

基于抽象故障树的化工事故预警^①

马超, 杜军威, 胡强

(青岛科技大学 信息科学技术学院, 青岛 266061)

通讯作者: 杜军威, E-mail: d-jw@163.com

摘要: 情景是分析事件的发生、发展及可能的后果的有效机制, 然而, 基于情景的预警机制或缺乏有效的模型支撑或受制于模型的局限性, 实践中难以推广. 抽象故障树是同类事故故障树的高层抽象, 综合历史案例与专家经验, 能够刻画事故的成因的机理、情景演化过程及可能的后果, 能够有效支撑基于情景的预警分析. 提出一种基于抽象故障树的化工事故预警方法, 基于抽象映射计算事件危害度及节点重要度, 将情景演化的割集模型转换为贝叶斯网络模型, 采用 Board 法对事故危害进行风险度量 and 防御事件排序, 实现基于情景的不同演化路径的事故风险预测及最佳应对策略推荐, 实验结果显示了该方法用于事故分析预警的有效性.

关键词: 故障树; Board 法; 贝叶斯网络; 事故预警

引用格式: 马超, 杜军威, 胡强. 基于抽象故障树的化工事故预警. 计算机系统应用, 2018, 27(9): 151-156. <http://www.c-s-a.org.cn/1003-3254/6516.html>

Chemical Accident Early Warning Analysis Based on Abstract Fault Tree

MA Chao, DU Jun-Wei, HU Qiang

(Information Science and Technology Academy, Qingdao University of Science and Technology, Qingdao 266061, China)

Abstract: Scenarios are effective mechanisms for analyzing the occurrence, development, and possible consequences of an accident. However, lack of effective model to model or limitation of models to analysis, scenario-based early warning mechanisms are difficult to popularize in practice. Abstract fault tree is a high-level abstraction of the same kind of fault tree. Based on historical cases and expert experiences, it can characterize the mechanism, evolution process, and possible consequences of the accident, and can effectively support scenario-based early warning analysis. A method of early warning of chemical accidents based on abstract fault tree is proposed. Based on the abstract map relation, hazard degree, and importance level of nodes are calculated. The scenario-evolved cutting set model is transformed into Bayesian network model. Board method is used to measure risk of accident hazard. The ranking of defense events can be used to predict the accident risk and propose the best coping strategies based on different evolution paths of scenarios. The experimental results show the effectiveness of this method in accident analysis and early warning.

Key words: fault tree; Board method; Bayesian network; early warning

化工生产具有高温、高压、高电流、工艺流程复杂、操作要求严格等特点, 存在燃烧、爆炸、中毒、腐蚀等危险因素, 任何环节中的“小事件”都可能因处置不当而导致重大安全事故^[1]. 实践中, 化工企业生产

① 基金项目: 国家自然科学基金(61273180); 山东省自然科学基金项目(ZR2012FL17); 山东省重点研发计划(2018GGX101052, 2016GGX101031); 山东省优秀中青年科学家科研奖励基金(BS2015DX010)

Foundation item: National Natural Science Foundation of China (61273180); Natural Science Foundation of Shandong Province (ZR2012FL17); Key Research and Development Plan of Shandong Province (2018GGX101052, 2016GGX101031); Outstanding Young and Middle-Aged Scientists Award Foundation of Shandong Province (BS2015DX010)

收稿时间: 2018-01-14; 修改时间: 2018-02-09; 采用时间: 2018-02-26; csa 在线出版时间: 2018-08-16

和管理人员却常忽视这样“琐碎”事件与情景,而这些事件往往是形成诱发事故的隐患,如何准确分析“小事件”成因、演化及可能危害,形成对事故前期征兆的准确监测、识别、预防与控制的预警机制,是降低事故发生概率、减少事故损失的重要安全举措^[2]。

