引用格式:马赞,王鹏,赵长啸,等. 隐蔽故障计算模型审定要求分析[J]. 电光与控制,2019,26(7):51-55. MA Z, WANG P, ZHAO C X, et al. Airworthiness certification requirement analysis for hidden failure calculation models[J]. Electronics Optics & Control, 2019, 26(7):51-55.

隐蔽故障计算模型审定要求分析

马 赞[1,2], 王 鹏[1], 赵长啸[1], 胡剑波[2]
(1. 中国民航大学民航航空器适航审定技术重点实验室,天津 300300;
2. 空军工程大学装备管理与无人机工程学院,西安 710051)

摘 要: 隐蔽故障概率计算对初始适航系统安全性评估结果会产生重大影响,其计算模型具有复杂多样的特性,如何对这些模型的安全性进行审查,成为型号研制和适航审定中的一个关键问题。分析隐蔽故障计算的影响因素,提出计算模型的审定要素和要点,并结合当前普遍应用的工程方法以及计算模型进行评估,发现安全性问题,可有效促进型号安全性水平。

关键词: 适航审定; 隐蔽故障; 计算模型; 安全性评估
中图分类号: V37 **文献标志码**: A **doi**:10.3969/j.issn.1671-637X.2019.07.010

Airworthiness Certification Requirement Analysis for Hidden Failure Calculation Models

MA Zan[1,2], WANG Peng[1], ZHAO Chang-xiao[1], HU Jian-bo[2]
(1. Civil Aircraft Airworthiness Certification Technology Key Laboratory of Tianjin, Civil Aviation University of China, Tianjin 300300, China; 2. Equipment Management and UAV Engineering College, Air Force Engineering University, Xi'an 710051, China)

Abstract: The probability calculation of hidden failures has a significant impact on the safety assessment results of the initial airworthiness system. Its computational model has complex and diverse characteristics. How to review the security of these models has become a key issue in model development and airworthiness certification. This paper analyzes the factors influencing hidden failure calculation, proposes the certification elements and key points of the calculation model, and uses the currently widely-used engineering methods and calculation models as an example to evaluate and find safety issues, which can effectively promote the safety level of the aircraft.

Key words: airworthiness certification; hidden failure; calculation model; sefety evaluation

0 引言

隐蔽故障是指已经发生但对飞机没有可察觉的影响,并且不可被监控措施监测到的故障,其只能通过维修任务进行检查和修理。隐蔽故障总是有一个相应的检查时间,其本身并不会导致危害,但会使保护机制功能丧失或降低安全裕度,从而增加后续失效条件引起危害的风险。CCAR25.1309条款[1]中明确要求在进行初始适航系统安全性评估时需要重点考虑隐蔽故障的危害性影响。

涉及隐蔽故障的计算较为复杂,目前市面上的商用分析软件要么没有隐蔽故障计算功能,要么处理模型过于保守,增加了无法符合适航要求的风险,也加大了系统设计难度。空客、波音等国际主流主机厂及系统集成商自主建立了精确的隐蔽故障计算方法及模型,但对我国实行严格技术封锁,并且各公司所采用模型的保守程度及计算方法不尽相同,局方如何判定其合理性及保守性成为当前型号审查中面临的关键问题之一。

国内外对民机隐蔽故障也有一些研究,但主要是从运行可靠性的角度对风险进行评估或检查间隔的确定。如戴顺安等[2]结合ARP5150的风险评估理念,利用实际运行维修数据确定故障规律,建立定量风险评估方法;贾宝惠等[3]综合考虑隐蔽功能系统的维修策略、可靠度函数和维修成本,提出一种平均不可靠度和成本率函数优化检查及恢复间隔的模型;LIENHARDT

收稿日期:2018-07-24 修回日期:2018-09-06
基金项目:国家自然科学基金委员会-中国民航局民航联合研究基金(U1533105)
作者简介:马 赞(1984—),男,天津人,硕士,助理研究员,研究方向为适航审定、系统安全性评估等。

等[4]提出以更新维修风险为约束,节约成本为目标的隐蔽故障维修解决方法;刁海飞等[5]基于MSG-3分析原理,从使用性和经济性出发,建立了隐蔽故障检测间隔确定模型。但目前尚未有相关研究从初始适航安全性角度梳理隐蔽故障模型的审定方法。

