智能无人系统控制实践

第七章 健康管理与安全评估

作者：戴训华 中南大学

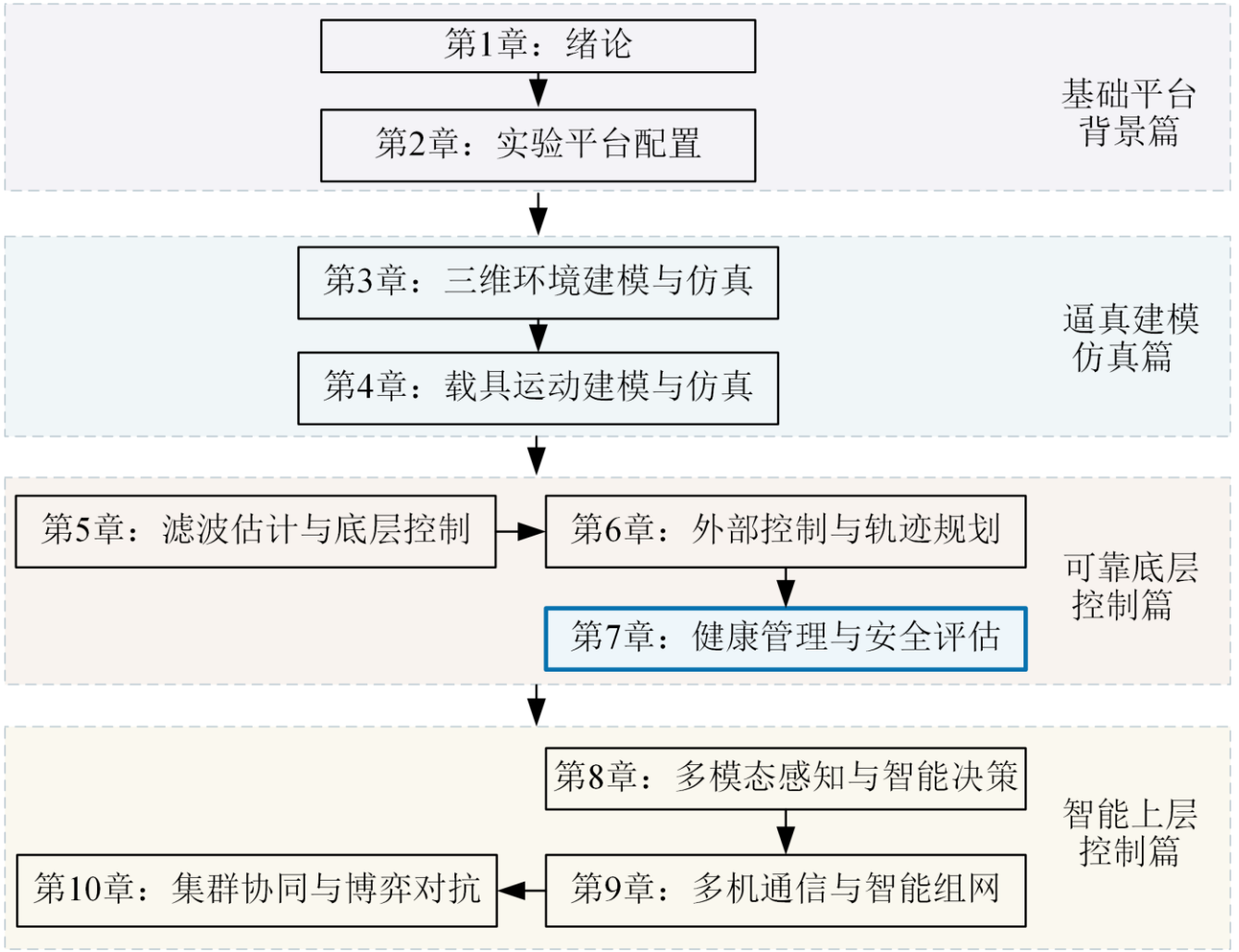
主页：https://faculty.csu.edu.cn/daixunhua

邮箱：dai.xh@csu.edu.cn

平台官网：https://rflysim.com

配套教材





教材：戴训华，全权，任雪峰. 智能无人系统控制实践[M]. 北京：电子工业出版社，2026.

本章学习目标

学完第七章能够完成什么

1. 区分异常、故障、失效，解释健康状态与任务风险的联系。
2. 建立故障模型，设计可追溯的注入、采集与自动测试流程。
3. 用证据评价诊断、预测与风险结果，识别数据和模型的适用边界。
4. 把安全决策接入控制闭环，通过分层测试检验效果与代价。

本章主线：从正常运行走向带故障的安全运行。

本章目录

健康管理与安全评估：本章学习路线

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

7.1.1 背景意义
教材对应：第7.1.1节

7.1.2 健康与安全的区别与联系
教材对应：第7.1.2、7.1.2.3节

7.1.3 无人系统健康管理
教材对应：第7.1.2.1节

7.1.4 算法开发挑战与验证
教材对应：第7.1.1节

7.1.1 背景意义：贯穿任务

控制回答“怎样飞”，健康管理还要回答“还能飞多久”

贯穿任务：巡检多旋翼，观察动力退化后怎样完成或安全结束任务。

正常跟踪
位置与姿态 → 识别退化
动力与传感 → 判断能力
返航与降落 → 执行验证
动作与结果

已有基础：动力学、状态估计与控制使运动可控。

新增问题：部件变化后，原有控制效果、控制余量与后果还可靠吗？

7.1.1 背景意义：术语边界

先分清观测异常、内部故障与功能失效

概念	巡检任务中的例子	概念要点
异常	振动或电流高于同工况参考	观测偏离同工况的正常参照
退化／故障	轴承磨损、推力效率下降；传感器偏置	性能劣化／内部异常状态
失效	无法维持规定姿态或完成规定功能	丧失完成规定功能的能力
外部扰动	阵风、碰撞接触、外部电磁干扰	环境对系统的外部作用； 本章按广义故障一并讨论

一次异常不等于一次故障；没有明显误差，也不能直接排除退化。

7.1.1 背景意义：动力故障与控制补偿

电机推力变小，飞机为何还能暂时稳住?

