# 总论（Chapter 1）

## ！！！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。

**维修性工程：**在产品设计中，保证产品不会由于保养和修理不当、装配的差错而引起事故；保证所设计的硬件不会因为正常的维修作业而伤害维修人员。

**试验工程：**对试验过程进行安全性分析，鉴别试验过程中可能出现的危险，并采取相应措施。

**制造工程：**制造人员除了控制执行制造工艺本身的安全外（如焊接安全、机床操作安全），必须了解与安全性有关的零部件，防止制造上的差错导致在生产和使用时发生事故。

**工业卫生与保健 ：**人员健康，职业病防控。

**质量检验和控制**：质检部门要防止和尽量减少生产有安全性缺陷的产品。

**维修工程**：维修人员应保证所制定的装备维修计划在实际执行时符合安全性要求。

装备使用和维修人员的教育：操作、维修规程的教育，教育受训者熟练掌握要领，防止事故和减少损失。

**包装、贮存和运输**

### 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（Chapter 2）

## 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**

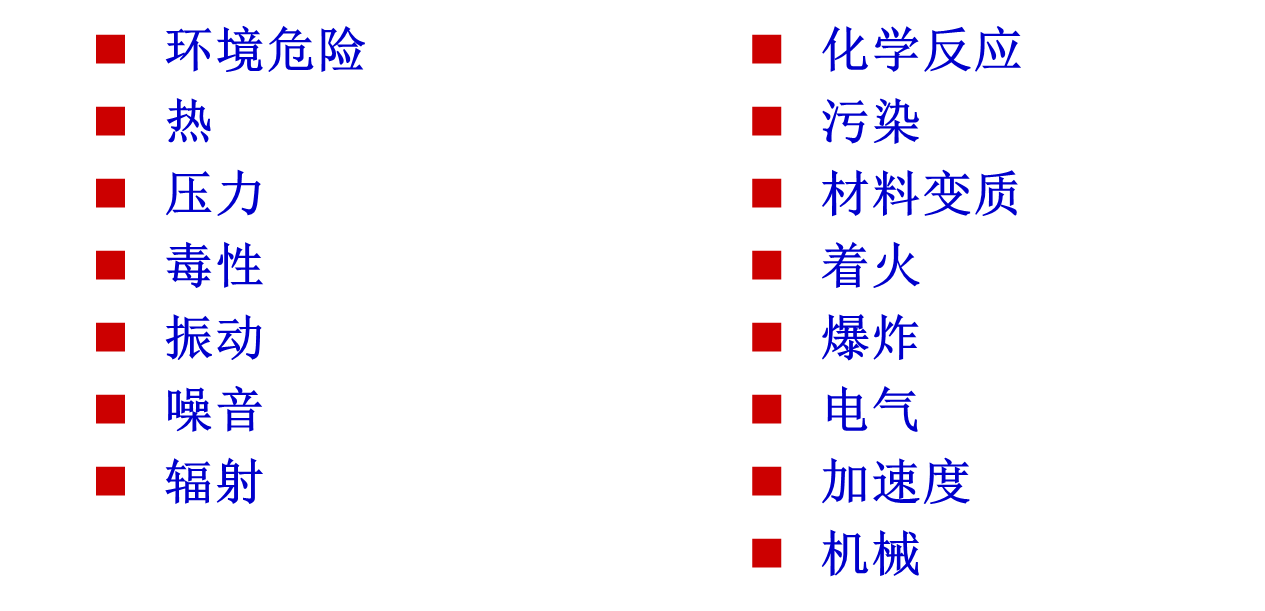
### **安全忍受极限**

·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：



# 安全性工程管理（Chapter 3）

安全性工作标准：GJB900A-2012“装备安全性工作通用要求”

