

# 深圳市无人机行业协会团体标准

T/ SZUAVIA 002-20XX

## 多旋翼无人机系统安全性分析规范

Safety analysis specification for unmanned aircraft system with multi-rotors

(工作组讨论稿)

2019.04.24

XXXX – XX – XX 发布

XXXX – XX – XX 实施

深圳市无人机行业协会

发布

## 前 言

工业和信息化部电子第五研究所

# 多旋翼无人机系统安全性分析规范

## 1 范围

本标准规定了多旋翼无人机系统安全性分析的实施步骤和细则，便于应用与广大生产厂商、销售商和用户的相关人员全面准确地使用和实施多旋翼无人机系统安全性分析标准。

本标准适用于民用多旋翼无人机系统的设计、生产、销售、管理和使用。

## 2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

## 3 术语与定义

### 3.1

#### 事故

造成人员伤亡、职业病、装备损坏、财产损失或环境破坏的一个或一系列意外事件。

### 3.2

#### 危险

可能导致事故的状态。

### 3.3

#### 安全性

产品具有的不导致人员伤亡、职业病、装备损坏、财产损失或不危及人员健康和环境的能力。

### 3.4

#### 危险严重性

某种危险可能引起的事故后果的严重程度。

## 4 安全性分析步骤

安全性分析可按下述步骤进行：

- a) 对于多旋翼无人机系统，明确其性能特性和使用特性，分析其危险三要素（危险物质、威胁目标、触发机制）；

- b) 识别（包括与每项任务有关的故障和失效方式等）危险源，即识别多旋翼无人机系统运行或为完成所需的操作会发生什么样的故障或失效，以及潜在的各种危险是什么；
- c) 在危险源识别的基础上，进行危险机理分析，确定导致危险或事故发生的根本原因；
- d) 进行风险分析，确定危险的严重等级及发生概率等级；
- e) 根据风险分析进行风险评价，确定降低风险的对策，并根据危险机理分析制定安全性要求，指导安全性设计；
- f) 重复第 d-e 步，直到风险降低到可接受水平；
- g) 针对残余风险，建立使用安全保障体系。