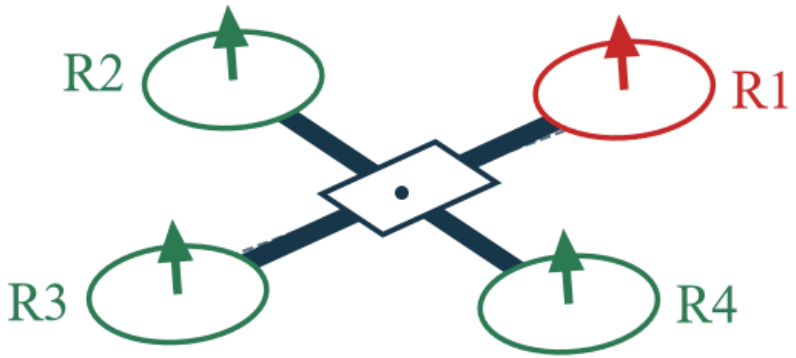
单旋翼推力损失：补偿与饱和

$\eta_1 = 0.9$：恢复悬停；$\eta_1 = 0.6$：持续下沉

实际推力 f_i

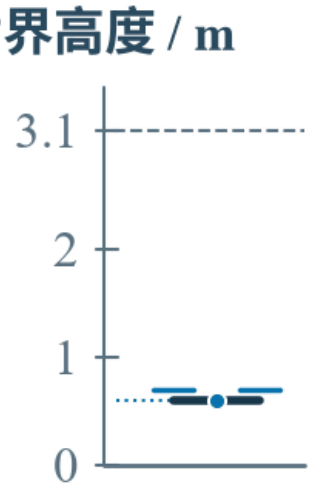
$\eta_1 = 0.6$

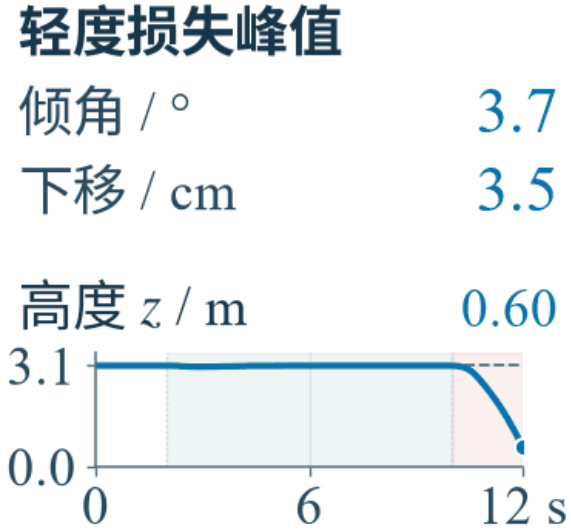
水平参考



指令 $u_1 = 1.50$ (≤ 1.50)　　实际 $f_1 = 2.21$ N

固定航向，力矩优先；零力矩合力上限 0.90 mg



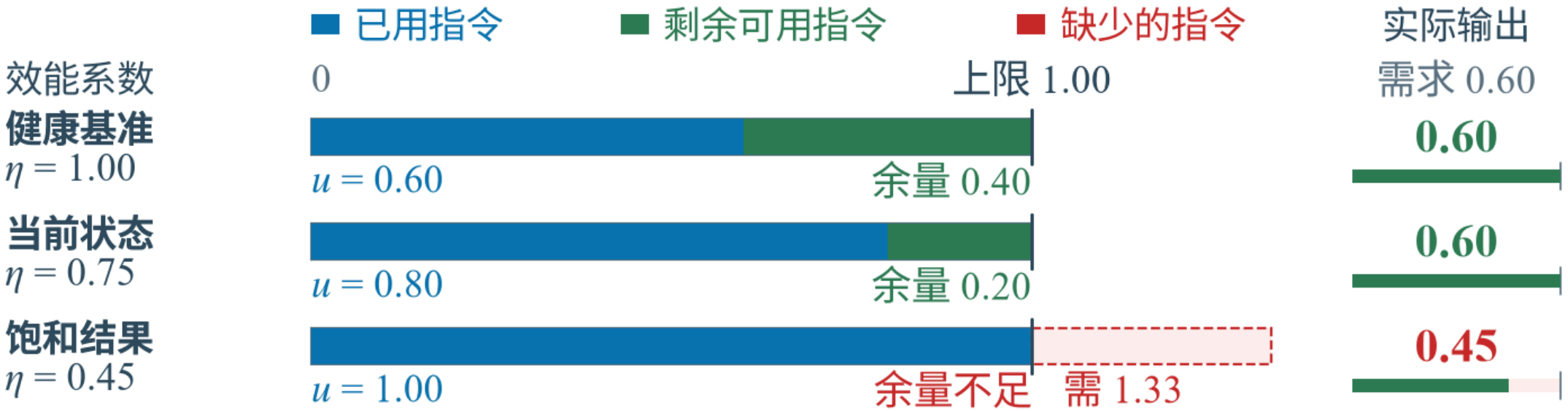


图：单旋翼效能下降与闭环补偿（MuJoCo仿真；效能系数1→0.9→0.6）。
轻度损失可补偿；重度损失在固定航向、力矩优先约束下，不能保持高度。

7.1.1 背景意义：控制补偿

误差暂时没变，控制余量可能已被消耗

补偿消耗余量；饱和后输出不足



输出保持 0.60，余量 0.40 → 0.20；饱和后输出短缺 0.15

图：准静态推力分配示意（效能系数＝输出÷指令）；控制余量＝指令上限–所需指令。

7.1.1 背景意义：一步计算

同一个需求，用三组数算清“补偿”和“上限”