本文针对隐蔽故障计算模型审定要求进行分析,梳理审定要素及要点。依据相关要点对某型号故障计算模型进行审查,发现了安全性问题,可有效促进型号安全性水平。

1 系统安全性评估计算过程

CCAR25.1309条款对系统安全性提出了要求,并建议按照SAE ARP4761[6]的方法开展系统安全性评估相关工作,而故障树(FTA)建立及定量计算是其中的主要组成部分。

故障树定量分析一般包括如下步骤:1)获取输入信息;2)确定故障树最小割集;3)确定底事件的失效率;4)确定底事件的风险事件和暴露时间;5)执行FTA数值计算;6)输出分析结果。

故障树定量分析必须基于最小割集,最小割集是底事件的组合,因此进行故障树定量分析必须要确定故障树底事件的数据模型。而故障树底事件中通常会不可避免地包含隐蔽故障,为支持故障树定量计算,表明对CCAR25.1309条款的符合性,需要准确地识别隐蔽故障,确定其风险暴露时间,形成隐蔽故障及其相关故障组合情况的概率计算模型,严格控制隐蔽故障维修内容及活动。

2 审定关注要素及重点

如图1所示,多重隐蔽故障计算依托计算理论基础和工程应用条件两方面实现。其中:在计算理论基础工作中,基于一定的数学理论和假设,形成合理的或保守的故障计算模型,并且衍生与之对应的应用条件要求;而在工程应用条件中,则需要针对故障组合的分析对象,提出独立性假设,识别隐蔽故障,确定失效率、暴露时间、故障顺序、响应阶段等故障参数,作为计算模型的准确输入,从而形成计算结果。

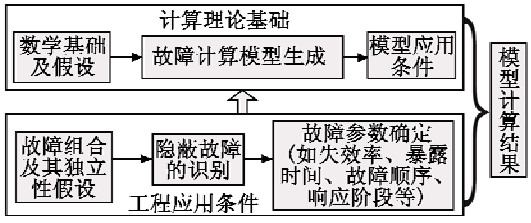

图1 隐蔽故障计算过程

Fig. 1 Calculation process of the hidden failures

基于以上计算过程和步骤,结合当前普遍采用的数学模型基础,分析隐蔽故障计算审定要素,清单见表1。

表1 多重隐蔽故障审定要素清单

Table 1 List of certification elements on multiple hidden failures

故障计算过程		审定要点
计算理论基础	数学基础及假设	1)失效概率分布函数适用性及保守性审查 2)故障简化计算保守性审查
	模型生成及应用	模型原理合理性及保守性审查
工程应用条件	故障组合及独立性假设	故障间独立性假设确认审查
	隐蔽故障识别	隐蔽故障识别准确性及完整性审查
	故障参数确定	1)风险暴露时间保守性审查 2)失效状态响应阶段保守性审查 3)失效顺序正确性审查 4)失效率追溯性及正确性审查

2.1 失效概率分布函数适用性及保守性审查

飞机上的不同系统或部件根据其特性不同,其寿命服从连续型随机变量的概率分布,常用的有指数分布、正态分布、威布尔分布等。对于不同的机载系统及设备,其寿命服从的分布如表2所示。

表2 不同机载系统失效概率分布推荐

Table 2 Recommendation on failure probability distributions of the different airborne systems

系统	指数分布	威布尔分布	正态分布
空气管理系统	选用(部分电子部件)	推荐	-
液压能源系统	选用(液压控制逻辑盒)	推荐	-
气源系统	选用	推荐	选用
电子飞行仪表系统	推荐	选用	-
飞机动力装置系统	选用(电子控制器)	适用	-
APU系统	选用	适用	-
电源系统	推荐	选用	-
布线系统	选用	推荐	-
起落架控制系统	选用	适用	选用
水/废水系统	-	适用	选用(部分机械产品)

注:“推荐”、“适用”、“选用”3种表述的分布适用性依次降低。“选用”项括号中给出了其适用的部件举例。

但在实际的民机系统安全性定量评估中,出于计算便利性等方面考虑,各种结构或部件并非按照推荐分布进行可靠性计算,而是采用指数分布替代其他分布类型,对所有系统或部件给出可靠性指标。对于这种工程近似方法产生的误差进行仿真分析,设形状参数 $m=2$,尺度参数 $t_0=6000$。仿真结果如图2和图3所示。

