电力通信网安全风险计算模型

高会生，李聪聪

（华北电力大学电子与通信工程系，河北 保定 071300）

摘要：首先介绍了电力通信网风险三要素：资产、威胁和脆弱性的相关概念并举例进行说明，阐述了三者与风险之间的关系以及如何根据这三个要素计算风险值。为得到较为客观的风险计算结果，对现有的几种风险计算方法进行比较分析得出其优缺点。将风险三要素之间的相互关联性考虑到风险计算过程当中，提出了一种改进的电力通信网风险计算模型，并通过实例对其进行验证，该模型应用灵活，既可用于计算单因素的风险也适用于各因素间组合风险的计算。

关键词：电力通信网； 风险计算； 资产； 威胁； 脆弱性

Risk calculation modeling in electric power communication system

GAO Hui-sheng , LI Cong-cong

（Department of Electronic and Telecommunication Engineering, North China Electric Power University, Baoding 071003, China）

Abstract: This paper introduces the conception of asset, threat and vulnerability which are the three factors of risk in electric power commcuication network.The relationship between the three factors and riskis expatiated,and how to calculate the risk value by the three factors is expained.For an external risk calculate result,it analyses several risk calculate methods of existing and gives their advantages and shortcomings. In the process of risk calculation, this paper takes the relation of the three factors of risk into account, proposes an improved risk calculation method of electric power commcuication network,and test its effectiveness with examples. This model applyied agility, it can be used in single factor risk caculate and integrated factors risk calculation.

Key words: electric power communication; risk calculation; asset; threat; vulnerability

中图分类号： TP393 文献标识码： A 文章编号： 1003-4897(2007)14-0050-04

0 引言

电力通信网作为国家专用通信网之一已经逐渐发展成为以光纤、无线移动通信、卫星、微波、载波等多种功能齐全的通信方式为手段。随着电力系统自动化水平的不断提高，电力通信网在电力生产和电力调度中发挥着越来越重要的作用，对电力通信网进行风险分析、风险计算，确保其稳定运行具有非常现实的意义[1]。

风险分析作为风险评估中的重要组成部分，主要内容为确定威胁利用资产的脆弱性发生安全事件的可能性，并结合资产的价值从而来确定系统风险的过程。风险分析的核心部分就是如何计算风险。风险可以看成是一个函数，参数应包括资产的价值、威胁出现频率以及脆弱性的严重程度，可以用不同的方法来关联这些参数的，比较常用的有相乘法和矩阵法。本文在对风险评估的流程进行详细了解，分析和总结现有风险分析中的计算方法的基础上，提出了一种较为具体的风险计算模型。

1 风险分析

1）风险相关的三要素分别为：资产、威胁、脆弱性[2]。

① 资产（Asset）：对单位具有价值的东西。

电力通信网资产可从各种形态考虑，物理的（如光缆、交换机、SDH设备等）和逻辑的（如体系结构、通信协议、各种业务、数据文件等）；硬件的（如：光端机、路由器、配线架等）和软件的（如：Oracle、Sybase数据库，MS IIS应用系统）；有形的（如建筑、设备等），无形的（如企业形象、客户关系等）；静态的（如规定等）和动态的（如过程等）；技术的和管理的；人力的、物力的、财力的、知识的和时间的；等等。根据描述和理解的需要，可以从不同角度，依据不同特性来划分资产形态[3]。

② 脆弱性（Vulnerability）：资产或资产中称被威胁利用的弱点。

脆弱性本身并不对资产造成损害，只有在一定条件得以满足时（被威胁利用）才会对资产产生影响。脆弱性一般分为组织脆弱性和技术脆弱性。组

织脆弱性是指组织的政策或实践中可能导致未授权行为的弱点。技术脆弱性是指系统、设备和直接导致未授权行为的弱点。电力通信网中技术脆弱性如：Oracle、MS SQL 等主要关系型数据库的自身安全漏洞，核心的网络设备，如路由器、交换机等存在安全漏洞；管理脆弱性有：省局统一的 WEB 网站向外发布信息并提供网上信息服务，但很多分局和分公司仍允许以拨号、DDN 专线、ISDN 等方式单独接入互联网，存在着由多个攻击入口进入电力内部网的可能，还有在电力内部网络中非法安装和使用未授权软件等。

③ 威胁（Threat）：可能对资产或单位造成损害的事故的潜在原因。威胁由多种属性来刻画：威胁的主体（威胁源）、能力、资源、动机、途径、可能性和后果。

威胁一般分为自然威胁和人为威胁，人为威胁又分为有意的和无意的。电力通信网中自然威胁有地震、火灾、静电等，人为的恶意威胁如：偷盗电缆、破坏通信基站，无意的如：人员操作失误等。