$$y = \eta u, \quad 0 \le u \le 1, \quad u = \min(0.60/\eta, 1)$$

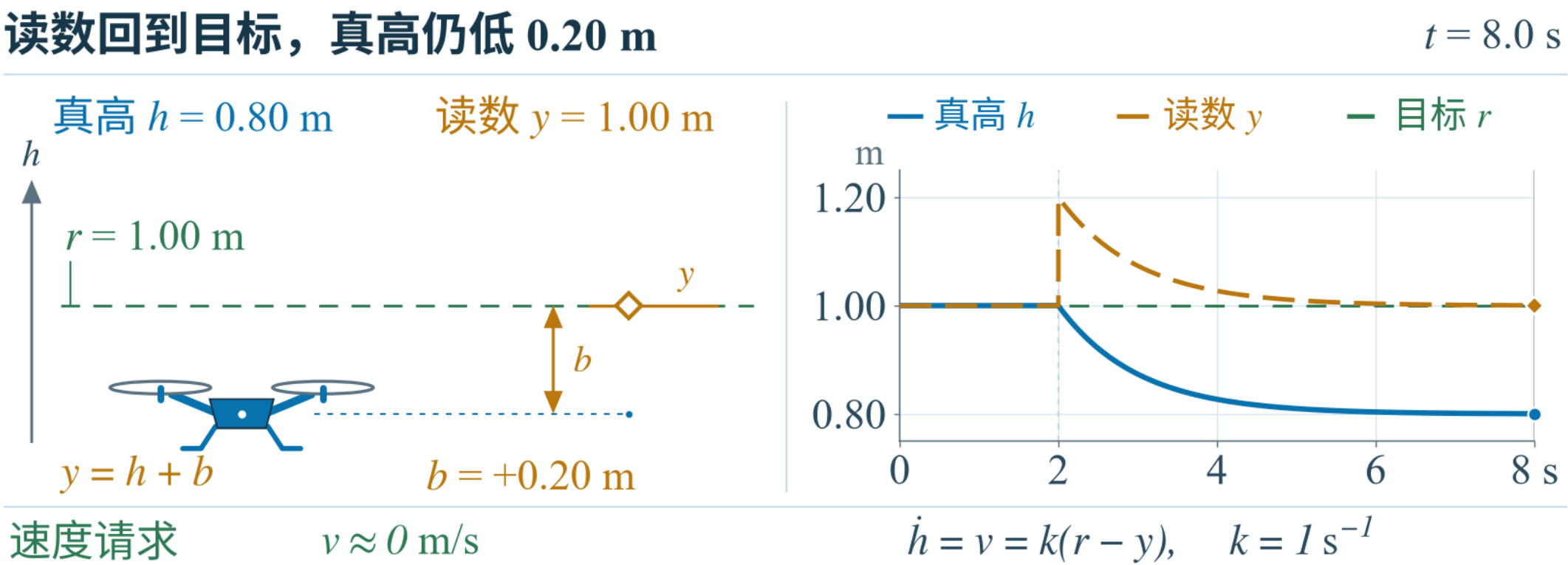
η：效能系数（输出÷指令）；u：归一化指令（上限为1）；y：归一化输出。

状态	效能系数	需要／实际指令	实际输出
健康	1.00	0.60 / 0.60	0.60
可补偿退化	0.75	0.80 / 0.80	0.60
超过能力	0.45	1.33 / 1.00	0.45

健康监测要同时看“完成了什么”和“为此付出了多少控制余量”。

7.1.1 背景意义：传感器故障

读数回到目标，实际高度为什么仍会偏离



图：测量持续偏高时，反馈动作可能把机体带离实际目标

7.1.1 背景意义：不同系统的安全需求

对象不同，危害的形成路径也不同

对象	代表性危害	设计与运行关注点
具身智能系统 如机械臂、机器狗	碰撞、挤压、夹持失控	限速限力、人机距离 与受控停机
无人驾驶车辆	失控、制动不足、 感知遗漏	可停止空间、交通参与者 与接管降级
无人飞行器	姿态失控、 动力不足与坠落	剩余控制能力； 降落区域、地面人员与财产

聚焦无人机：失效后难以就地停车，又难堆硬件冗余，更依赖健康管理。

安全性取决于任务、环境与保护措施，不能只由对象类别判断。

本章目录

健康管理与安全评估：本章学习路线

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

7.1.1 背景意义
教材对应：第7.1.1节

7.1.2 健康与安全的区别与联系
教材对应：第7.1.2、7.1.2.3节

7.1.3 无人系统健康管理
教材对应：第7.1.2.1节

7.1.4 算法开发挑战与验证
教材对应：第7.1.1节

7.1.2 健康与安全的区别与联系：两个观察角度

健康问“状态怎样”，安全问“后果能否接受”

健康管理

看什么：效率、磨损、偏置、振动、剩余能力。

输出什么：异常位置、故障程度、趋势和不确定性。

安全评估

看什么：失控路径、受影响的人与物、处置时间与保护。

输出什么：风险判断、约束和可接受的运行方式。

参照教材表7.1：两者的数据来源、评估周期与关键技术

数据来源：机载实时传感器数据
评估周期：实时或短时监测
关键技术：检测、诊断、寿命预测

数据来源：历史运行与外部观测
评估周期：设计与运行各阶段
关键技术：故障树与失效模式分析

相同健康状态放进不同任务环境，可能需要不同的安全决策。

7.1.2 健康与安全的区别与联系：目标与平台数据

健康管理增强自身恢复，安全评估降低事故影响

健康管理

目标导向：提高系统自我感知与恢复能力。

典型应用：自驾仪失效保护、机载故障预测与健康管理（PHM）系统。

安全评估

目标导向：降低事故发生概率与影响范围。

典型应用：适航认证、任务风险评估。

RflySim 中两类模块的数据来源（教材第7.1.2.3节）

数据： PX4 日志或状态估计	**数据：** CopterSim／RflySim3D 真值
性质： 间接估计，含误差与噪声	**性质：** 上帝视角，不含测量噪声
用途： 运行中实时感知与预警	**用途：** 评估故障前后的任务效果