目前事故预警机制多体现为一些行业的安全法规、安全规章制度,因缺乏面向事故过程演化的分析与预测机制,难以真正指导企业安全生产和事故预防。情景是综合历史案例和专家经验,分析事件的发生、发展及可能的后果的有效机制,基于情景的预警机制已成为公共安全领域重要安全举措^[3]。由于情景不是某个具体事件的投影,而是无数同类事件和预期风险的集合^[4]。如何建模历史事故案例及对大量的事故案例进行聚类 and 同化?是支持基于情景预警、应急决策的基础,也是指导企业建立面向事故预警机制的有效途径。基于故障树(Fault Tree, FT)的事故成因分析是安全分析领域常用方法^[5],近些年化工安全监管部门已建立了大量基于故障树的事事故成因模型,形成了该领域的事事故预警机制的知识库。而,基于单个案例的基本事件及其割集或径集进行事故预测或防护推荐^[6],不能直接应用到情景预测分析中;同时基于故障树的事事故预测,存在事件间的冗余、不独立、共因模式、互斥模式等复杂约束,直接利用故障树结构计算是NP问题^[7,8]。贝叶斯网络(Bayesian Networks, BN)可以方便计算P(事故|事件)和P(事件|事故)两类分析模式^[8,9],近些年广泛应用于多类事故模型的分析与预测中,转换为贝叶斯网络是复杂故障树模型分析的有效途径,文献[8-11]研究了静态故障树、动态故障树及存在约束的故障树可以转换为贝叶斯网络并得到与故障树等价的分析;将故障树转换为贝叶斯网络在实际中也得到大量的应用,如:Khakzad^[8]在安全分析中比较了故障树模型与贝叶斯网络模型, Mohammadfam 等人^[12]使用贝叶斯网络方法管理和改进员工的安全行为,杨昌昊等^[13]研究故障树转换为贝叶斯网络应用于故障诊断。这些研究都是基于单故障树的基本事件分析,难以直接适用基于历史案例事故情景的预警分析。

本文面向化工安全领域,基于事故调研形成的大量故障树模型,给出一种基于抽象故障树的事事故预警方法。在故障树基本事件割集的基础上,提出一种包含全部事件的割集的扩展方法,将扩展后的割集子树转换为贝叶斯网络模型,实现精确分析情景发生时的不

同演化路径的事事故概率和事事故危害度,确定情景的最佳防范策略,实现面向事事故演化过程的层进式预警策略,从而能按照不同优先级实现对事事故情景的快速响应,达到事事故预警的目的。

1 基于抽象故障树的事事故模型

故障树是演绎地表示事事故发生原因及其逻辑关系的逻辑树图,在化工事事故分析中,故障树的顶点表示为事事故,中间节点和叶子表示事事故发生的直接原因、间接原因或根原因。由于同类事事故在具体事事故案例中因果差异较大,为了能够实现事事故的综合因果分析,定义两类故障树:描述某个具体事事故发生的故障树定义为案例故障树,刻画某个具体事事故的演化过程;描述同类案例故障树的抽象综合定义为抽象故障树,刻画同类事事故的所有可能事件因果演化过程。案例故障树的节点表达为事事故演化过程的具体事件,抽象故障树节点表达为具体事件的抽象,如抽象故障树的抽象事件“易燃气体挥发”在案例故障树对应的节点可以是“甲基乙基酮挥发”、“丙烯酸甲酯挥发”等具体事件。

定义1.故障树结构定义为四元组 $FT = (V, G, E, v_0)$,其中,

- 1) V 代表故障树的节点集合;
- 2) G 为逻辑门集合, $\forall g \in G$, 定义逻辑门的类型 $Type(g) \in \{And, Or\}$;
- 3) E 为抽象故障树的边集合, $E \subseteq V \times G \cup G \times V$;
- 4) v_0 代表根节点, $V_L = \{v \in V \wedge \nexists g \in G, (v, g) \in E\}$ 为叶子节点, $V_M = \{v | v \in V \wedge (\exists g \in G, (v, g) \in E)\}$ 为中间节点。

考虑到化工事事故的事件演化关系多为“And”、“Or”关系,且非时序关系可以通过“And”、“Or”树结构变化可以等价转换,本文的故障树结构仅考虑“And”和“Or”关系。将节点的定义域来自抽象事件的一类故障树称为抽象故障树;节点的定义域来自具体事件的一类故障树称为案例故障树。

由于抽象故障树是同类案例故障树的抽象综合,案例故障树可以映射为该类型抽象故障树的局部结构,映射关系可以确定抽象故障树事件节点在具体事事故案例中发生的频次,从而形成了抽象故障树的不同节点对顶节点的影响概率差异,依据映射具体案例发生的频次定义抽象故障树节点的发生概率。发生概率值大小依赖于映射案例数的多少,映射越多发生概率越大,