安全性工作是一个迭代过程，随着研制工作的开展而不断深入。特别**危险分析、风险评价、设计改进、措施验证**等工作，需要反复迭代才能达到最优方案。

要注重安全性基础数据的收集整理和利用，它是所有工作的基础。

## 安全性工作的目标和要求

根据任务要求开展安全性设计；

在系统寿命周期内消除系统中的危险，或将其风险降低到可接受的水平；

考虑并应用以往的安全性资料；

在采用新技术新材料时，寻求最小风险；

尽可能在论证、设计、研制中考虑各种安全特性，尽量减少使用中为改善安全性进行的改装；

在寿命周期的早期考虑系统的安全性及危险器材的处置；

在技术更改时应控制风险；

安全性信息、资料收集整理和管理。

## ！！实施安全性工作的要点

**建立健全安全性组织机构。**开展安全性工作，必须要有健全的安全性机构，这是开展安全性工作最基本的条件。

**强调安全性设计的重要性。**

**危险分析是安全性工作的核心。**进行安全性设计需要确定存在的危险，这就依赖于各种危险分析。

**安全性工作计划是开展安全性工作的关键。**有效的安全性工作的实施，必须靠良好的工作计划予以保障，安全性工作计划是安全性工作中最重要的文件，它决定了安全性工作的广度和深度。

**信息是安全性工作的基础。**

## 完整的安全性过程

收集和评审经验教训

明确系统的定义

系统危险分析（核心步骤）

确定危险

危险的分类和评估

消除或控制危险的措施（关键步骤）

系统组成部分的修改

所采取措施的效果评估

偶然事故或差错分析

系统及其组成部分的试验和验证

记录成文

## 安全性工作总体策划

安全性管理的职能是计划、组织、监督和指导，管理的对象是系统寿命周期内与安全性有关的所有活动，但重点是研制过程中的设计、分析和验证。

**最核心的工作是制定安全性计划和安全性工作计划。**

# 安全性设计（Chapter 4）

安全性设计是指在系统（或装备）研制过程中，通过各种设计活动来消除和控制各种危险，其目的在于防止所设计的系统在研制、生产、使用和保障过程中发生导致人员伤亡和设备损坏的各种意外事故，提高系统的安全性。

通过分析发现问题，通过设计解决问题。

安全性设计是保证系统**满足**规定的安全性**要求**最关键和有效的措施。

## 安全性要求

安全性要求应该物理含义明确，可检查、可验证。目的是为了影响设计，提高装备的安全性水平。

·先进性

·可行性

·经济性

·合理性

·针对性

### 定性要求

定性要求是订购方从产品的使用效能和使用适应性出发，为保证产品的安全性而对产品的设计提出的技术要求和具体的设计原则，包括风险接受准则。

### 定量要求

针对特定损失事件或事故后果发生的概率（或频率）提出的定量要求，也就是“**安全性指标**”。

**具有特定的对象和指定的事故后果；**

**以风险或概率为度量参数；**

**以“可接受（或不可接受）水平或范围”的方式表述。**

目前比较普遍采用定性定量相结合的安全性要求，即**风险评价指数判别准则**。

## 安全性设计思路和方法（14种设计原则）

危险三角形：危险物质、触发机制、威胁目标。

根据采取安全性措施的优先顺序，安全性设计思路和方法大致可包括14种。

### 控制能量

基于“任何事故影响的大小直接与所含能量有直接关系”的原理。

这是设计一个安全系统必须做出的最大努力。

应考虑能源的类型以及能量的转移或转换的速度/大小。

### 固有安全性设计

固有安全性是产品设计所赋予的安全性，进行固有安全性设计是避免事故发生的最有效方法。

1、通过设计消除危险；

2、控制危险严重性。

### 隔离

隔离是最常用的安全性措施。

### 闭锁、锁定和联锁

**闭锁**防止某事件发生或防止人、物进入危险区域；反之，**锁定**保持某事件或状态，或避免人、物等脱离安全的限制区域。

**将开关锁在开路位置，防止电路接通（造成意外启动）是闭锁；**

**将开关锁在闭路位置，防止电路切断（造成意外断电）称为锁定。**

**联锁**装置规定了事件发生的次序，从而避免事件的意外组合。电气设备常采用联锁装置。

安全装置应设置联锁，使安全装置被旁路时设备不工作。

### 概率设计和损伤容限（对机械结构）

机械结构常采用安全系数法，使结构或材料的强度远大于可能承受应力的计算值

从统计学来说，应力和强度的分布曲线永远相交，但在实际工作中，**当最小强度大于最大应力时，认为它们不会相交，该产品存在安全裕度。**安全裕度可表示为最小强度与最大应力之比，或应力不超过屈服强度的90%的状态。

**损伤容限**是指结构在规定的无维修使用期内，能够**耐受**由缺陷、裂纹或其他损伤引起的**破坏而不损害使用安全的能力**。

### 降额（对电子元器件）

使电子元器件以承受低于其额定值的应力方式使用。相当于机械设备采用安全系数法。

实现降额的方法是降低元器件的工作应力，或提高元器件的强度。

### 冗余

采用冗余设计时应注意防止共因（模）故障

* 共因故障
  + **由于同一个原因导致系统内多个部件同时发生故障的现象。如果多个同时故障的部件的故障模式相同，则称为共模故障。**
* 确保备份之间的独立性是关键
  + **相异和隔离**

