文章编号：1000-3673（2016）04-1265-06 中图分类号：TM 721 文献标志码：A 学科代码：470 40

改进功能分解的二次系统风险评估方法

曹志昆[1]，章杜锡[2]，董树锋[1]，郭创新[1]
（1. 浙江大学 电气工程学院，浙江省 杭州市 310027；
2. 国网宁波供电公司，浙江省 宁波市 315016）

An Improved Method of Secondary System Risk Assessment Based on Functional Decomposition

CAO Zhikun[1], ZHANG Duxi[2], DONG Shufeng[1], GUO Chuangxin[1]
(1. School of Electrical Engineering, Zhejiang University, Hangzhou 310027, Zhejiang Province, China;
2. Ningbo Electric Power Bureau, Ningbo 315016, Zhejiang Province, China)

ABSTRACT: Probability assessment of functional failure is key procedure in secondary system risk assessment based on functional decomposition. This paper proposed models and algorithms for probability assessment of functional failure based on functional graph of information pieces. In this approach, leaf functions were first decomposed to functional graph, consisting of logical nodes and logical connections. Reduction of connection matrix was then performed to yield logical expression of function state in terms of states of logical nodes and connections. Two methods of evaluating probability of functional failure were presented, i.e. accurate method and approximate method. Assessment procedure was illustrated with a case study on data acquisition function.

KEY WORDS: risk assessment; secondary system; functional decomposition

摘要：在基于功能分解的二次系统风险评估中，对于功能失效概率的评估是整个评估过程中关键的一环。针对目前方法中需要建立可靠性框图、主观性强等不足，提出了基于功能图的功能失效概率评估模型，并将基于可靠性框图的评估方法进行推广，使之可以直接根据功能图计算功能的失效概率。该方法首先将叶功能分解成只含逻辑节点和逻辑连接的有向连通图，接着根据邻接矩阵求得功能状态关于逻辑节点和逻辑连接状态的表达式，并分别给出计算功能失效概率的精确方法和近似方法。最后，使用测量数据采集功能的算例说明所提评估方法的计算过程。

关键词：风险评估；二次系统；功能分解
DOI：10.13335/j.1000-3673.pst.2016.04.042

基金项目：国家自然科学基金资助项目(51207136)；教育部高等学校博士学科点专项科研基金资助项目(20120101120157)。
Project Supported by National Natural Science Foundation of China(NSFC)(51207136) and The Research Fund for the Doctoral Program of Higher Education(20120101120157).

0 引言

现代电网一次系统和二次系统之间的联系越来越紧密，电力二次系统的安全风险给一次系统的安全运行引入了许多不确定因素，评价电力二次系统的风险已是一个紧迫的问题。

目前针对电力二次系统风险评估的研究已有一些成果。文献[1]从二次设备、信息安全和人为风险 3 个方面对电力二次系统风险评估的研究现状作了综述。文献[2-4]研究了二次设备的风险评估方法。文献[5-9]考虑了继电保护系统、控制系统和电力通信网对电力系统安全风险的影响。文献[10]分析了电力信息网的攻击模式。文献[11-12]研究了在电力通信网受到网络攻击情况下电网的可靠性和安全风险。文献[13-14]提出了提高电力信息系统安全性的措施。文献[15-16]研究了电力信息系统的安全体系设计方法。文献[17-18]研究了认知可靠性和人因可靠性的定量评估方法。上述研究没有对电力二次系统故障对二次系统本身和一次系统所带来的影响提出整体的评估方法。基于电网运行控制人员更为关心“电力二次系统既定的业务功能能否完成，若不能完成将带来怎样的后果”的现实，文献[19]提出了以电力二次系统的业务功能为基础，对电力二次系统进行规范化分解，分析功能失效的可能性和功能失效所带来的后果与损失。该方法能体现电力二次系统作为一个整体对于电力生产的重要性，使电网运行人员能够准确、直接地掌握电力二次系统风险水平，从而满足实际电力生产、管理的需要。

在基于功能分解的电力二次系统风险评估中，对软件功能失效概率的评估是关键的一步，文献[19]