健康管理依据带噪声的估计值，安全评估可借仿真真值复核后果。

7.1.2 健康与安全的区别与联系：情境改变后果

同样的动力退化，返航还是就近降落要看场景

近距离， 备降区清晰	远距离， 逆风且电量低	下方有人， 降落风险高
可选动作 证据满足时可低速返航	**可选动作** 余量不足时就近备降	**可选动作** 先改航避开人群， 再择点降落
必须补充的证据 姿态可控、余量足够、 落点可达	**必须补充的证据** 返航耗能、风估计、 航段剩余能力	**必须补充的证据** 可选落点、可达范围、 地面人员与财产

判断顺序：剩余能力 → 可执行的动作 → 各动作的后果与约束。

7.1.2 健康与安全的区别与联系：关键指标

可靠、可用与安全各有判据，可信依靠多维证据

概念	问题	直观例子
可靠性	规定时段内能持续完成规定功能吗?	巡检途中是否发生功能失效
可用性	需要使用时，是否处于可用状态?	维修等待会减少可用时间
安全性	运行与故障后果的风险是否受控?	检测到危险后及时受控降落
可信性	有哪些证据支持对系统的依赖?	可靠性与安全等多维证据

7.1.2 健康与安全的区别与联系：安全性与安保性

有意攻击可经控制链演变为物理危害

安全性 **Safety**	关注故障或运行异常造成的非故意伤害， 控制人员、设备与环境承受的风险。
安保性 **Security**	防御有意攻击或操纵，保护观测、指令与通信链路 免受未授权干预。

安保失效可能沿控制链转化为物理危害：

攻击
传感器欺骗
➡
观测/链路异常
位置报告失真
➡
控制误动作
误判偏差并转向
➡
物理危害
可能越界或碰撞

异常被采信且保护未阻断时，才可能逐步发展为危害。
通信攻击建模见课件7.2“传感器与通信故障”。

7.1.2 健康与安全的区别与联系：健康与寿命直觉

电池“还有多少电”和“已经老了多少”不是一回事

量	回答的问题	还需要哪些条件
SOC 荷电状态	这一次还剩多少可用电量?	当前容量估计、充放电状态
SOH 健康状态（本课以容量计）	相对参考电池退化了多少?	先约定评价指标（容量或内阻）
RUL 剩余可用寿命	距寿命终点还可使用多久?	终止阈值、未来工况与预测区间