2)《信息安全风险评估指南》中对风险进行分析要从这几个关键要素出发，具体如图 1 所示。

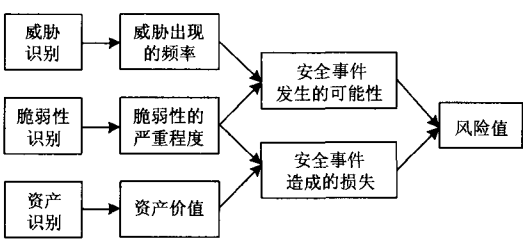


图 1 风险分析原理

Fig.1 Risk analysis principle chart

图 1 中介绍了风险相关的几个关键要素：资产、威胁、脆弱性。每个要素都有各自的属性，资产的属性是资产价值，脆弱性的属性是被威胁利用后给资产造成影响的严重程度，威胁的属性是威胁发生的可能性。

3)计算风险值遵循如下几个步骤：

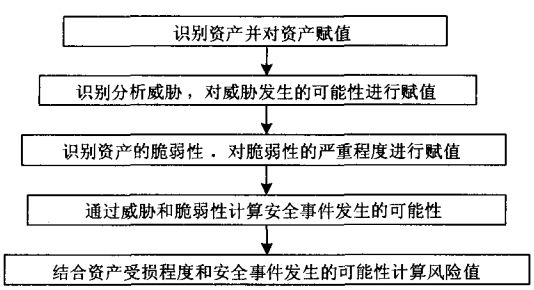


图 2　风险值计算步骤

Fig.2 Risk value calculate step

2　风险计算方法

2.1 相乘法

相乘法原理：

$$R = f(A,V,T) = A \times V \times T \text{。}$$

式中：R、A、V、T 分别代表风险、资产、脆弱性、威胁。

对资产、威胁、脆弱性分别赋值，然后再进行相乘。该方法特点是简单明确，直接按照统一公式计算，就可以得到所需要的结果。在风险值计算中，通常需要对三个要素确定的另一个要素值进行计算，因此相乘法在风险分析中得到广泛采用。但是该方法参考的因素不够全面，只是简单的将三个关键要素相乘，其前提是资产、威胁、脆弱性三者应该是独立不相关的，但实际上脆弱性是隶属于资产的，而威胁要利用脆弱性才能对资产造成影响，所以计算结果具有片面性。

2.2 矩阵测量法

$Z = f(x,y)$，函数 f 采用矩阵形式表示。以要素 x 和要素 y 的取值构建一个二维矩阵，矩阵内 $m*n$ 个值为要素 Z 的取值。

该方法进行风险计算时，通常要对两个要素确定的另一个要素进行计算，例如：威胁和脆弱性确定安全事件发生的可能性值、由资产和脆弱性确定的安全事件的损失值以及由安全事件的可能性值和损失值确定的风险值。矩阵法通过构造两两要素计算矩阵，可以清晰罗列要素的变化趋势，具有较好的灵活性。

表 1 矩阵图示法

Tab.1　Matris chart method

Y / X	Y_1	…	Y_j	…	Y_n
X_1	Z_{11}	…	Z_{1j}	…	Z_{1n}
…	…	…	…	…	…
X_i	Z_{i1}	…	Z_{ij}	…	Z_{in}
…	…	…	…	…	…
X_m	Z_{m1}	…	Z_{mj}	…	Z_{mn}

矩阵法中虽然能够清晰地表示出风险的变化，但由于赋值过程由专家评判给出，人的主观因素起到很重要的作用，所以计算结果不具有客观性。

以上两种计算方法在风险分析中得到了广泛的应用，除此外还有基于威胁等级的风险计算方法[2]，是直接考虑威胁、威胁对资产产生的影响以及威胁发生的可能性来确定风险。这三种方法都是从资产、威胁、脆弱性来考虑，但只是三者的简单组合，并未深入考虑其关联性，本文提出的风险计算模型则

增加了其间的关系。

3 风险计算模型

一种常用的风险计算方法为[2]：

$$R = F(A,V,T) = F(A_a, P(V_a,T)) \quad (1)$$

式中:R 表示风险，A 表示资产价值，V 表示脆弱性，T 表示威胁，A_a 指资产的相对价值，V_a 是某一资产本身脆弱性的严重程度，T 是未考虑资产脆弱性时威胁发生的频率。

分析上式，对其进行改进给出如下风险计算形式化的表示：

$$R=F(A,V,T)=F(I(A_a,\partial_a),P(V_a,T))= F(I(A_a,\partial_a),P(V_a,T\times\beta(V_i,T_j))) \quad (2)$$