通过建立可靠性框图进行评估。然而，建立系统或设备的可靠性框图需要依赖专家的经验，主观性较强，且该方法无法考虑信息流的方向，且需要根据是否存在冗余配置单独评估，通用性不高。本文以功能分解后得到的功能图为基础，对功能失效的概念作了定义，将基于可靠性框图的评估方法[20]进行推广，使之可以直接依据功能图计算出功能的失效概率，从而克服了上述不足。

1 二次系统分解及风险评估

1.1 系统功能树

在对系统进行分解前，需要对二次系统风险评估中使用的几个概念进行定义和描述。

定义 1：系统(System)以业务为区分，包含软件、硬件、人员和组织，具有物理边界并能执行一系列综合任务的功能集合。如继电保护系统、安全自动控制系统等。

定义 2：功能(Function)在系统中，独立执行某个任务的信息和物理设备的集合。对于一个复杂的系统，一个功能可能包含多个子功能(Sub Function)。如继电保护系统中的过电流保护功能。

依据上述概念定义和功能划分原则，可以将系统分为系统层、功能层等若干层次，如图 1 所示。其中，位于最后一层的功能称为叶功能。

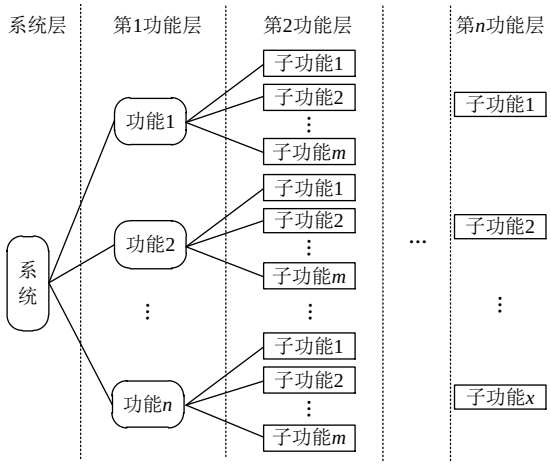


图 1 系统功能树状结构

Fig. 1 Hierarchy of functions of a system

1.2 基于功能树的风险评估

基于以上分层分解，对于一个包含 n 个子功能层的系统而言，其风险基本运算可由以下 2 个式子共同表示：

$$R_{\mathrm{SYS}} = S_{\mathrm{condition}} \sum_{j=1}^{k_1} (\omega_{F_{1,j}} R_{F_{1,j}}) \tag{1}$$

$$R_{F_{m,i}} = \sum_{j=1}^{k_{m,i}} (\omega_{F_{m+1,i,j}} R_{F_{m+1,i,j}}),\ m = 1,\ldots,n-1 \tag{2}$$

式中：R_{SYS} 为整个系统的风险值；$S_{\mathrm{condition}}$ 为系统状态系数，表示当前系统状况；$R_{F_{1,j}}$ 为第 1 层第 j 个功能风险；$\omega_{F_{1,j}}$ 为其权值；k_1 为该系统第一层功能总数。$R_{F_{m,i}}$ 为第 m 层第 i 个功能的风险；$k_{m,i}$ 为第 m 层第 i 个功能包含的下一层子功能数；$R_{F_{m+1,i,j}}$ 为第 m 层第 i 个功能的第 j 个子功能的风险；$\omega_{F_{m+1,i,j}}$ 为其权值。

1.3 功能图

从 1.2 节可知：计算叶功能的失效概率是整个风险评估中关键的一环。对叶功能进一步分解就可以得到功能图，功能图中的主要元素包括：实体、逻辑节点和逻辑连接。

实体：电力二次系统中客观存在的二次设备、电力软件和控制人员等。

逻辑节点：电力二次系统中交换数据或执行任务的最小部分。逻辑节点是二次设备、电力软件和控制人员的整体或部分的行为和方法的抽象，如变电站自动化系统中负责模拟量采集的智能电子设备可以抽象为电流互感器逻辑节点、电压互感器逻辑节点等。