### 状态监控

**监控装置的工作必须具有最高的可靠性水平。**

### 故障-安全

* + **故障-安全设计确保故障不会影响系统安全，或使系统处于不会伤害人员或损坏设备的工作状态。**
  + **故障-安全设计要保证：**
    - **保护人员安全；**
    - **保护环境，避免引起爆炸或火灾之类的灾难事件；**
    - **防止设备损坏；**
    - **防止降低性能使用或丧失功能。**

往往和状态监控相结合

#### 故障-安全消极设计

当系统发生故障时使系统停止工作，并且将其能量降低到最低值，系统在采取纠正措施之前不工作，而且不会由于不工作而是危险产生更大的损坏。如用于电路或设备保护的保险丝或断路器。

#### 故障-安全积极设计

在采取纠正措施或启动备用系统之前，使系统保持接通并处于安全状态。采用备用冗余设计通常是故障-安全积极设计的组成部分。如红绿灯系统发生故障时，信号转换成红灯亮。

#### 故障-安全工作设计

能使系统在采取纠正措施前继续安全工作。这种类型最可取。阀门不同使用方式就能达到故障-安全工作设计的目的。

### 告警

* + - **视觉告警**
    - **听觉告警**
    - **嗅觉告警**
    - **触觉告警**
    - **味觉告警**
  + **在某些关键情况下，常同时采用视觉和听觉等类告警。**

### 标志

* + **标志是一种很特殊的目视告警和说明手段，是最常用的告警方法。**

### 损伤抑制

* + **必须采取各种可能抑制损伤的的方法，尽可能保证即使发生了事故，人员和设备仍可免受损伤。**

### 逃逸、救生与营救

* + **逃逸和救生是指人们使用本身携带的资源自身救护所作的努力。营救是指其他人员救护在紧急情况下受到危险的人员所作的努力。**
    - **核心是逃逸和救生设备/营救设备**

逃逸、救生和营救对于所需的场合来说是极为重要的，但只能作为最后依靠的手段来考虑和应用。

### 薄弱环节

所谓薄弱环节指的是系统中容易出现故障的部分，它将在系统的其它部分出故障并造成严重的设备或人员伤亡之前发生故障，因此可以利用薄弱环节来限制故障、偶然事件或事故所造成的损伤。

## 方法总结

* 控制能量、消除和控制危险：最根本的原则；
* 隔离、闭锁/锁定和联锁、概率设计和损伤容限、降额、冗余：避免发生事故的手段，通常属于保护装置；
* 状态监控、故障-安全：在无法避免危险时，尽量避免损失，事故前；
* 告警、标志：对危险或事故的提示；
* 损伤抑制、逃逸/逃生和营救：事故后尽量降低损失的手段；
* 薄弱环节：很特殊但又很有效的方法。

## 安全性验证

### 安全性验证的目的：

在寿命周期内检验产品中安全性关键的硬/软件、规程是否符合产品规范和安全性要求，即**装备及其组成部分是否达到合同规定的安全性水平**，能否安全地执行规定的功能和能否按规定的方式安全使用；同时**对采取对采取的安全性措施的有效性和充分性进行确认**，从而保证安全性确实已设计和制造到系统中。

### 验证方法：

试验、演示、检查、分析

安全性验证应首先考虑采用试验和演示的方式

## 安全性评价

* 根据已作的安全性工作和已知条件，对产品风险水平进行估计。
  + **其目的是在产品转入下一工程阶段、进行试验及交付前，对产品的安全性或风险水平进行综合评价。**

