



## 7.4 故障危害与安全评估



### 本章目录

## 故障危害与安全评估

### 第七章 健康管理与安全评估

7.1 健康管理与安全评估基础

7.2 统一故障建模框架

7.3 虚实安全强化与故障数据方法

**7.4 故障危害与安全评估**

7.5 故障诊断与健康预测

7.6 安全决策与整机改进

7.7 故障注入接口与算法开发框架

7.8 例程实验与虚实验证

7.9 习题与课堂讨论

### 本节 4 个教学单元

#### 7.4.1 场景与危害

教材对应：第7.1.2.2、7.1.2.4节

#### 7.4.2 安全分析方法

教材对应：第7.1.2.2、7.1.2.4节

#### 7.4.3 可靠性与任务指标

教材对应：第7.1.2.4节

#### 7.4.4 风险排序与设计改进

教材对应：第7.1.5.3、7.1.2.5节



### 7.4.1 场景与危害：健康与安全

## 飞得稳、能巡检、风险可接受是三个判断

贯穿设定：单电机效能降至正常的70%，其余条件不变；健康与安全的区分见课件7.1。

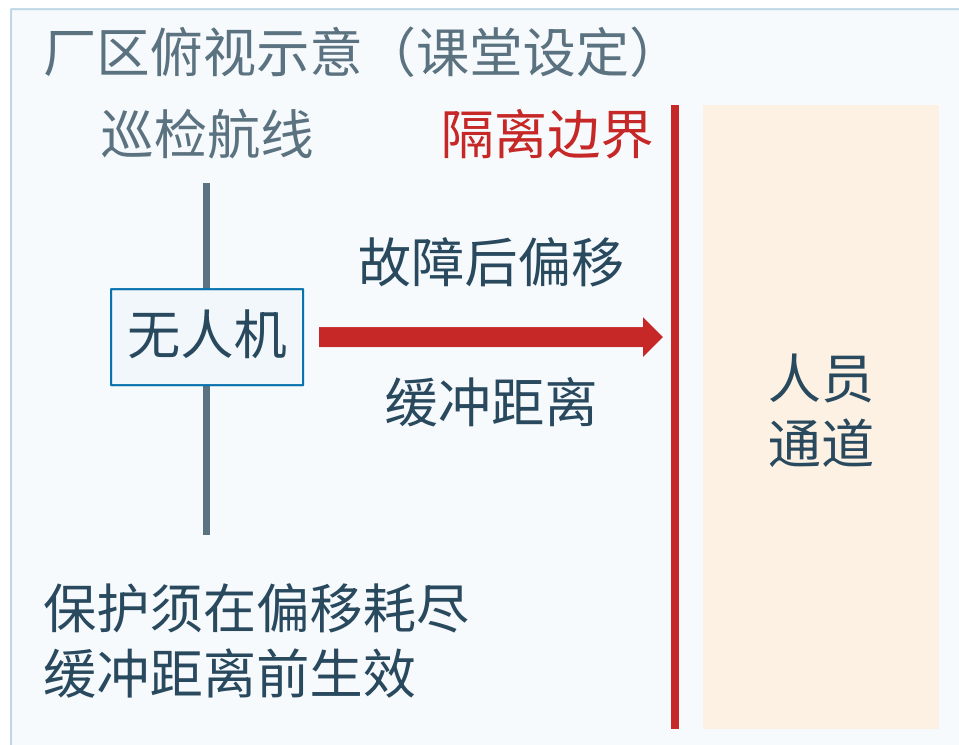
| 判断对象 | 具体看什么                | 巡检案例                    |
|------|----------------------|-------------------------|
| 健康状态 | 部件状态和性能是否偏离正常        | 电机效能下降；<br>控制补偿可能掩盖运动异常 |
| 任务能力 | 约束内能否获取合格巡检结果        | 能否保持航迹、拍清目标并返航          |
| 安全性  | 人员、设备与环境的风险<br>是否可接受 | 偏航、降落是否伤人<br>或损坏设施      |