预测维护的价值不在于报出一个寿命数，而在于支持提前安排任务与维护。

7.1.2 健康与安全的区别与联系：剩余寿命

同样的健康状态，为什么剩余寿命不同

同一SOH，不同条件RUL

假设未来退化率保持

当前：第100次循环

情景 A

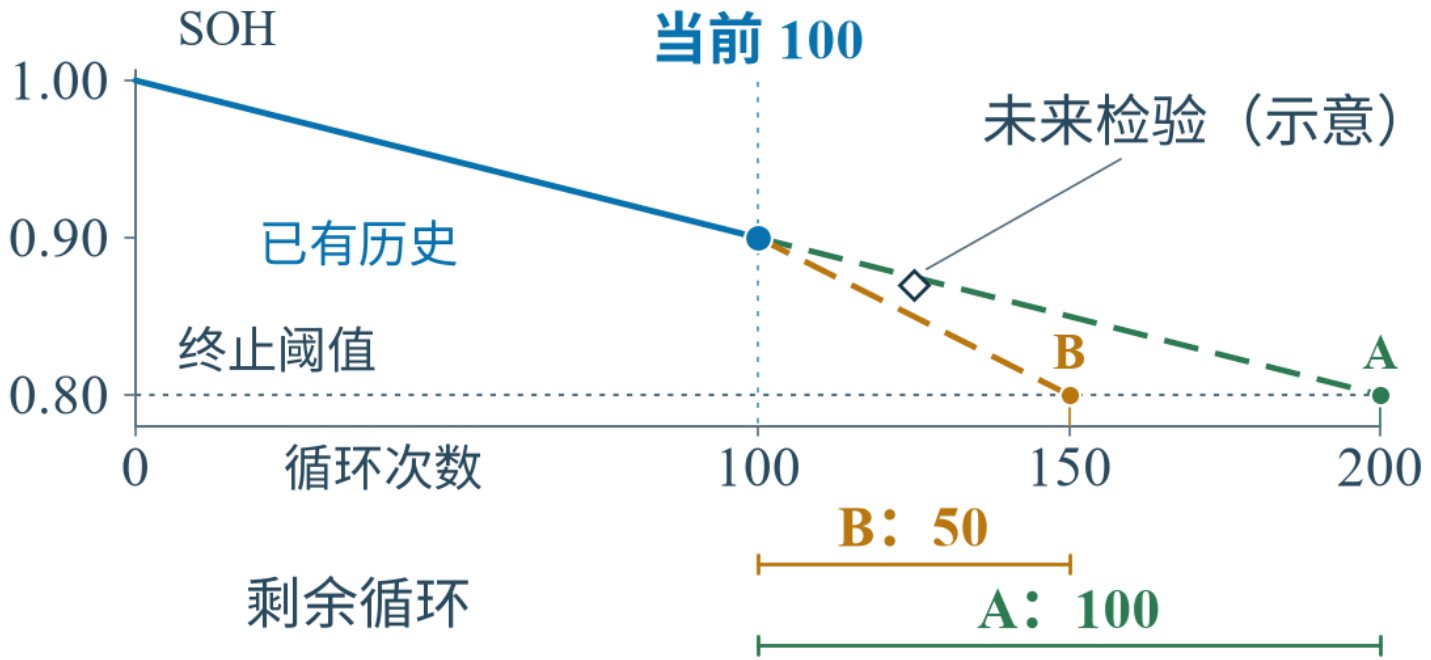
SOH = 0.90

每次退化 0.001

情景 B

SOH = 0.90

每次退化 0.002



图：固定当前健康状态，改变未来退化条件，寿命预测随之改变

本章目录

健康管理与安全评估：本章学习路线

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

7.1.1 背景意义
教材对应：第7.1.1节

7.1.2 健康与安全的区别与联系
教材对应：第7.1.2、7.1.2.3节

7.1.3 无人系统健康管理
教材对应：第7.1.2.1节

7.1.4 算法开发挑战与验证
教材对应：第7.1.1节

7.1.3 无人系统健康管理：基于状态维护的开放系统架构（OSA-CBM）

六个功能环节，把测量转化为维护与运行建议

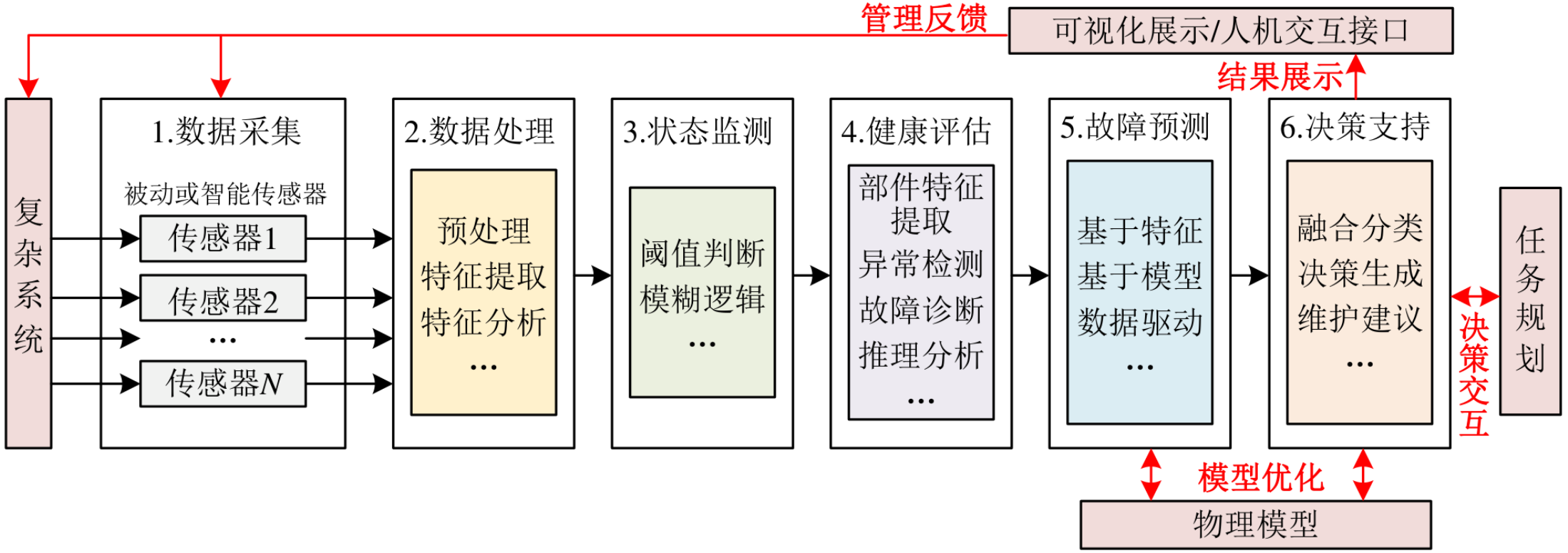


图7.1 复杂系统OSA-CBM架构图：故障预测与健康管理（PHM）的六个核心功能