逻辑连接：逻辑节点之间的通信链路，是信息传送的途径，具有方向性。逻辑连接可以视为对通信信道的抽象。

功能由若干交换信息的逻辑节点和逻辑连接组成。信息片是信息的实体，包含待传输的信息和要求的属性。通过功能图可以知道功能完成涉及的逻辑连接、逻辑节点及它们之间的信息片流向。以 SCADA 系统中测量数据采集功能为例，该功能的软硬件示意图如图 2 所示，图中包含 6 个实体，抽象成功能图如图 3 所示，该功能图是一个有向连通图。

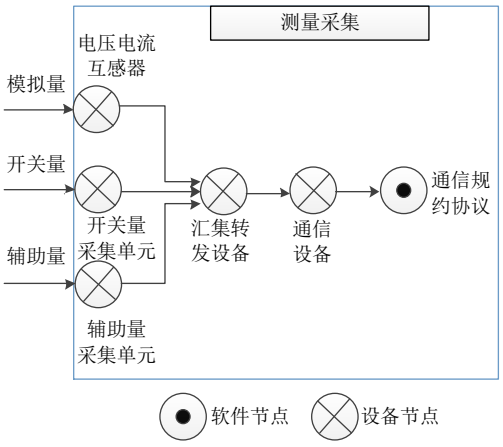


图 2 测量数据采集软硬件结构

Fig. 2 Structural diagram of hardware and software of data acquisition

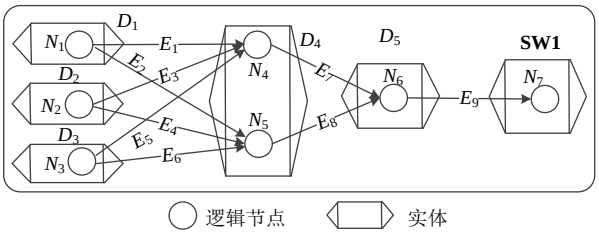


图 3　测量数据采集功能图

Fig. 3　Functional diagram of data acquisition

2　基于功能图的失效概率评估

2.1　分析假设

在分析功能失效概率时，本文作如下假设：

1）不考虑功能失效的连锁效应，即认为同层功能失效互相独立。

2）功能本身以及功能图中每一逻辑节点和逻辑连接(下文分别称为节点和连接)均有且仅有 2 种状态：正常和失效。若信息片能由某连接的首端正确传输至末端，则称该连接正常，反之则称该连接失效。若某节点接收到的信息片能被正确处理并发送至该节点后续的所有连接，则称该节点正常，反之则称该节点失效。通常用一个取值为 0 或 1 的变量来表征功能、节点或连接的状态，该变量值取 0 表示失效，取 1 表示正常。

3）功能图中各节点、连接的状态相互独立。

一般来讲，信息系统的功能是通过信息片在逻辑节点之间按照既定方向顺畅流动来完成的，功能完成的标志是末端的逻辑节点(下文称之为末端节点)正确接收到所需信息片。若功能图中存在从首端节点 E_i 出发至末端节点 E_j 的路径，则称首端节点 E_i 与末端节点 E_j 相联。本文对功能正常和失效定义如下：若功能图中任一末端节点 E_t 均能正确接收到来自与 E_t 相联的各首端节点的信息片，则称功能正常完成，反之则称功能失效。

在功能图中，若某路径上的所有逻辑节点和逻辑连接均不失效，则称该路径有效，亦即其首端节点产生的信息片可经此路径正确传输至末端节点。于是，功能正常完成的充要条件为：功能图中任意一对相联的首端节点和末端节点之间均至少存在一条有效路径。下文即利用此结论来评估功能失效概率。