故障大小描述部件，危害大小还取决于任务与环境。

## 7.4 故障危害与安全评估

### 7.4.1 场景与危害：运行场景

### 相同的推力下降，场景改变后果



#### 空旷试验场

**后果：**航迹偏差、任务中止，可受控降落

**条件：**隔离区、平坦降落点、剩余推力

#### 厂区人员通道

**后果：**进入人员活动区，存在人员碰撞风险

**条件：**人员位置、缓冲距离、告警与响应延迟

#### 输电设施附近

**后果：**碰撞线路、设备，设施损伤及次生影响

**条件：**设施间距、风扰、定位与避障能力

评估对象写成“故障+场景+飞行阶段+防护条件”，才能比较改进前后。

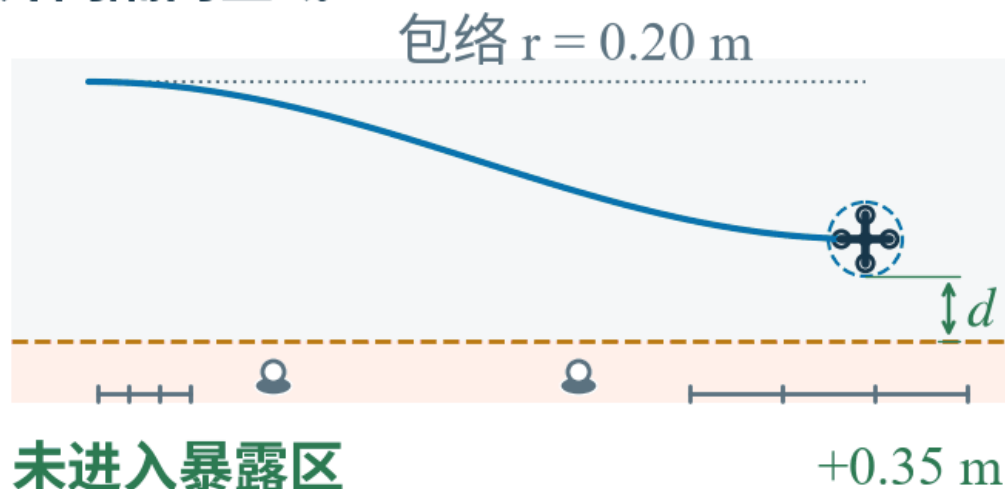
## 7.4.1 场景与危害：环境暴露

### 同一偏移轨迹进入不同的暴露区

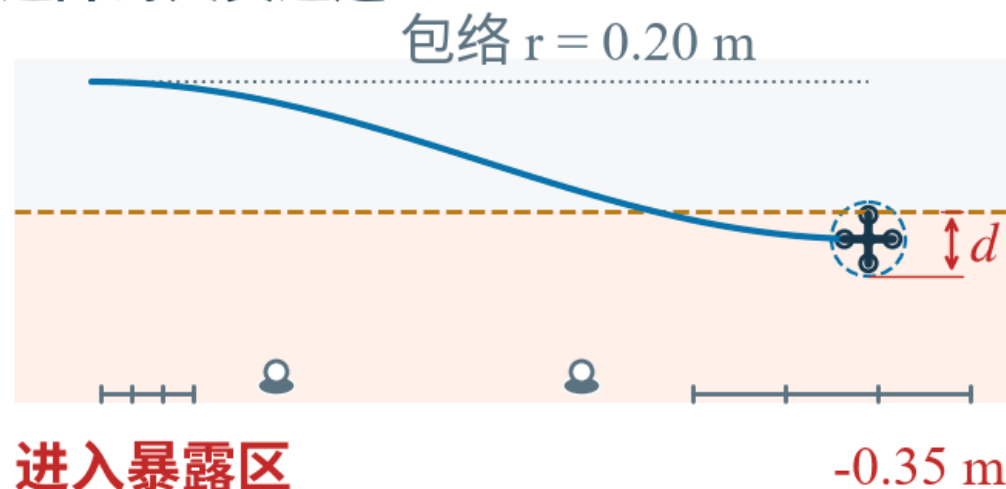
固定故障与偏移轨迹，只改变环境边界；数值为机体轮廓净距。

同一偏移轨迹，暴露条件不同

开阔隔离区域



近障碍人员通道



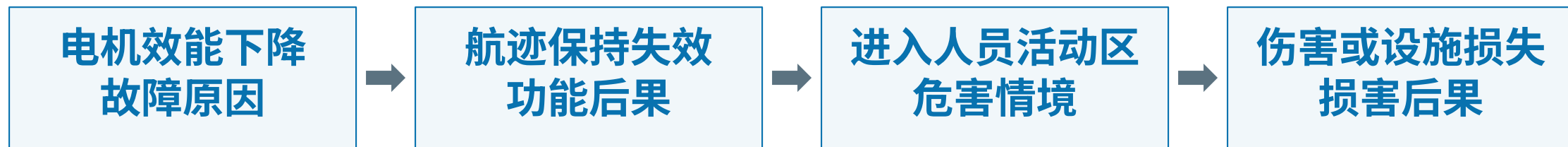
$t = 6.0 \text{ s}$

$d$  为包络净距；负值表示进入暴露区，不代表已发生碰撞

图：环境暴露示意；净距为负表示进入暴露区，不代表已发生碰撞。

### 7.4.1 场景与危害：风险表达

## 故障通过功能失效和暴露形成危害



$$\text{风险} = \text{发生概率} \times \text{严重程度}$$

教材式(7.1)

- **量化后果：** 概率无单位；严重程度以损失金额计时，乘积是该事件的期望损失。
- **经验档位：** 严重程度为有序档位时，乘积只用于排序比较。
- **数字口径：** 写清事件、时段与单位，如每次任务越界、每小时部件失效。

### 7.4.1 场景与危害：航空分级的适用范围

## 航空设计保证等级按失效后果规定开发强度

**设计保证等级（DAL）：**按失效后果规定开发与验证的严格程度。

| 失效后果     | 每飞行小时概率要求         | DAL     | 后果含义          |
|----------|-------------------|---------|---------------|
| 灾难性      | $<10^{-9}$        | DAL A   | 可能导致失事或人员重大伤亡 |
| 危害性      | $<10^{-7}$        | DAL B   | 安全裕度严重削弱，乘员受伤 |
| 重大       | $<10^{-5}$        | DAL C   | 可能导致任务中断或地面损伤 |
| 次要／无安全影响 | $<10^{-3}$ 或定性（D） | DAL D／E | 影响轻微；E级无概率限制  |

概率要求针对失效后果，属有人航空器语境；无人机目标按运行条件确定。

### 7.4.1 场景与危害：无人系统安全适配

## 无人机的风险目标由具体运行条件确定

工程目标先确定场景、事件与适用依据；特定运行风险评估（SORA）按运行概念评定地面与空中风险，再定所需防护与证据。

| 教材列举的应用 | 每飞行小时最大故障率               | 教材给出的运行特点    |
|---------|--------------------------|--------------|
| 航拍／娱乐   | $10^{-3} \text{ h}^{-1}$ | 低风险场景        |
| 工业巡检    | $10^{-4} \text{ h}^{-1}$ | 有一定任务载荷与飞行时长 |
| 城市物流    | $10^{-5} \text{ h}^{-1}$ | 低空飞行，飞越人口密集区 |
| 大型／军用   | $10^{-7} \text{ h}^{-1}$ | 高安全等级系统      |