通过仿真可知,对于属于后3种寿命分布类型的设备,在其平均故障间隔时间(MTBF)内,以指数分布近似计算其失效概率,虽然结果与真实值存在一定的误差,

但结果是保守的，存在的前提假设是维修检查后的设备与新设备完全相同，该假设可通过设备维修手册或设备维修大纲中规定进行“大修”得以确认。

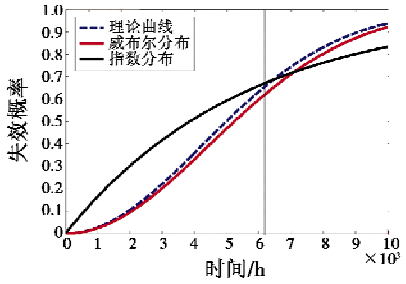

图 2　指数分布与威布尔分布失效概率曲线

Fig. 2　Failure probability curve of exponential distribution and Weibull distribution

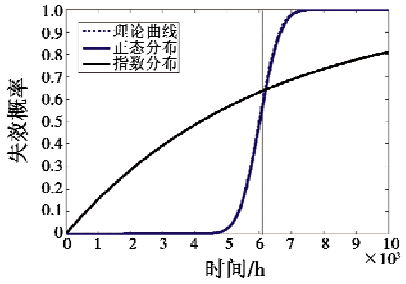

图 3　指数分布与正态分布失效概率曲线

Fig. 3　Failure probability curve of exponential distribution and normal distribution

2.2　故障简化计算保守性审查

为降低工程应用中的计算难度，常将指数分布故障计算简化为 $P=\lambda t$（λ 为失效率，t 为风险时间或暴露时间），并确保其保守性，应满足以下条件。

1）确保装机的设备或零部件已经过初期的筛选磨合，并规划了预防性维修措施，使得可以正常使用中的产品失效率近似为常数。对于早期设备零部件的筛选，可通过加速寿命实验，对实验数据拟合威布尔分布，根据其形状参数 m 进行判断，$m<1$ 处于早期失效阶段，$m=1$ 处于偶然失效阶段。

2）确保 $\lambda t<0.1$。用 λt 近似代替 $F(t)=1-e^{-\lambda t}$ 的过程由泰勒级数展开实现，即

$$F(t)=1-e^{-\lambda t}=1-\left(1-\lambda t+\frac{\lambda^2 t^2}{2}+\min(\lambda^2 t^2)\right)=\lambda t-\frac{\lambda^2 t^2}{2}+\min(\lambda^2 t^2)\ 。\tag{1}$$

以式(1)中 λt 近似表示累计失效概率 $F(t)$，即

$$F(t)\approx\lambda t\ 。\tag{2}$$

对于上式近似计算，所产生的相对误差为

$$\left|\frac{F(t)-\lambda t}{F(t)}\right|=\frac{0.5\lambda^2 t^2-\min(\lambda^2 t^2)}{\lambda t-0.5\lambda^2 t^2+\min(\lambda^2 t^2)}\approx\frac{\lambda t}{2}\ 。\tag{3}$$

从图 4 结果看，λt 约为 0.1 时相对误差是5.08%，这是可以接受的；否则，不能进行简化。

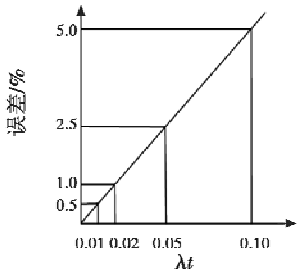

图 4　用 λt 近似代替 $F(t)$ 的相对误差

Fig. 4　The relative error of $F(t)$ approximately replaced by λt

2.3　模型原理合理性及保守性审查

对民机隐蔽故障的计算模型应在完整列举可能的失效组合场景基础上，对各场景的失效概率进行计算，并最终形成平均失效概率模型。例如，对于图 5 所示的隐蔽故障的计算，假设事件 1 存在隐蔽故障，并假设其对应的维修时间间隔为 T_1，设 $T_1=nT_0$，则事件 1 的暴露时间为 T_1，事件 2 处于风险的时间为 T_0。