2.2　评估流程

功能失效概率评估的流程图如图 4 所示，下面分节对各个步骤分别作详细介绍。

2.2.1　功能分解

按照第 1 节所述的原则与方法，分解功能涉及的软硬件，将其抽象成逻辑节点和逻辑连接，从而得到功能图。

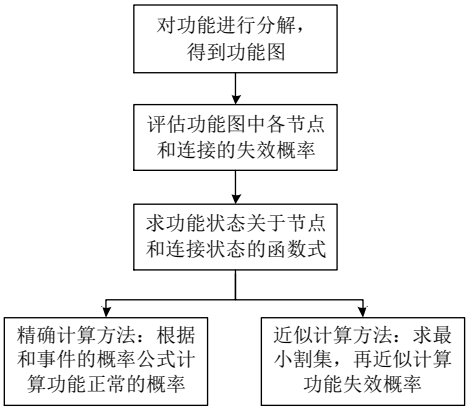


图 4　功能失效概率评估流程图

Fig. 4　Flow chart of evaluating the probability of functional failure

2.2.2　分析逻辑节点和逻辑连接的失效概率

逻辑节点可能是二次设备、软件或人员，可以根据已有研究成果进行单独分析。目前针对电力软件运行可靠性的相关研究还较少，可以采用历史统计的方法来得到软件的故障概率，即认为软件的故障概率是一个定值表示为

$$U=\frac{f\cdot T_{\mathrm{MTTR}}}{T} \tag{3}$$

式中：f 为自投入以来该软件故障的次数；T_{MTTR} 为每次故障的平均修复时间(h)；T 为软件自投入以来的运行时间。

逻辑连接是对通信信道的抽象，对于冗余配置或非冗余配置的信道可以采用不同的失效概率进行处理。

2.2.3　求功能状态关于节点和连接状态的函数式

在本小节和第 3 节中，加号和 Σ 表示逻辑或运算，乘号和 Π 表示逻辑与运算。

在本步骤中，首先根据功能图的拓扑关系建立其邻接矩阵。邻接矩阵是一个方阵，其阶数等于功能图中节点个数。它的对角线元素全为 1，非对角线元素 N_{ij} 由式(4)给出：

$$N_{ij}=\begin{cases}e_{ij}, & \text{功能图中存在从节点}i\text{至}j\text{的连接}\\ 0, & \text{功能图中不存在从节点}i\text{至}j\text{的连接}\end{cases} \tag{4}$$

其中 e_{ij} 是表征节点 i 至节点 j 逻辑连接 E_{ij} 状态的变量，$e_{ij}\in\{0,1\}$。

接着逐一消去邻接矩阵中与功能图中间节点(既非首端节点，也非末端节点的节点)相对应的行列，消去前后须保持功能状态关于节点和连接状态的逻辑关系式不变。消去中间节点 k 后，原邻接矩阵中与节点 k 对应的行和列被消去，邻接矩阵的阶数减 1。以带撇的符号表示新邻接矩阵的元素，不

带撇的符号表示原邻接矩阵的元素，对于非对角元素有如下关系

$$N'_{ij}=N_{ij}+N_{ik}N_{kj} \tag{5}$$

对角线元素仍保持 1 不变。

设功能图中编号为 1 至 p 的节点为首端节点，编号 q 至 n 的节点为末端节点，将中间节点全部消去之后，得到形如式(6)的方阵：

$$\boldsymbol{N}'=\begin{array}{c}\\1\\\vdots\\p\\q\\\vdots\\n\end{array}\begin{array}{c}\begin{array}{cccccc}1 & \cdots & 0 & N_{1q} & \cdots & N_{1n}\end{array}\\\begin{bmatrix}\vdots & \ddots & \vdots & \vdots & \ddots & \vdots\\0 & \cdots & 1 & N_{pq} & \cdots & N_{pn}\\0 & \cdots & 0 & 1 & \cdots & 0\\\vdots & \ddots & \vdots & \vdots & \ddots & \vdots\\0 & \cdots & 0 & 0 & \cdots & 1\end{bmatrix}\end{array}=\begin{bmatrix}1 & \boldsymbol{N}'_{\mathrm{u}}\\0 & 1\end{bmatrix} \tag{6}$$

