

汽车产品安全

风险评估与风险控制指南

1 范围

本标准给出了汽车产品安全风险评估的基本过程以及风险控制的基本方法。

本标准适用于汽车产品缺陷分析、认定等过程中,对已销售的汽车产品可能出现的危险事件或情形进行风险评估与风险控制。

2 术语和定义

下列术语和定义适用于本文件。

2.1

汽车产品危险 hazard of motor vehicle product

由于设计、制造或标识等原因使汽车整车、系统、总成或零部件等处于一种不安全状态,并以汽车整车、系统、总成或零部件故障或失效的形式表现。

2.2

汽车产品安全风险 safety risk of motor vehicle product

由汽车产品危险导致的可能危及人身、财产安全的危险事件或情形的严重性与发生可能性的综合。

注:本标准中的危险事件或情形既包括已发生的,也包括可能发生的。

2.3

严重性 severity

危险事件或情形对人身、财产安全的损害程度。

2.4

可能性 probability

汽车产品在其使用寿命周期内发生危险事件或情形的概率。

注:可能性是对危险事件或情形发生的概率预测,不等同于过往市场故障或失效数据的统计。

2.5

风险评估 risk assessment

确定危险事件或情形的严重性与发生可能性的综合水平等级的过程。

2.6

风险控制 risk control

减小或避免危险事件或情形发生的策略与措施。

2.7

风险评估对象 objects of risk assessment

可能存在故障或失效的批次汽车产品。

3 总则

风险评估与风险控制基本流程如图1所示。

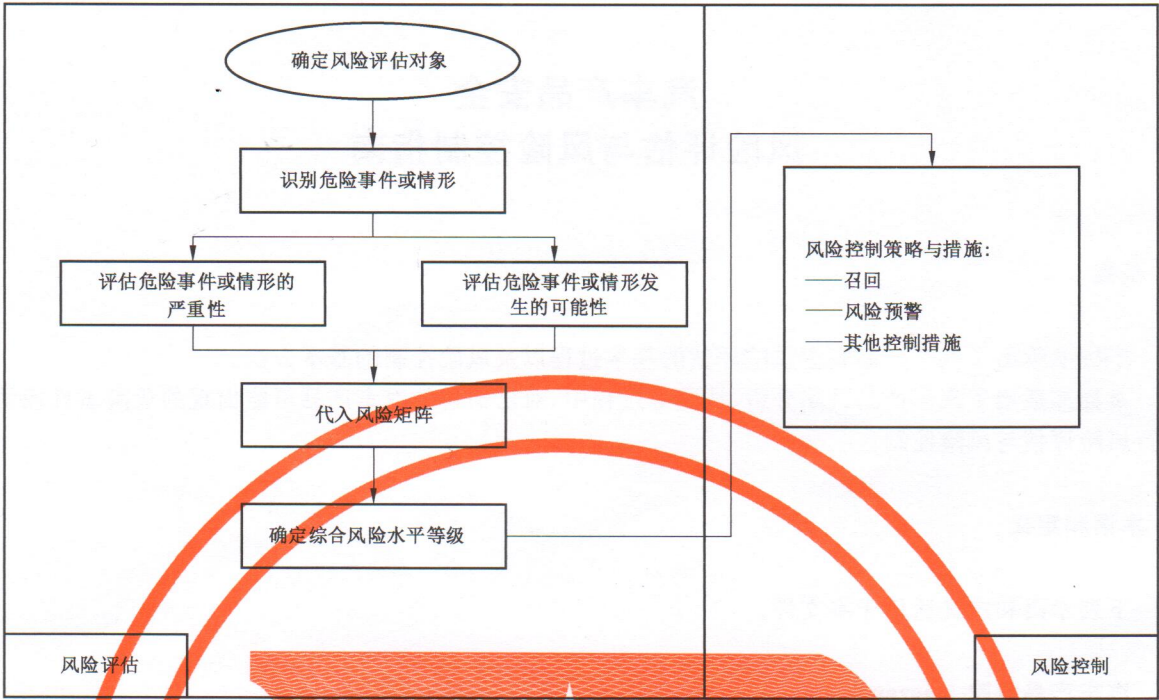


图 1 风险评估与风险控制基本流程

本标准中,风险评估是通过分别评估危险事件或情形的严重性和发生可能性等级,并代入风险矩阵,确定综合风险水平等级的过程。风险控制对象是已销售的汽车产品,风险控制责任主体根据综合风险水平等级制定相应的风险控制策略与措施,以减小或避免危险事件或情形的发生。