# 安全性分析（Chapter 5）

安全性分析也可以称为危险分析，它是安全性工程的核心内容，是安全性设计、评价的基础。

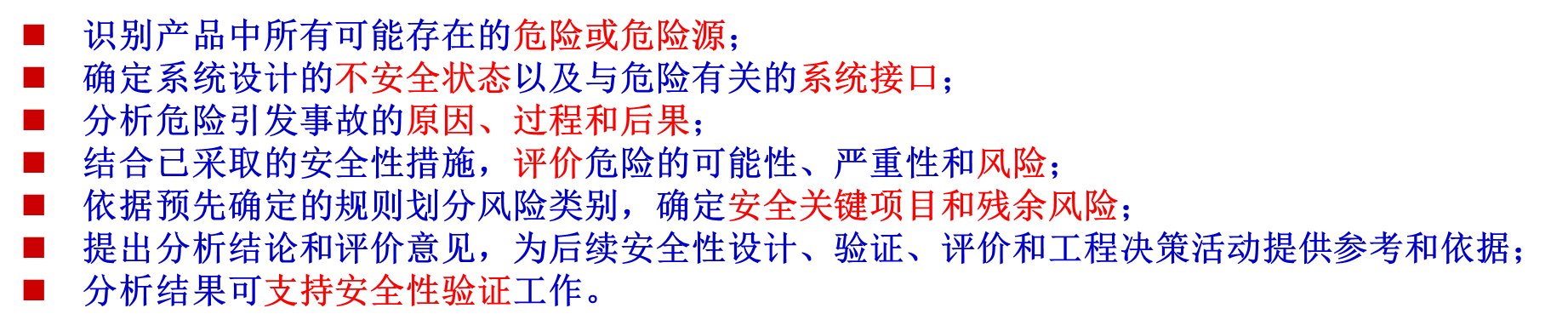
确定潜在的危险，估计这些危险对人员伤害、设备损坏或环境破坏的严重性和可能性

**安全性分析应从研制阶段早期开始并贯穿整个寿命周期。**

## 目的

识别危险，评价事故风险，以便在寿命周期的各个阶段中消除或控制这些危险。

## 作用

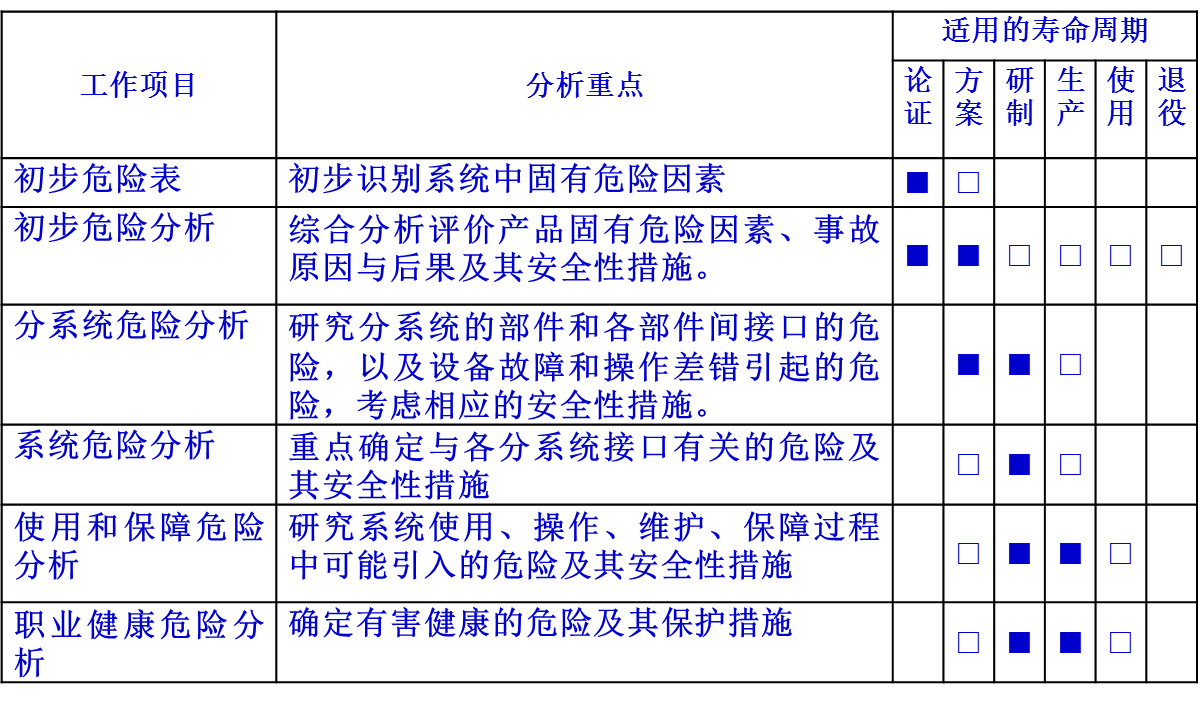


## 安全性分析基本流程

* 在不同阶段，由于可获取的数据及信息的不同，安全性分析的重点也有所不同。
  + **论证阶段和方案阶段初期，安全性分析重点在于考察产品固有危险特性，即识别分析第一类危险源；**
  + **方案阶段后期和工程研制阶段，安全性分析的重点是第二类危险源，对故障、接口以及产品使用操作等有关的危险进行全面分析和综合评价。**