取式(6)分块矩阵 $\boldsymbol{N}'_{\mathrm{u}}$ 中所有不恒为 0 的元素作逻辑与运算($N_{ij}\equiv 0$ 表明原功能图中不存在从节点 i 至 j 的路径，故不予考虑)，得式(7)：

$$G=\prod_{\substack{1\le i\le p\\ q\le j\le n\\ N_{ij}\neq 0}} N_{ij} \tag{7}$$

式(7)即为当逻辑节点全都正常工作时功能状态 G 关于连接状态的函数式。

为了考虑功能状态与节点状态之间的关系，首先将式(7)化成最简与–或表达式，得到

$$G=G_1+\cdots+G_k=\sum_{i=1}^{k}G_i \tag{8}$$

其中式(8)的 G_i 是由一系列表征连接状态的变量取逻辑与运算得到的，记作 $G_i=\prod_j e_j$。e_j 所对应连接为 E_j，将 E_j 两端节点的状态分别记作 v_{j1} 和 v_{j2}，令 $h(e_j)=e_j v_{j1}v_{j2}$，$H_i=\prod_j h(e_j)$，由式(8)得到

$$H=H_1+\cdots+H_k=\sum_{i=1}^{k}H_i \tag{9}$$

式(9)即为功能状态 H 关于节点和连接状态的逻辑函数式。功能正常完成的充要条件是式(9)右端至少存在一项 $H_i=1$。

2.2.4 计算功能失效概率

下面给出 2 种计算功能失效概率的方法：精确方法和近似方法。其中，近似方法具有下列优点：计算量小于精确方法；当节点和连接的失效概率都很小时，近似计算的误差也很小；近似方法可同时得到功能的失效模式。

1）精确计算法。

得到功能状态关于节点和连接状态的表达式之后，即可利用事件和的概率公式计算功能状态为正常的概率：

$$\begin{aligned}P(H=1)=P(\bigcup_{i=1}^{k}H_i=1)=&\sum_{i=1}^{k}P(H_i=1)-\\&P(H_1=1\cap H_2=1)-\cdots-P(H_{k-1}=1\cap H_k=1)+\\&P(H_1=1\cap H_2=1\cap H_3=1)+\cdots+\\&(-1)^{k-1}P(\bigcap_{i=1}^{k}H_i=1)\end{aligned} \tag{10}$$

式(10)中第 2 个等号右端每一项均可表示为相应节点和连接正常工作的概率之积，利用第 2.2.2 节的结果即可求得功能正常工作的概率。用 1 减去式(10)的结果即为功能失效概率。

2）近似计算法。

本文将满足下列 2 个条件的节点–连接集合称为功能的最小子集：1）当此集合中包含的所有节点和连接都有效时，该功能正常完成；2）当此集合中任一节点或连接失效时，该功能失效。

将式(9)中 H_i 所对应的节点和连接集合记作 M_i，$\{M_1,\ldots,M_k\}$即为功能的所有最小子集，由此可求得功能的最小割集。割集是由某些节点和连接组成的集合，当此集合中的节点和连接全部失效时功能失效。割集反映了功能的失效模式，即哪些节点和连接的失效将导致功能的失效。割集的阶数等于该割集中元素的个数。最小割集是满足下述条件的割集：只要此割集中任一节点或连接不失效，功能就可正常完成。根据所有最小子集求出所有最小割集的方法如下。

1）根据以下判据逐个考察功能图中的节点和连接，求出所有一阶最小割集：若仅包含单个节点(或连接)的集合 C_1 同时是 $M_1,\ldots,M_k$ 的子集，则 C_1 是一个一阶最小割集。

2）依次令 k=2,…,$n_{\max}$($n_{\max}$ 等于功能图中节点和连接总数)，重复执行下述步骤，求出功能的所有最小割集：若 1 阶至 k–1 阶最小割集均已求出，则求 k 阶最小割集的方法如下：从所有节点和连接中任选 k 个元素，得到所有可能的组合，将上述任意一种组合所对应的节点–连接集合记作 C，若 C 同时为 $M_1,\ldots,M_k$ 的子集，且任何阶数小于 k 的最小割集均不是 C 的子集，则 C 是一个 k 阶最小割集。