7.1.3 无人系统健康管理：观测链

采集、处理与监测：先确认观测是否可信

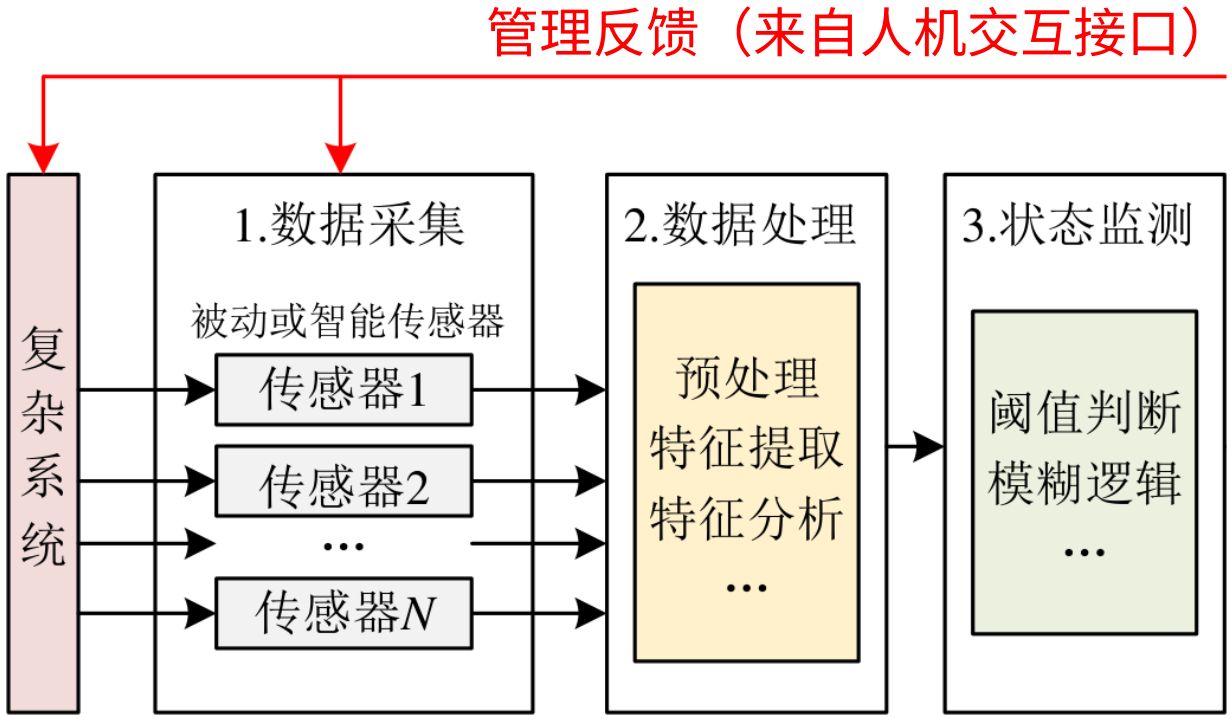


图7.1（左部）数据采集、处理与状态监测

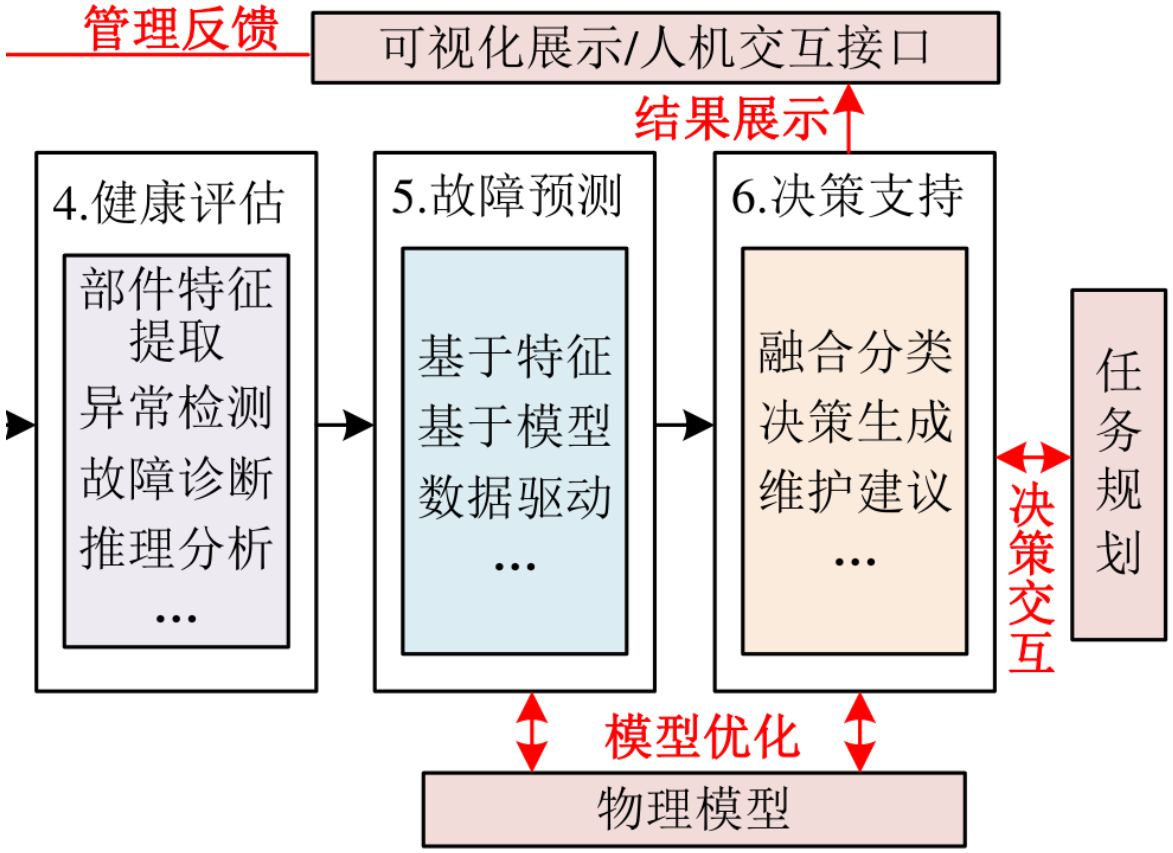
1.数据采集：电流、转速、振动与控制指令，保留时间戳和单位。

2.数据处理：时间对齐、按工况分段，提取特征，保留偏置线索。

3.状态监测：与同工况参考比较，检测异常并形成事件。

7.1.3 无人系统健康管理：判断与行动链

诊断解释现在，预测估计未来，建议连接行动



4.健康评估： 诊断故障位置、类型、程度与可信程度。

5.故障预测： 在给定未来工况下估计退化趋势与寿命区间。

6.决策支持： 结合任务约束，给出动作建议，执行后复查。

图7.1（右部）健康评估至决策支持

7.1.3 无人系统健康管理：从数据到建议

同一条电机记录，在每个环节产生不同的信息

环节	本例输入或输出	向下游必须说明
测量与处理	电流、转速、振动；同工况窗口	时间、单位、缺失率与处理方法
检测与诊断	偏差事件；动力效率下降的证据	故障类型、程度与不确定性
预测与建议	剩余能力；缩短任务或维护建议	未来工况、约束及有效期限