式中:∂_a 代表资产受损程度，$0<\partial_a\le 1$，它表示安全事件发生后对资产的影响程度或者说是资产的受损害程度，资产遭受损失后它的资产价值可能会完全丧失即 $\partial_a=1$，此时风险最大，但是资产受损后资产价值不可能一点不受影响，所以 $\partial_a\neq 0$。

$\beta(V_i,T_j)$ 为布尔函数[4]，表示如下：

$$\beta(V_i,T_j)=\begin{cases}1 & \text{威胁}j\text{能利用脆弱性}i\text{对资产造成影响}\\ 0 & \text{威胁}j\text{不能利用脆弱性}i\text{对资产造成影响}\end{cases} \quad (3)$$

I 函数代表安全事件造成的损失，不同的威胁对同一资产或者整个系统造成的影响不同，导致价值的损失也不同，但应当以资产的相对价值为衡量标准。

P 函数代表威胁利用脆弱性导致安全事件发生的可能性。

该模型可以计算多种资产、多个威胁、多个脆弱性的整体风险值，也可以计算单个资产在多个威胁多个脆弱性下的风险值，还有单个威胁对多个脆弱性、多种资产产生的风险值，同理可以计算某一脆弱性的风险值，还可以得到资产、威胁、脆弱性两两组合的联合风险值。

1）某种资产在 N 个威胁 M 个脆弱性下的风险计算

$$R=F(I(A_a,\partial_a),P(V_a,T\times\beta(V_i,T_j)))= A_a\times\partial_a\times\sum_{i=1}^{M}\sum_{j=1}^{N}V_{ai},T_j\times\beta(V_i,T_j)= \sum_{i=1}^{M}\sum_{j=1}^{N}A_a\times\partial_a\times V_{ai}\times T_j\times\beta(V_i,T_j) \quad (4)$$

2）某个威胁对 K 种资产、M 个脆弱性的风险计算

$$R=F(I(A_a,\partial_a),P(V_a,T\times\beta(V_i,T_j)))= \sum_{a=1}^{K}A_a\times\partial_a\times\sum_{i=1}^{M}V_{ai}\times T_j\times\beta(V_i,T_j)= \sum_{a=1}^{K}\sum_{i=1}^{M}A_a\times\partial_a\times V_{ai}\times T_j\times\beta(V_i,T_j) \quad (5)$$

3）某个威胁和某个脆弱性对 K 种资产的联合风险计算

$$R=F(I(A_a,\partial_a),P(V_a,T\times\beta(V_i,T_j)))= \sum_{a=1}^{K}A_a\times\partial_a\times V_{ai}\times T_j\times\beta(V_i,T_j)= \sum_{a=1}^{K}A_a\times\partial_a\times V_{ai}\times T_j\times\beta(V_i,T_j) \quad (6)$$

4）K 种资产、N 个威胁、M 个脆弱性下系统总的风险计算

$$R=F(I(A_a,\partial_a),P(V_a,T\times\beta(V_i,T_j)))= \sum_{a=1}^{K}A_a\times\partial_a\times\sum_{i=1}^{M}\sum_{j=1}^{N}V_{ai}\times T_j\times\beta(V_i,T_j)= \sum_{a=1}^{K}\sum_{i=1}^{M}\sum_{j=1}^{N}A_a\times\partial_a\times V_{ai}\times T_j\times\beta(V_i,T_j) \quad (7)$$

上面给出了单项资产、单个威胁、威胁和脆弱性的组合以及三者组合的风险，同理可以计算单个脆弱性、资产与脆弱性组合、资产与威胁组合的风险。在实际中风险一般不是独立的，常常是组合而产生的，所以该模型应用较为灵活，贴近于实际，根据计算结果可以得到哪种资产较重要，哪种威胁导致安全事件发生的可能性最大，哪种脆弱性的潜在影响最大。

表 2 风险值-风险等级对应表

Tab.2 Risk value-risk grade relation table

等级	标识	风险定义	区间划分
5	很高	风险很高，导致系统受到非常严重的影响	>480
4	高	风险高，导致系统受到严重影响	361～480
3	中	风险中，导致系统受到中等影响	241～360
2	低	风险低，导致系统受到一般影响	121～240
1	很低	风险很低，导致系统受到较小的影响	0～120

