本章目录

虚实安全强化与故障数据方法

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 5 个教学单元

7.3.1 虚实安全强化与仿真节点
教材对应：第7.1.4、7.1.5.1节

7.3.2 触发与用例设计
教材对应：第7.1.5.2节

7.3.3 自动测试与事件证据
教材对应：第7.1.5.2节

7.3.4 日志同步与标签
教材对应：第7.1.5.4节（故障数据标签）

7.3.5 数据划分与质量
教材对应：第7.1.5.4节

7.3 虚实安全强化与故障数据方法

7.3.1 虚实安全强化与仿真节点：安全强化训练框架

六个模块连接数据、判断、动作与整机改进

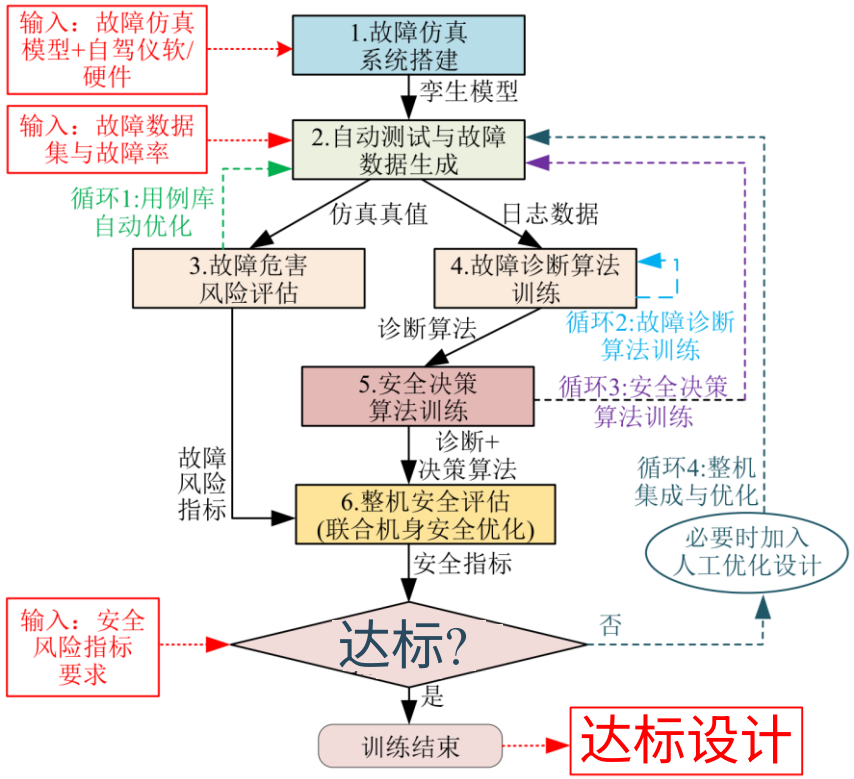


图7.6 安全强化训练框架

积累（模块1、2）：建仿真、做测试，获得工况与故障数据。

诊断（模块4）：用日志训练诊断，判断故障部位与原因。

决策（模块5）：结合任务与能力，训练并选择响应动作。

评估（模块3、6）：评估危害与整机，检验并更新设计。

7.3.1 虚实安全强化与仿真节点：自动测试与数据分流

真值用于评估后果，日志用于形成诊断证据

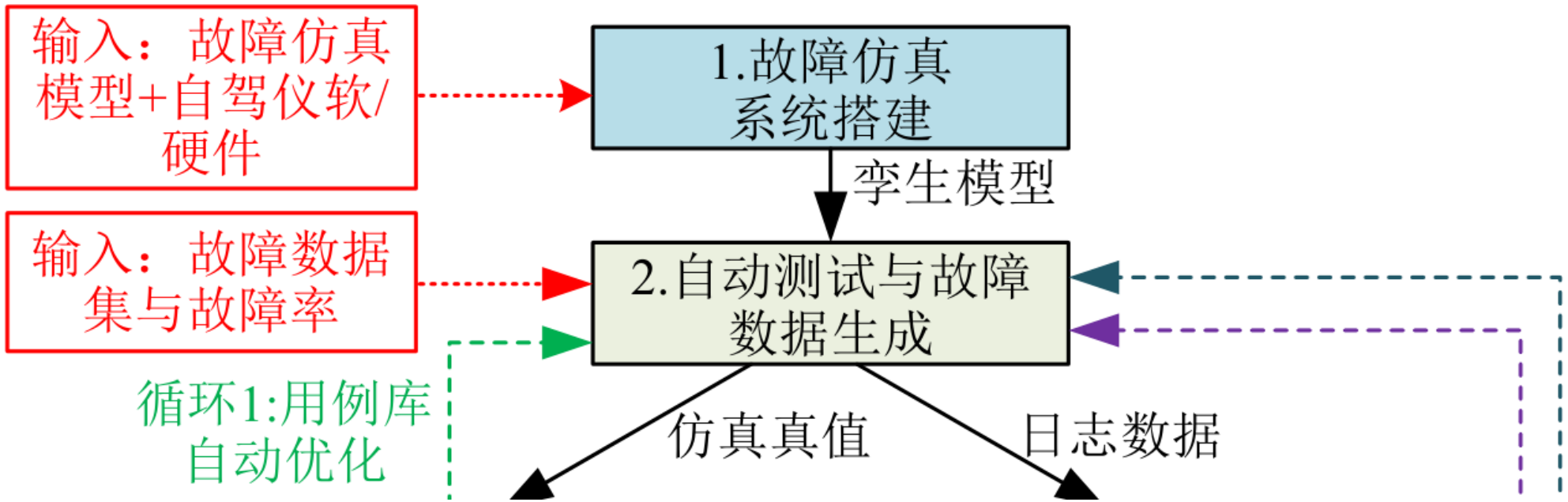


图7.6（上部）仿真系统、测试数据与用例库优化

循环1调整测试覆盖；故障发生率取自可靠性依据，测试注入比例用于组织样本。