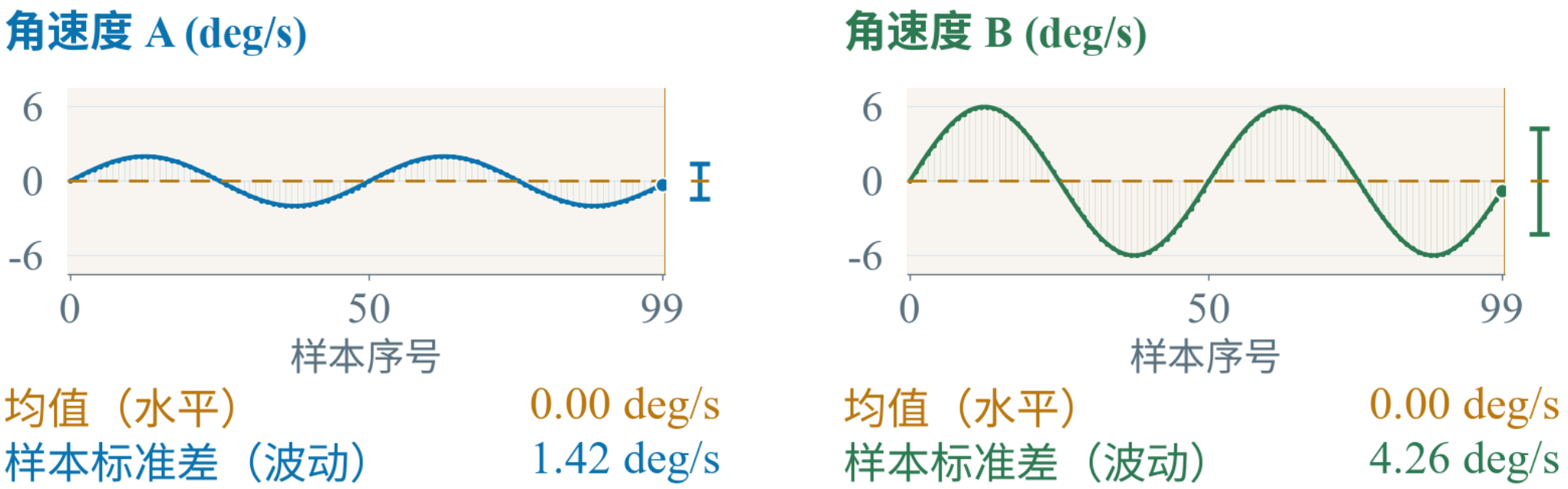
完整的健康管理交付“有条件的行动依据”，而不是孤立的异常标签。

7.1.3 无人系统健康管理：窗口与特征

平均值相同，两段信号仍可能很不一样

均值相同，波动不同

100 Hz　窗口 100/100



均值（水平）	0.00 deg/s	均值（水平）	0.00 deg/s
样本标准差（波动）	1.42 deg/s	样本标准差（波动）	4.26 deg/s

图：同一时间窗口内，均值描述中心水平，标准差描述波动

7.1.3 无人系统健康管理：残差算例

残差：比较实际测量与健康参照

同工况：健康参照 $\hat{y} = 6000\,\mathrm{r/min}$；测量 $y = 5400\,\mathrm{r/min}$。

残差

$$r = y - \hat{y} = 5400 - 6000 = -600\,\mathrm{r/min}$$

相对残差

$$r_{\mathrm{rel}} = \frac{y - \hat{y}}{\hat{y}} = -0.10$$

结果解释： 当前转速比健康参照低10%，需要结合电压、载荷和其他传感量解释。

检验方法： 用健康数据建立参照；用独立健康与故障数据评价阈值、误报和漏报。

7.1.3 无人系统健康管理：时间与决策延迟

时间窗口决定：能看清细节，也会带来等待

设置	能得到什么	需要付出的代价
100 Hz采样、100点窗口	观察约1 s范围内的统计特征	窗口需要积累； 突发变化可能被平滑
每0.1 s滑动更新	较频繁地更新判断	相邻窗口重叠， 样本并不独立
异常连续确认	抑制单点噪声造成的误报	确认时间增加， 可能延迟处置

