本章目录

习题与课堂讨论

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 3 个教学单元

7.9.1 概念辨析与指标
教材对应：第7.4节，习题1–5

7.9.2 故障建模与接口
教材对应：第7.4节，习题6–8

7.9.3 安全方案设计
教材对应：第7.4节，习题9–10

7.9 习题与课堂讨论

7.9.1 概念辨析与指标：健康管理框架

习题1–2：一条报警信息，距离健康管理还差什么？

题1： 简述健康管理与安全评估的区别与联系。

题2： 简述故障预测与健康管理（PHM）体系与OSA-CBM标准架构的核心层级及职责。

情境： 系统只报“电机异常”，但没有程度、有效时间和任务影响。

讨论： 报警能否直接决定返航？哪些环节需要继续提供证据？

知识回顾：课件7.1；教材第7.1.2.1节（健康管理）、第7.1.2.3节（区别与联系）

7.9 习题与课堂讨论

7.9.1 概念辨析与指标：健康管理框架

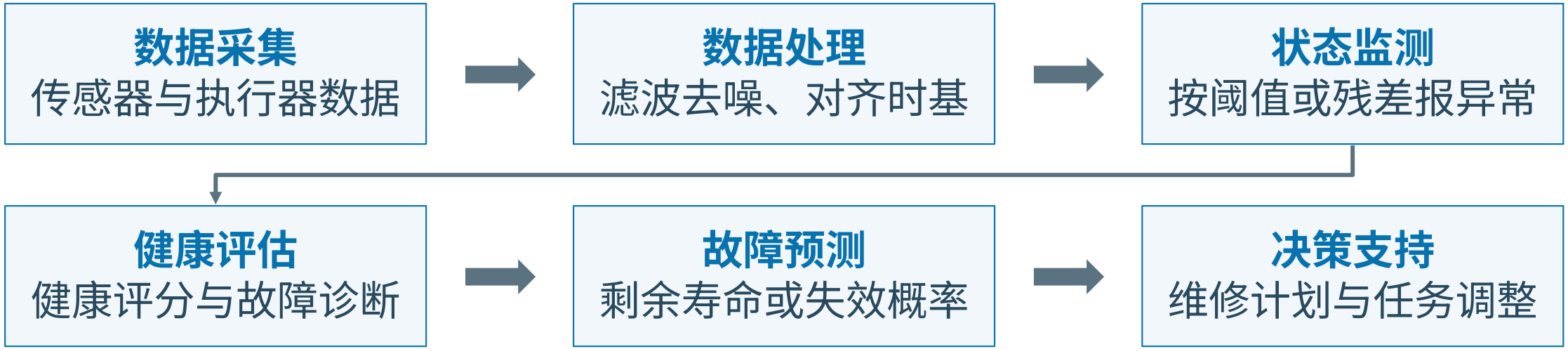
习题1参考：按表7.1对比健康管理与安全评估

维度	健康管理	安全评估
评估对象	系统内部运行状态	系统对外部造成的潜在风险
数据来源	机载实时传感器数据	历史运行数据、外部观测数据
评估周期	实时或短时监测	设计与运行各阶段
关键技术	状态检测、故障诊断、寿命预测	FTA、FMEA、事故数据分析
目标导向	提高系统自我感知与恢复能力	降低事故发生概率与影响范围

