中华人民共和国国家军用标准

FL 0101

GJB 5852—2006

装备研制风险分析要求

Risk analysis requirements for materiel development

2006—12—15 发布

2007—05—01 实施

国防科学技术工业委员会 发布

目　次

前　言

本标准的附录 A 和附录 B 是资料性附录。

本标准由中国航天科技集团公司提出。

本标准由中国航天标准化研究所归口。

本标准起草单位：中国航天标准化研究所、中国船舶重工集团公司舰船研究院、哈飞航空工业股份有限分司、中国核工业标准化研究所。

本标准主要起草人：李福秋、任立明、周海京、王　华、伍平洋、遇　今、洪国钧、刘宝成、杨华庭。

装备研制风险分析要求

1 范围

本标准规定了装备研制风险分析的通用要求和有关风险分析的步骤和方法。

本标准适用于装备研制阶段的风险分析。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单(不包含勘误的内容)或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GJB 813 可靠性模型的建立与可靠性预计

GJB 1391 故障模式、影响及危害性分析程序

GJB/Z 768A 故障树分析指南

3 术语和定义

下列术语和定义适用于本标准。

3.1

风险 risk

在规定的技术、费用和进度等约束条件下，对不能实现装备研制目标的可能性及所导致的后果严重性的度量。风险对任何项目都是固有的，包括技术风险、费用风险和进度风险，在装备研制的任何阶段都可能产生。