## 研制各阶段安全性分析工作（ 初步危险表+5种分析工作）



### 论证阶段安全性分析

重点开展的安全性分析工作有：编制初步危险表（PHL），开展初步危险分析（PHA）

### 方案阶段安全性分析

在该阶段的安全性分析工作主要有：

·进一步修改完善PHA，修订安全关键项目；

·对设计进行详细的**分系统危险分析（SSHA）**，以评价产品的硬件或软件试验中的风险；

·如条件允许，进一步开展**系统危险分析（SHA）**

### 工程研制阶段安全性分析

在安全性分析工作方面，此时的装备研制已具体化，应分析实际的硬件和软件产品，考查整个产品实际的接口，对前期的SSHA和SHA进行补充完善。

还应开展**使用与保障危险分析（O&SHA）**和**职业健康危险分析（OHHA）。**

## ！！常用的安全性分析方法

安全性分析包括定性分析和定量分析。

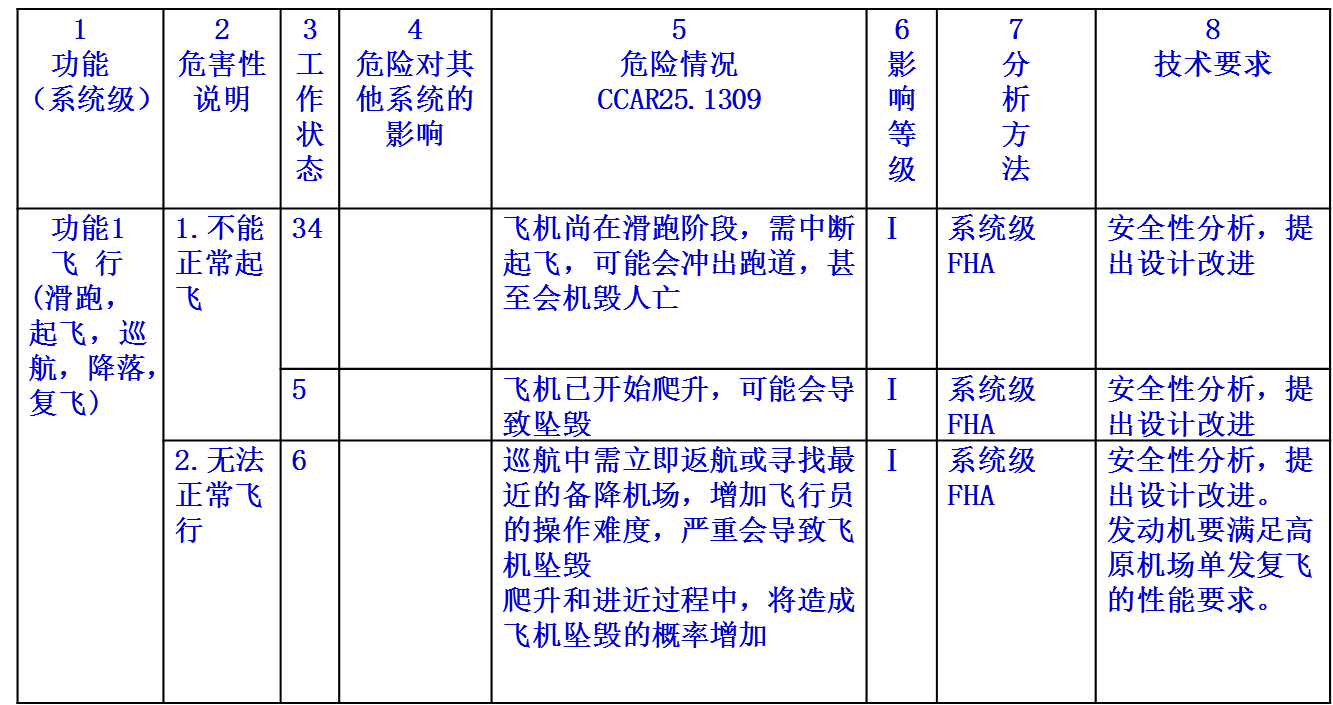
**定性分析**用于检查、分析和确定可能存在的危险、危险可能做成的事故、以及可能的影响和防护措施。