联系：健康状态与预测是安全评估的输入，二者共同支撑任务与处置决策。

7.9.1 概念辨析与指标：健康管理框架

习题2参考：六个功能块把数据逐层变成决策建议



第七层 人机交互：展示监测、评估、预测与建议，并接收阈值与维护反馈

报警：本例的“电机异常”只是状态监测的输出，经后三块处理才成为任务建议。

7.9.1 概念辨析与指标：安全评估方法与指标

习题3、5：方法选错，比算错一个数更危险

题3：常用安全评估方法各回答什么问题？怎样为巡检无人机选择方法？

题5：航空领域中，分析MTBF、DAL、ALARP的含义及其在安全评估中的意义。

辨析： “MTBF为1000 h，因此第999 h之前不会失效”，错在哪里？

辨析： “诊断准确率达到99%，因此满足某个DAL”，为什么不能推出？

知识回顾：课件7.4「安全分析方法」单元，以及「航空分级的适用范围」「无人系统安全适配」「平均故障间隔时间」页；教材第7.1.2.2节、第7.1.2.4节

7.9 习题与课堂讨论

7.9.1 概念辨析与指标：安全评估方法与指标

习题3参考：功能后果、部件原因与失效组合分别分析

方法	起点	巡检案例
FHA 功能危害评估	功能丧失 或输出错误	失去高度控制的后果
FMEA 失效模式 与影响分析	部件的具体 失效模式	电机退化对姿态与任务的影响
FTA 故障树分析	已定义的顶事件	不可控下降的故障组合

其余方法：FMES汇总FMEA结果；SSA综合评估；CCA/CMA查冗余独立性；ASA/PASA做整机级评估。

7.9 习题与课堂讨论

7.9.1 概念辨析与指标：安全评估方法与指标

习题5参考：MTBF看统计，DAL看保证，ALARP看风险

术语	参考要点	不能替代什么
MTBF	平均故障间隔时间＝ 总运行时间÷故障次数	统计平均， 不能保证个体寿命
DAL	设计保证等级A–E，按失效后果分级； 规定开发与验证的严格程度	不是诊断准确率等级
ALARP	最低合理可行：风险降至合理可行的 尽可能低水平，并保留论证证据	不是“零风险”宣言

MTBF用于可靠性统计，DAL规定开发保证要求，ALARP指导风险降低。

7.9 习题与课堂讨论

7.9.1 概念辨析与指标：安全评估方法与指标

习题5参考：DAL按失效后果严重度分为A–E五级

DAL A	DAL B	DAL C	DAL D	DAL E
灾难性	危害性	重大	次要	无安全影响
$< 10^{-9}$	$< 10^{-7}$	$< 10^{-5}$	$< 10^{-3}$	无概率要求

读法：失效后果定严重度，严重度定每飞行小时概率目标与DAL。

含义：DAL规定开发与验证的严格程度；诊断准确率属于算法指标。

依据：FAA、EASA、CAAC等适航认证采用，DO-178C、DO-254以此分级。

详见：课件7.4「航空分级的适用范围」页，含DAL的含义与适用条件。

7.9.1 概念辨析与指标：任务驱动指标

习题4：完成任务、保持健康和留有裕度如何同时评价?

题4：分析任务完成概率、任务健康度和任务安全裕度的定义与关系。

已知：剩余电量足够，但某电机接近控制上限；任务终点上方风更强。

要求：为三项指标分别写出计算对象、必要条件和一种可观测输入。

追问：能够勉强完成一次任务，是否意味着可以继续重复派飞?

知识回顾：课件7.4「任务指标」「安全裕度算例」页；教材第7.1.2.4节

7.9 习题与课堂讨论

7.9.1 概念辨析与指标：任务驱动指标

习题4参考：概率、评分和物理裕度应分别报告

指标	本课操作性定义	应报告的条件
任务完成概率	给定场景下成功完成任务的概率	成功判据、任务分布与统计区间
任务健康度	状态与任务需求匹配的评价量	变量、归一化、权重与验证依据
任务安全裕度	距选定能力或安全约束的余量	约束、量纲、模型及不确定性

本例：完成概率可能仍高，但推力裕度偏低；
可观测PWM饱和时长、风速与电量；重复派飞先看退化趋势。

本章目录

习题与课堂讨论

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 3 个教学单元

7.9.1 概念辨析与指标
教材对应：第7.4节，习题1–5

7.9.2 故障建模与接口
教材对应：第7.4节，习题6–8

7.9.3 安全方案设计
教材对应：第7.4节，习题9–10

7.9.2 故障建模与接口：IMU故障建模

习题6：怎样让IMU故障既可注入，又可诊断?