反之越小;同时由于故障树结构层次的差异,故障树中不同节点的发生对顶事件的贡献度不一,由此根据故障树的层次结构定义不同节点在故障树的重要度,重要度的值大小依赖于树结构,离根节点越近值越大,反之值越小。

2 基于抽象故障树的预警分析

抽象故障树为同类事故高度综合和抽象的一类故障树,包含了各类事故案例的事故原因的演化路径,基于抽象故障树可以刻画事故不同层面情景演化,基于故障树模型的情景表现为故障树的不同层次事件的组合,可以通过分析抽象故障树,预测情景的不同演化路径的风险,实现面向抽象故障树事件分析与预警。主要技术体系包含情景演化计算和情景演化风险评价两部分:第一部分借助于贝叶斯网络模型进行运算,第二部分借助于 Borda 序值法进行风险度量^[14]。

2.1 故障树割集的贝叶斯网络转换

由于情景表现为故障树结构的节点组合,传统的基于基本事件的故障树分析方法难以直接应用到情景预测与分析。通过将抽象故障树转化为贝叶斯网络结构,根据抽象故障树的逻辑组合关系确定贝叶斯网络的结构,形成贝叶斯网络结构,根据割集事件在贝叶斯网络中信念的传递更新,求解割集所对应的子网,进而根据子网的结构求解顶事件发生的概率。从割集中的基本事件对应的节点开始,沿着构造的贝叶斯网络进行信念传递,直到顶事件对应的节点为止,信念传递的路径组合得到割集事件演化所对应的网络拓扑结构,进而通过节点之间的传递关系推算割集演化得到的事故概率。逻辑门描述的就是父子事件之间的概率关系,它与贝叶斯网络中联接强度的概念是相对应的。具体定义如定义 2。

定义 2. 故障树 And 门转换语义: V_M 为输出, V_{B1} 、 V_{B2} 是与门 $\text{And}(V_{B1}, V_{B2})$ 输入, 则 And 门对应的贝叶斯网 V_M 的概率分布为: $P(V_M = 1 | V_{B1} = 1, V_{B2} = 1) = 1$, $P(V_M = 1 | \text{else}) = 0$ 。

定义 3. 故障树 Or 门转换语义: V_M 为输出, V_{B1} 、 V_{B2} 是或门 $\text{Or}(V_{B1}, V_{B2})$ 输入, 则 Or 门对应的贝叶斯网 V_M 的概率分布为: $P(V_M = 1 | V_{B1} = 0, V_{B2} = 0) = 0$, $P(V_M = 1 | \text{else}) = 1$ 。

定义 4. 信念: $Bel(x) = P(x|ev)$, 即在有已知证据 ev 的情况下, 事件 x 发生的条件概率, 反映在一定环境

下某一事件发生的可能性。

ev 包含以 x 为故障树中根节点的子树 e_{xt} 和故障树中其他关联部分 e_{xo} , 那么信念:

$$Bel(x) = P(x|ev) = \frac{P(x|e_{xt}, e_{xo})}{P(e_{xt}|e_{xo})} = \frac{P(e_{xt}|x)P(x|e_{xo})}{P(e_{xt}|e_{xo})} \quad (1)$$

令 $\alpha = 1/P(e_{xt}|e_{xo})$, $\lambda(x) = P(e_{xt}|x)$, $\pi(x) = P(x|e_{xo})$, 此时,

$$Bel(x) = \alpha\lambda(x)\pi(x) \quad (2)$$

其中 $\lambda(x)$ 为诊断支持, $\pi(x)$ 为预测支持。

根据网络信念传播与更新的原理式 (2), 可计算出顶事件 T 的信念值, 也就是顶事件的发生概率。

具体计算步骤:

Step1. 依据故障树不同逻辑门的语义, 将抽象故障树转换为贝叶斯网络模型。

Step2. 依据情景, 计算情景关联的事件集合。

Step3. 依据割集事件在贝叶斯网络中信念传递更新, 求解基于割集扩展的贝叶斯子网。

Step4. 由割集扩展得到的子网的底事件开始, 逐层进行概率运算。

Step5. 判断当前节点是否包含顶节点, 不包含执行 Step6, 否则执行 Step9。

Step6. 依据事件间的连接门, 计算关联节点间的连接概率 P , 并计算当前事件对预测的支持 π 。

Step7. 由于故障树中底事件节点的概率是由历史事故统计而来, 式中 $\lambda(x)$ 为 (1, 1), 归一化因子 α 近似为 (1, 1), 信念公式可简化为: $Bel(x) = \pi(x)$ 。