3.2

风险分析 risk analysis

进行风险识别、风险发生的可能性及后果严重性分析、风险排序的过程，是风险管理的一部分。

4 通用要求

4.1 风险分析过程一般分为三个步骤，即风险识别、风险发生的可能性及后果严重性分析和风险排序。风险分析的过程见图1。

4.2 风险分析过程的输入至少应包括如下内容：

a) 装备研制的合同和/或研制任务书；

b) 装备研制风险管理的目的和目标；

c) 风险管理计划；

d) 风险分析方法选择准则、风险排序准则和风险接受准则；

e) 装备工作分解结构及研制阶段；

f) 装备研制经费概算；

g) 计划进度要求；

h) 装备已有的可利用的信息和试验数据等。

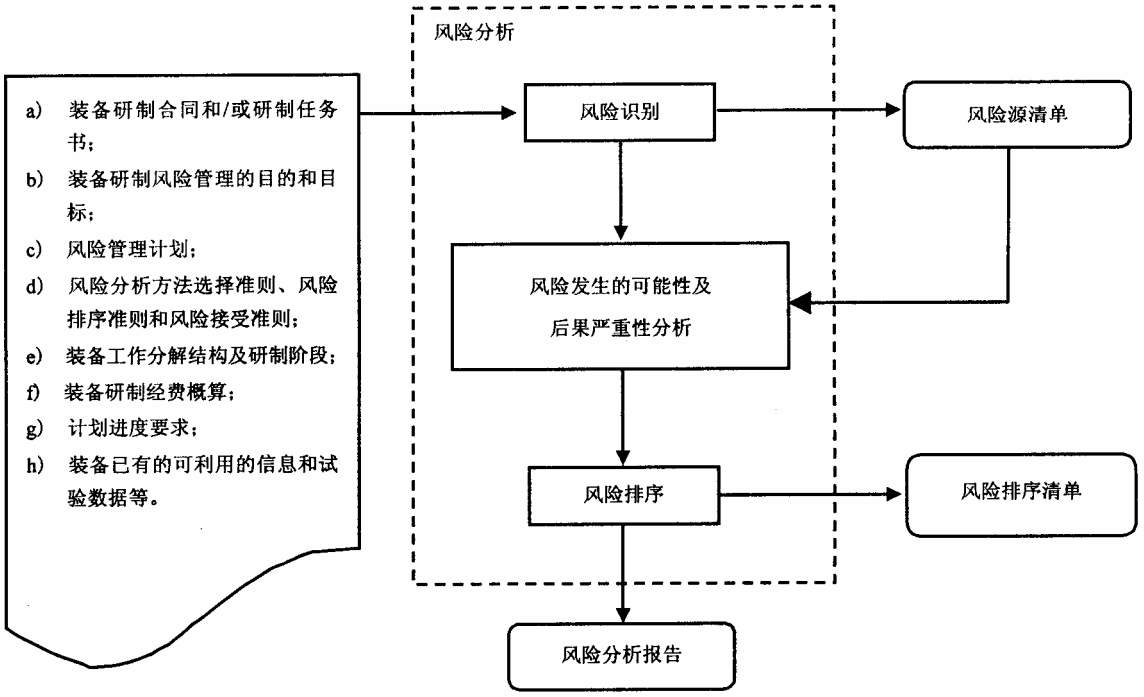

图 1　风险分析过程

4.3　风险分析的输出包括风险源清单、风险排序清单和风险分析报告等文档。

4.4　风险分析作为风险管理的关键过程之一，应按风险管理计划开展，随着装备研制的进展反复迭代、不断深入，并贯穿于整个装备研制的全过程。

4.5　风险识别一般应在装备研制的各阶段，按装备的工作分解结构逐一仔细辩识风险。

4.6　在装备可用资源充分的情况下应尽量采用定量风险分析方法。

4.7　风险分析报告的编写、校对、审批应按照审批程序执行。

4.8　风险分析应由项目负责人组织实施，风险分析人员应具备装备研制经验和风险分析能力。

4.9　风险分析应配备必要的技术和物质资源。

4.10　风险分析过程中，应将有关信息及时传递并上报装备研制风险管理部门。

5　风险分析步骤及方法

5.1　风险识别

5.1.1　风险识别的输入

风险识别是对装备研制的各个方面，特别是关键技术过程进行考察研究，从而识别和记录风险源的过程，即确定风险源。识别风险源是风险分析工作的基础。识别风险源的输入是：

a)　装备研制技术风险、进度风险和费用风险的判据；

b)　相似装备的经验、教训及有关数据；

c)　工程模型、样机研制及试验结果或预测数据；

d)　其它可利用的信息；

e)　专家意见等。

5.1.2　风险识别方法

风险识别应参考相似装备的研制经验，发挥专家和集体智慧。装备研制风险识别可采用如下方法(不限于此)：

a)　检查单法：根据经验和可获得的信息，将装备研制可能的风险源列在检查单上，检查装备研制

是否存在检查单中所列出的或类似的风险源并统计汇总。装备研制各阶段识别风险源的线索表参见附录 A；

b) 流程图法：给出装备研制的工作流程、各个阶段之间的相互关系，帮助风险识别人员分析和了解装备研制的具体环节，通过对装备研制流程的分析，发现和识别存在风险的环节；

c) 头脑风暴法：采用会议的方式，与会者提出自己的意见，充分交流，互相启迪，总结归纳形成结论；

d) 反复函询法：将风险识别有关的问题征求专家意见，并将返回意见经过整理、归纳，将结果反馈给专家，再次征求意见，如此反复直到专家的意见稳定。

5.1.3 风险识别的输出

风险源清单是风险识别的输出，为风险发生的可能性及后果严重性分析提供信息输入，至少应包括风险源名称、风险源编号、风险发生的原因和风险可能导致的后果等项目。风险源清单格式示例见图 2。

装备名称：　　装备研制阶段：

序号	风险源	风险源编号	风险发生的原因	风险可能导致的后果	备注

注 1：风险源编号由装备代号＋研制阶段代码＋数字编码三部分内容组成。

注 2：各阶段代码：方案阶段－F　工程研制阶段－G　定型阶段－D。

编写　　日期　　审核　　日期　　第　页　　共　页

图 2　风险源清单格式示例

5.2 风险发生的可能性及后果严重性分析

5.2.1 概述

风险发生的可能性及后果严重性分析是对识别出来的风险特别是重大风险进一步分析，确定每一个风险事件发生的可能性，判定后果严重性和关键过程对预期目标偏离的程度。

5.2.2 风险发生的可能性及后果严重性分析方法

5.2.2.1 风险评价指数法

由熟悉装备每个风险区及产品分解结构的风险问题的专家，在进行风险识别的基础上，分析风险发生的可能性及其后果严重性，确定风险等级及风险处理的优先次序。

5.2.2.2 故障模式影响及危害性分析(FMECA)