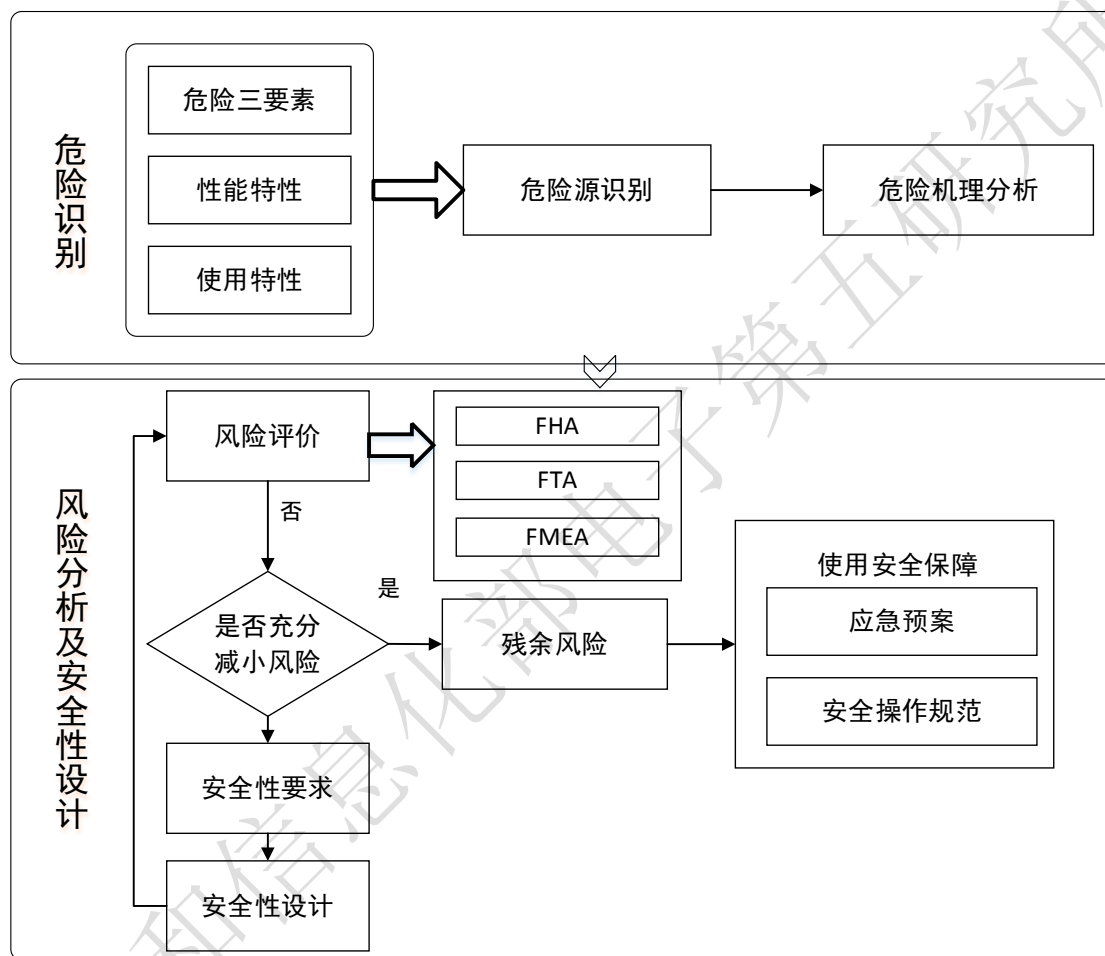


图1 多旋翼无人机系统安全性分析步骤

## 5 危险识别

识别可能由无人机系统本身或外围设备产生或由于人与无人机系统的相互干扰而产生的危险或危险状态，使在进行无人机系统设计，和进行风险评价时，便于危险分析。

### 5.1 产品特性分析

为了识别危险源，需要明确产品的具体特性，包括性能特性、使用特性以及危险三要素。

#### 5.1.1 性能特性

明确产品的功能及组成，例如电驱的多旋翼无人机系统一般的组成及功能为：

- a) 无人机机体：包括机身，机臂和脚架。用于支撑安装产品的功能部件；
- b) 供电系统：包括电池和开关。为产品提供电源；
- c) 动力系统：包括桨叶、电机和电调。实现旋翼转动，为产品提供升力；
- d) 飞控系统：包括主控系统、电子罗盘、加速度计、陀螺仪、气压计、GPS 等。对产品的飞行状态进行调整，使得其能够按照指令动作；
- e) 通讯系统：包括信号发射器、地面基站。实现地面对无人机的遥控、控制；
- f) 任务系统：包括相机、云台和图传。实现产品的拍摄功能，并将其传输给地面。

### 5.1.2 使用特性

明确无人机的应用场景、使用环境，以及环境条件对无人机系统的影响。同时明确无人机的操作过程，分析操作使用过程中人员及操作系统本身对无人机系统运行的影响。

### 5.1.3 危险三要素

- a) 危险物质：系统中的基本危险源，如高温、高压等能量源、有毒物质等，决定了事故危害的大小。
- b) 触发机制：导致危险向事故转移的一个或多个事件，如设备故障、操作失误、外部干扰等，并且这些事件之间达成特定的时间、空间逻辑关系才会导致事故发生。触发机制决定了发生事故的可能性。
- c) 危害目标：它是指可能会受到伤害或损失的对象，包括人、物或者环境等外部对象，决定了事故影响的范围。

## 5.2 危险源识别

识别危险源时，应从整套装备的各个方面来进行考虑：

- a) 设备方面：无人机、地面控制站。
- b) 设备的使用环境：地形、气候、电磁环境、障碍物等。
- c) 相互关系方面：无人机系统本身，无人机系统与其他相关设备之间，人鱼无人机系统相互交叉干涉而形成的危险。