**最低合理可行（ALARP）：**在合理可行范围内继续降低风险，权衡风险降低与所需时间、成本和难度。



## 7.4 故障危害与安全评估



### 本章目录

## 故障危害与安全评估

### 第七章 健康管理与安全评估

7.1 健康管理与安全评估基础

7.2 统一故障建模框架

7.3 虚实安全强化与故障数据方法

**7.4 故障危害与安全评估**

7.5 故障诊断与健康预测

7.6 安全决策与整机改进

7.7 故障注入接口与算法开发框架

7.8 例程实验与虚实验证

7.9 习题与课堂讨论

### 本节 4 个教学单元

#### 7.4.1 场景与危害

教材对应：第7.1.2.2、7.1.2.4节

#### 7.4.2 安全分析方法

教材对应：第7.1.2.2、7.1.2.4节

#### 7.4.3 可靠性与任务指标

教材对应：第7.1.2.4节

#### 7.4.4 风险排序与设计改进

教材对应：第7.1.5.3、7.1.2.5节



## 7.4 故障危害与安全评估

### 7.4.2 安全分析方法：安全设计流程

### 安全需求沿分解与集成过程接受检验

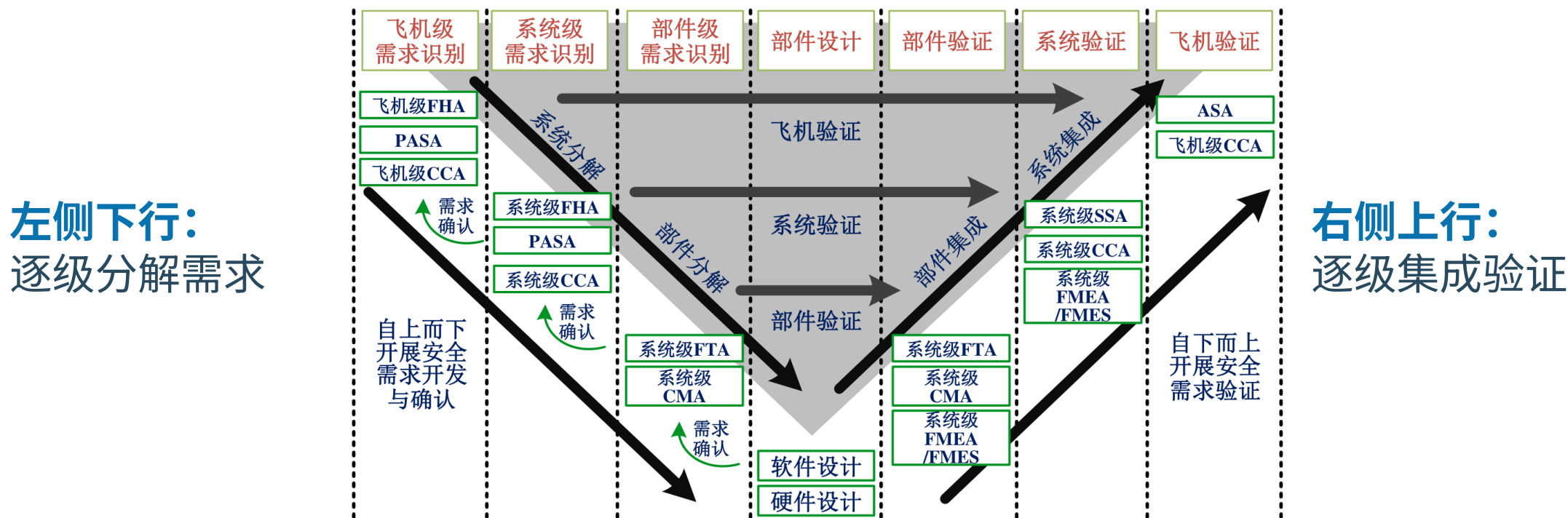


图7.2 载人航空器安全设计流程

绿框标出各阶段的安全分析；局部放大依次看需求、实现与验证三侧。

### 7.4.2 安全分析方法：需求识别与确认

## 功能后果决定需要分配的安全要求

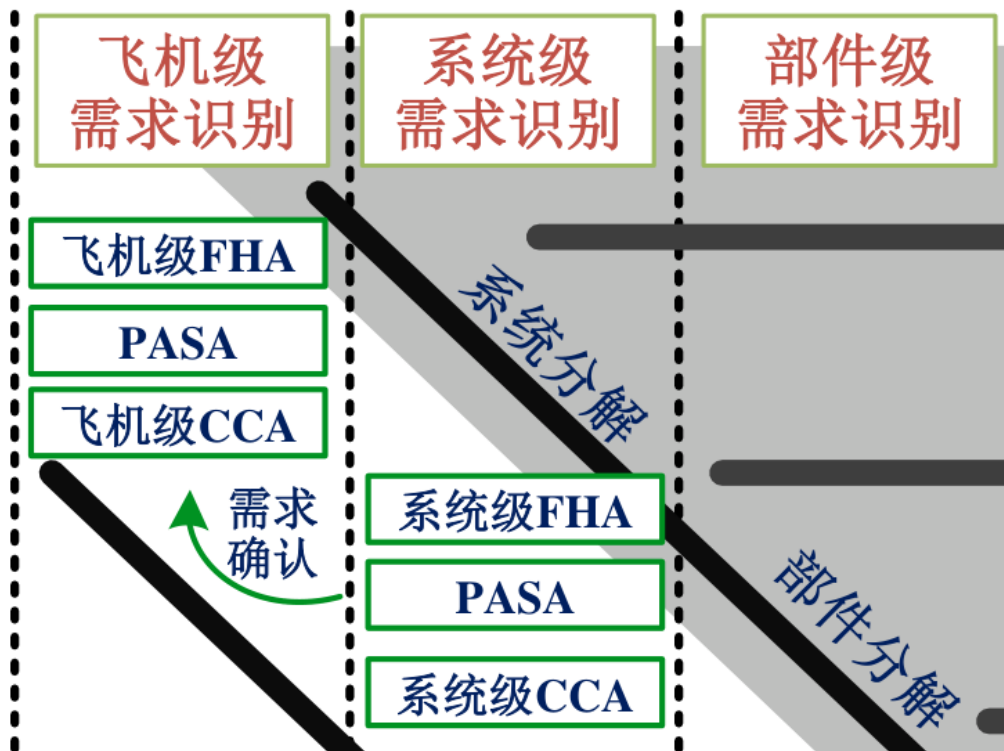


图7.2 (需求侧)