用 $A_i(i=1,\ldots,m)$表示每一最小割集中节点和连接全部失效的随机事件，功能失效的概率即为

$$\begin{aligned}P(\bigcup_{i=1}^{m}A_i)=&\sum_{i=1}^{m}P(A_i)-P(A_1\cap A_2)-\cdots-\\&P(A_{m-1}\cap A_m)+P(A_1\cap A_2\cap A_3)+\cdots+\\&(-1)^{m-1}P(\bigcap_{i=1}^{m}A_i)\end{aligned} \tag{11}$$

节点和连接失效的概率一般很小，故可忽略上式中次数较高的项，在降低计算量的同时仍可得到误差较小的结果。

3　算例分析

以图 5 所示的测量数据采集功能为例，逻辑节点和逻辑连接的失效概率如表 1—2 所示，大写字母 V 和 E 分别表示功能图中的逻辑节点和逻辑连接，小写字母 v 和 e 分别表示相应节点或连接的状态。其中，节点 V_7 到节点 V_6 的通信信道有冗余配置，故连接 E_9 的失效概率较小。

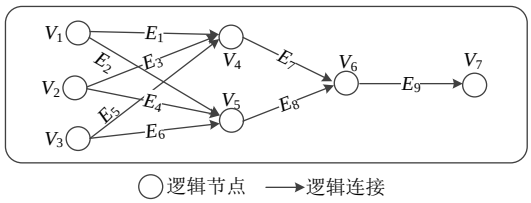


图 5　测量数据采集功能算例的功能图

Fig. 5　Case study on the functional diagram of data acquisition function

表 1　逻辑节点的失效概率

Tab. 1　Probability of failure of logical nodes

节点编号	V_1	V_2	V_3	V_4	V_5	V_6	V_7
失效概率	0.008	0.002	0.003	0.002	0.003	0.003	0.001

表 2　逻辑连接的失效概率

Tab. 2　Probability of failure of logical connections

连接编号	E_1	E_2	E_3	E_4	E_5	E_6	E_7	E_8	E_9
失效概率	0.008	0.009	0.002	0.005	0.005	0.009	0.002	0.008	0.000 6

按照 2 中介绍的算法，消去节点 4、5、6，得到化简后的邻接矩阵为

$$\boldsymbol{N}'=\begin{array}{c}\\1\\2\\3\\7\end{array}\begin{array}{c}\begin{matrix}1 & 0 & 0 & (e_1e_7+e_2e_8)e_9\\0 & 1 & 0 & (e_3e_7+e_4e_8)e_9\\0 & 0 & 1 & (e_5e_7+e_6e_8)e_9\\0 & 0 & 0 & 1\end{matrix}\end{array}\begin{array}{l}\left.\begin{matrix}\\\\\\\end{matrix}\right]\\\\\\\end{array}\tag{12}$$

于是 G 和 H 如表 3 所示。

由精确计算方法可得功能状态为正常的概率是 0.982 096，功能失效概率即为 0.017 904。

若采用近似计算方法，首先得到功能的所有最小割集如表 4 所示。

表 3　式(8)与(9)中的 G_i 与 H_i

Tab. 3　G_i and H_i in Eqs. (8) and (9) respectively

i	G_i	H_i
1	$e_1e_3e_5e_7e_9$	$e_1e_3e_5e_7e_9v_1v_2v_3v_4v_6v_7$
2	$e_2e_3e_5e_7e_8e_9$	$e_2e_3e_5e_7e_8e_9v_1v_2v_3v_4v_5v_6v_7$
3	$e_1e_4e_5e_7e_8e_9$	$e_1e_4e_5e_7e_8e_9v_1v_2v_3v_4v_5v_6v_7$
4	$e_2e_4e_5e_7e_8e_9$	$e_2e_4e_5e_7e_8e_9v_1v_2v_3v_4v_5v_6v_7$
5	$e_1e_3e_6e_7e_8e_9$	$e_1e_3e_6e_7e_8e_9v_1v_2v_3v_4v_5v_6v_7$
6	$e_2e_3e_6e_7e_8e_9$	$e_2e_3e_6e_7e_8e_9v_1v_2v_3v_4v_5v_6v_7$
7	$e_1e_4e_6e_7e_8e_9$	$e_1e_4e_6e_7e_8e_9v_1v_2v_3v_4v_5v_6v_7$
8	$e_2e_4e_6e_8e_9$	$e_2e_4e_6e_8e_9v_1v_2v_3v_5v_6v_7$