危险和危险状态可以列表，对于不同应用场景的无人机系统，其危险源不尽相同。大致可分为下述各项。

### 5.2.1 多旋翼无人机系统硬件失效或故障引起的危险

- a) 动力系统故障；
- b) 控制系统故障；
- c) 供电系统故障；
- d) 通讯系统故障；
- e) 任务系统故障；

### 5.2.2 多旋翼无人机系统结构件引起的危险

无人机机架、机臂等结构件发生变形、断裂等故障。

### 5.2.3 危险环境或条件

- a) 不利的导航环境

- b) 不利的天气或大气条件
- c) 外部威胁，如固定的障碍物，飞鸟撞击，附近的其他飞行器等。

#### 5.2.4 干扰产生的危险

电磁、射频干扰：由于电磁干扰、射频干扰，使无人机系统发生失控，造成危险或事故发生。

#### 5.2.5 人因差错产生的危险

- a) 无人机飞手决定错误或判断失误；
- b) 在禁飞区内操作；
- c) 异常/意外的控制输入；
- d) 错误的操作/行为。

### 5.3 危险机理分析

分析事故放生的根本原因，为后续安全性设计提供基本依据。

## 6 风险分析

由于多旋翼无人机系统规格、尺寸、应用场景的不同，其使用环境及操作亦各异，其危险的种类和程度亦不同，因此需评价多旋翼无人机系统在设计、操作、使用、故障诊断和维护时的风险。经过风险分析后，可以为后续的安全性要求、安全性设计提供改进意见，避免和降低防线，指导制定使用保障安全措施。

### 6.1 风险分析的要求

- a) 风险分析应由无人机及其系统的开发者或用户在系统设计初期进行。
- b) 当系统设计定型，再完成最后的全面的风险分析并保留文件。
- c) 风险分析的步骤：
  - 1) 确定系统危险源和任务阶段；
  - 2) 进行风险评价；
  - 3) 确定降低风险的安全性设计要求和选择使用保障策略类型；
  - 4) 确定风险是否降低到可接受水平。

### 6.2 任务阶段/工作方式

产品飞行时，为了制定无人机操作和功能要求，将整个飞行过程氛围七个飞行阶段，如下文所述。但是在进行FHA时，根据安全性要求，在考虑功能危险时，一些阶段产品实现的功能是相同的，因此可将这七个阶段简化合并为三个阶段，分别为地面、航站和航行。飞行计划阶段与产品功能无关，因而在FHA中不考虑，将启动/地面活动/滑行阶段和着陆后阶段合并为地面阶段，将发射/起航阶段和下降/最后进场/着陆阶段合并为航站阶段，将航行/巡航阶段和空中作业阶段合并为航行阶段。

#### 6.2.1 飞行计划阶段

包括与计划飞行航线、潜在意外事故定位、确定适合的控制和非有效载荷数据链覆盖等等。飞行计划极端包括文件归档和实施飞行计划。

#### 6.2.2 启动/地面移动/滑行阶段

这一阶段始于航空器和地面控制站部分签出，发动机或电源启动、起飞前通讯检查、地面移动，ATC 许可/指令等等。

### 6.2.3 发射/起航阶段

这一阶段始于根据飞行需求提供动力。包括所有的通讯交换，爬升，直到到达初始航行平稳。

### 6.2.4 航行/巡航阶段

包括所有不属于其他飞行阶段的巡航飞行，爬升和下降，直到进入空中作业或下降和到达阶段。

### 6.2.5 空中作业阶段

这一阶段包括除了运送飞机以外的任何飞行活动。例如监视、搜索和营救、重复飞行模式等。

### 6.2.6 下降/最后进场/着陆阶段

始于从巡航高度下降或到达初始进场点。

### 6.2.7 着陆后阶段

着陆后阶段包括起落架发出承重信号，或飞行到达终点之后的所有活动。包括地面移动、滑行、固定无人机、发动机刹车、从无人机项地面控制站部分或地面保障部分，无人机刹车等。