题6：设计惯性测量单元（IMU）传感器故障建模方案，并说明可用于诊断的关键特征。

建模要求：说明真值、故障项和测量值的关系；写清单位、坐标系和时序。

诊断要求：偏置、噪声、冻结（卡死）、延迟各选至少一种特征，并说明原因。

验证要求：比较健康与故障段；补充机动、振动等非故障对照。

知识回顾：课件7.2；教材第7.1.3.3–7.1.3.4节（故障建模方法与思路）

7.9.2 故障建模与接口：IMU故障建模

习题6参考：用不同特征区分偏置、噪声、冻结与延迟

$$\tilde{a}(t) = a(t-\tau) + b(t) + k_n n(t)$$

$\tilde{a}, a, n$为测量、真值、噪声；τ, b, k_n为延迟、偏置、噪声增益。
各加速度量单位为$\mathrm{m/s^2}$；冻结即测量保持固定值（见课件7.2「组件故障模型」页）。

故障	可比较的特征	排除的混淆
偏置／噪声	均值或残差／去均值后的方差	姿态、振动与工况变化
冻结	输出保持固定值，变化率与方差近零	真实静止、量化限制
延迟	动态信号互相关或相位滞后	时钟不同步与链路积压

7.9.2 故障建模与接口：自动注入与采集

习题7：自动注入如何形成可追溯的数据集？

题7：给出RflySim自动化故障注入与数据采集的流程要点。

必须包含：用例配置、版本、准备、基线、触发、采集、终止、恢复与评价。

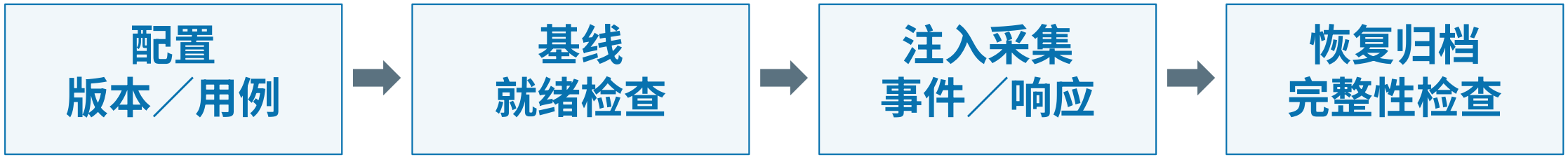
记录问题：注入命令时间、模型生效时间和日志时间是否属于同一个时钟？

异常分支：未起飞、日志缺失或未确认故障生效时，该轮结果怎样标记？

知识回顾：课件7.3、7.8.3、教材第7.1.5.2节；例程e9_data_collect、e18_FaultLogTimestamp
位于[安装目录]/RflySimAPIs/7.RflySimPHM/0.ApiExps/

7.9.2 故障建模与接口：自动注入与采集

习题7参考：每轮测试写清起点、事件、结束与恢复



保存：用例ID、随机种子、版本、单位、统一时基的时间戳、命令和原始日志。

结束：按时间、任务或保护阈值终止；有效试验的超时与失败须保留并计入评价。

核对：故障生效证据、健康对照与恢复后状态；时钟不同源时先标定映射。

7.9.2 故障建模与接口：加速度计噪声注入

习题8：在SITL中设置加速度计噪声增益0.5

题8：基于RflySim工具链，在软件在环（SITL）仿真中使得加速度计噪声增益为0.5，并总结该接口具体协议。

目录：[安装目录]/RflySimAPIs/7.RflySimPHM/1.BasicExps/e4_SensorFault/
先读其中的Readme.pdf。

检查：区分接口参数p（Readme称噪声增益）与噪声支路乘数k；
核对模型版本、故障ID与槽位。

交付：报文字段表、触发与恢复过程，以及健康、注入、恢复三段的三轴加速度比较。

知识回顾：课件7.3.1、7.7；教材第7.1.5.1节、第7.2.1节（故障建模与注入框架）

7.9.2 故障建模与接口：加速度计噪声注入

习题8参考：故障ID选择类型，浮点槽位承载参数

```
silInt = [123542] + [0] * 7
silFloat = [0.5, 0.0] + [0.0] * 18
mav1.sendSILIntFloat(silInt, silFloat)
```

层次	本例内容
报文	校验值1234567897；载具ID；8个整数；20个float32
参数槽位	整数槽0写123542（加速度计噪声）；浮点槽0写p=0.5
模型通道	UDP端口30100+2(ID−1)；直达模型中的故障模块