Step8. 根据信念公式计算出上层事件 V_M 的信念值, 执行 Step5。

Step9. 得到当前割集发生的概率。

2.2 基于 Borda 序值法进行事故的预警推荐

Borda 序值法是一种经典的投票表决法, 依据投票人通过投票表达出对各候选人的偏好次序, 然后对候选人从高到低进行评分并累加, 得分最高者最终获胜。依据 2.1 提供算法可以计算不同演化路径的事件发生概率及事件重要度概率, 是一个典型的两目标优化问题。因此, 我们使用 Borda 序值法对事故以及其包含的节点事件进行重要度排序, 计算每种演化路径的不同风险值。

设 N 为风险包含因素数, 设 i 为某一特定风险,

k 表示某一准则原始风险矩阵只有两个准则. 用 $k=1$ 表示风险影响 I , $k=2$ 表示风险概率 P . 如果 r_{ik} 表示风险 i 在准则 k 下的风险等级, 则风险 i 的 Borda 数可由下式给出: $b_i = \sum (N - r_{ik})$, 某一因素的 Borda 序值即为比这个风险因素的 Borda 数大的风险因素的个数^[14].

通过对事故定性分析和定量分析综合考虑, 采用 Borda 法综合考虑情景发生时的事故概率和事故影响两方面的因素, 对事故进行评估的方法.

算法的具体步骤如下:

Step1. 由事故损失和事故概率确定事故等级分布.

Step2. 由求得割集的概率和对应的历史事故损失确定割集的初步风险等级.

Step3. 由割集的概率和对应的历史事故损失, 根据 border 法求得每个割集对应的 border 数值.

Step4. 根据 border 数值, 计算割集对应的 border 序值.

Step5. 根据 border 序值对割集的重要度进行排序.

Step6. 得到割集对应事故的重要度排序, 即事故重要度排序.

Step7. 根据事故重要度排序, 进行事故预警推荐.

为了合理的求得节点的重要度, 我们使用 borda 法权衡节点概率和危害度. 具体步骤与割集重要度计算方法一致.

3 案例分析

为了充分论证方法的有效性, 本文结合石化安监部门整理的泄露着火爆炸型抽象故障树进行实例分析, 其结构如图 1 所示.

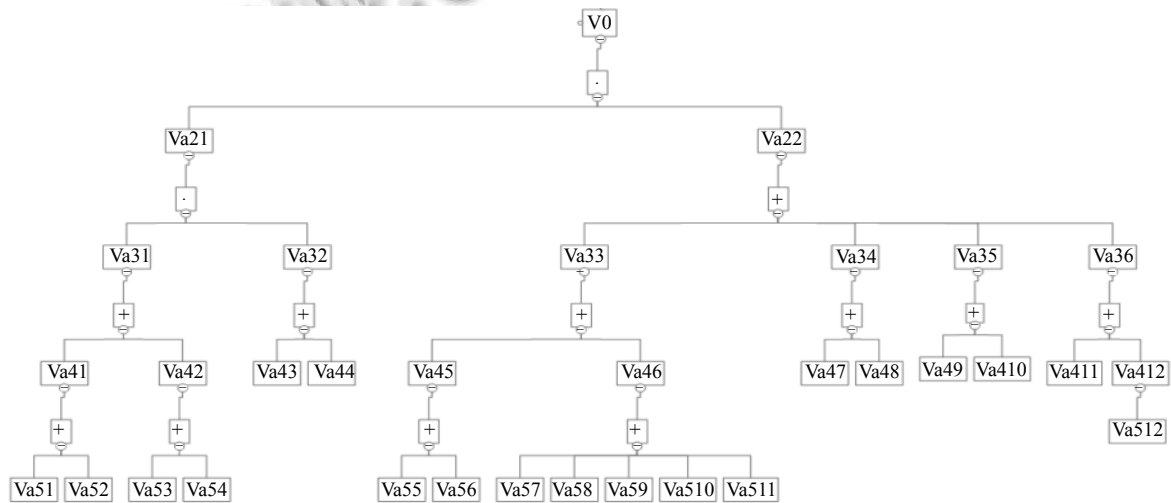


图 1 泄露着火爆炸型抽象故障树

图 1 泄露着火爆炸型抽象故障树中每一个字符节点表示一个事件, 各节点的的具体含义表示如表 1 所示.