7.3.1 虚实安全强化与仿真节点：诊断与策略反馈

诊断和决策分别训练，再一起接受整机评价

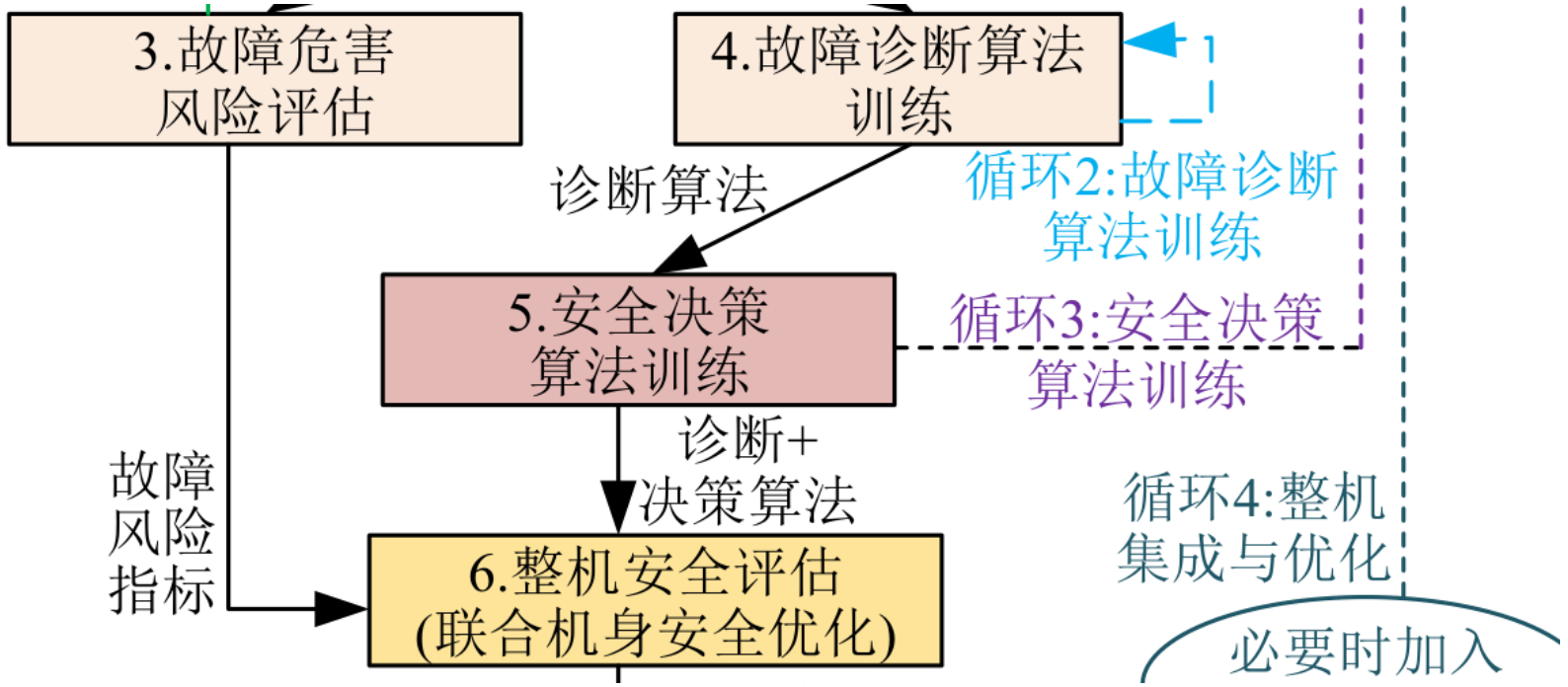


图7.6（中部）诊断、决策与整机评估的不同输入

循环2：改诊断，减少误报与漏报。

循环3：改动作，降低故障后的危害。

联合评价：把识别结果和执行后果一起检查。

7.3.1 虚实安全强化与仿真节点：虚实节点

三类节点验证的对象不同

节点	自驾仪运行位置	机体与传感器来源
SITL（软件在环）	计算机中的自驾仪程序	运动模型、模拟传感器
HITL（硬件在环）	真实飞控硬件	运动模型、模拟传感器
真机实验	真实飞控硬件	实物机体、执行器与传感器