最后将风险值与下表风险区间对应即可确定其风险等级的高低。

4 实例分析

根据上面的风险计算模型，结合电力通信网实例对其进行验证。给出关键资产，结合脆弱性、威

胁分别计算它们的单独风险和整体组合风险。

下面以某供电局的电力系统通信为例，例中给出关键资产：光纤，并根据其一段时间内的故障报告给出如下几种光纤具有的脆弱性和存在的威胁，资产的受损程度根据故障后的平均维修时间给出，平均维修时间越长，受损程度越严重；威胁的发生频率由故障次数给出；脆弱性的严重程度由平均故障时间得到，具体参数如表 3 所示。

表 3 光纤故障参数表

Tab.3 Optic-fiber failure parameter table

造成事故后的平均维修时间/h			故障次数/次				
			运输车辆	现场施工	火灾	恶意破坏	气候条件
			17	46	24	37	18
平均故障时间/h	架空高度	516	193	342	271	268	
	地埋深度	238		181		179	
	防护强度	488		192			117
	环境铺设	357		192	188	266	59
	设计问题	469	163	264	227		120

表 4 光纤计算实例

Tab.4 Optic fiber risk calculate example

			光纤		资产价值		5
资产受损程度 / 安全事件发生的可能性			威胁种类及其发生频率列表				
			运输车辆	现场施工	火灾	恶意破坏	气候条件
			2	5	3	4	2
脆弱性严重程度	架空高度	4	0.3 / 1	0.5 / 1	0.4 / 1	0.4 / 1	0 / 0
	地埋深度	2	0 / 0	0.3 / 1	0 / 0	0.3 / 1	0 / 0
	防护强度	4	0 / 0	0.4 / 1	0 / 0	0 / 0	0.2 / 1
	铺设环境	3	0 / 0	0.3 / 1	0.3 / 1	0.4 / 1	0.1 / 1
	设计问题	4	0.3 / 1	0.4 / 1	0.4 / 1	0 / 0	0.2 / 1

由于光纤在电力通信中占有非常重要的地位，经过专家打分将资产价值量化为 5，将故障时间及故障次数四舍五入量化为 1-5 后给出的威胁发生频率和脆弱性程度，维修时间四舍五入量化为 0～1，具体如表 4 所示。

根据上表中的数据可以综合计算光纤的综合风险值为：340，风险等级处于中级，应提高重视，采取安全措施。各种脆弱性中架空高度对光纤威胁强度最大，架空高度太低，过往运输车辆很容易挂断，在易产生火灾的地方会被烧断，并且偷盗光缆的人能够顺利剪断光纤，但是如果架空高度过高的话，施工人员不宜进行操作，如果操作失误，也将会引起光纤中断、混线等故障，所以应该根据要架设光缆的周边环境合理地选择架空高度。威胁中现场施工最严重，修桥盖房、修地下管道等会受到光纤的架空高度、地埋深度的影响；各种施工还受到光纤防护强度的高低、光纤铺设环境的好坏及光纤设计问题的影响，施工对光纤的各种脆弱性都有影响，并且平时各种施工较多，所以会对光纤构成较大的威胁，因此，施工活动中应提高注意，尽量避开光纤铺设的地方。

5 总结

目前我国在电力通信领域中风险评估研究较少，主要是借鉴电力系统和信息安全等领域中风险评估的相关知识。本文从风险的三个关键要素出发，分析总结现有的风险计算方法，在此基础上进行了拓展，引出了资产受损程度变量，和威胁能否成功利用脆弱性的二值函数，对风险的计算考虑较为全面，使计算结果相对客观，并且将此风险计算模型灵活运用，适用于计算风险要素的单项风险以及组合风险。

参考文献

[1] 李瑾，夏向东. 电力通信网络安全管理策略[J]. 湖北电力,2005,(12):100-102.
LI Jin, XIA Xiang-dong.Safety Management Tactics of the Electric Power Communication Network[J].Hubei Electric Power,2005,(12):100-102.

[2] 范红，冯登国. 信息安全风险评估方法与应用[M]. 北京：清华大学出版社，2006.
FAN Hong,FENG Deng-guo. Information Security Risk Assessment Method and Application[M].Beijing: Tsinghua University Press,2006.

[3] 闽京华，王晓东. 信息安全的资产评估方法[J]. 网络安全技术与应用，2005,(10)：10-13.
MIN Jing-hua,WANG Xiao-dong.Asset Assessment Method of Information Security[J].Network Security Technology and Application,2005,(10):10-13.

[4] 李智勇，牛旭明. 信息安全风险评估中的风险计算[J]. 综合电子信息技术，2006，32(2)：42-47.
LI Zhi-yong, NIU Xu-ming. Risk Calculation in Information Security Risk Assessment[J].Integrate Electron Technology,2006,32(2):42-47.