根据前面介绍的故障树叶子节点的概率统计与赋值规则, 得到泄漏型着火爆炸抽象故障树的各个叶子节点的发生概率如表 2 所示.

假设以 Va57 油品喷溅引起的静电火花发生为情景, 通过割集概率求解算法, 结合 border 法求解得到包含该情景的各割集重要度排序如表 3 所示.

该类事故属于泄露着火爆炸型事故, 事故原因一般为混合气体遇点火源引发的着火爆炸, 包含事件如表 1 所示. 由油品喷溅引起的静电火花事件, 定位到泄

露着火爆炸型抽象故障树. 通过对抽象故障树求全割集, 我们可以找到包含哨兵事件相关事故割集如表 3 所示, 基于上诉算法, 可以对割集的重要度进行排序. 如表 3 所示, 其中重要度最高的事故割集为 ecs1, 由此我们可以确定事故发生最有可能的一种形式, Va51 物料输送速度过快引起挥发加剧和 Va43 容器内可能存在的空气, 混合形成爆炸性混合气体, 遇 Va57 油品喷溅引发的静电火花最终导致着火爆炸事故. 通过上述算法可以对节点的重要度进行计算, 由于 Va57 已经显现, 当我们针对 Va57 进行处理的同时, 应该着重防止 Va43 的发生, 所以此时有关人员, 应当立马检查当前设备有没有漏气现象的发生, 并采取相应的处理. 若

没有,则依据重要度排序,逐一关联事件进行排查。

4 结论

本文提出基于抽象故障树的化工事故预警分析方法,可以实现面向事故演化过程的预警,相对于固定模

式的企业安全规章制度,该方法可以有效借鉴历史经验提供更加有针对性的预警措施,并随着事故案例的丰富而愈加更加精确。从而使企业安全生产人员能够快速、准确的进行相应的应急处理,为事故预防、应急和救援处置节省宝贵的时间。

表1 基本事件的符号和名称

代号	名称	代号	名称
V0	容器内爆炸性混合气体遇点火源引发的爆炸	Va49	冲击和摩擦
Va21	容器内形成爆炸性混合气体空间	Va410	绝热压缩
Va22	点火源	Va411	明火
Va31	容器内可燃物料挥发性组分积聚	Va412	自燃放热
Va32	容器内存在空气	Va51	物料输送速度过快引起挥发加剧
Va33	电点火源	Va5	输送油料温度过高引起挥发加剧
Va34	高温点火源	Va53	阀门渗漏
Va35	冲击点火源	Va54	误操作阀门
Va36	化学点火源	Va55	电气设备产生火花
Va41	容器内可燃物料轻质组分急剧挥发	Va56	雷击火花
Va42	容器外部可燃物料进入容器内并挥发	Va57	油品喷溅引起的静电火花
Va43	容器内部存在空气	Va58	油、水、气混输引起的静电火花
Va44	外界空气进入容器内	Va59	用铁管测试罐内液位引起的静电火花
Va45	电火花	Va510	输油流速过快引起的静电火花
Va46	静电火花	Va511	带电鹤管插入油面引起的静电火花
Va47	高温表面	Va512	油罐内硫化物自燃
Va48	热辐射		

表2 基本事件的概率分布

节点	Va43	Va44	Va47	Va48	Va49	Va410	Va411	Va51	Va52	Va53
概率	(0.8, 0.2)	(0.9, 0.1)	(0.6, 0.4)	(0.5, 0.5)	(0.4, 0.6)	(0.9, 0.1)	(0.8, 0.2)	(0.2, 0.8)	(0.2, 0.8)	(0.6, 0.4)
节点	Va54	Va56	Va57	Va58	Va59	Va510	Va511	Va512	Va61	
概率	(0.3, 0.7)	(0.2, 0.8)	(0.6, 0.4)	(0.7, 0.3)	(0.5, 0.5)	(0.2, 0.8)	(0.3, 0.7)	(0.7, 0.3)	(0.4, 0.6)	