表 4　功能的最小割集

Tab. 4　Minimal cut sets

阶数	割集
1	$\{E_9\},\{V_1\},\{V_2\},\{V_3\},\{V_6\},\{V_7\}$
2	$\{E_1,E_2\},\{E_1,E_8\},\{E_1,V_5\},\{E_2,E_7\},$ $\{E_2,V_4\},\{E_3,E_4\},\{E_3,E_8\},\{E_3,V_5\},$ $\{E_4,E_7\},\{E_4,V_4\},\{E_5,E_6\},\{E_5,E_8\},$ $\{E_5,V_5\},\{E_6,E_7\},\{E_6,V_4\},\{E_7,E_8\},$ $\{E_7,V_5\},\{E_8,V_4\},\{V_4,E_5\}$

若只考虑式(11)的一次项，功能失效概率为 0.017 6，相对误差为 1.70%；只计算至二次项，功能失效概率为 0.017 916 8，相对误差为 0.071 49%。可见近似计算所得结果的相对误差较小。

4　结论

本文提出的基于信息片有向图的功能失效概率评估模型和算法具有以下几个特点：

1）功能图分解是对二次设备、软件、信道的抽象，物理意义明确，分解过程简单客观。

2）对于二次设备冗余配置的情况，只要更改逻辑节点和逻辑连接的失效概率值，对分解过程没有影响，通用性好。

3）近似计算方法不仅具有计算量小、相对误差小的特点，还能同时得到功能的失效模式。

参考文献

[1] 郭创新，陆海波，俞斌，等．电力二次系统安全风险评估研究综述[J]．电网技术，2013，37(1)：112-118.
Guo Chuangxin，Lu Haibo，Yu Bin，et al．A survey of research on security risk assessment of secondary system[J]．Power System Technology，2013，37(1)：112-118(in Chinese).

[2] 吴姜，王奕，王仁民．电气二次设备风险量化评估体系设计[J]．中国电力，2013，46(1)：75-80.
Wu Jiang，Wang Yi，Wang Renmin．Design of quantitative risk assessment system for secondary equipment of power system[J]．Electric Power，2013，46(1)：75-80(in Chinese).

[3] 陈建国，刘友波，林呈辉，等．电力系统二次主设备运行风险的属性熵权测度评估[J]．华东电力，2013，41(3)：514-518.
Chen Jianguo，Liu Youbo，Lin Chenghui，et al．A novel assessment algorithm for operation risk of power system secondary equipment based on attribute entropy measurement theory[J]．East China Electric Power，2013，41(3)：514-518(in Chinese).

[4] 黄明辉，蔡泽祥，曹建东，等．电力系统二次设备风险评估模型和方法[J]．广东电力，2012，25(2)：5-8，76.
Huang Minghui，Cai Zexiang，Cao Jiandong，et al．Risk assessment model and method for secondary equipment in power sys-tem[J]．Guangdong Electric Power，25(2)：5-8，76(in Chinese).

[5] Lei Hangtian，Singh C，Sprintson A．Reliability modeling and analysis of IEC 61850 based substation protection systems[J]．IEEE Transactions on Smart Grid，2014，5(5)：2194-2202.

[6] 陈为化，江全元，曹一家．考虑继电保护隐性故障的电力系统连锁故障风险评估[J]．电网技术，2006，30(13)：14-19．
Chen Weihua，Jiang Quanyuan，Cao Yijia．Risk assessment of power system cascading failure considering hidden failures of protective relaying[J]．Power System Technology，2006，30(13)：14-19(in Chinese)．

[7] Liu Nian，Zhang Jianhua，Wu Xu．Asset analysis of risk assessment for IEC 61850-based power control systems—Part I：methodology[J]．IEEE Transactions on Power Delivery，2011，26(2)：869-875．