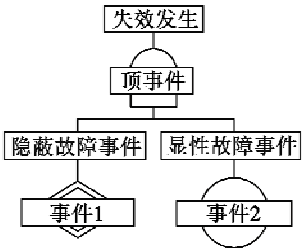

图 5　隐蔽故障计算故障树结构

Fig. 5　Fault tree structure of the hidden-failure calculation

表 3　隐蔽故障计算分析

Table 3　Calculation and analysis of the hidden failures

情况	当前飞行	显性故障发生在当前飞行中，第一次飞行发生隐蔽故障	显性故障发生在当前飞行中，第二次飞行发生隐蔽故障	显性故障发生在当前飞行中，第 i 次飞行发生隐蔽故障	显性故障发生在当前飞行中，第 $n-1$ 次飞行发生隐蔽故障	显性故障发生在当前飞行中，最后一次飞行发生隐蔽故障	该情况下的总概率
1	潜伏期内首次飞行	$\lambda_1T_0\lambda_2T_0$	–	–	–	–	$\lambda_1T_0\lambda_2T_0$
2	潜伏期内第二次飞行	$\lambda_1T_0\lambda_2T_0$	$\lambda_1T_0\lambda_2T_0$	–	–	–	$2\lambda_1\lambda_2T_0^2$
i	潜伏期内第 i 次飞行	$\lambda_1T_0\lambda_2T_0$	$\lambda_1T_0\lambda_2T_0$	$\lambda_1T_0\lambda_2T_0$	–	–	$i\lambda_1\lambda_2T_0^2$
$n-1$	潜伏期内第 $n-1$ 次飞行	$\lambda_1T_0\lambda_2T_0$	$\lambda_1T_0\lambda_2T_0$	$\lambda_1T_0\lambda_2T_0$	$\lambda_1T_0\lambda_2T_0$	–	$(n-1)\lambda_1\lambda_2T_0^2$
n	潜伏期内第 n 次飞行	$\lambda_1T_0\lambda_2T_0$	$\lambda_1T_0\lambda_2T_0$	$\lambda_1T_0\lambda_2T_0$	$\lambda_1T_0\lambda_2T_0$	$\lambda_1T_0\lambda_2T_0$	$n\lambda_1\lambda_2T_0^2$

对该结构的场景分析及概率计算见表3,并可得出平均每次飞行的失效概率为

$$p_f = \frac{1}{n}\sum_{i=1}^{n} i\lambda_1\lambda_2 T_0^2 = \frac{n+1}{2}\lambda_1\lambda_2 T_0^2 = \frac{1}{2}\lambda_1\lambda_2 T_0(T_1 + T_0) \quad 。 \tag{4}$$

另外,理论推导的数学模型都会有一些约束条件或应用假设,应检查所采用计算模型的约束条件或应用假设已得到符合,才可以使用相应的模型进行计算。

2.4 故障间独立性假设确认审查

故障树最小割集的故障概率计算前提条件是各故障相互独立。对于该独立性的假设,需通过 ARP4761 中共因分析的方法进行确认,包括共模分析、区域安全性分析和特定风险分析。

2.5 隐蔽故障识别准确性及完整性审查

当没有正确识别隐蔽故障时,其暴露时间将被错误地设置为平均飞行时间 T_0,而实际上隐蔽故障的暴露时间通常会远大于 T_0,这就错误地导致该隐蔽故障的发生概率变小,对安全性需求符合的判断产生不利影响。因此,对隐蔽故障识别准确性和完整性的审查对结果判断产生关键影响。目前,对隐蔽故障的识别可通过定义来判断。但是,以信息技术和信息集成为主要特征的现代高科技快速发展,带来了事故特征、模式的深刻变革,出现了许多新的隐蔽故障,如系统交联不良、系统组件之间非预期相互作用、系统能力不及等。这些通过传统的定义和经验无法进行有效识别,需要采用一种系统性的思维来解决,如 STAMP/STPA[7]。

2.6 风险暴露时间保守性审查

风险时间/暴露时间是故障概率计算的重要数据输入,只有准确确定了各故障树底事件的风险时间或暴露时间,才可能获得有效的故障概率计算结果。不同类型基本事件具有不同的风险时间或暴露时间。