**功能危害评估 (FHA)：**  
从功能后果提出安全目标。

### 初步飞机级安全评估

**(PASA)：** 早期检查风险分配；  
图中系统级列应为PSSA。

### 共因分析 (CCA)：

追查同时破坏多通道的根源。

### 7.4.2 安全分析方法：部件设计与分析

## 部件实现需要同时检查传播路径和独立性

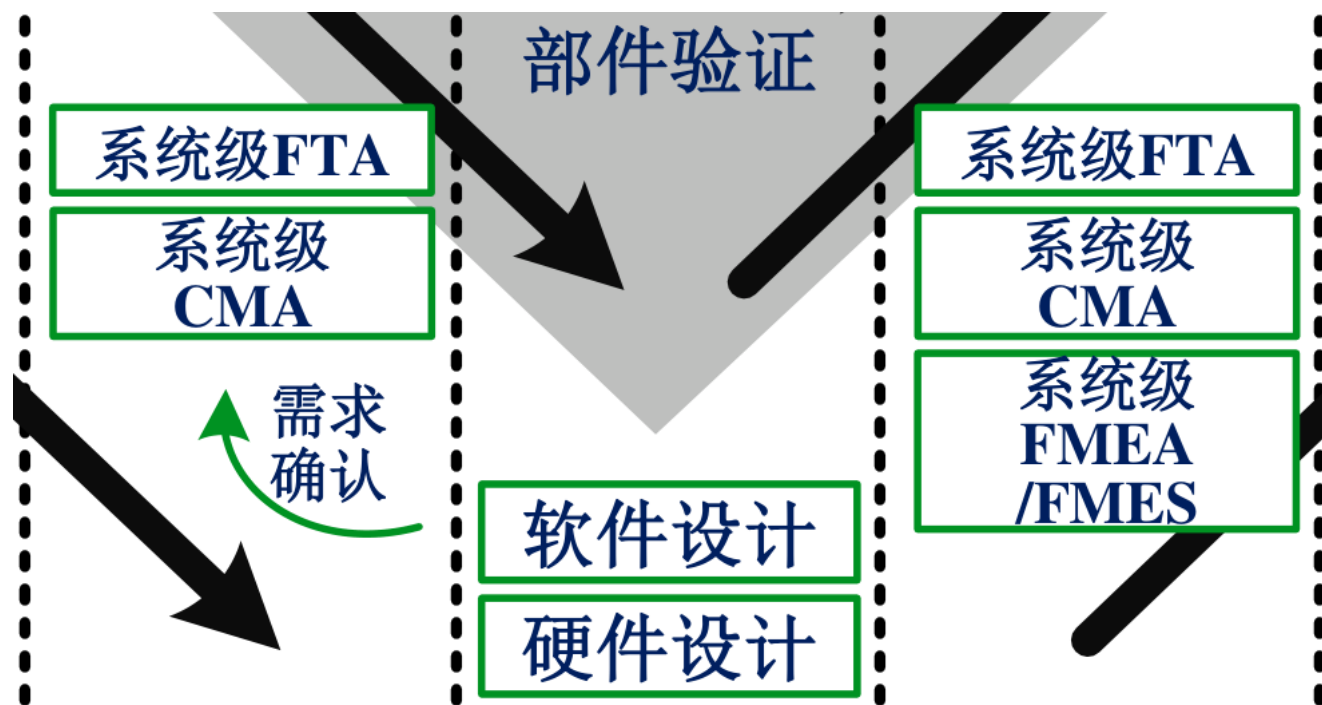


图7.2 (实现侧)

**故障树分析 (FTA)：**  
从顶层危害展开组合路径。

**共模分析 (CMA)：**  
检查冗余通道的独立性。

**失效模式与影响分析 (FMEA)：**  
从部件追踪系统影响。

**失效模式与影响总结 (FMES)：**  
汇总结果供上层使用。

### 7.4.2 安全分析方法：集成与验证

## 验证结果回到系统与整机的安全目标

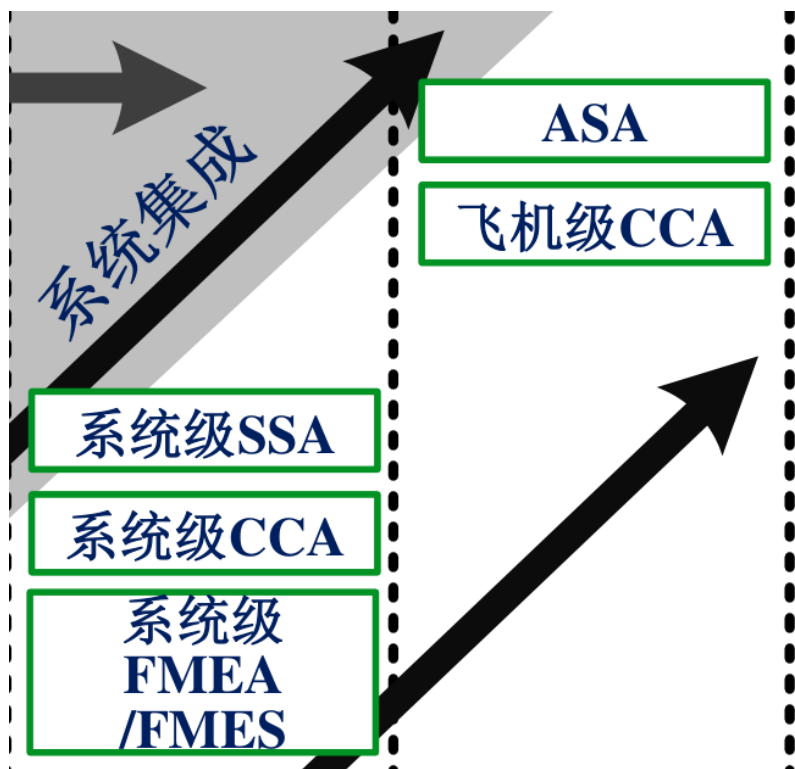


图7.2（验证侧）

### 系统安全性评估（SSA）：

用架构、概率和试验证据核对系统目标。

### 飞机级安全评估（ASA）：

审查整机集成的交互影响。

### 巡检对应：

检查保护动作、隔离距离与整机剩余能力。

### 7.4.2 安全分析方法：代表方法的衔接

### 三种分析各回答一个具体问题

| 方法与方向         | 巡检中的输入             | 得到的可审查结果              |
|---------------|--------------------|-----------------------|
| FHA<br>功能→后果  | 航迹保持失效；厂区人员暴露      | 越界危害、隔离距离<br>保护响应要求   |
| FMEA<br>部件→系统 | 单电机效能下降<br>监测与控制能力 | 局部与任务影响<br>措施及责任人     |
| FTA<br>顶事件→组合 | 顶事件：越出人员隔离边界       | 独立路径、事件组合<br>共因与防护薄弱点 |