**定量分析**用于检查、分析并确定具体危险、事故及其影响可能发生的概率，比较装备采用安全措施或更改设计方案后概率的变化。**定量分析必须以定性分析作为依据**

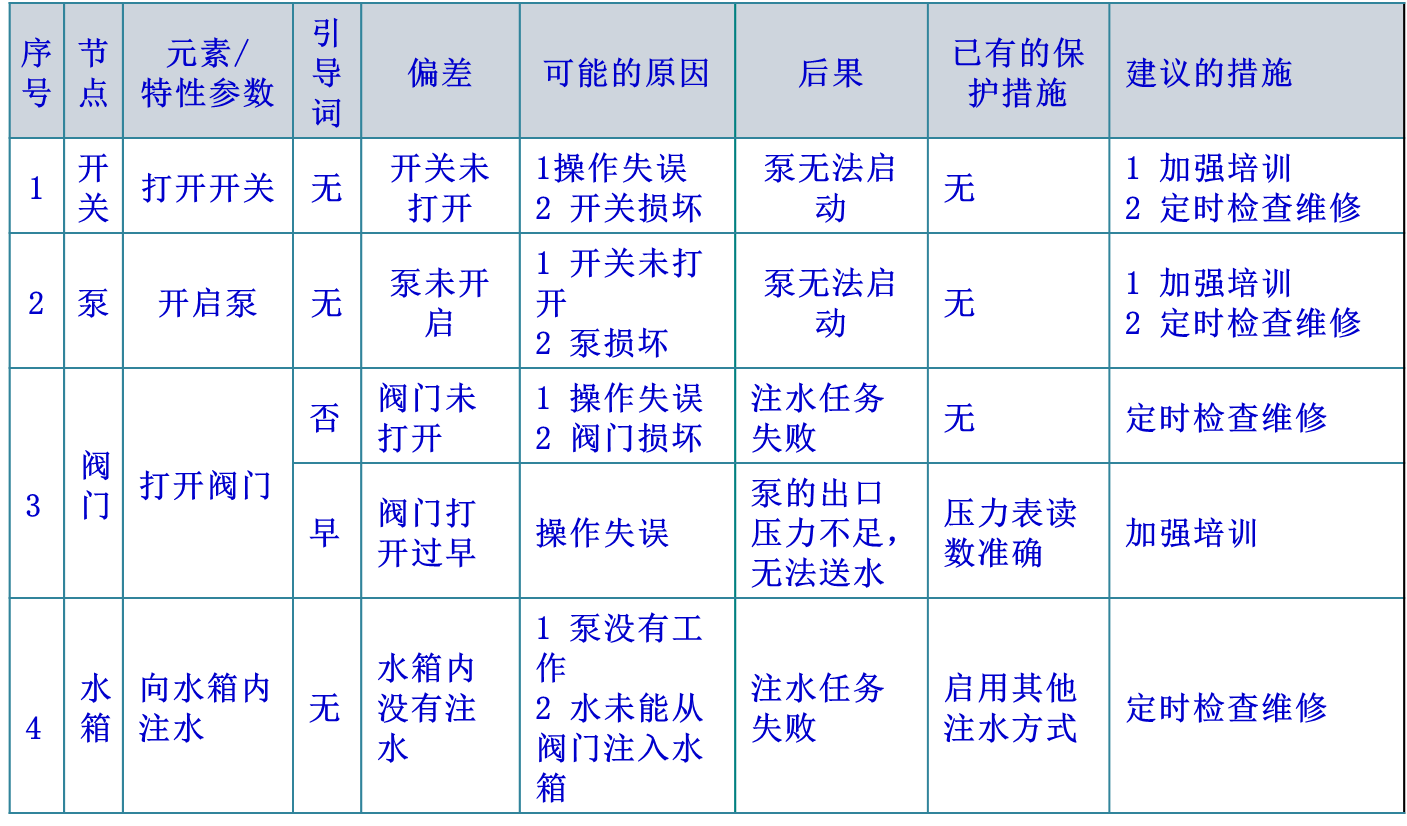
### 能量跟踪与屏蔽分析法ETBA

### ！！功能危险评估法（FHA）

见软件安全性复习讲义



### 危险与运行分析法HAZOP



### ！！区域安全性分析法ZSA

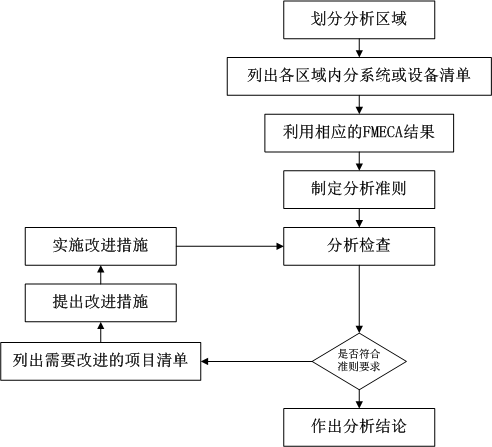
通过区域划分的方法对组成系统的分系统或设备及其接口的安装位置进行系统地分析和连续地检查，评价在故障和无故障情况下各分系统或设备潜在的相互影响以及其安装存在的固有危险的严重程度。