确定所有可能的故障，根据对每一个故障模式的分析，确定故障模式的影响，找出单点故障，并按故障模式的严酷度及其发生概率确定其危害性。FMECA 分两步骤完成，即故障模式及影响分析(FMEA)和危害性分析(CA)。具体方法按 GJB 1391 的规定。

5.2.2.3 故障树分析(FTA)

是一种逻辑因果关系图，描述系统中各种事件之间的因果关系，将拟分析的重大风险作为“顶事件”，“顶事件”的发生是由于若干“中间事件”的逻辑组合所导致，“中间事件”又是由各个“底事件”逻辑组合所导致。这样自上而下地按层次进行因果逻辑分析，逐层找出风险发生的必要而充分的所有原因和原因组合。具体方法按 GJB/Z 768A 的规定。

5.2.2.4 可靠性预计

根据以往积累的信息，运用自下而上综合的方法对未来的产品的可靠性进行预先计算的过程。可靠性预计作为风险分析的一种方法，找出须重点关注的单元和环节并确定其影响程度，进行定量分析，作

为进行风险处理的依据。具体方法按 GJB 813 的规定。

5.2.2.5 建模与仿真

在计算机上或实体上建立系统的有效模型，虚拟地复制产品或过程，并在较容易获得和易于操作的真实环境中模仿这些产品或过程，采用建模和仿真发现系统或过程存在的问题，可作为分析风险问题的有力手段。

5.3 风险排序

5.3.1 概述

风险排序是对风险发生可能性及后果严重性的综合量化结果进行排序，找出关键和重要的风险。除考虑综合影响外，对于发生的可能性大或后果影响严重的风险应给予特别的关注。风险排序清单是风险处置的依据。

5.3.2 风险排序方法

5.3.2.1 专家多次投票法

专家组成员分别就每项风险的顺序进行投票，统计投票结果，并将投票结果反馈给专家组，专家组成员则再次投票，如此反复直到结果不再有任何变化。一般只经过几次投票就会产生最后的结果。如果风险数目很大，可将风险分为若干组进行排序，一般情况下，每次投票中需要排序的对象不应超过 10 项。

5.3.2.2 专家会签法

专家组成员分别对每项风险进行打分，如认为是最重要的风险打 10 分，最次要的风险打 1 分，根据自己的经验对其余的按相对重要性分别打 1－10 分，汇总各位专家打分的结果，统计每个风险所得分数的总和，按得分的多少排序。

5.3.2.3 两两比较法

专家组集体讨论，将各待排序的风险两两比较，将比较结果进行矩阵运算，获得各见险的排序。具体过程如下：

用 a_{ij} 表示风险 i 比 j 的相对重要程度，

风险 i 比风险 j 绝对重要　　$a_{ij}=9$；

风险 i 比风险 j 重要得多　　$a_{ij}=7$；

风险 i 比风险 j 重要　　$a_{ij}=5$；

风险 i 比风险 j 稍微重要　　$a_{ij}=3$；

风险 i 与风险 j 一样重要　　$a_{ij}=1$。

介于中间的 a_{ij} 为 2、4、6、8，$a_{ij}>0$，$a_{ji}=1/a_{ij}$，$a_{ii}=1$。

将两两比较结果列在一个判断矩阵中：

$$\begin{array}{c} \\ A_1 \\ A_2 \\ A_i \\ A_j \\ A_n \end{array}\begin{pmatrix} A_1 & A_2 & A_i & A_j & A_n \\ a_{11} & a_{12} & a_{1i} & a_{1j} & a_{1n} \\ a_{21} & a_{22} & a_{2i} & a_{2j} & a_{2n} \\ a_{i1} & a_{i2} & a_{ii} & a_{ij} & a_{in} \\ a_{j1} & a_{j2} & a_{ji} & a_{jj} & a_{jn} \\ a_{n1} & a_{n2} & a_{ni} & a_{nj} & a_{nn} \end{pmatrix}$$

将判断矩阵的每一行分别相加，再将所得的列向量归一化(每一项除以列中各行之和)，即得出各风险 A_1、A_2……A_n 的相对重要度，依次排序。

5.3.2.4 风险评价指数排序法

对装备研制的风险进行排序，排序的过程是对风险进一步评价的过程，从风险发生可能性的大小及可能造成后果的严重性进行综合度量。以风险评价指数量化排序结果的示例见图 3，图中风险指数(R)为严重性和可能性的乘积。纵坐标是风险发生的可能性，横坐标是风险的后果严重性。以可能性和严重性的等级乘积表示风险指数，指数越高，风险越大。