对于在整个飞行过程中被使用的某个组件显性功能丧失或故障,其风险时间等于平均飞行时间。

仅在特定飞行阶段才使用组件显性功能丧失或故障,存在两种情况:1) 处于风险时间等于从飞行开始到所考虑的阶段结束时所耗用时间,例如“起落架放下”,并且可通过地面检查判定用于放下起落架的设备组件正常工作,对于起落架放下所需的设备风险时间是从地面检查到飞行中“起落架放下”结束的时间;2) 已知在使用某组件之前该组件正好在工作,并且仅在特定的飞行阶段才使用,则风险时间等于从功能检查到所考虑的飞行阶段结束时所耗用时间,例如“自动着陆”,并且通过模式运行前的初始化检查可知相关组件工作正常,这种情况下,风险时间是从初始化检查到飞机接地时为止的时间段。

隐蔽故障的暴露时间一般为它所对应的检查间隔时间。需要确认隐蔽故障的暴露时间间隔,对于 I,II 类失效状态中的隐蔽故障,需要检查该间隔是否在 CCMR 及维修大纲中进行了记录。在 PSSA 的计算过程中,可通过分配的安全性目标计算各隐蔽故障最大风险暴露时间,所采用的风险暴露时间应不大于该值。

2.7 失效状态响应阶段保守性审查

响应阶段是指飞行过程中的特定阶段,该阶段由于失效状态发生而导致不期望的影响发生,其不同于整个飞行期间。在一次飞行过程中,可能有多个响应阶段,例如“起落架放下”,其响应阶段为“起落架开始放下”到“起落架放下完成”,“自动着陆”功能的响应阶段为“启动自动着陆功能”到“完成自动着陆”,该值对每飞行小时的概率计算产生较大影响。

例如,当事件在整个飞行期间都可能发生时,FAR/CS 中的安全目标是以该次飞行中任一小时的概率表述的,即 HAZ→安全目标是 10^{-7} 每飞行小时。其中,10^{-7} 是该次飞行中一小时时段内最大能接受的故障组合的发生概率,所以在一次飞行中会发生危险的几率是 $10^{-7}T_0$。

当事件仅在飞行中的一个特定响应阶段(约 6 min)才可能发生时,安全目标可以用该次飞行的特定阶段的概率表述,即 HAZ→该飞行特定阶段内安全目标是 10^{-8}。其中,10^{-8} 是该次飞行特定阶段内最大能接受的故障组合的发生概率,所以在一次飞行中会发生危险的几率是 10^{-8}。

需要确认失效状态的响应阶段。通常对于安全性影响较小的失效状态,即使有特定的响应阶段存在,出于对计算简化的考虑,也可保守地认为其响应阶段为整个飞行阶段。飞行时间增加,计算所得失效状态发生概率保守。

2.8 失效顺序正确性审查

多重故障组合的概率计算结果除与各底事件参数相关外,还可能取决于其故障的具体顺序。这些事件则定义为故障顺序相关事件(也称为顺序事件)。在分析过程中,所要求故障顺序约束不同,产生的概率计算结果差异较大。例如一个由 3 个元件故障导致顶事件的故障组合情况,当考虑故障顺序时,则应增加故障顺序因子参与计算,如图 6 所示。例如要求 1 号元件故障首先发生,然后 2 号元件故障,最后发生 3 号元件故障,则故障顺序因子 $P_{seq} = k/n! = 1/3! = 1/6$,而 $P_{top} = (P_{f1} \cdot P_{f2} \cdot P_{f3})/6$。

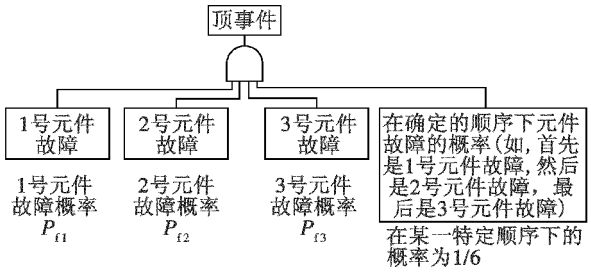

图 6　考虑失效顺序的故障树建立

Fig. 6　Fault tree in consideration of the failure sequence

2.9　失效率追溯性及正确性审查

与风险时间/暴露时间相同,底事件失效率也是故障概率计算的重要数据输入。只有准确确定了各故障树底事件失效率,再结合准确的风险时间或暴露时间,才可能获得有效的故障概率计算结果。因此,审查员应该对失效率的来源及准确性进行严格的判定。