ZSA是一种定性的分析方法，主要用于：

**1、评价各分系统和各设备之间的相容性**

2、确定系统各区域及整个系统存在的危险并评价其严重程度

ZSA的主要优点是分析较简单、直观性好，但要求分析人员对系统的设计、安装及使用有丰富的经验。



#### ZSA的分析准则分为

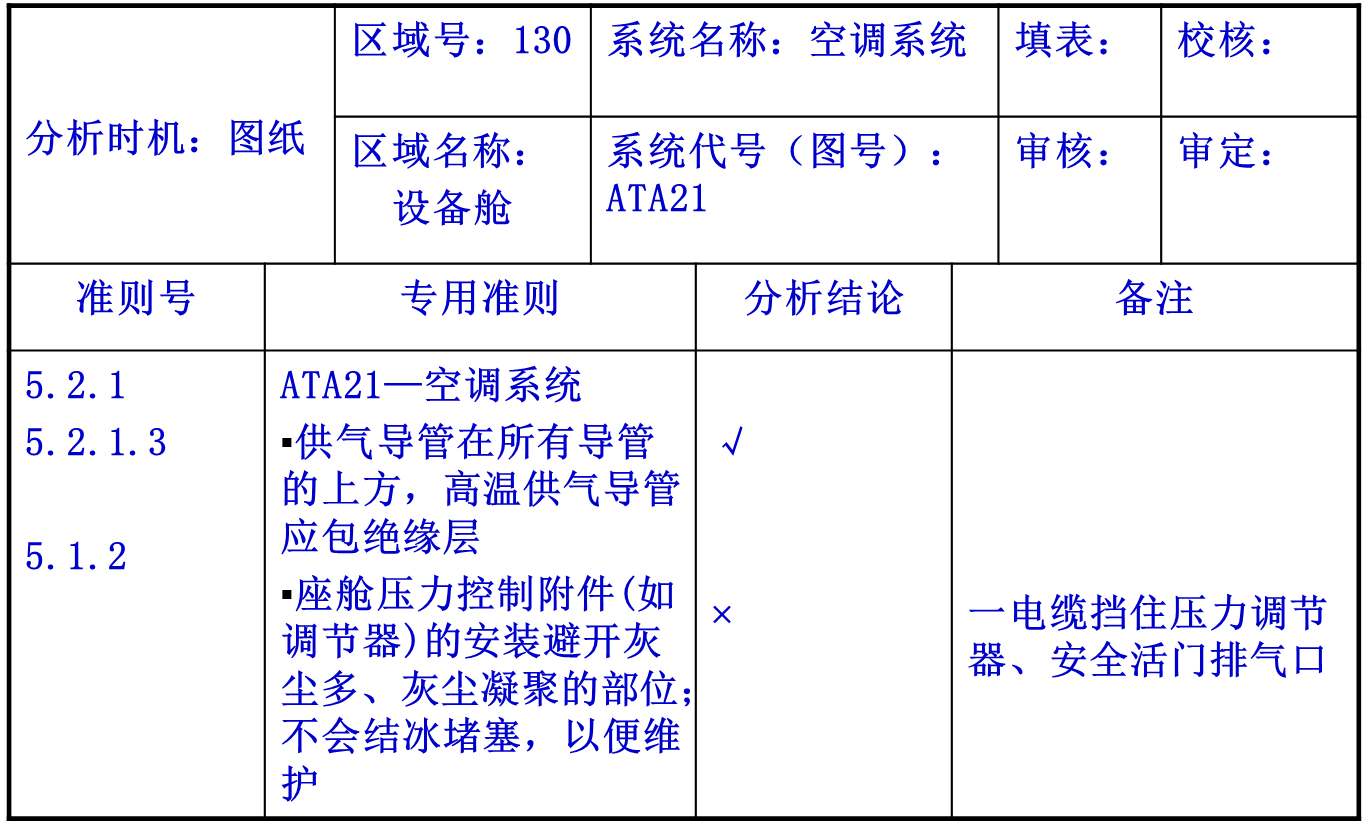
##### 通用准则

通用准则规定了在系统和设备的安装、互相影响、维修及环境等方面，在区域内各系统、设备均应满足的要求(安全性)，具有共性。

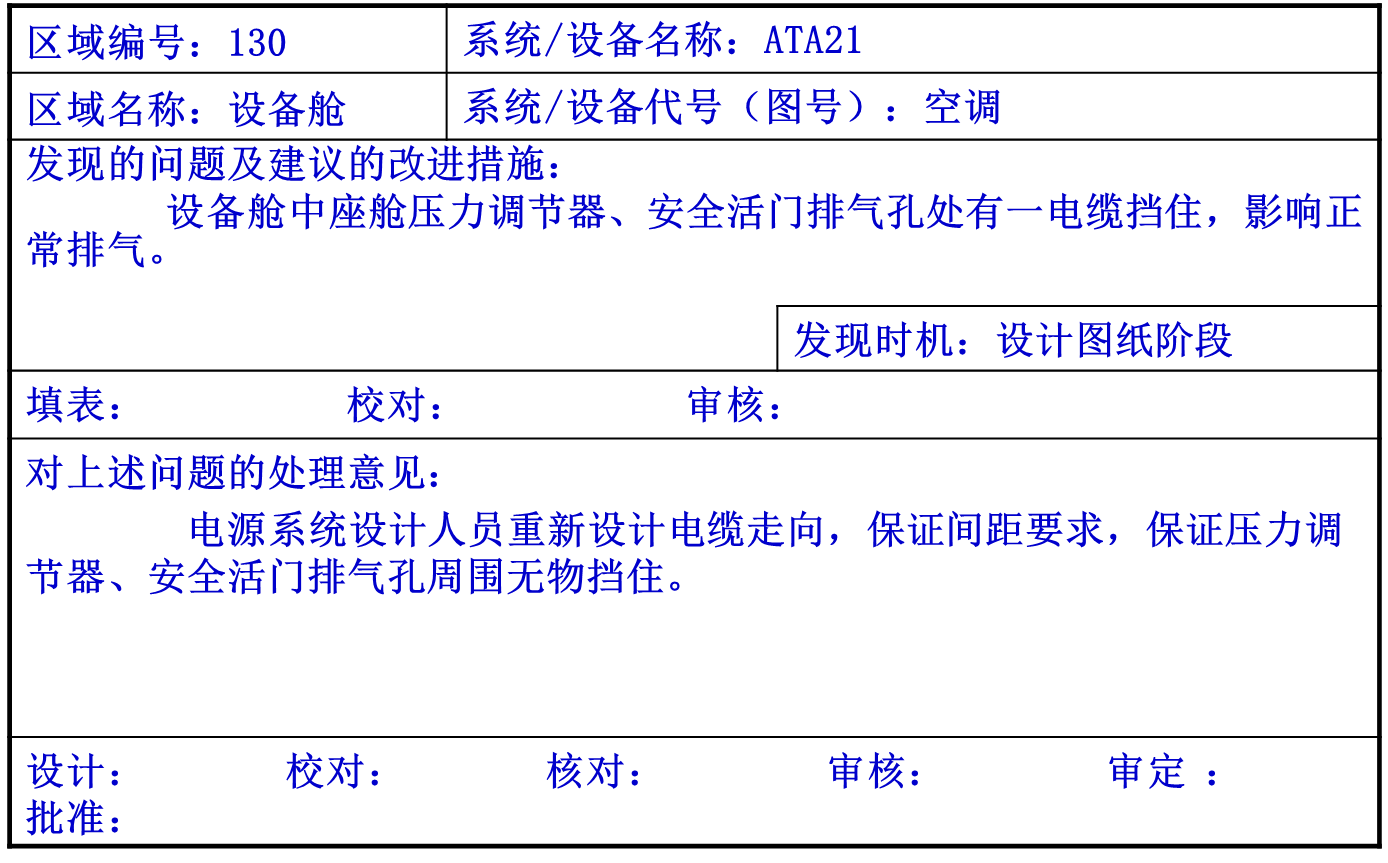
##### 专用准则

以系统、设备为对象，根据其特点，提出在其所经过的各区域内考虑本系统与其他系统/设备之间在安装、相互影响、维修环境及功能等，应满足的有关具体要求

#### ZSA记录表



#### ZSA问题登记表



# 风险评估与安全性验证

## 风险的特点

客观性

主观性

普遍性

社会性

不确定性

可测定性

发展性

## 风险管理流程

系统安全工作如何开展？

**安全---危险---风险**

安全首先是一个管理问题，安全管理也就意味着风险管理。

所有的安全性分析方法都隐含着风险管理流程

* 风险管理流程类似于质量管理中的PDCA循环，是一种迭代的闭环过程。包括：

### 风险规划

确定一套完整全面、有机配合、协调一致的**风险管理策略和方法**，并将其形成文件的过程

### 风险评估

它是风险管理工作中的“查找问题”阶段，包括：风险识别、风险分析和风险排序。

#### 风险识别

识别危险（源）

#### 风险分析

考察已辨识出的危险，查找原因，并用概率和后果表征其影响

#### 风险排序

便于决策

### 风险处理（风险决策）

风险处理是指采取各种管理手段、方法和技术去处理解决已知的风险。

降低事故发生的可能性或减轻危害程度

### 风险监控

一方面是通过风险规划、辨识、估计、评价、处理全过程的监视和控制，从而保证风险管理能达到预期的目标。

另一方面是对决策落实情况进行监控，形成**闭环迭代管理**。

## 风险的定性估计

* 风险评估指数（Risk Assessment Code，RAC）法是最常用的定性风险评价方法。

## 风险的定量估计

* 重点是对可能性的估计，也就是发生概率的估计。