7.9.2 故障建模与接口：加速度计噪声注入

习题8参考：先分清接口参数p与噪声支路乘数k

$$k = 0.2 + 0.8p = 0.2 + 0.8 \times 0.5 = 0.6$$

符号：k为噪声支路乘数；p为浮点槽0的接口参数（Readme称噪声增益）。

正常支路：噪声输入乘0.2；先记录同工况下的三轴基线。

本课口径：教材与Readme都称p为噪声增益，取p=0.5，得k=0.6。

另一读法：若要求支路乘数k=0.5，则p=(0.5−0.2)/0.8=0.375。

恢复与新用例：按模型源码，同一ID发参数0恢复幅值；新用例先重新初始化模型。

7.9.2 故障建模与接口：加速度计噪声注入

习题8参考：基础e4_SensorFault的准备、启动与结束

目录：[安装目录]/RflySimAPIs/7.RflySimPHM/1.BasicExps/e4_SensorFault/
入口为Readme.pdf与FaultInjectAPITest.py。

准备模型：MATLAB 2022B及以上运行Init.m → MulticopterModel.slx执行Build → 右键运行GenerateModelDLLFile.p生成DLL。

启动注入：管理员身份运行MulticopterModelSITL.bat → 双击Python38Run.bat → 第95行silFloat改为[0.5,0] → python FaultInjectAPITest.py。

正常结束：脚本约50 s打印Sim End后自动退出；
在SITL命令窗口按任意键，关闭CopterSim、QGC与RflySim3D。

注意：SITL脚本会覆盖CopterSim模型目录中的同名DLL，并重启已运行的CopterSim。

7.9.2 故障建模与接口：加速度计噪声注入

习题8参考：按时间线确认注入生效，再比对日志

5 s	20 s	20–50 s	约50 s
解锁（arm）	注入p=0.5	悬停中观察响应	打印Sim End

现象：Readme示例（参数30）中姿态控制紊乱、无法定点悬停；
p=0.5时支路乘数为0.6，推断现象明显弱于示例，以日志对比为准。

日志判据：[安装目录]/Firmware/build/px4_sitl_default/instance_1/log/的ulg转csv，
比较_sensor_combined_0.csv中accelerometer_m_s2[0]–[2]注入前后的波动。