可能性					风险指数
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
	1	2	3	4	5

严重性

图 3　风险排序图

5.3.3　风险接受准则

已排序的风险应按照风险接受准则确定其可接受或不可接受。按照风险评价指数排序法进行风险排序所确定的风险接受准则示例见表 1。

表 1　风险接受准则示例

风险指数	风险级别	说明
$R \geq 20$	最大风险	不可接受风险
$15 \leq R < 20$	高风险	不可接受风险
$10 \leq R < 15$	中等风险	不可接受风险
$4 \leq R < 10$	低风险	可接受风险
$R < 4$	最小风险	可接受风险

5.3.4　风险排序清单

综合考虑风险发生的可能性及后果的严重性，根据风险接受准则，对已识别的风险按照采取措施的优先次序排序，排序结果列入风险排序清单。推荐的风险排序清单格式示例见图 4。

装备型号名称：　　研制单位：

排序	风险源编号	最大风险	高风险	中等风险	低风险	最小风险	风险类型	备注
		*	*	*	*	*	**	

注 1：风险源编号与图 2 一致。

注 2：(*)根据风险接受准则适当地标记风险指数值。

注 3：(**)指出风险类型，例如：技术、费用或进度。

填写　　日期　　审核　　日期　　共　　页　　第　　页

图 4　风险排序清单格式示例

5.4　风险分析报告

风险分析应形成文件，跟踪并记载风险分析过程所进行的活动和分析结果，编写风险分析报告。风险分析报告应履行审批手续。报告至少应包括如下内容：

a)　概述：描述被分析对象的名称、功能特点、任务要求、工作分解结构中所处位置、所处的研制

阶段等；

b) 风险分析过程：描述进行风险分析的过程及分析方法、风险等级划分准则、风险排序准则和接受准则等；

c) 分析结果：列出风险源清单和风险排序清单(可作为附件)，必要时可对高风险项目提出处置措施建议；

d) 结论：总结风险分析工作，得出结论和建议；

e) 附件。

风险分析报告示例参见附录B。

附 录 A
（资料性附录）
装备研制各阶段风险源线索表

A.1 方案阶段

方案阶段的风险源主要有：

a) 方案论证中新技术成分采用过多；
b) 方案论证中大型试验考虑不当；
c) 方案论证不充分，对难点与困难认识不足等；
d) 不重视保障性要求；
e) 采用不成熟的新技术；
f) 参数设计缺少优化；
g) 各种要求的分配缺少权衡研究；
h) 接口协调不够；
i) 更改过多控制不严；
j) 引用标准剪裁不准；
k) 设计周期不能保证；
l) 未及早制定切实可行的费用目标；
m) 进度目标不切实际，难以实现；
n) 资源供应不能满足进度要求；
o) 权衡研究未考虑进度问题；
p) 方案阶段未充分考虑各种影响因素；
q) 方案论证未经不同方案对比和优选；
r) 未开展工艺可行性分析；
s) 技术风险对费用和进度的影响不够等。

A.2 工程研制阶段

工程研制阶段的风险源主要有：

a) 权衡不周，分配不当；
b) 未进行各种专门的设计分析(如应力和应力－强度分析、最坏情况分析、潜在分析、FMECA、FTA、安全性分析等)；
c) 元器件选择使用不当；
d) 生产定点不当与多变；
e) 产品特点分析不够；
f) 设计提出过高的工艺要求，制造能力达不到；
g) 未有或未实施适宜的设计准则、规范和程序；
h) 设计评审不充分；
i) 未在项目的早期启动试验规划、编制试验计划(包括主系统、分系统的所有研制试验和鉴定试验)；
j) 试验方案不能保证取得可信的结果；
k) 设计提出过高的人员技能和要求；
l) 不成熟或未经验证的技术在生产前尚不能得到充分的改进或验证；

