency of exposure to hazardous (E) and description

score	description
10	Continuous
6	per day
3	Once a week, or occasionally
2	Monthly
1	Several times a year
0.5	Very rare

Table 4 shows that accident may result in the loss of the consequences (C) and description.

Table 4. Score C and description

score	description
100	Disaster, many deaths
40	Disaster, several fatalities
15	serious, one death
7	Serious injury
3	Major accidents, disability
1	Small accident, minor injuries

4. Real-time assessment models

4.1 Assessments Model

First, calculates the risk value D_i for each hazard, and then sum total of this assignment as the risk value, and prompts to the operator. There are many hazards prevention and control measures for each hazard. The score of prevention and control measures will be multiplied by the effect of e_j , divided by the total risk value of risk sources. With reference to table 1, the system reaches the safety risk assessment risk rating. The mathematical model can be described by Equation 2:

$$\sum_{i=1}^n \left(\sum_{j=1}^k e_j D_i (a_i - b_i) m_j \% + D_i b_i \right) / \sum_{i=1}^n D_i \quad (2)$$

Table 5 shows the value of a_i and b_i .

Table 5. Relation of a_i , b_i and D_i

D_i	Level of risk	a_i	b_i
>320	Extremely risk	0.6	0.0
160~320	High risk	0.75	0.4
70~160	Significant risk	0.9	0.6
20~70	General risk	0.95	0.75
<20	Slightly risk	1	0.85

The effects of a_i and b_i is that for a specific hazard, based on level of risk, risk rating of security risk assessment can be limited in scope. For example, the value of D_i is >320, so the level of risk is extremely risk. For this hazard, even if the operator take protective measures is perfect, in the best case the risk level of this job is the high risk. On the other hand, the level of risk is slightly risk, even if the operator take no protective measures, in the worst case the risk level of this job is the low risk. Meanwhile, the models combine the level of risk and risk rating of security risk assessment well.

Where $m_j\%$ means the percentage level of protective measure's control effect to a specific hazard, and for hazard with k - prevention measures, equation is given by Equation 3:

$$\sum_{j=1}^k m_j \% = 1 \quad (3)$$

Where k is the count of prevention measures. After that, the operator can easily score on the prevention measures to avoid the uncertainty scores.

Where e_j means the effect of protective effect to a specific hazard, and $e_j \in [0,1]$. When a hazard with the appropriate control measures can be prevented, then the value of e_j is great; else the value of e_j is small.

4.2 Experimental data

For example, cutting trees, the system calculate level of security risk based on mathematical model.

Table 6. Parameter values of cutting trees

Hazard	D	a	b	e
Traffic accident	60	0.95	0.75	0.8
falling	84	0.9	0.6	0.8-0.9
Electric shock	135	0.9	0.6	1
Hurt by fallen trees	90	0.9	0.6	0.8-1

The description of hazards prevention measures for each hazard is no detail. According by parameter values of table 6, the system Calculates scoring rate of security risk assessment : $(54.6+72.4+117.45+76.68) / (60+84+135+90) =0.87$, With reference to table 1, conclusion is Low risk. Result value of 0.87 close to the 0.9 is realistic.

5. Conclusion

Real-time risk assessment plays an important role in the production. The models combine LEC method and risk rating of security risk assessment well. By adjusting the value of each parameter, their corresponding relationship is flexible. With the models, operator can view the level of hazard risk, and know the effect of prevention measures that will be taken, then gain risk level of this job. For primary operator, all information can be warned before work, so accidents can be prevented obviously. At the same time, large amounts of date from routine work can also serve as the basis for statistical analysis and offer reference and decision service to policy makers.

The value of coefficient largely depends on experience with professional staff according to different operations, different circumstances to determine, and the final

value needs further study, standardization to make assessment more objective and reasonable.

Reference

1. State Grid Corporation: The Security Risk Assessment Norm to Power Supply Enterprises. China Electric Power Press, Beijing (2008)
2. State Grid Corporation: Supply Enterprise Security Risk Identification and Prevention Operations Manual. China Electric Power Press, Beijing (2008)
3. Ge Fengshan, and MaWanquan: New Power System Security Risk Management System and Evaluation Methods. China Electric Power Press, Beijing (2008)
4. LI Wen-yuan: Risk assessment of power systems: models and applications. IEEE Press and Wiley & Sons Inc, U.S. (2005)