表3 割集对应的各种信息

割集	包含节点	重要度	概率(%)	风险等级	Borda 数值	Borda 序值
ecs1	Va51, Va43, Va57	110	33.6	高	15	0
ecs2	Va51, Va44, Va57	96	37.8	高	14	1
ecs3	Va52, Va43, Va57	42	9.6	低	4	6
ecs4	Va52, Va44, Va57	65	10.8	中	6	5
ecs5	Va53, Va43, Va57	88	28.8	中	10	3
ecs6	Va53, Va44, Va57	25	32.4	低	7	4
ecs7	Va54, Va43, Va57	39	14.4	低	4	6
ecs8	Va54, Va44, Va57	101	16.2	高	11	2

参考文献

- Combes R, Barratt M, Balls M. An overall strategy for the testing of chemicals for human hazard and risk assessment under the EU REACH system. *Alternatives to Laboratory Animals*, 2003, 31(1): 7-19.
- Wood MH, Fabbri L, Struckl M. Writing seveso II safety reports: New EU guidance reflecting 5 years' experience with the directive. *Journal of Hazardous Materials*, 2008, 157(2-3): 230-236. [doi: 10.1016/j.jhazmat.2007.12.089]
- Ahmed DM, Sundaram D, Piramuthu S. Knowledge-based scenario management —process and support. *Decision Support Systems*, 2010, 49(4): 507-520. [doi: 10.1016/j.dss.2010.06.004]
- 盛勇, 孙庆云, 王永明. 突发事件情景演化及关键要素提取

- 方法. 中国安全生产科学技术, 2015, 11(1): 17–21.
- 5 马志刚, 靳明程, 陈衍涛, 等. HAZOP 研究与故障树分析在合成氨装置危险辨识中的应用. 中国安全生产科学技术, 2012, 8(10): 85–90.
- 6 Ruijters E, Stoelinga M. Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools. *Computer Science Review*, 2015, (15–16): 29–62. [doi: [10.1016/j.cosrev.2015.03.001](https://doi.org/10.1016/j.cosrev.2015.03.001)]
- 7 Bobbio A, Portinale L, Minichino M, *et al.* Improving the analysis of dependable systems by mapping fault trees into Bayesian networks. *Reliability Engineering & System Safety*, 2001, 71(3): 249–260.
- 8 Khakzad N, Khan F, Amyotte P. Safety analysis in process facilities: Comparison of fault tree and Bayesian network approaches. *Reliability Engineering & System Safety*, 2011, 96(8): 925–932.
- 9 林青, 戴慧珺, 任德旺. 基于贝叶斯网络的不确定因果逻辑量化分析方法. 计算机系统应用, 2016, 25(9): 27–34. [doi: [10.15888/j.cnki.csa.005329](https://doi.org/10.15888/j.cnki.csa.005329)]
- 10 Wu XG, Liu HT, Zhang LM, *et al.* A dynamic Bayesian network based approach to safety decision support in tunnel construction. *Reliability Engineering & System Safety*, 2015, 134: 157–168.
- 11 王广彦, 马志军, 胡起伟. 基于贝叶斯网络的故障树分析. 系统工程理论与实践, 2004, (6): 78–83. [doi: [10.3321/j.issn:1000-6788.2004.06.014](https://doi.org/10.3321/j.issn:1000-6788.2004.06.014)]
- 12 Mohammadfam I, Ghasemi F, Kalatpour O, *et al.* Constructing a Bayesian network model for improving safety behavior of employees at workplaces. *Applied Ergonomics*, 2017, 58: 35–47. [doi: [10.1016/j.apergo.2016.05.006](https://doi.org/10.1016/j.apergo.2016.05.006)]
- 13 杨昌昊, 胡小建, 竺长安. 从故障树到故障贝叶斯网映射的故障诊断方法. 仪器仪表学报, 2009, 30(7): 1481–1486. [doi: [10.3321/j.issn:0254-3087.2009.07.027](https://doi.org/10.3321/j.issn:0254-3087.2009.07.027)]
- 14 Rao SK, Kopparty BR. A note on borda method. *Economics Bulletin*, 2015, 35(3): 1969–1975.