分析文档的价值，是把危害转成可检验的设计要求。

### 7.4.2 安全分析方法：功能危害评估

## 先按功能丧失、错误和意外激活寻找危害

固定场景：厂区边缘巡检，邻近人员通道；功能为“在隔离边界内保持航迹”。

| 功能失效模式 | 可信后果         | 形成的安全要求                |
|--------|--------------|------------------------|
| 丧失航迹保持 | 侧向漂移可能越入人员通道 | 保留隔离余量；<br>在越界前触发有效保护  |
| 航迹目标错误 | 飞错目标，压缩设施间距  | 核对目标与边界<br>拒绝不可执行指令    |
| 意外激活运动 | 准备阶段伤及近旁作业人员 | 建立解锁（arm）条件<br>与人员隔离联锁 |

功能级记录确定“要避免什么”，部件级分析再确定“什么会导致它”。

### 7.4.2 安全分析方法：失效模式与影响分析

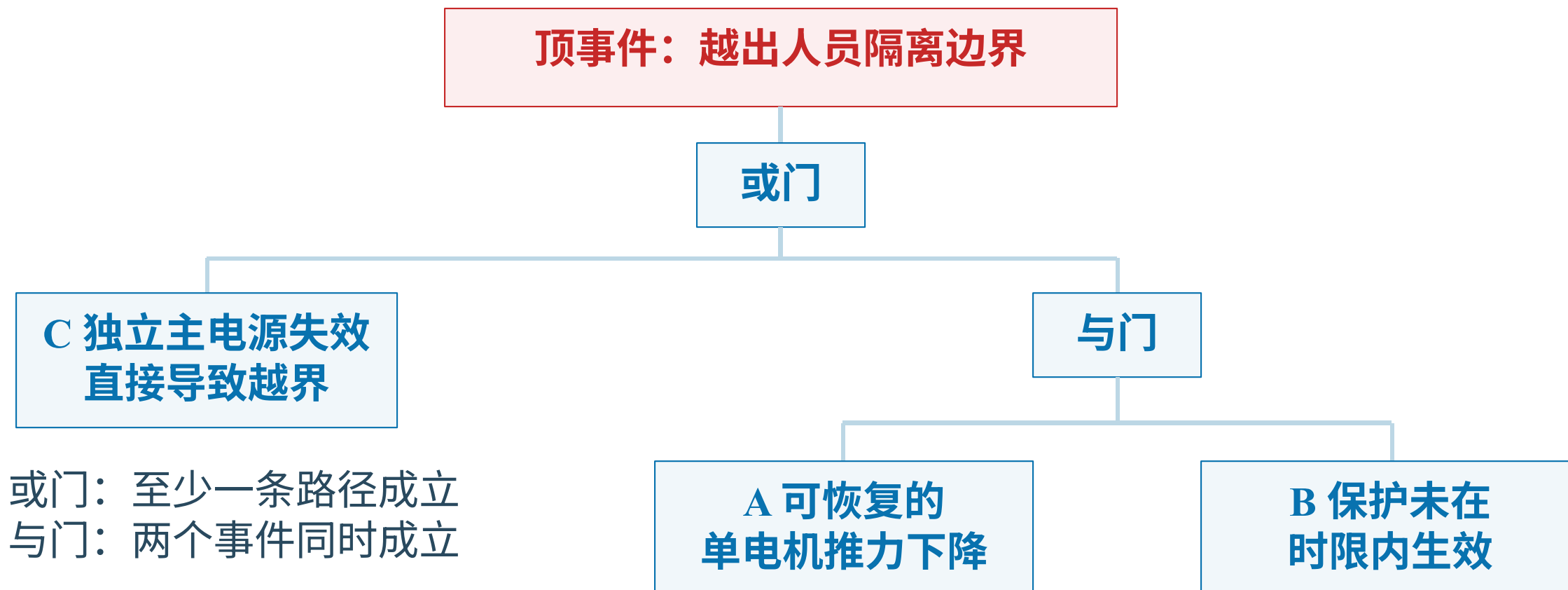
## 一行FMEA把原因、影响与防护串起来

| 记录字段     | 厂区巡检的填写实例                 |
|----------|---------------------------|
| 对象／模式／原因 | 单电机；效能降至70%；绕组损伤为假设原因     |
| 局部与系统影响  | 推力不足 → 其他电机补偿 → 控制余量减小    |
| 阶段与场景危害  | 转弯或阵风中航迹偏移；可能越入人员活动区      |
| 监测和改进措施  | 动力残差、输出饱和、航迹偏差；告警并转向安全降落区 |
| 验证与责任记录  | 记录告警时延、最小隔离距离、动作效果、版本和负责人 |

先写因果链与防护证据，再填严重度、发生、探测档位（定义见7.4.4）。

### 7.4.2 安全分析方法：简单故障树

## 越界顶事件由单独路径或组合路径触发



### 7.4.2 安全分析方法：故障树算例

### 组合概率先检查独立性，再做代入

理论算例：每次30 min任务， $P(A) = 0.002$ ,  $P(B) = 0.1$ ,  $P(C) = 0.0001$ 。

假设：三事件相互独立；概率无单位；仅覆盖图中的两条路径。

$$P(A \cap B) = P(A)P(B) = 0.002 \times 0.1 = 0.0002$$

$$P(T) = P(C) + P(A)P(B) - P(C)P(A)P(B) = 0.00029998$$

$T$  = 越出人员隔离边界，约0.0300%/次任务；越界与受伤是两个事件。

$$P(A \cap B) = P(A)P(B | A)$$

存在依赖时，用条件概率；  
冗余硬件也可能有共因失效。



## 7.4 故障危害与安全评估



### 本章目录

## 故障危害与安全评估

### 第七章 健康管理与安全评估

7.1 健康管理与安全评估基础

7.2 统一故障建模框架

7.3 虚实安全强化与故障数据方法

**7.4 故障危害与安全评估**

7.5 故障诊断与健康预测

7.6 安全决策与整机改进

7.7 故障注入接口与算法开发框架

7.8 例程实验与虚实验证

7.9 习题与课堂讨论

### 本节 4 个教学单元

#### 7.4.1 场景与危害

教材对应：第7.1.2.2、7.1.2.4节

#### 7.4.2 安全分析方法

教材对应：第7.1.2.2、7.1.2.4节

#### 7.4.3 可靠性与任务指标

教材对应：第7.1.2.4节

#### 7.4.4 风险排序与设计改进

教材对应：第7.1.5.3、7.1.2.5节



### 7.4.3 可靠性与任务指标：平均故障间隔时间

## 平均故障间隔时间来自累计运行与故障计数

平均故障间隔时间（MTBF）：

可修复系统在修复后恢复运行，到下次故障的平均运行时间。

$$\widehat{\text{MTBF}} = \frac{T_{\text{op}}}{N_f} = \frac{2000 \text{ h}}{4} = 500 \text{ h} \quad \text{教材式(7.2)}$$