SITL便于重复与批量测试；HITL检查板上执行；真机补充实际物理证据。

7.3.1 虚实安全强化与仿真节点：教材平台图

控制量和反馈在三类节点中闭合

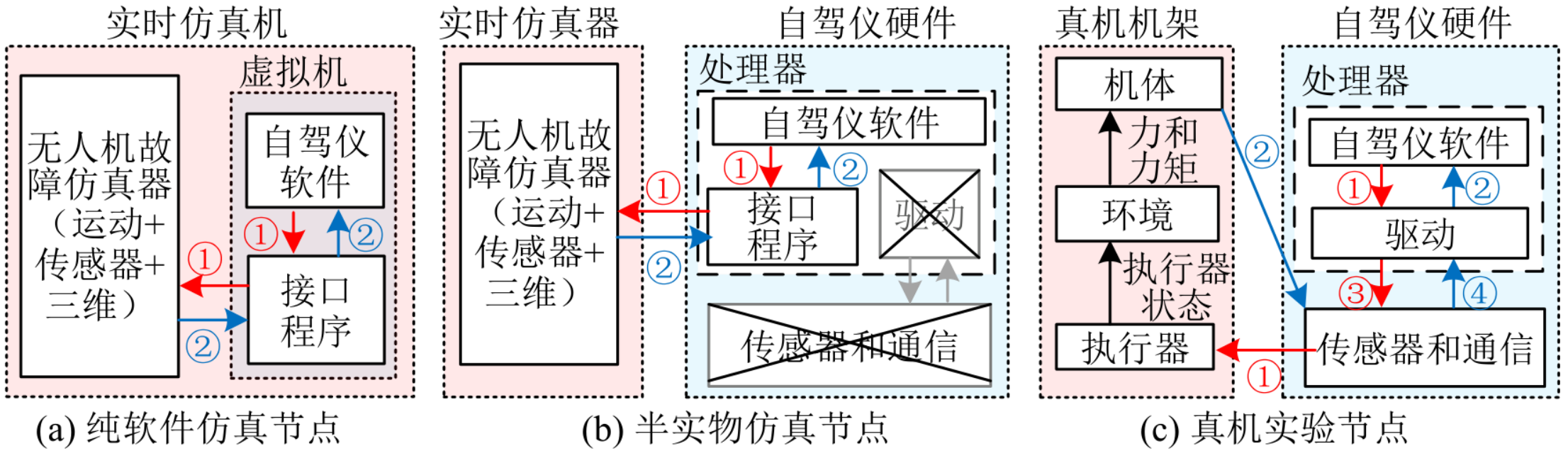
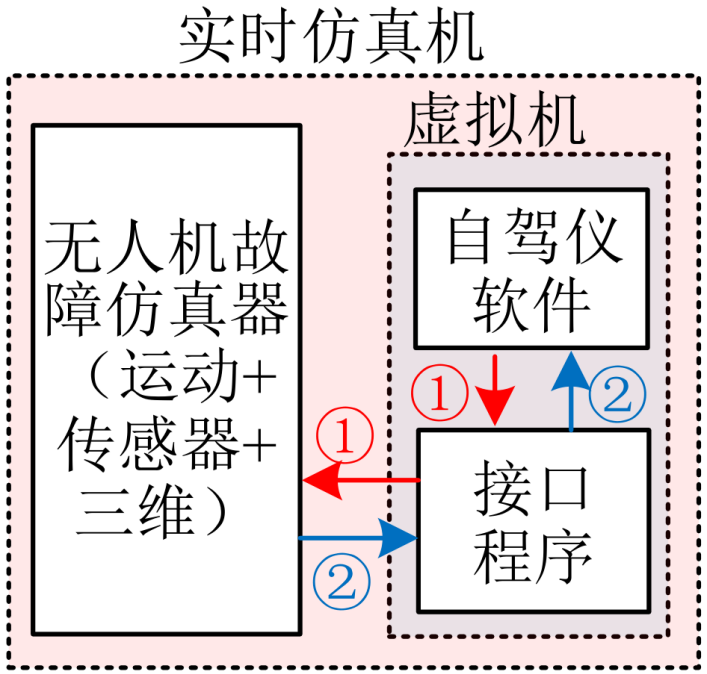