（下转第 76 页　continued on page 76）

压产生对人有危险。调试接线如图 7 所示。

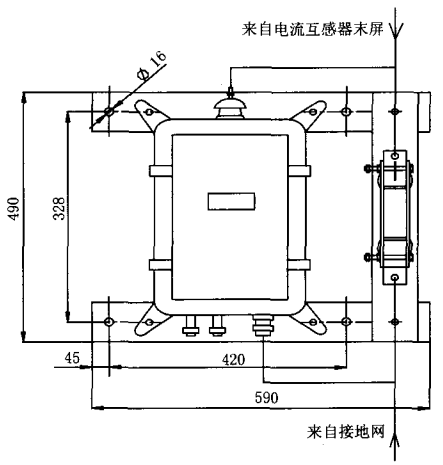
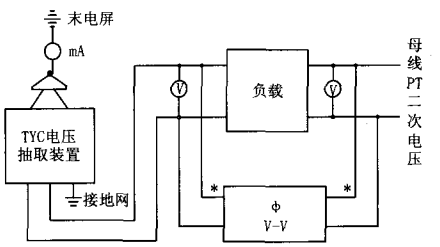


图 6 电压抽取装置安装示意图

Fig.6 Equipment of receiving voltage installment diagram



V-V 为钳型相位电压表

图 7 调试接线图

Fig 7 Debugging diagram

接好线后先将接地刀拉开（最好先不带负载），此时抽取装置接入末屏。对于 220 kV 系统此时抽取装置一次将会有 300~400 V 的电压，对于 110 kV 系统会有 200~300 V 的电压，所以调试时不要接触接地刀的上部和抽取装置绝缘套管的裸露部位及过电压保护器的带电部位。先不带负载粗调把电压调到与系统的 PT 二次电压相接近，然后合上刀闸将负载接入再拉开接地刀进行细调使电压幅值及相位与系统的相一致即可。

4 结束语

TYC 系列电压抽取装置已经获得了国家专利，并且通过了北京电力科学研究院的各项型式试验。此系列装置已经在长春的东丰变、合心变，哈尔滨的哈南变，沈阳的沈东变、齐齐哈尔冯屯变、青铜峡水电站、清河电厂、营口、牡丹江、通辽等广泛应用，并取得了良好的经济技术效益。电压抽取装置能为保护和测控装置提供 2 组 100 V 及 58 V 的标准电压，精度满足运行要求。电压抽取装置以它的经济、可靠、方便的特点将会越来越广泛地被电力系统所应用。

参考文献

[1] 宋继成.220~500 kV 变电所电气接线设计[Z].
SONG Ji-cheng.The Transformer Substation Electricity Designs in 220-500 kV System[Z].

收稿日期：2006-12-09；　修回日期：2007-01-18

作者简介：
金鹏飞（1975-），男，大专，助理工程师，从事继电保护工作。E-mail:hyjpf2006@126.com

（上接第 53 页　continued from page 53）

[5] 葛瑞金，陈长松. 信息安全风险评估量化模型的研究[J]. 信息网络安全，2005, (9).
GE Rui-jin,CHEN Chang-song.Research of Information Security Risk Assessment Measure Modeling[J]. Information Network Security,2005,(9).
[6] 刘恒，吕述望. 基于模型的安全风险评估方法[J]. 计算机工程，2005, (5)：129-131.
LIU Heng, Lü Shu-wang. Research in the Models of the Security Risk Assessment Technology[J]. Computer Engineering,2005[5]:129-131.
[7] Yacovy.Haimes.Risk Modeling,Assessment,and Management[M]. Wiley Interscience,2004.

收稿日期：2006-12-25；　修回日期：2007-03-10

作者简介：
高会生（1963-），男，教授，硕士导师，研究方向为通信网的管理和风险评估、电力系统通信；
李聪聪（1983-），女，硕士研究生，研究方向为电力通信系统安全风险评估。E-mail:sweetlcc@sohu.com

（上接第 72 页　continued from page 72）

些相对较为快速、全面、完善的功能检验方法，采用上述方法接线进行试验，不必在工作中频繁的更换测试接线，提高了工作效率、减少了错误的产生和在运行的电流回路上操作的次数，能有效地降低电流回路开路的可能性，如能在工作开始前熟悉相关图纸资料和上述方法，相对厂家提供的试验方案经对比，主要功能的检验能节省好几个小时的时间，以便能有更多的时间处理其它事情。以保证在规定时间内保质保量地完成母差保护的检验任务。

收稿日期：2006-11-25；　修回日期：2006-12-30

作者简介：
林　启（1980-），男，助理工程师，大专，长期从事继电保护维护与管理工作。E-mail: linkui_sw@yahoo.com.cn