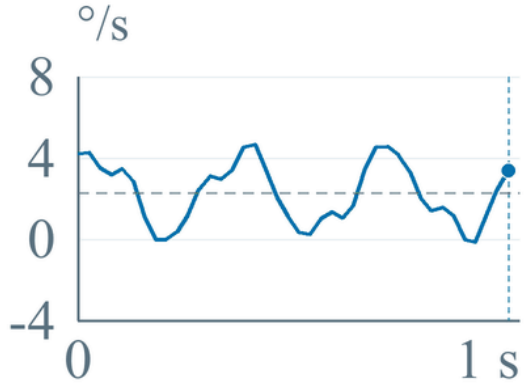
诊断精度之外，还要问：结论来得及改变故障后果吗？

7.1.3 无人系统健康管理：分类依据

把信号变成特征，再与已知状态比较

联合特征支持判断，边界处需补证据

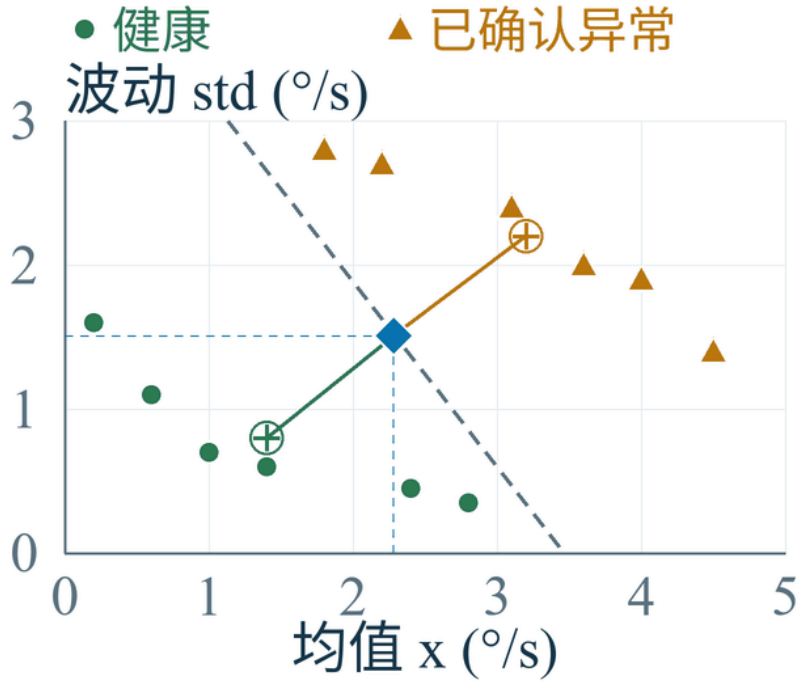
合成角速度



均值 x = 2.28 °/s

波动 = 1.51 °/s

窗口映射为特征点



新样本 C

到类中心的距离

单位：°/s

健康 1.13

异常 1.15

两类距离接近

需补证据

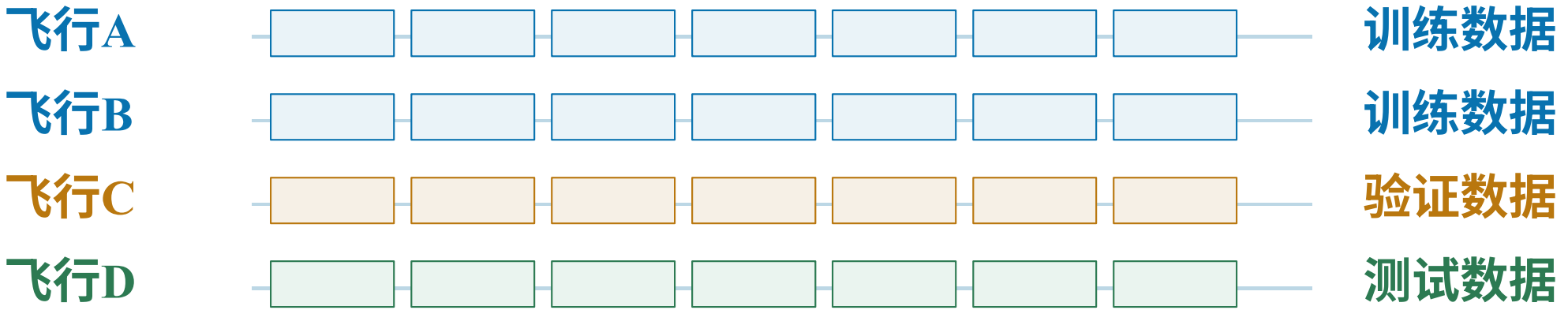
⊕ 类中心

图：已知标签提供比较依据，新样本通过相同特征进入分类空间

7.1.3 无人系统健康管理：独立检验

模型见过相邻数据，还能算独立测试吗

先按整次飞行分组，再在各组内切窗口；同一次飞行的相邻窗口留在同一组。



离线训练：特征与标签配对

标签来自已核实的状态或故障记录；
按时间对齐，作为学习与评价依据。
在线输入使用可获得的观测特征。

独立测试：用保留飞行检验

归一化与模型由训练集拟合；
验证集用于选参，测试集保留到最后。
同时查看误报、漏报和判断延迟。

本章目录

健康管理与安全评估：本章学习路线

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

7.1.1 背景意义

教材对应：第7.1.1节

7.1.2 健康与安全的区别与联系

教材对应：第7.1.2、7.1.2.3节

7.1.3 无人系统健康管理

教材对应：第7.1.2.1节

7.1.4 算法开发挑战与验证

教材对应：第7.1.1节

7.1.4 算法开发挑战与验证：开发难点

算法开发面临组合、数据、实时、迁移与指标五个难点

组合多：故障位置、强度、时刻、工况和环境相互耦合，单一悬停用例不够。

真数据少：严重故障代价高，仿真覆盖与实物证据需要互相补充。

实时资源有限：诊断耗时、数据延迟与决策切换共同占用处置窗口。

迁移有条件：同一方法换机型、传感器或任务后，需要重新核对模型和阈值。

指标与工具不统一：缺乏统一评估指标，异构平台的评估工具难以通用。

7.1.4 算法开发挑战与验证：分层运行

控制、诊断和预测，应在不同时间尺度上协作

运动控制	测量 → 估计 → 控制分配 → 执行 典型为毫秒级（数百 Hz），及时修正运动
故障诊断	数据窗口 → 异常检测 → 类型／程度 典型窗口0.1–1 s，兼顾证据积累与检测延迟
预测与决策	未来能力 + 任务约束 → 降级／返航／维护 典型为分钟到架次，任务决策响应新风险

紧急保护按风险时限独立响应，不等寿命预测；各层用带时间戳的信息协作。

7.1.4 算法开发挑战与验证：分层证据

仿真扩大覆盖，实物证据检验模型遗漏

阶段	重点得到的证据	仍需补充
离线记录	数据质量、检测率、误报和延迟	动作执行后的后果
软件在环（SITL）	大规模故障组合下的闭环响应	模型误差、真实硬件约束
硬件在环（HITL）	计算负载、链路和时序效应	实物动力与传感差异
受控实物验证	规定条件下的实际响应	试验未覆盖的工况

7.1.4 算法开发挑战与验证：平台支撑

RflySim 从五个方面支撑健康管理与安全评估

极限工况批量测试：设置极端天气、卫星导航干扰、通信中断与电量骤降。

SITL／HITL 闭环评估：SITL 验证功能正确性，HITL 检验延迟与硬件扰动。

状态监控与可视化：仿真中观测状态变量、健康指标与诊断输出。

数据导出与训练：经 Python、Simulink、ROS 导出运行数据，离线训练模型。

仿真到实物迁移：自动代码生成把算法部署到真机，再检验一致性。

练习与讨论

练习：误差小、温度高，应该怎样继续判断?

现象：高度误差不超过0.1 m，某电机温度升高；
控制指令比健康参照高20%。

问题1：哪些是观测事实？哪些仍是关于原因的假设?

问题2：还应采集哪些信息，才能区分动力退化、载荷改变与风扰?

问题3：为什么不能只凭高度误差小就继续原巡检任务?

参考要点

参考：先补证据，再用剩余能力约束任务

事实与假设：温度和指令变化是事实；电机故障、阵风和载荷变化是待区分的解释。

补充观测：转速、电流、电压、载荷与风；采用相同工况的健康参照。

区分判据：先看指令升高是单路还是四路，再看温升与风的关系。

推力效能下降：同推力需求下指令升高；电流和温升须结合机理判断。

载荷增加：四路指令同时升高，各电机温升相近。

风扰：指令随航向或风向波动并伴随倾角，风停后恢复。

任务决策：检查控制余量、返航耗能和落点，必要时缩短任务或执行保护。

易错点：小误差可能来自控制补偿；不能把正常跟踪直接当成健康证明。

本节小结

从“看见异常”走到“知道还能做什么”

概念：异常、故障和失效对应不同层次；退化既可能被补偿，也可能耗尽控制能力。

判断：健康描述状态与能力，安全还取决于任务、环境、受影响对象和保护措施。

方法：从采集、处理和诊断走向预测与行动建议，再用离线记录、SITL、HITL 与受控实物分层检验结果。

易错点：把现象当原因、把当前健康当任务安全、把单层仿真结果当完整证据。

下一步：把可能的故障写成模型，才有可重复的注入、比较和改进。