图7.7 软件/半实物仿真和真机实验系统

7.3.1 虚实安全强化与仿真节点：纯软件节点

软件在环由接口程序交换模型数据



(a) 纯软件仿真节点

图7.7(a) 纯软件仿真节点

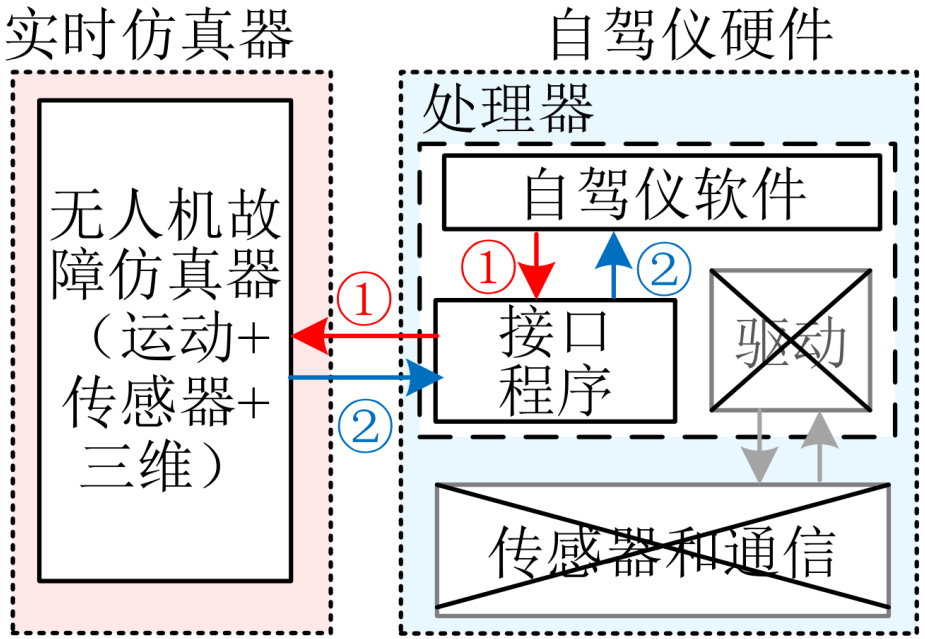
控制链： 自驾仪软件给出执行器控制量，仿真器更新机体运动。

反馈链： 模拟传感器产生测量，自驾仪计算估计并反馈控制。

注入位置： 电机效能在模型动力链中改变，飞控仍处理其运动响应。

7.3.1 虚实安全强化与仿真节点：半实物节点

半实物仍依赖载具与传感器模型



(b) 半实物仿真节点

图7.7(b) 半实物仿真节点

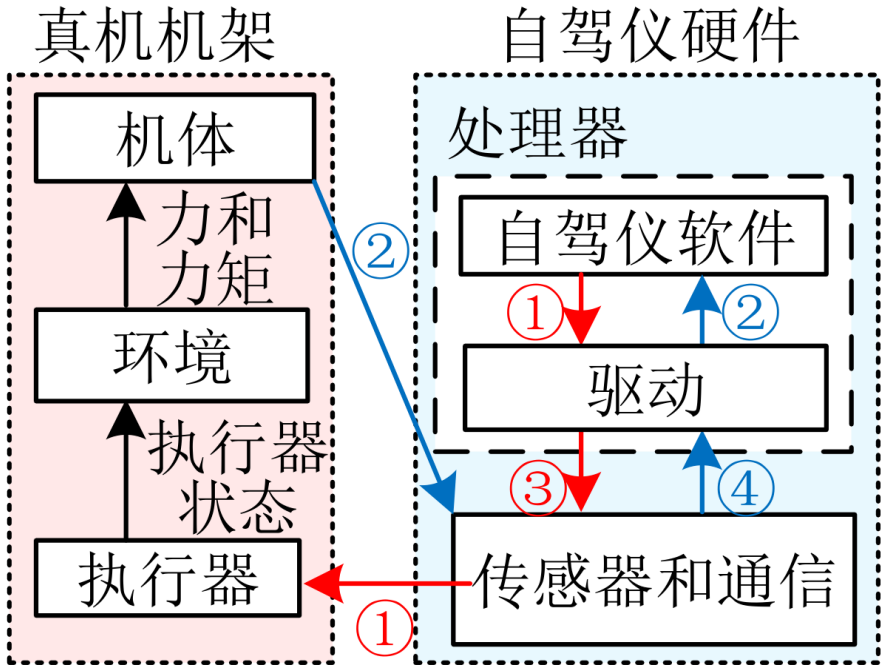
真实部分： 飞控处理器、固件执行、接口与通信时延。

模拟部分： 机体运动、电机动力与传感器测量。

模型故障： 仍由仿真器的故障DLL接收与响应；DLL即动态链接库（见课件4.9）。

7.3.1 虚实安全强化与仿真节点：真机节点

真机把驱动、执行器和传感器接入闭环



(c) 真机实验节点