## 6.3 产品失效状态

产品的故障或失效是多旋翼无人机系统一项主要的危险源，对产品硬件的分析需要详细。

将产品的失效状态划分为两类，功能丧失和功能错误。功能丧失是指产品该项功能完全失效，且不可恢复。功能错误是指某项功能的输入、程序逻辑或输出不正常。飞机级功能及其可能考虑的失效状态如表1所示。

表1 飞机级功能及其可能考虑的失效状态

飞机级功能	失效状态
无人机机组与相关人员之间的内部通讯	丧失无人机机组与相关人员之间的内部通讯功能
	无人机机组与相关人员之间的内部通讯功能错误
无人机机组与ATC之间的外部通讯	丧失无人机机组与ATC之间的外部通讯功能
	无人机机组与ATC之间的外部通讯功能错误
无人机飞手与邻近交通中的飞行员的外部语言通讯	丧失无人机飞手与邻近交通中的飞行员的外部语言通讯功能
	无人机飞手与邻近交通中的飞行员的外部语言通讯功能错误
由无人机部分到ATC的外部非语言通讯	丧失由无人机部分到ATC的外部非语言通讯功能
	由无人机部分到ATC的外部非语言通讯功能错误
无人机部分与邻近交通的外部非语言通讯	丧失无人机部分与邻近交通的外部非语言通讯功能
	无人机部分与邻近交通的外部非语言通讯功能错误
与附属服务的外部通讯	丧失与附属服务的外部通讯功能
	与附属服务的外部通讯功能错误
估计位置和方向信息	丧失估计位置和方向信息功能
	估计位置和方向信息功能错误
确定路径	丧失确定路径功能

	确定路径功能错误
估算即时数据	丧失估算即时数据功能
	估算即时数据功能错误
提供无人机飞行控制指令	丧失提供无人机飞行控制指令功能
	提供无人机飞行控制指令功能错误
提供无人机飞行控制反馈	丧失提供无人机飞行控制反馈功能
	提供无人机飞行控制反馈功能错误
提供无人机非飞行控制指令	丧失提供无人机非飞行控制指令功能
	提供无人机非飞行控制指令功能错误
提供无人机非飞行控制反馈	丧失提供无人机非飞行控制反馈功能
	提供无人机非飞行控制反馈功能错误
提供感知和躲避交通的能力	丧失提供感知和躲避交通的能力功能
	提供感知和躲避交通的能力功能错误
提供躲避结构、障碍和地势的能力	丧失躲避结构、障碍和地势的能力功能
	躲避结构、障碍和地势的能力功能错误
提供躲避大气或气象危险的能力	丧失躲避大气或气象危险的能力
	躲避大气或气象危险的能力错误
提供躲避云的能力	丧失躲避云的能力
	躲避云的能力错误
提供躲避未经授权的领空的能力	丧失躲避未经授权的领空的能力
	躲避未经授权的领空的能力错误
提供躲避低于最低能见度区域的能力	丧失躲避低于最低能见度区域的能力
	躲避低于最低能见度区域的能力错误