4 风险评估

4.1 风险评估基本程序

风险评估的基本流程主要包括:

- 确定风险评估对象;
- 识别危险事件或情形;
- 评估危险事件或情形的严重性;
- 评估危险事件或情形发生的可能性;
- 确定综合风险水平等级。

4.2 确定风险评估对象

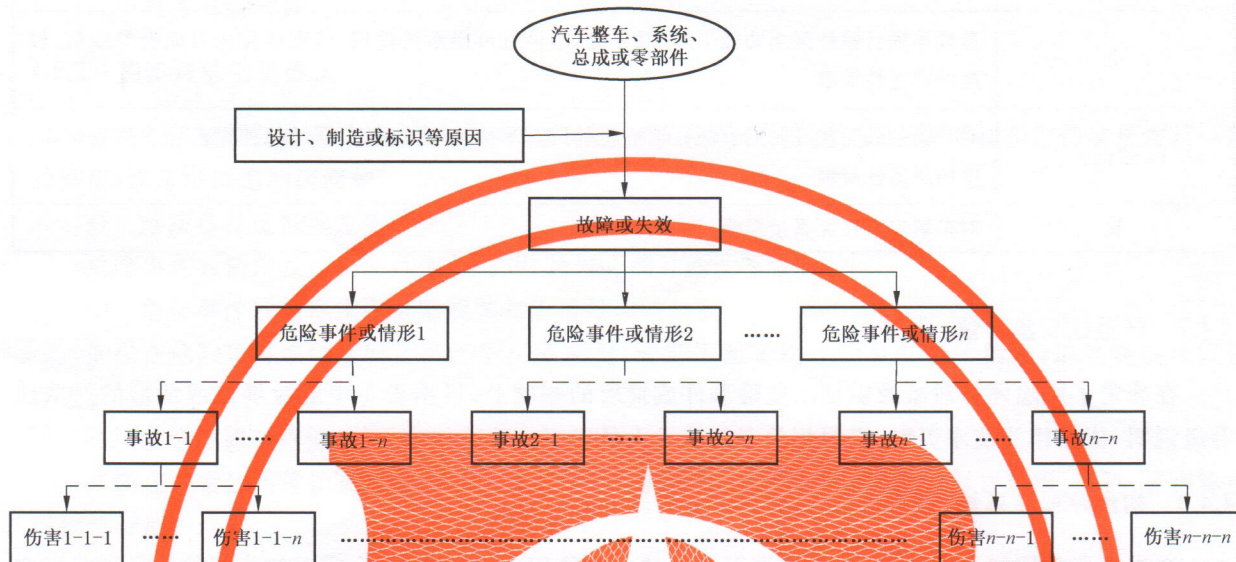
在评估过程中,需要根据汽车产品故障或失效的具体情况进行合理的分析和追溯后才能确定风险评估对象,尤其要分析故障或失效是否与汽车产品的设计、制造或标识等原因相关:

- 如果由设计原因导致了汽车产品故障或失效,风险评估对象是所有可能采用了同样设计的批次汽车产品;
- 如果由制造原因导致了汽车产品故障或失效,风险评估对象是所有可能采用了同样制造过程的批次汽车产品;
- 如果由标识原因导致了汽车产品故障或失效,风险评估对象是所有可能采用了同样标识的批次汽车产品。

4.3 识别危险事件或情形

4.3.1 风险传递过程

识别危险事件或情形首先要研究风险传递过程,对汽车产品故障或失效进行技术分析,并模拟可能出现的危险事件或情形以及可能引发的事故或伤害的场景。风险传递过程如图 2 所示。