图7.7(c) 真机实验节点

①与②： 执行器控制输出、机体运动状态。

③与④： 控制与传感数据的传输电信号。

验证范围： 固件、驱动、实物响应及环境共同决定结果。

7.3.1 虚实安全强化与仿真节点：虚实并行与交叉验证

同一任务分发到不同节点，真机数据校正仿真

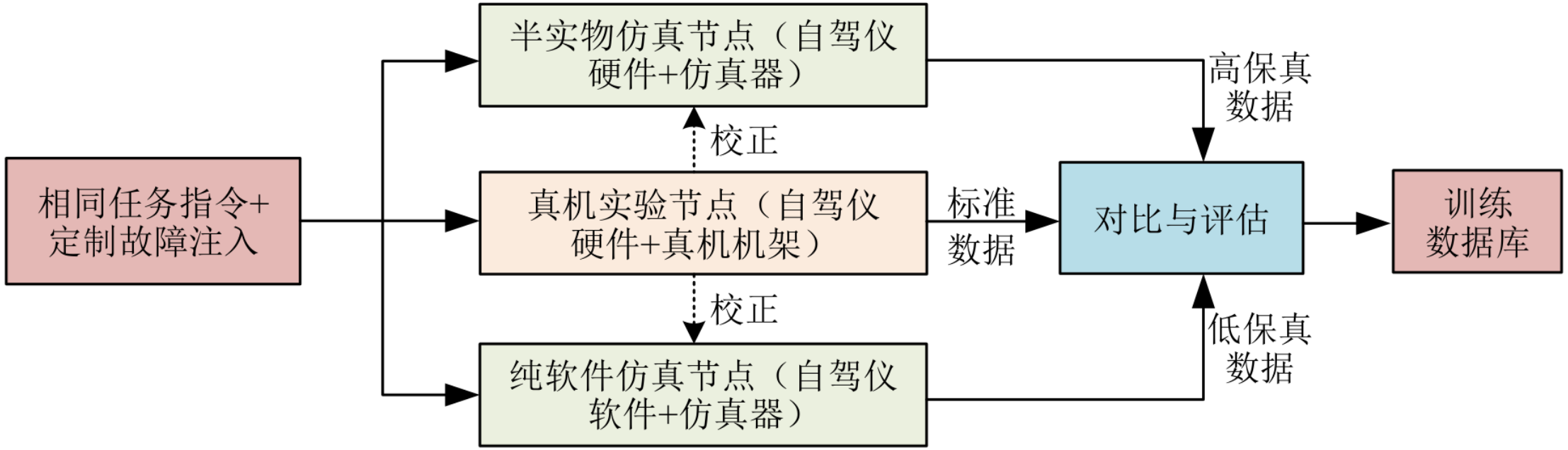


图7.8 虚实结合并行实验与交叉验证

硬件在环（HITL）接入真实飞控；软件在环（SITL）批量覆盖；真机校准目标工况。

7.3.1 虚实安全强化与仿真节点：虚实结果的可比性

比较前先对齐输入、坐标、事件与版本

对应图7.8：真机节点给出标准数据，校正半实物与纯软件节点；三类响应进入对比与评估。比较之前，三类条件先对齐。

输入与工况	变量与事件	版本与误差
指令：同任务与故障注入	**坐标：**同方向与单位	**软件：**固件与控制器版本
初态：同初始状态与载荷	**时间：**统一时间基准	**模型：**模型与传感器版本
扰动：匹配风扰条件	**事件：**核对故障生效时刻	**归因：**参数、时序或工况
	延迟：如实保留不平移	