m） 采用新技术、新工艺或新的工作流程，生产工艺过程未经验证；
n） 对特殊过程的过程参数未进行鉴定或验证；
o） 加工工艺不稳定，经常更改；
p） 设施、设备不能满足工艺要求；
q） 无适宜的专用工装、工具，不能防止加工中出差错；
r） 手工操作，未采用自动化或半自动化的加工和测试手段；
s） 采购产品未经充分验证和筛选；
t） 产品测试性不满足要求；
u） 没有建立和保持强有力的技术状态管理系统，随意更改设计；
v） 设计采用了未成熟技术；
w） 设计分析缺少工具与指南；
x） 设计人员知识结构不适应；
y） 疏忽可生产性设计；
z） 设计工具落后，先进设计工具应用不够；
aa） 未对试验中出现问题做深入分析，留下隐患；
bb） 预算周期内投资进程不稳定或资金不能及时到位；
cc） 冗余性能能力占去过多费用，即所做出的费用－性能权衡不够适宜；
dd） 研制后期才发现问题需要工程更改，增加费用、拖延进度；
ee） 技术风险对费用和进度的影响考虑不够等。

A.3 定型阶段(设计定型和生产定型阶段)

设计定型和生产定型阶段的风险源主要有：
a） 技术状态疏于管理；
b） 制造缺乏最佳途径分析；
c） 制造计划缺乏人员培训规划和具体实施措施；
d） 质量计划和检验要求及有关评审程序未纳入制造计划；
e） 工艺方案不够完善；
f） 没有制定合理经济的工艺路线；
g） 工艺规程编制脱离现场实际；
h） 专用工艺装备和设备不完善；
i） 缺乏工艺技术验证；
j） 缺乏对工艺人员和工人的培训；
k） 忽视工艺评审；
l） 工艺文件准备不充分；
m） 对采购质量控制不严；
n） 工艺更改失控；
o） 多余物控制不严；
p） 对不合格品未及时采取措施；
q） 工艺装备及设备不适应产品设计的需要；
r） 试验未考虑最终使用环境，未考虑使用周期的极端情况和最恶劣的环境条件；
s） 重大更改或改型后未进行验证；
t） 定型试验不充分；
u） 技术风险对费用和进度的影响考虑不够等。

附 录 B
（资料性附录）
××卫星风险分析示例

B.1 概述

××卫星在发射任务中止后整星及地面设备面监的问题是地面贮存，由于长时间贮存对整星、分系统和部件的影响会给该星下次发射带来一定的风险。本示例是对由于长时间贮存对××卫星带来的风险进行分析。

B.2 风险识别

B.2.1 识别风险源

经分析，由于长时间贮存可能使卫星产生的风险因素主要有如下几点：

a) 环境控制不严，潮气侵入、尘粒污染等因素，造成星上某些元器件、部件或设备失效，原材料性能退化，给卫星带来需要更换设备或部件，延误进度，影响发射任务的风险；

b) 长期贮存、环境或其它因素的影响，对产品造成潜在的故障隐患，但通过贮存期间检测或贮存后测试或试验并未暴露出来，有可能在卫星上天后发生故障，对完成任务造成不同程度的影响（依故障部位不同而影响后果不同）；

c) 增加贮存时间对于一些使用寿命较短的元件或材料，可能会导致卫星上天后某些元件已经达到使用寿命期限，在整星尚未达到设计寿命时，就已提前失效，根据失效部位的不同，对整星造成程度不同的不利影响；

d) 贮存过程中操作、测试或贮存后检测不当，或由于试验类别或试验量级定得不适当，量级过低不能检测出由于卫星贮存或更换设备给卫星引入新的潜在失效模式，量级过高又有可能对卫星造成不必要的损伤，从而对卫星任务的完成造成风险。

B.2.2 风险源清单

表 B.1 为××卫星长期贮存的风险源清单。

表 B.1 风险源清单

装备名称：××卫星

装备研制阶段：贮存阶段

序号	风险源	风险发生的原因	风险可能导致的结果	备注
1	贮存环境控制不严	潮气入侵，尘粒污染等	延误进度，影响发射任务	
2	试验方案考虑不周	试验未暴露出故障隐患	卫星上天后发生故障	
3	元件或材料选用不当	寿命较短的元件或材料，因贮存时间增加导致提前失效	对整星造成不同程度的影响	
4	试验方案考虑不周	试验类别或量级选择不当，不能检测出或引入新的失效	对卫星造成损伤，影响卫星任务的完成	