注 1: 风险从原因端向结果端传递,其表现形式由最初单一的、确定的某个原因分化为若干不同的危险事件或情形,最终导致各种程度不一的事故或伤害。风险传递过程中各种情形发生的可能性从开始时的确切发生(如设计、制造或标识等原因)直至降低到很小的概率(如某种特定的伤害)。

注 2: 由于汽车产品技术和使用环境的复杂性,某个故障或失效可能引发多种伤害情形,而预测某种伤害情形发生的概率几乎是不可能的。例如:汽车产品的电气线路短路(故障或失效)会导致电气线路过热或烧蚀(危险事件或情形),可能引发车辆火灾(事故),造成人员轻度烧伤(伤害情形 A)、重度烧伤(伤害情形 B)或烧死(伤害情形 C),在风险评估时,要对上述 A、B、C 三种伤害情形的发生概率进行预测几乎无法完成,但“电气线路过热或烧蚀”这一危险事件或情形具有相对的确定性,具备开展风险评估的条件。

图 2 风险传递过程示意图

4.3.2 主要危险事件或情形的辨识

在进行风险传递过程分析时,大多数情况下可以在多种危险事件或情形中确定主要危险事件或情形,并对主要危险事件或情形开展风险评估。少数不易区分主、次危险事件或情形的,可先设定任一危险事件或情形为主要危险事件或情形,并对其开展风险评估。

在确定了主要危险事件或情形的综合风险水平等级后,再考虑其他危险事件或情形对风险评估结果的影响,并适当提高综合风险水平等级。

4.4 评估危险事件或情形的严重性

4.4.1 危险事件或情形的严重性等级说明

危险事件或情形严重性评估分为初步评估和结果修正两个步骤。严重性分为 5 个等级:高、较高、中、较低、低,各等级的说明如表 1 所示。

表 1 危险事件或情形的严重性等级说明

严重性等级	严重性等级说明
高	具有突发性,且不可控,可能严重危及人身、财产安全
较高	具有突发性,且可控性降低,可能危及人身、财产安全
中	造成车辆行驶性能或功能下降,但可控,车辆有可能继续使用,若继续使用可能会导致高、较高的严重性等级
较低	对车辆行驶性能或功能有部分影响,但可控,车辆可继续使用,若继续使用可能会导致较高、中的严重性等级
低	对车辆安全性无直接影响

4.4.2 严重性初步评估

在确定了风险评估对象及识别出危险事件或情形的基础上,根据表 1 中危险事件或情形的严重性等级说明,依据相关技术资料,组织相关专业技术人员进行严重性初步评估。

4.4.3 初步评估结果修正

在进行严重性初步评估后,考虑到汽车产品技术和使用环境的复杂性,需对初步评估结果进行一定的修正,修正可考虑的因素如下:

a) 易受伤害人群

易受伤害人群应包括儿童、老人、病人等对危险事件或情形造成的伤害耐受力较低的人群。如果汽车产品危险潜在危害的人群是易受伤害人群,应提高严重性等级。

b) 车辆类型

不同的车型在用途、车速、准载人数、重量、几何尺寸、主被动安全水平、载货性质等方面对严重性存在一定的影响。如:高速跑车,大中型客车、货车等高速、高负荷车辆,以及危险品货物运输车辆等,应提高严重性等级。

除了上述修正因素外,在进行严重性等级初步评估结果修正时,还可根据故障或失效模式、车辆事故深度调查情况、人员伤亡程度以及缺陷工程分析试验结果等因素,进行综合分析后修正。

4.5 评估危险事件或情形发生的可能性

4.5.1 危险事件或情形发生的可能性等级

危险事件或情形发生的可能性分为 5 个等级:高、较高、中、较低和低。可能性评估包括初步评估和结果修正两个步骤。可能性评估的方法主要包括:定量法、定性法和定量定性结合法。