- **统计口径：**  $T_{\text{op}}$ 是累计有效运行时间（h）； $N_f$ 是同一故障定义下的计数。
- **运行条件：** 机型、载荷、环境、维修规则和观察范围一致，结果才便于比较。
- **估计的含义：** 500 h是样本均值，不是保证寿命，也不保证每次任务无故障。

### 7.4.3 可靠性与任务指标：失效率与概率

## 失效率有时间单位，任务概率没有时间单位

恒定速率算例：故障间隔独立、同分布且服从指数分布；任务内不计维修。

$$\lambda = \frac{1}{\text{MTBF}}$$

$\lambda$ ：恒定失效率，单位 $\text{h}^{-1}$ ；

$t$ ：任务时长，单位 $\text{h}$ 。

$$R(t) = e^{-\lambda t}$$

$R(t)$ ：任务期内无故障的概率，无单位。

$$F(t) = 1 - e^{-\lambda t}$$

$F(t)$ ：至少一次故障的概率，无单位；

$\lambda t \ll 1$ 时才有 $F(t) \approx \lambda t$ 。

任务时长改变故障概率；恒定失效率也要有工况依据。

### 7.4.3 可靠性与任务指标：可靠性代入

### 五百小时MTBF对应怎样的巡检任务可靠性

$$\hat{\lambda} = \frac{4}{2000 \text{ h}} = 0.002 \text{ h}^{-1}, \quad t = 0.5 \text{ h}$$

$$F(0.5) = 1 - e^{-0.002 \times 0.5} = 0.0009995 \approx 0.09995\%$$

| 任务时长   | 至少一次故障的概率 | 对应的无故障概率  |
|--------|-----------|-----------|
| 15 min | 0.04999%  | 99.95001% |
| 30 min | 0.09995%  | 99.90005% |
| 60 min | 0.19980%  | 99.80020% |