#### 6.4 影响等级及安全性目标

安全性是风险低于风险边界的状态。因此在判断无人机是否符合安全性，则要为其确定风险边界，即为安全性目标。

衡量风险，需要考虑的两个变量是危害的严重程度以及相应的严重程度的危害发生概率。

##### 6.4.1 失效状态影响等级

在判断失效状态的影响等级前，需要明确其影响的对象：

##### a) 地面非相关人员

指与飞行操作无关的普通人。这一类的对象对于无人机操作、风险等相关知识都不了解。

##### b) 无人机机组

与无人机操作相关的人员，作为飞行机组或发射与复原人员。无人机机组也可以包括任务负载的操作者、任务负载的分析员或技术专家。

##### c) 空域用户

搭乘商业、军事或私人航空器的机组人员或乘客。这一类对象对于有人机的操作飞行等具有较深的认识，但是对于无人机不了解。

##### d) ATC 服务人员

负责航空交通管制的人员或系统。

##### e) 无人机系统



包含硬件和软件部分的整个无人机系统。包括无人机本体、地面控制站、通讯系统和相关设备。  
失效状态根据其影响的严重程度可以划分为：

- a) 无安全影响：失效状态对安全性无影响，如失效状态对无人机使用能力和人员工作及安全无影响。
- b) 轻微的：失效状态对安全性没有显著影响，相关人员的工作也在能力范围内。或者失效状态包括在安全裕度或功能性能方面轻微降低，机组成员的工作负担轻微增加。
- c) 重大的：失效状态会降低无人机性能或相关人员处理无人机不利飞行状态的能力。
- d) 危险的：失效状态急剧降低无人机的性能，大幅度降低相关人员处理不利运行状态的能力。
- e) 灾难性的：妨碍无人机继续安全飞行和着陆，将会导致多人死亡，通常会使无人机坠毁。

“Ⅰ类”表示灾难性影响，“Ⅱ类”表示危险影响，“Ⅲ类”表示重大影响，“Ⅳ类”表示轻微影响。

具体的无人机失效状态影响等级如表2所示：

表2 无人机失效状态影响等级

	对地面上的人的影响	对无人机机组的影响	对空域用户的影响	对航空交通管制（ATC）的影响	对无人机系统的影响
灾难性的	可以导致地面上一人或多人死亡的无人机失效状态	可以导致无人机机组死亡或丧失行为能力的无人机失效状态	可以导致空域用户或乘客经历如下伤害的无人机失效状态：死亡；或空中撞击；或与障碍物或地形发生碰撞；或不能继续安全飞行并着陆的航空器状态	可以导致 ATC 发出的行动造成以下情况的无人机失效状态：与航空器，障碍物或地形发生撞击；或飞行终止失控（如尾流颠簸，或静止不动等等）	无人机系统的失效状态可以导致：失控或不按预期线路飞行；或不可控的地面撞击；或在除了可以恢复的点以外的任意位置发生地面撞击
危险的	会导致地面上的一人或多人重伤的无人机失效状态	会导致无人机机组身体痛苦或工作压力过大（如不能依靠飞行机组准确完整的完成他们的任务）的无人机失效状态	可以导致空域用户或乘客经历如下伤害的无人机失效状态：差点发生空中碰撞；有人航空器采取紧急程序；突然的躲避机动超过了有人航空器的使用阈值；有人机上发生了重伤；身体危难或工作压力过大，减弱了有人机机组人员的任务完成能力	可以导致 ATC 发出的行动造成以下情况的无人机失效状态：距离过近导致的 A 类跑道入侵（RI）或操作失误（OE）；飞行器间的距离减少到标准距离的 22.9%以下	会减弱无人机应对不利的操作条件的能力到以下程度的无人机系统失效状态：安全裕度或功能能力大幅度减弱；计划外不可控的飞行终止；强制无条件尽快着陆
重大的	会导致地面上的一人或多人中等	会导致无人机机组身体不适或工	可以导致空域用户或乘客经历如	可以导致 ATC 发出的行动造成以	会减弱无人机应

