# 总论

## 概念

### 安全

不发生可能造成人员伤亡、职业病、设备损坏、财产损失或环境损害的状态。

安全是一种客观状态。安全性是一种保证事物处于安全状态的能力。

### 安全性

保证己方人员、设备、设施、财产、环境等免于遭受灾难事故或意外损失的特性，这种特性就是其安全性。

**产品具有的不导致人员伤亡、装备损坏、财产损失或不危及人员健康和环境的能力。（GJB900A-2012《装备安全性工作通用要求》）**

### 安全性工程

·应用工程技术和管理方法，以系统使用效能为目标、以时间、费用、技术水平等为约束，在全寿命周期各个阶段对系统的安全特性进行优化，使其达到可接受的事故风险水平。

·ALARP原则

### 安全性工程的本质

核心：危险/事故

宗旨是：在合理可行的范围内追求最低事故风险

研究对象：系统中各种可能的危险。

应用系统工程手段解决装备的安全性问题

“系统”的“安全特性”

变被动为主动

### 安全性工作与其它工作的接口关系

**设计工程**：对装备安全性影响最大的是设计工程。

**人素工程**：研究装备与人的接口，防止由于人的原因造成事故，消除由于不适应人员的要求而造成的职业病和伤亡。

**可靠性工程**：要全力找出影响安全的故障，分析其安全性后果，提出改进措施和建议。

### 安全性与可靠性

#### 传统观点：

安全性与可靠性互相交叉，在通常情况下，可靠的产品也就意味着安全的产品；但在有些情况下，可靠的未必是安全的，安全的也未必是可靠的。

有些学者认为：安全性是从可靠性引申而来的。

#### 个别观点：

安全是从最终结果是否造成损失来判断的，可靠则是从是否完成功能的角度来判断的。

安全性应从整个系统的层面来研究，可靠性则可以在任何一个层面（主要还是在系统内部）。

故障是可靠性的终点，安全性的起点。

# 15类危险

## 概念

“危险”是安全性工程研究的对象。

**危险**：可能导致事故的状态。

**事故**：造成人员伤亡、职业病、设备损坏或财产损失的一个或一系列意外事件。

危险和事故是同一现象的两个不同阶段，危险代表一种可能性，事故则是一系列事件的最终结果。



### 危险三要素

#### 危险物质（Hazard Element）；

指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。

#### 触发机制（Initiating Mechanism）；

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。

#### 危害目标（Target and Threat）

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。

### 危险源

有许多危险源（危险因素）直接或间接威胁着人员、装备本身以及周围环境。武器装备涉及的危险源包括：环境、加速度、污染、辐射、电击、着火、爆炸、温升、毒物、振动、冲击等等，包含了人们目前所认识的全部危险源。它们均是一种潜在的危险，在一定条件下将引发事故。

所谓危险源，是引发危险的根本原因，它们通常来源于：

* + **物质或产品固有的危险特性（如能量或毒性）**
  + **有害的环境**
  + **产品（硬件或软件）的故障或失效**
  + **人员行为失误（包括由心理、生理等因素所引起的行为失误）**

产品固有的危险特性包括：

* + **产品中或产品使用的材料中的固有危险；**
  + **设计缺陷；**
  + **制造缺陷。**

一般而言，设计问题是上述诸因素中最重要的方面。

* + **设计人员不仅可能在设计产品时引入了设计缺陷，形成产品自身的危险，还可能缺乏正确控制产品及其材料中危险的能力。**

制造缺陷一般由不正确的生产工艺造成，但某些情况下，设计人员也应对此负责。

### 危险分类

#### 第一类危险源

系统中存在的、可能发生意外释放的能量或危险物质称作第一类危险源

#### 第二类危险源

导致约束、限制能量的措施失效或破坏的各种不安全因素称为第二类危险源。（人、物、环境）

#### 共同作用

* 一起事故的发生往往是两类危险源共同起作用的结果。
  + 第一类危险源的存在是事故发生的**前提**，没有第一类危险源就谈不上能量或危险物质的意外释放，也就无所谓事故。
  + 另一方面，如果没有第二类危险源破坏了第一类危险源的控制措施，也不会发生能量或危险物质的意外释放。第二类危险源的出现是第一类危险源导致事故的**必要条件**。