**结论：**  $\lambda t \ll 1$  时，任务时长翻倍，故障概率约翻倍（同一故障定义与工况）。

### 7.4.3 可靠性与任务指标：任务指标

## 任务指标回答能否完成、是否匹配、离边界多远

### 任务完成概率

**定义：**给定任务目标、运行环境与资源约束下，成功完成预期任务的概率。

**综合：**健康、环境不确定性、故障风险、任务复杂度。

**巡检判据：**先定成功判据，如拍清全部目标并返航，再统计同条件任务的成功比例。

### 任务健康度

**定义：**实时状态（剩余电量、组件温度、冗余能力）与任务载荷需求的匹配程度。

**表示：**常用归一化得分，便于跨平台、跨任务比较。

**巡检判据：**剩余电量与冗余能否撑完剩余航段并返航；不足即调整或中止任务。

### 任务安全裕度

**定义：**完成任务时，对故障传播、路径偏离等风险的容忍能力。

**关注：**对地面人员、关键设施引发不安全事件的可能性。

**巡检判据：**到人员隔离边界的最小余距，单位m，须大于延迟期间的偏移量。

教材的任务指标未指定统一公式；成功判据、任务时段和裕度单位均须明确。

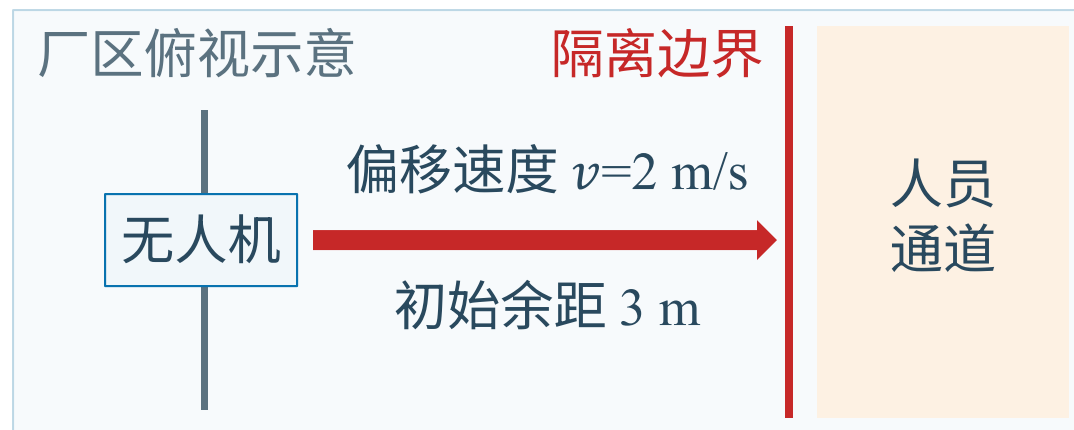
## 7.4 故障危害与安全评估

### 7.4.3 可靠性与任务指标：安全裕度算例

## 延迟耗掉隔离余量，动能描述撞击条件

### 延迟耗掉的隔离距离

假设恒速，忽略制动和定位误差。



$$d = v\tau = 2 \times 1.5 = 3 \text{ m}$$

$\tau=1.5 \text{ s}$ 后偏移3 m，余距剩0 m。

结论：隔离距离须大于 $v\tau$ ，再加制动与定位误差余量。

### 撞击动能估算

假设质量2 kg，撞击速度5 m/s。

$$E = \frac{1}{2}mv^2 = \frac{1}{2} \times 2 \times 5^2 = 25 \text{ J}$$

$m$ ：质量 (kg)； $v$ ：速度 (m/s)。

坠地时可作e8\_SafetyAssExp的FallEnergy。

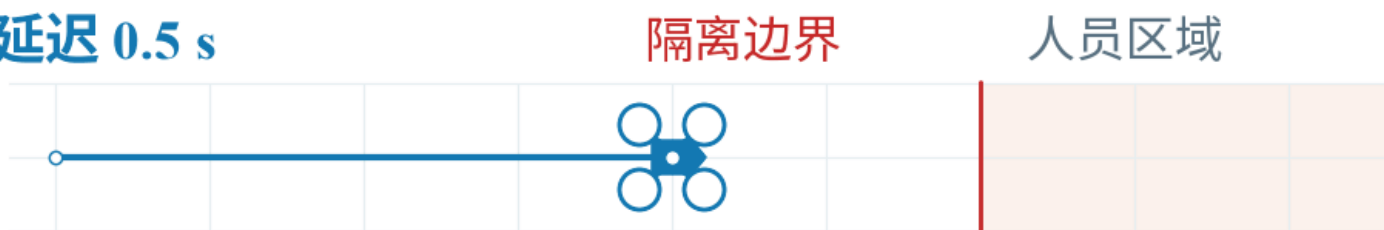
动能描述撞击条件；伤害程度还取决于碰撞部位、结构和防护。

### 7.4.3 可靠性与任务指标：安全裕度算例

## 保护晚一步，留给制动的距离就少一截

同样速度、同样制动，响应晚了就可能越界

保护延迟 0.5 s



已停止

速度 0.0 m/s

剩余距离 1.0 m

保护延迟 1.5 s



已停止

速度 0.0 m/s

越界距离 1.0 m

初始余距 3 m

初速 2 m/s；制动减速度 2 m/s<sup>2</sup>

时间 3.0 s

图：响应延迟与有限制动共同消耗余距（质点运动学对照）。

实际隔离距离还须考虑机体尺寸与定位误差。

### 7.4.3 可靠性与任务指标：概率证据与验证

## 统计、监测与仿真各提供不同证据

| 证据来源    | 直接提供什么                         | 影响解释的条件             |
|---------|--------------------------------|---------------------|
| 运行统计    | 累计运行时间、故障数以及任务条件               | 故障定义一致；报告完整说明统计不确定性 |
| 在线监测与保护 | 机内测试（BIT）；检测、隔离和恢复（FDIR）的时延及效果 | 发现故障后，保护动作须在场景约束内生效 |
| 随机仿真    | 蒙特卡罗：按输入分布抽样后的事件频率             | 分布与模型可信；稀有事件需要足够样本  |

故障注入比例服务于测试覆盖，真实发生概率需要独立依据。



## 7.4 故障危害与安全评估



### 本章目录

## 故障危害与安全评估

### 第七章 健康管理与安全评估

7.1 健康管理与安全评估基础

7.2 统一故障建模框架

7.3 虚实安全强化与故障数据方法

**7.4 故障危害与安全评估**

7.5 故障诊断与健康预测

7.6 安全决策与整机改进

7.7 故障注入接口与算法开发框架

7.8 例程实验与虚实验证

7.9 习题与课堂讨论

### 本节 4 个教学单元

#### 7.4.1 场景与危害

教材对应：第7.1.2.2、7.1.2.4节

#### 7.4.2 安全分析方法

教材对应：第7.1.2.2、7.1.2.4节

#### 7.4.3 可靠性与任务指标

教材对应：第7.1.2.4节

#### 7.4.4 风险排序与设计改进

教材对应：第7.1.5.3、7.1.2.5节



### 7.4.4 风险排序与设计改进：任务驱动故障等级 任务后果分类描述还能完成什么

| 教材任务后果示例 | 剩余任务与控制能力       | 巡检中的判断重点      |
|----------|-----------------|---------------|
| A 灾难性    | 失控，无法安全迫降       | 失控路径、人员或设施暴露  |
| B 危险     | 无法返航或降级，但能可控迫降  | 迫降区与剩余控制能力    |
| C 严重     | 任务失败，可返航或执行替代任务 | 中止任务后的风险和质量要求 |
| D 轻微     | 任务可完成，质量下降仍可接受  | 图像质量、航迹与剩余余量  |
| E 无安全影响  | 预设任务与质量未受影响     | 仍检查人员、设施与环境风险 |

A-E是教材任务后果的示例标记，不是DAL；任务成功也需要满足场景安全约束。

### 7.4.4 风险排序与设计改进：风险优先级

### 经验优先级数排序时保留严重后果的优先权

风险优先级数（RPN）采用经验档位：严重度S、发生档位O、探测困难度D。  
D越大，越难及时发现。

$$RPN = S \times O \times D$$

| 课堂假设的后果 | S/O/D（1-5档） | RPN与优先规则      |
|---------|-------------|---------------|
| 人员区越界   | 5/2/2       | 20；严重人员危害优先处理 |
| 图像质量下降  | 2/5/4       | 40；可参考排序安排改进  |

本课档位含义：S=5为严重人员危害；O=2低、O=5高；D=2较易发现、D=4较难发现。  
档位和RPN无概率单位。

### 7.4.4 风险排序与设计改进：动态排序与改进

## 有效改进改变风险路径，再按残余风险排序

理论设计比较：任务仍为30 min，保持A、C的概率不变。  
假设有效保护使B的失败概率由0.1降至0.02。

| 设计状态   | 故障树模型中的越界概率                    | 对应的改进记录              |
|--------|--------------------------------|----------------------|
| 改进前    | $0.00029998 \approx 0.0300\%$  | A与B组合路径占较多风险         |
| 保护改进假设 | $0.000139996 \approx 0.0140\%$ | 待验证告警延迟<br>动作成功与最小距离 |