	伤害的无人机失效状态	作压力明显增加或削减无人机机组的效率和效果的情况的无人机失效状态	下伤害的无人机失效状态: 重大的飞行员违规 (PD); 采用不正常的程序; 温和的规避机动; 有人机上出现身体痛苦或不严重的伤害; 飞行人员的工作压力剧增, 造成飞行人员效率降低	下情况的无人机失效状态: 距离过近导致的 B 类跑道入侵 (RI) 或操作失误 (OE); ATC 工作压力明显增加; 飞行器间的距离减少到标准距离的 23%-43.9%	件的能力到以下程度的无人机系统失效状态: 安全裕度或功能能力明显减弱; 计划外不可控的飞行终止; 强制按实际情况尽快着陆
轻微的	会导致地面上的一人或多人轻微伤害的无人机失效状态	会导致无人机机组工作压力略微增加的无人机失效状态	可以导致空域用户或乘客经历如下伤害的无人机失效状态: 轻微的飞行员违规 (PD); 有人机的机组人员工作压力轻微增加;	可以导致 ATC 发出的行动造成以下情况的无人机失效状态: 距离过近导致的 C 类跑道入侵 (RI) 或操作失误 (OE); ATC 工作压力中度增加; 飞行器间的距离减少到标准距离的 44%-65.9%;	会导致以下情况的无人机系统失效状态: 安全裕度或功能能力轻微减弱; 计划外不可控的飞行终止; 在合适位置非计划性着陆
无安全影响的	对地面上的人的影响可忽略的无人机失效状态	对无人机机组的工作压力无明显影响的无人机失效状态	可以导致空域用户或乘客经历如下伤害的无人机失效状态: 无安全影响的飞行员违规 (PD); 对航空器操作无安全性影响对有人机的机组人员的影响可忽略; 造成不便	可以导致 ATC 发出的行动造成以下情况的无人机失效状态: 距离过近导致的 C 类操作机动 (OD) 或接近事件 (PE); ATC 工作压力轻度增加; 飞行器间的距离减少到标准距离的 66%以上	对安全性的影响可忽略的无人机系统失效状态

#### 6.4.2 失效状态的定性概率术语

当使用定性的分析来决定

a) 频繁的

指那些预见到在每架无人机的整个寿命期间会发生多次的失效状态。

b) 可能的

指那些预见到在每架无人机的整个寿命期间会发生一次的失效状态。

c) 微小的

指在每架无人机的总的寿命期间内不太可能发生,但是当考虑到该类型无人机的许多无人机的总的运行寿命则可能发生几次。

d) 极微小的

指在每架无人机的总的寿命期间内没有预见到会发生某失效状态,但是当考虑到该类型所有无人机的总的运行寿命时则可能发生几次。

e) 极不可能的

指在某型无人机的所有无人机的整个运行周期不太可能发生。

### 6.4.3 安全性目标

图2为风险矩阵图,该图用于根据危险影响等级和概率等级确定每个失效状态的安全性目标。危险影响等级和概率等级之间存在着一种符合逻辑的可接受的反比关系:

- 无安全性影响的失效状态无概率要求;
- 要求轻微的失效状态的发生概率等级不能超过可能的;
- 要求重大的失效状态的发生概率等级不能超过微小的;
- 要求危险的失效状态的发生概率等级不能超过极微小的;
- 要求灾难的失效状态的发生概率等级不能超过极不可能的,且不能是由单点失效导致的。

影响等级 概率等级	无安全性影响	轻微的	重大的	危险的	灾难的
频繁的	绿色	黄色	红色	红色	红色
可能的	绿色	黄色	红色	红色	红色
微小的	绿色	绿色	黄色	红色	红色
极微小的	绿色	绿色	绿色	黄色	红色
极不可能的	绿色	绿色	绿色	绿色	黄色

注:红色表示高风险,黄色表示中等风险,绿色表示低风险

图2 风险矩阵图

### 6.5 风险评价方法

为了确定危险的风险等级,制定安全性目标,需采用一定的方法进行风险评价。常用的风险评价方法包括功能危险分析,故障树分析,和故障模式、影响及危害性分析。

#### 6.5.1 功能危险分析(FHA)

功能危险性评估是对功能进行系统而全面的检查,以确定这些功能的失效状态并按其严重性进行分类的过程,是无人机设计或改进过程中安全性评估的第一步。该评估方法起始于无人机概念设计阶段,并为后续研制提供设计需求和安全性需求的重要依据。FHA分析结果是下一步安全性评估流程(如PSSA和SSA)的必要输入,也为后续系统、子系统设计构架提出安全性设计需求,帮助确认系统架构的可接受性,发现潜在问题和所需的设计更改,确定所需进一步分析的需求范围。FHA通常在两个级别上进行,分别为无人机级FHA和系统级FHA。

FHA过程是一种自上而下识别功能失效状态和评估其影响的方法,应按照如下过程进行评估工作:

- 确定与分析层次相关的所有功能
- 确定并说明与这些功能相关的失效状态,考虑在正常和恶化环境下的单一和多重失效;
- 确定失效状态的影响;

- d) 根据失效状态对其进行分类（灾难性的、危险的、重大的、轻微的和没有安全性影响的）；
- e) 给出用于证明失效状态影响分类所要求的支撑材料
- f) 提出用于验证失效状态满足安全性需求的符合性验证方法。

### 6.5.2 故障树分析（FTA）

风险分析中的故障树分析方法一般用于当确定了灾难性的系统故障后，以该故障为顶事件，通过由上向下的严格按层次的故障因果逻辑分析，逐层找出故障事件的必要而充分的直接原因，最终找出导致顶事件发生的所有原因和原因组合。在具有基础数据时计算出顶事件发生概率和底事件重要度，安全性目标等定量指标。

FTA在安全性分析中的应用步骤如下：

- a) 系统定义；
- b) 确定故障判据；
- c) 确定顶事件；
- d) 建造故障树；
- e) 故障树规范化、简化和模块分解；
- f) 定性分析；
- g) 定量分析，确定各层级设备安全性目标。

### 6.5.3 故障模式、影响及危害性分析（FMECA）

利用FMECA方法，识别安全性分析中所有可能的故障模式、发现故障危险源、分析可能产生安全性影响、确定危险的严重性和可能性（即风险），消除或控制有危险故障安全性关键产品，制定有效改进措施，以提高产品的安全性水平。

FMECA在安全性分析中的应用步骤如下：

- a) 系统定义，包括危险严重性等级和风险指数分类的定义；
- b) 故障模式分析；
- c) 故障原因分析；
- d) 故障影响分析；
- e) 故障检测方法分析；
- f) 发生概率等级分析；
- g) 危险严重性分析；
- h) 确定风险指数；
- i) 改进与补偿措施分析；
- j) 完成安全性分析报告。

## 7 安全性设计

### 7.1 安全性设计要求

应进行最小风险设计，消除危险或将风险降低到可以接受的程度。安全性设计的一般要求有：

- a) 通过设计消除已判定的危险或降低风险；
- b) 应尽量减轻事故中人员的伤害和设备的损坏；
- c) 必须消除 I、II 级危险；
- d) 危险物质及其操作应该注意隔离；

- e) 设备的位置安排应使工作人员尽量避免危险；
- f) 采用机械隔离或屏蔽的方法保护冗余分系统；
- g) 应尽量减少人为差错所导致的危险；
- h) 应尽量减少恶劣环境条件所导致的危险；
- i) 不能消除的危险，应考虑采取补偿措施；
- j) 当不能通过设计消除危险是，应给出警告和标记；
- k) 应重视系统中软件可能带来的危险；
- l) 对设计准则进行评审。

在实际的安全性设计过程当中，要有重点、有针对性、持续地采取安全性措施，消除危险或降低危险。才去的安全性措施的优先次序一般为：

- a) 最小风险设计：首先在设计上消除危险，若不能消除已判定的危险，应通过设计方案的选择将其风险讲到订购方可接受水平；
- b) 采用安全装置：采用永久的、自动的或其他安全装置，使风险减少到订购方可接受水平，并且应规定对安全装置做定期的性能维护；
- c) 采用告警装置：采用告警装置来标示或检测危险，并向有关人员发出适当的告警信号

## 7.2 多旋翼无人机系统避障设计

针对无人机实际飞行可能遇到的地形障碍、建筑物障碍、移动障碍等进行避障的软硬件系统设计。

## 7.3 多旋翼无人机系统通讯安全设计

保障无人机与地面站的通讯链路的准确畅通。

## 7.4 多旋翼无人机系统飞行安全设计

包含无人机的飞行策略，迫降策略，应急策略等。

## 7.5 多旋翼无人机系统操作安全说明

针对无人机飞手制定无人机系统的操作要求。

---