#### 内在危险

**由系统内因造成的。主要源于以下几个方面：**

* + **系统故障，属于系统的特定状态（如电线的交叉连接）；**
  + **物理危险，这些危险总是存在于系统中（如热表面、锐边等）；**
  + **功能故障，通常需要有触发事件的存在（如部件或者设备故障）；**
  + **人为故障，如控制错误、维护错误、监控错误等，可以有或者没有功能故障。**

#### 外在危险

**有系统外部影响造成的。主要原因有：**

* + **物理原因（如天气）；**
  + **同等平台（如其它飞机）；**
  + **人（如破坏、劫机等）**

#### 设备故障与缺陷

* + **主动故障与被动故障**
    - 主动故障指的是造成直接不利影响的故障（如发动机的功能丧失或者性能下降）。
    - 被动/潜在/隐蔽故障。例如系统的某条通道中可能存在缺陷，但系统仍能运行，但是所存在的故障是不可检的。
  + **显性故障与非显性故障**
    - 数字技术应用下的主动/被动故障
  + **独立与非独立故障**
    - 独立的主动故障与被动故障的组合往往是危险的。
    - 实际系统中的故障往往是非独立的。
    - 共因/共模问题或级联影响
  + **损耗与随机故障**

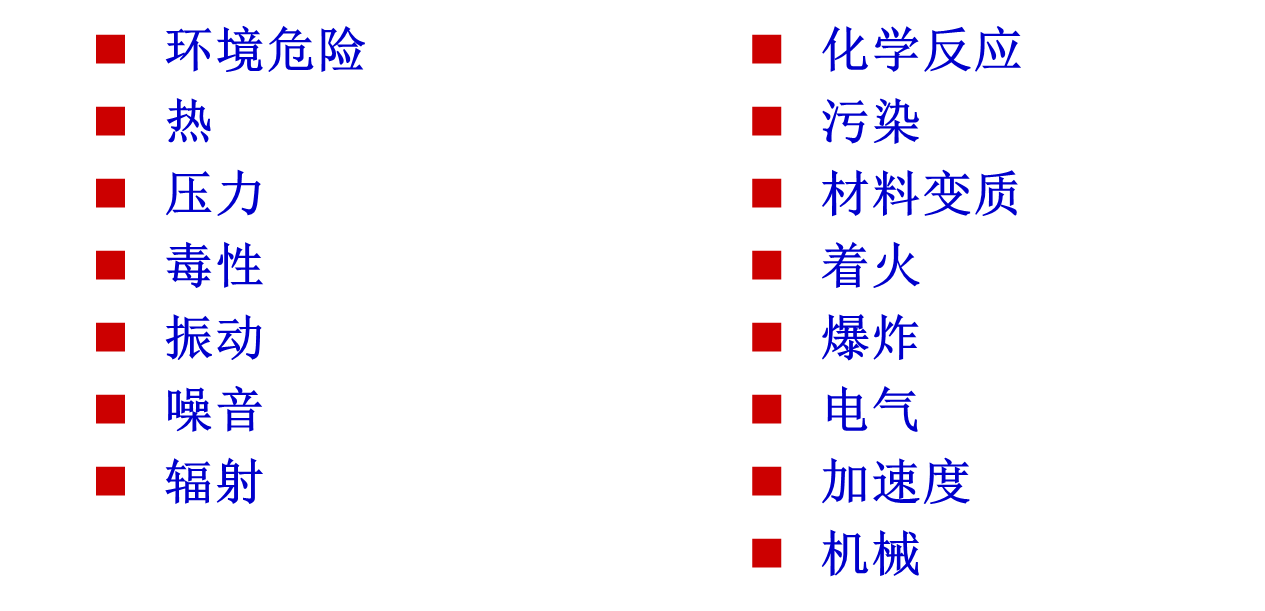
### **安全忍受极限**

·忍受极限是大多数人能够忍受某一危险源能量而不产生有害效应的极限值。

·安全忍受极限是使最敏感的人能够忍受而不产生有害效应的极限值，通常是忍受极限再加上一个安全系数。

## 15种常见的危险

GJB/Z99中按照物理现象划分，给出了15种常见的危险：



# 14种合计原则

# 5种分析工作

# 2种分析技术

FHA