[8] 李梅．电力信息网络的风险评估技术研究[D]．保定：华北电力大学，2007．

[9] Falahati B，Fu Yong，Wu Lei．Reliability assessment of smart grid considering direct cyber-power interdependencies[J]．IEEE Transactions on Smart Grid，2012，3(3)：1515-1524．

[10] 苏盛，吴长江，马钧，等．基于攻击方视角的电力 CPS 网络攻击模式分析[J]．电网技术，2014，38(11)：3115-3120．
Su Sheng，Wu Changjiang，Ma Jun，et al．Attacker's perspective based analysis on cyber attack mode to cyber-physical system[J]．Power System Technology，2014，38(11)：3115-3120(in Chinese)．

[11] Zhang Yichi，Wang Lingfeng，Xiang Yingmeng，et al．Power system reliability evaluation with SCADA cyber security considerations[J]．IEEE Transactions on Smart Grid，2015，6(4)：1707-1721．

[12] Bompard E，Gao Ciwei，Napoli R，et al．Risk assessment of malicious attacks against power systems[J]．IEEE Transactions on Systems，Man，and Cybernetics—Part A：Systems and Humans，2009，39(5)：1074-1085．

[13] 刘刚，梁野，李毅松，等．数字证书技术在电力二次系统中的实现及应用[J]．电网技术，2006，30(S1)：71-75．
Liu Gang，Liang Ye，Li Yisong，et al．Realization and application of certificate in secondary part power system[J]．Power System Technology，2006，30(S1)：71-75(in Chinese)．

[14] 周静，卢利锋，雷煜卿，等．量子密钥技术提升电力系统二次防护安全性研究[J]．电网技术，2014，38(6)：1518-1522．
Zhou Jing，Lu Lifeng，Lei Yuqing，et al．Research on improving security of protection for power system secondary system by quantum key technology[J]．Power System Technology，2014，38(6)：1518-1522(in Chinese)．

[15] 胡炎，谢小荣，辛耀中．电力信息系统现有安全设计方法分析比较[J]．电网技术，2006，30(4)：36-42．
Hu Yan，Xie Xiaorong，Xin Yaozhong．Analysis and comparison of existing security design methods for power information system[J]．Power System Technology，2006，30(4)：36-42(in Chinese)．

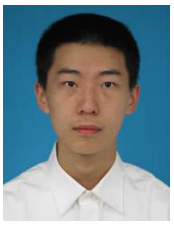
[16] 胡炎，谢小荣，辛耀中．一种定量化的电力信息系统安全体系设计方法[J]．电网技术，2006，30(2)：7-13．
Hu Yan，Xie Xiaorong，Xin Yaozhong．A quantitative security architecture design method for power information system[J]．Power System Technology，2006，30(2)：7-13(in Chinese)．

[17] Marsegerra M，Zio E，Librizzi M．Quantitative developments in the cognitive reliability and error analysis method(CREAM) for the assessment of human performance[J]．Annals of Nuclear Energy，2006，33(10)：894-910．

[18] Wang Ansi，Luo Yi，Tu Guangyu，et al．Quantitative evaluation of human-reliability based on fuzzy-clonal selection[J]．IEEE Transactions on Reliability，2001，60(3)：517-527．

[19] 俞斌．基于功能分解的电力二次系统风险评估方法研究[D]．杭州：浙江大学，2013．

[20] Billinton R，Allan R．Reliability Evaluation of Engineering Systems：Concepts and Techniques[M]．Second Edition．New York and London：Plenum Press，1992．


曹志昆

收稿日期：2015-08-01。

作者简介：

曹志昆(1990)，男，硕士研究生，主要研究方向为配电网状态估计、二次系统风险评估，E-mail：czk_dee@zju.edu.cn；

章杜锡(1983)，男，高级工程师，主要从事电网调度技术，E-mail：temple_zju@163.com；

董树锋(1982)，男，通信作者，讲师，主要研究方向为状态估计和有源配电网分析、风险评估，E-mail：dongshufeng@zju.edu.cn；

郭创新(1969)，男，教授，博士生导师，研究方向为智能电网和分布式能源并网、风险评估，E-mail：guochuangxin@zju.edu.cn。

（责任编辑　王晔）