4.5.2 可能性初步评估

在故障或失效模式、样本质量和数量满足定量分析要求的情况下,可采用统计学方法中的趋势预测模型[如韦伯分布(Weibull Distribution)模型等]或工程分析方法预测汽车产品在其使用寿命周期内发生危险事件或情形的概率,可能性的初步评估结果根据故障或失效模式的行业平均水平确定。

在样本质量和数量无法满足定量分析的情况下,可组织相关专业技术人员进行定性法的方式进行评估。定性法评估原则如下:

- 若危险事件或情形发生的原因由材料、零部件结构设计、生产工艺、软件控制策略、整体布置或零部件匹配等设计因素导致,可能性的初步评估结果可为高或较高;
- 若危险事件或情形发生的原因由材料加工、机械加工、零部件装配或生产管理不当等制造因素导致,可能性的初步评估结果可为较高、中或较低;
- 若危险事件或情形发生的原因由车辆无标识或错误标识等因素导致,可能性的初步评估结果可为高或较高。

4.5.3 初步评估结果修正

在进行可能性初步评估后,考虑到汽车产品技术和使用环境的复杂性,需对初步评估结果进行一定的修正,修正可考虑的因素如下:

a) 危险事件或情形发生的条件

危险事件或情形发生的条件非常苛刻,适当降低可能性等级。

b) 危险事件或情形发生前能被感知而被排除或限制

如果在危险事件或情形发生前能够被感知到,或发生前车辆有明显的警示信息,适当降低可能性等级。

c) 日常维修可排除危险事件或情形的发生

车辆在日常使用维护过程中,存在故障或失效的系统、总成或零部件能够得到更换、调整,适当降低可能性等级。

d) 车辆使用频次

如果风险评估范围内的车辆使用频次超过正常车辆,危险事件或情形发生的可能性将会增加,例如出租车、公共汽车、载货车等,适当提高可能性等级。

e) 车辆运行环境

对于长期在山地、高寒、高温、高湿等特殊气候环境以及路面状况差、含水量或含盐量过大等道路环境下运行的车辆,如果上述环境能够加快危险事件或情形的发生,适当提高可能性等级。

f) 已引发危及人身、财产安全案例

已发生引发危及人身、财产安全的案例时,应提高可能性等级,尤其已发生导致人员死亡的案例时,应将可能性等级提高到较高或高两个等级。

g) 同一故障或失效引发多种危险事件或情形

因同一故障或失效引发多种危险事件或情形,以主要危险事件或情形发生的可能性进行评估,结合考虑其他次要危险事件或情形,适当提高可能性等级。

除了上述修正因素外,在进行可能性等级初步评估结果修正时,还可根据已知的故障或失效发生率、已知案例发生的情形、车辆现场勘查情况以及缺陷工程分析试验结果等因素,进行综合分析后修正。

4.6 确定综合风险水平等级

在危险事件或情形的严重性等级和发生的可能性等级确定的基础上,通过查询风险评估矩阵(见图3)确定综合风险水平等级。综合风险水平等级分为五级:高(第5级)、较高(第4级)、中(第3级)、较低(第2级)、低(第1级)。

可能性	严重性				
	低	较低	中	较高	高
低	1	2	2	3	3
较低	2	2	3	3	4
中	2	3	3	4	4
较高	3	3	4	4	5
高	3	3	4	5	5

图 3 风险评估矩阵

5 风险控制

风险控制对象是已销售的汽车产品,风险控制责任主体是汽车产品生产者,风险控制责任主体应根据综合风险水平等级制定相应的风险控制策略与措施:

- 综合风险水平等级为高(第 5 级)和较高(第 4 级)的,汽车产品生产者应根据相应的法律法规实施召回活动,消除车辆安全隐患;
- 综合风险水平等级为中(第 3 级)的,汽车产品生产者通过分析国内外相关的召回案例,若存在类似召回案例的,汽车产品生产者应根据相应的法律法规实施召回活动;若没有类似召回案例,汽车产品生产者可自主处置;
- 综合风险水平等级为较低(第 2 级)和低(第 1 级)的,汽车产品生产者可自主处置。