凡有可能,应根据已在外场使用的类似设备失效率来检查所采用的失效率。工业其他相关失效率和/或模式分布的广泛来源包括 MIL-HDBK-217,MIL-HDBK-338,MIL-HDBK-978,Rome 实验室“可靠性工程师工具包”,可靠性分析中心(RAC)的非电子零件可靠性数据(NPRD)。尽管这些文件为某些部件类型的失效率预计提供基础,但仍有许多装置类型未包括在文件中,这一点对于复杂数字集成电路尤其突出,需要以逐个零件为基础加以考虑。

此外,获取部件安全性/可靠性基础数据的同时,应明确其对应的置信度。航空领域通常要求可靠性置信度应在 95% 以上,并保持所有数据置信度一致。

3　应用分析

根据以上审定要求分析,对某民机型号中隐蔽故障计算工作进行检查,主要存在问题及原因如下。

1) 计算模型不合理。型号研制中采用国内外主流的商用可靠性分析平台进行隐蔽故障概率计算。这些平台将隐蔽故障部件在两次视情检查间隔之间近似为不可修系统,其不可靠度随时间变化如图 7 所示,则模型采用模块不可靠度的锯齿形特性平均值。当 $\lambda t < 0.1$,简化公式为 $P = \lambda t/2$,而该计算方法只考虑了隐蔽故障本身的平均可靠度,没有考虑与其他失效组合影响的情况,并根据失效组合场景计算平均概率,因此该算法不能满足审定要求。

2) 失效率追溯性及正确性无法判断。由于国内缺少在运营阶段对设备安全性基础数据的收集,导致对失效率的判断完全依赖供应商提供的数据,无法形成有效的审查结果。

3) 隐蔽故障的识别不完整不准确。随着型号中综合模块化等高集成度系统的应用,时常出现系统交联不良、系统组件之间非预期相互作用、系统能力不及等新型的隐蔽故障,而这些故障形式并不能在早期进行有效识别。

4) 忽略对故障间独立性假设的获取,更缺少对此的 CCA 验证。

5) 数据计算过于保守。为确保数据计算的有效性,以及减小工作量,一般情况下会将风险时间、暴露时间及响应阶段进行保守计算。如将风险时间扩展到整个飞行阶段,使用隐蔽故障的最大暴露时间,将响应阶段扩展到整个飞行阶段,不考虑失效顺序因素等,但这样也会造成数据过于保守,增加设计无法满足安全性需求的风险。

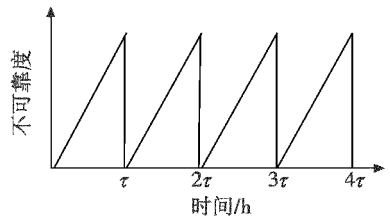

图 7　隐蔽故障模型 Q 曲线

Fig. 7　Q curve of hidden failure model

4　结束语

民用飞机的隐蔽性故障计算对初始适航系统安全性评估结果会产生重大影响。本文分析隐蔽故障计算模型审定要素和要点,并以具体型号工作为例进行分析,发现安全性问题,可有效指导对隐蔽故障计算的审定及验证工作。

参 考 文 献

[1] 中国民用航空局. CCAR-25-R4 中国民用航空规章第 25 部运输类飞机适航标准[S]. 北京:中国民航出版社,2011.

[2] 戴顺安,王烨,蔡景. 民用飞机隐蔽故障风险的定量评估方法研究[J]. 兵器装备工程学报,2016,37(6):162-165.

[3] 贾宝惠,刘涛,杨杭,等. 民机隐蔽故障维修间隔优化方法研究[J]. 航空制造技术,2015(s1):20-23.

[4] LIENHARDT B, HUGUES E, BES C, et al. Failure-finding frequency for a repairable system subject to hidden failures[J]. Journal of Aircraft, 2007, 45(5):1804-1809.

[5] 刁海飞,蔡景,林海彬,等. 基于多目标的隐蔽功能故障检测间隔优化方法研究[J]. 飞机设计,2014,34(3):33-36.

[6] SAE. SAE ARP4761 guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment[S]. [S.l.]:SAE International, 1996.

[7] LEVESON N. A new accident model for engineering safer systems[J]. Safety Science, 2004, 42(4):237-270.