C独立路径仍在：这部分残余风险要靠提高电源可靠性来降低。

初始排序 → 验证改进 → 更新风险数据库 → 重排序 → 补测残余风险

### 7.4.4 风险排序与设计改进：无人系统安全评估挑战

## 软件和场景改变后，旧风险结论需要复核

### 软件定义功能

**风险：**同一硬件，控制逻辑改变会改变剩余能力。

**措施：**固定状态与输入，检查功能边界。

### 软件缺陷触发

**风险：**极端输入或特定状态触发错误路径。

**措施：**异常输入、组合故障与边界回归测试。

### 学习模型与可解释性

**风险：**黑盒模型可解释性差；训练范围外的风、光照或新对象会影响判断。

**措施：**跨场景测试；独立监视与可执行回退。

### 版本与空中升级（OTA）

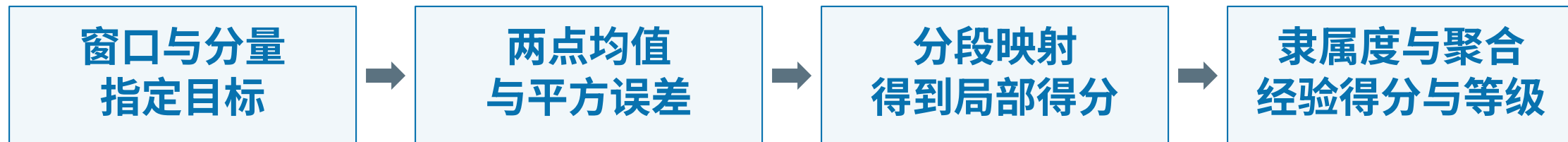
**风险：**新版本更改阈值、动作或接口约束。

**措施：**记录版本；复测保护时延与风险表。

传统评估以硬件可靠性为核心；智能系统还要验证行为、鲁棒性与可解释性。

### 7.4.4 风险排序与设计改进：安全评分机制

### SDK将误差经过规则映射成经验得分



$$e_i = (\bar{v}_i - v_{\text{cmd}})^2$$

$\bar{v}_i$ : 两点均值;  $v_{\text{cmd}}$ : 同分量目标。

| 代码档位         | 速度平方误差范围                | 局部得分      |
|--------------|-------------------------|-----------|
| 正常 (Nomal)   | $0 \leq e_i < 0.015$    | 0.999→0.9 |
| 轻微 (Slight)  | $0.015 \leq e_i < 0.04$ | 0.9→0.7   |
| 严重 (Serious) | $0.04 \leq e_i < 0.16$  | 0.7→0.4   |
| 危险 (Hazard)  | $0.16 \leq e_i < 0.5$   | 0.4→0.1   |

#### 映射与聚合

**隶属度**: 得分>0.9记为1, 其余沿用。

**时序修正**: 下降时乘以(1-降幅)。

**聚合**: 权重1/3/6/9/12加权平均。

$e_i \geq 0.5$ : 坠地分支, 本例得0.1。

速度以m/s输入时误差单位为 $\text{m}^2/\text{s}^2$ ; 得分是经验排序量, 不是事故概率。

### 7.4.4 风险排序与设计改进：评分算例

## 按代码规则手算：一个误差值怎样变成得分和等级

| 步骤     | 输入      | 计算                     | 结果        |
|--------|---------|------------------------|-----------|
| ① 定档   | $e=0.1$ | 严重档[0.04,0.16)         | 局部得分0.529 |
| ② 隶属度  | 0.529   | 不大于0.9，沿用              | 0.529     |
| ③ 时序修正 | 前一时刻0.8 | $0.8 \times (1-0.271)$ | 0.583     |

- ④ 聚合：0.8与0.583分属轻微、严重档，按权重3、6加权平均 $\approx 0.66$ 。
- ⑤ 等级：加权计数以严重档（权重6）最大，输出等级Medium。
- 结论：低档权重更大，少数大误差点就能明显拉低得分。



## 7.4 故障危害与安全评估



学习资料

### 定义、方法与适用范围可查阅官方材料

#### MTBF与恒定故障速率：NIST统计手册

<https://www.itl.nist.gov/div898/handbook/apr/section1/apr171.htm>

#### FMEA的内容、适用范围与维护：IEC 60812官方简介

<https://webstore.iec.ch/en/publication/26359>

#### 航空功能危害评估与设计保证：FAA咨询通告AC 25.1309-1B

[https://www.faa.gov/documentLibrary/media/Advisory\\_Circular/AC\\_25.1309-1B.pdf](https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_25.1309-1B.pdf)

#### 特定无人机运行风险与SORA公开文件：JARUS

<https://jarus-rpas.org/publications/>



### 练习与讨论

## 把空旷场地的记录改写到厂区人员通道

已知：单电机效能降至70%，航迹暂能维持；空场有隔离区，厂区邻近人员通道。

| FMEA字段 | 空旷场地示例              | 厂区人员通道：填写                |
|--------|---------------------|--------------------------|
| 暴露与后果  | 隔离区内<br>任务中止、设备损伤   | 暴露对象：____<br>最坏可信后果：____ |
| 监测与措施  | 监测控制余量<br>退出任务并受控降落 | 监测量：____<br>措施与生效条件：____ |
| 验证判据   | 隔离区内落地、动作响应可控       | 响应时限：____<br>人员隔离距离：____ |



## 7.4 故障危害与安全评估



参考要点

### 厂区记录增加人员暴露和保护时限

| 字段      | 参考填写                     |
|---------|--------------------------|
| 暴露与可信后果 | 人员通道；偏移越界后可能碰撞人员或设备      |
| 监测依据    | 航迹偏差、动力残差、输出饱和；关联故障发生时刻  |
| 措施和条件   | 停止巡检；剩余能力允许时转向无人降落区      |
| 响应判据    | 发现与执行总延迟小于剩余隔离距离允许的时限    |
| 证据与更新   | 记录最小距离、延迟、控制余量和版本；复核残余风险 |

同一故障的记录可复用，场景危害与保护条件必须随任务重写。



### 本节小结

## 评估把故障状态转成场景判断和改进依据

- **场景先行：**健康描述状态；任务能力描述功能；安全评估人员、设施与环境后果。
- **分析分工：**FHA定功能后果与要求，FMEA追踪部件影响，FTA检查组合与共因。
- **数字有条件：**失效率代入任务时长才得任务概率；独立性决定组合算法。
- **改进有证据：**经验评分与RPN支持比较；验证保护及时性与效果，更新残余风险。
- **易错点：**经验得分不是事故概率；MTBF是样本均值，不是寿命；告警改变的是探测档位D，后果被限制时严重度才下降。

识别风险以后，还要选择能够执行并经验证的保护动作。