编写 ××× 日期 审核 ××× 日期 第 页 共 页

B.3 发生的可能性及后果严重性分析

B.3.1 发生的可能性等级

对以上识别出的风险因素进行分析。这里采用风险评价指数法，按风险发生可能性及后果严重性划分为相应的等级，形成一种风险评估矩阵，并赋予一定的加权值来定性衡量风险大小。风险发生的可能性等级是对风险发生可能性的度量，见表 B.2。

表 B.2　风险发生的可能性等级

等级	发生可能性	
	产品个体	产品总体(或系统)
5	频繁发生	连续发生
4	在寿命期内出现若干次	频繁发生
3	在寿命期内可能有时发生	出现若干次
2	在寿命期内不易发生，但有可能	不易发生但有理由预期可能发生
1	很不容易发生，可以认为不会发生	不易发生，但仍有极小可能发生

B.3.2　后果严重性等级

风险后果的严重性等级是对风险严重程度的度量，见表 B.3。

表 B.3　风险的后果严重性等级

程度	等级	后果严重性
灾难的	4	人员死亡或系统毁坏或发射任务失败，或造成巨大经济损失，或生态环境遭受严重破坏
严重的	3	人员严重伤害或系统严重损坏造成重大经济损失，或发射进度延后三个月以上，或生态环境受到破坏
轻度的	2	人员轻度伤害或系统轻度损坏，或发射进度稍有延后，或轻度影响生态环境
轻微的	1	轻于 III 类的人员伤害或系统损坏或不影响任务完成，对计划进度影响可忽略不计

B.3.3　风险评价指数

风险指数＝可能性×严重性，指数表见表 B.4。

表 B.4　风险评价指数矩阵

可能性等级	严重性等级			
	4(灾难的)	3(严重的)	2(轻度的)	1(轻微的)
5(频繁)	5	10	15	20
4(很可能)	4	8	12	16
3(有时)	3	6	9	12
2(极少)	2	4	6	8
1(不可能)	1	2	3	4

B.3.4　风险接受准则

风险接受准则为：

a)　最大风险(A 类)：指数 $R \geq 20$ 为最大风险，不可接受，必须采取新的措施；

b)　高风险(B 类)：指数 $15 \leq R < 20$ 为高风险，不可接受，必须积极地管理和考虑备选措施；

c)　中等风险(C 类)：指数 $10 \leq R < 15$ 为中等风险，不可接受，需控制和监控；

d)　低风险(D 类)：指数 $4 \leq R < 10$ 为低风险，经评审后可接受；

e)　最小风险(E 类)：指数 $R < 4$ 为最小风险，不经评审即可接受。

B.4　风险排序

B.4.1　风险分析结果

风险分析结果见表 B.5。

表 B.5　风险分析结果

序号	风险源	危险严重性等级	危险可能性等级	风险评估指数	风险接受准则	备注
1	贮存环境控制不严	1	2	2	E 类	此风险主要对计划进度产生影响
2	试验方案考虑不周	4	2	8	D 类	此风险依故障隐患的部位不同而影响后果不同，如果是关键部位(如单点失效)，有可能造成整星失效，如果是非关键有效载荷或有冗余的部位，对整星的影响则较小
3	元件或材料选用不当	2	2	4	D 类	同上
4	试验方案考虑不周	3	2	6	D 类	同上

B.4.2　风险排序结果

由以上的分析按照风险发生的可能性及后果严重性排序见表 B.6。

表 B.6　风险排序清单

装备型号名称：××卫星　　研制单位：××院××所　　日期：×年×月×日

排序	风险源编号	最大风险	高风险	中等风险	低风险	最小风险	风险范围	备注
1	2				8		技术	
2	4				6		技术	
3	3				4		技术	
4	1					2	进度	

B.5　分析结论

通过以上的分析和论述，总结了对××卫星长期贮存风险进行的分析。总之，××卫星贮存的风险分析是一个长期的过程，尽管通过采取措施风险级别可以得到降低，但在整个贮存过程中，对每一个环节都要实施严格的质量控制和管理，对风险实施全程监控，杜绝任何可能增大风险的因素，将风险降至最低。