常见失败：编译时报故障模块版本错误 → 从故障模块库选对应模块替换；
缺少MATLAB 2022B及以上版本时无法生成DLL。

本章目录

习题与课堂讨论

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 3 个教学单元

7.9.1 概念辨析与指标
教材对应：第7.4节，习题1–5

7.9.2 故障建模与接口
教材对应：第7.4节，习题6–8

7.9.3 安全方案设计
教材对应：第7.4节，习题9–10

7.9.3 安全方案设计：分层安全决策

习题9：行为树和强化学习怎样分工？

题9：设计“行为树 + 强化学习”的分层安全决策架构与协同机制。

条件：诊断可能误报，观测可能过期，学习策略可能给出不可行动作。

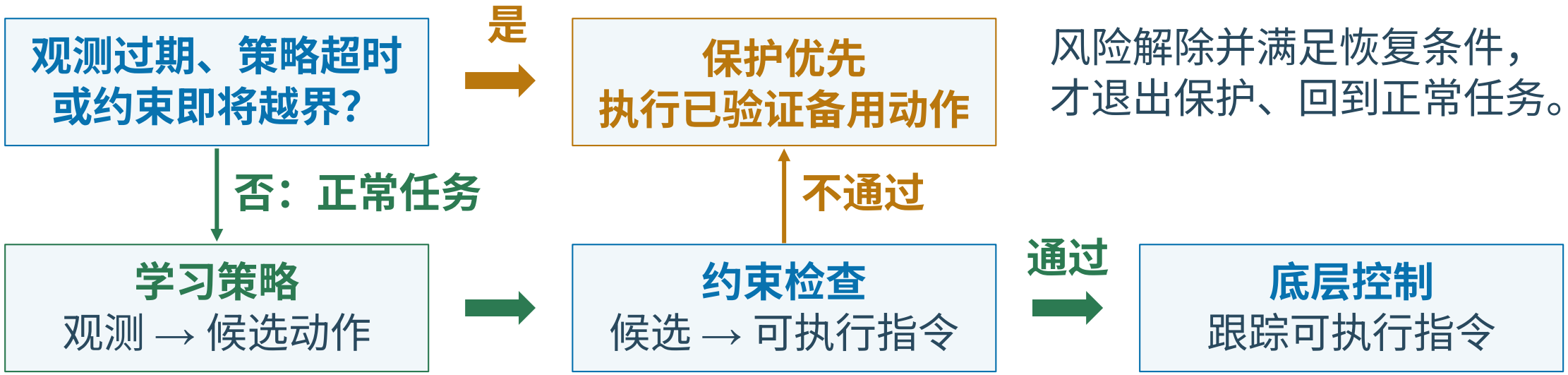
要求：标出正常任务、受约束策略、保护动作的优先级和输入输出。

验证：任务完成率之外，再统计约束违反、切换延迟和误触发代价。

知识回顾：课件7.6；教材第7.1.5.5节（安全决策算法训练）

7.9.3 安全方案设计：分层安全决策

习题9参考：安全约束决定何时允许策略参与



风险解除并满足恢复条件，
才退出保护、回到正常任务。

行为树组织优先级与切换；滞回、驻留与恢复条件避免反复跳转。

验证：约束违反、切换延迟、误触发代价，与任务完成率一起报告。

7.9.3 安全方案设计：复合扰动测试

习题10：阵风与载荷偏移，如何设计有效对照？

题10： 规划“阵风 + 载荷偏移”的自动化测试，并给出关键评价指标。

变量： 风强、风向、持续时间；载荷质量、偏移方向与距离。

对照： 为什么必须保留“无风无偏移、仅风、仅偏移、二者同时”四组？

评价： 如何比较跟踪、控制余量、任务结果以及对环境的潜在后果？

知识回顾：课件7.2、7.3；教材第7.1.3.2节（环境与结构故障）、第7.1.5.2节

7.9.3 安全方案设计：复合扰动测试

习题10参考：先分离主效应，再检验组合是否更危险

用例组	环境风	载荷偏移	比较目的
A 基准	无	无	正常误差与控制余量
B 风扰	有	无	风的单独影响
C 偏移	无	有	质心变化的单独影响
D 组合	有	有	交互作用与最不利组合

统一报告：跟踪误差、饱和时长、约束违反、完成率与处置时间；
随机工况保留重复试验，并报告统计区间。

本章小结：各节易错点

各节易错点：相近概念与操作顺序

7.1 概念： 现象≠原因；当前健康≠任务安全；单层仿真结果≠完整证据。

7.2 建模： 指令、转速与拉力系数不混用；偏置、噪声、时序改变不同特征。

7.3 数据： 用例条数≠已测次数；命令时刻≠生效时刻；先分完整飞行再切窗。

7.4 评估： 经验得分≠事故概率；MTBF是样本均值，不是单机寿命。

7.5 诊断预测： 标签不进输入；剩余寿命（RUL）只用历史数据，记录截尾≠失效。

7.6/7.8 决策验证： 模式请求≠运动受控；模型可信度≠安全概率。

7.7 注入： 发送≠生效；停发≠复位，全零ID也不清除模型锁存。

本章小结

健康管理让系统认识自身，安全决策让认识变成行动

概念：健康管理看内部状态与未来能力，安全评估看对外风险；
PHM按OSA-CBM六个功能块把数据变成决策建议。

方法：故障建模与数据 → 风险评估（FHA、FMEA、FTA与DAL）
→ 诊断与预测 → 安全决策与整机回归 → 注入接口与虚实验证。

边界：仿真与离线结果只在给定模型、版本与工况下成立；
MTBF、DAL与ALARP各管一层，不能互相替代。

易错点：把异常当故障、健康当安全、高准确率当可靠闭环；
混淆噪声增益p与支路乘数k；把时间阈值标签当故障真值。

衔接第八章：多模态感知与智能决策，把更可靠的观测带入安全决策。