结论：日志等长不等于已同步；事件延迟可能正是被测差异，不能平移消去。

本章目录

虚实安全强化与故障数据方法

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 5 个教学单元

7.3.1 虚实安全强化与仿真节点
教材对应：第7.1.4、7.1.5.1节

7.3.2 触发与用例设计
教材对应：第7.1.5.2节

7.3.3 自动测试与事件证据
教材对应：第7.1.5.2节

7.3.4 日志同步与标签
教材对应：第7.1.5.4节（故障数据标签）

7.3.5 数据划分与质量
教材对应：第7.1.5.4节

7.3.2 触发与用例设计：故障注入方法

三种注入方法对应不同实施条件

方法	施加异常的位置	适用条件
模型注入	DLL动力/传感器/环境模型 如噪声漂移、数据冻结	SITL / HITL；加载对应故障模型
源码注入	自驾仪驱动、调度或控制逻辑 如定位驱动丢星、死机卡顿	SITL / HITL / 真机； RflySim推荐方式之一
真机注入	实际执行器、传感器或机体 如继电器断电、刀片破桨	真机专用试验条件 课堂主线不使用

作用位置决定观察顺序，实施方法决定实验条件。

7.3.2 触发与用例设计：用例与运行记录

一条用例约定条件，一次记录提供证据

用例
条件与判据 → 执行
触发与重置 → 运行记录
日志与事件 → 数据样本
特征与标签

用例编号：标识任务、初值、故障设定和判据；同一编号可以重复运行。

运行编号：标识某一次执行；绑定日志、事件、版本及执行状态。

正常对照：保持任务与环境相同，关闭故障；用来分辨正常机动和异常响应。

比较的基础是控制条件，可信的结果还要能追溯到记录。

7.3.2 触发与用例设计：故障触发方式

固定触发便于比较，随机触发扩展工况

确定性触发

条件：预设时刻（如 15 s）、任务阶段或状态阈值满足时触发。

记录：保存条件表达式、满足条件的时刻及注入生效时刻。

用途：功能验证、边界测试与回归。

不确定性触发

条件：以设定概率在运行中触发，或按分布抽取时刻与参数。

记录：分布、范围、随机种子（可复现抽样序列）与每次取值。

用途：模拟低概率高风险事件；结合蒙特卡罗仿真扩大覆盖。

触发分布描述测试覆盖，现实发生概率需要独立证据。

7.3.2 触发与用例设计：生效证据与记录

注入方法不同，生效证据与记录内容也不同

方法定义：见课件7.3.2「故障注入方法」页；这里只看各方法的生效证据与记录内容。

方法	生效证据	记录内容
模型注入	模型参数或状态已切换， 真值响应随之改变	故障编号与参数、 注入命令时刻、仿真真值
源码注入 （推荐方式之一）	固件内部状态变化， 如定位精度下降、卫星数减少	固件版本、故障编号与参数、 飞控日志相关话题
真机注入	部件物理状态改变， 由独立测量确认	试验条件、操作时刻、 独立测量数据

本节用例：对照用例采用模型注入；配置中写明作用层、故障编号与参数。

7.3.2 触发与用例设计：对照用例

正常与故障组只改变被研究的因素

条件	正常用例 N01	故障用例 F01
共同条件	同一机型、模型、控制器；15 m 悬停	与正常组相同；保留环境与随机种子
故障设定	关闭故障；电机效能系数为 1	单电机效能系数设为 0.6
时序约定	0 s 解锁（arm）；5 s 起飞；25 s 结束	同一任务；15 s 触发所选故障
记录与判据	高度、速度、姿态、输出和事件；悬停误差与终止原因	相同变量；增加注入生效证据及故障后响应

示例设计：效能系数无单位，1 为正常；运行前核对通道、初值与停止条件。

本章目录

虚实安全强化与故障数据方法

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 5 个教学单元

7.3.1 虚实安全强化与仿真节点
教材对应：第7.1.4、7.1.5.1节

7.3.2 触发与用例设计
教材对应：第7.1.5.2节

7.3.3 自动测试与事件证据
教材对应：第7.1.5.2节

7.3.4 日志同步与标签
教材对应：第7.1.5.4节（故障数据标签）

7.3.5 数据划分与质量
教材对应：第7.1.5.4节

7.3.3 自动测试与事件证据：故障数据获取流程

测试程序把任务、数据和评价连成循环

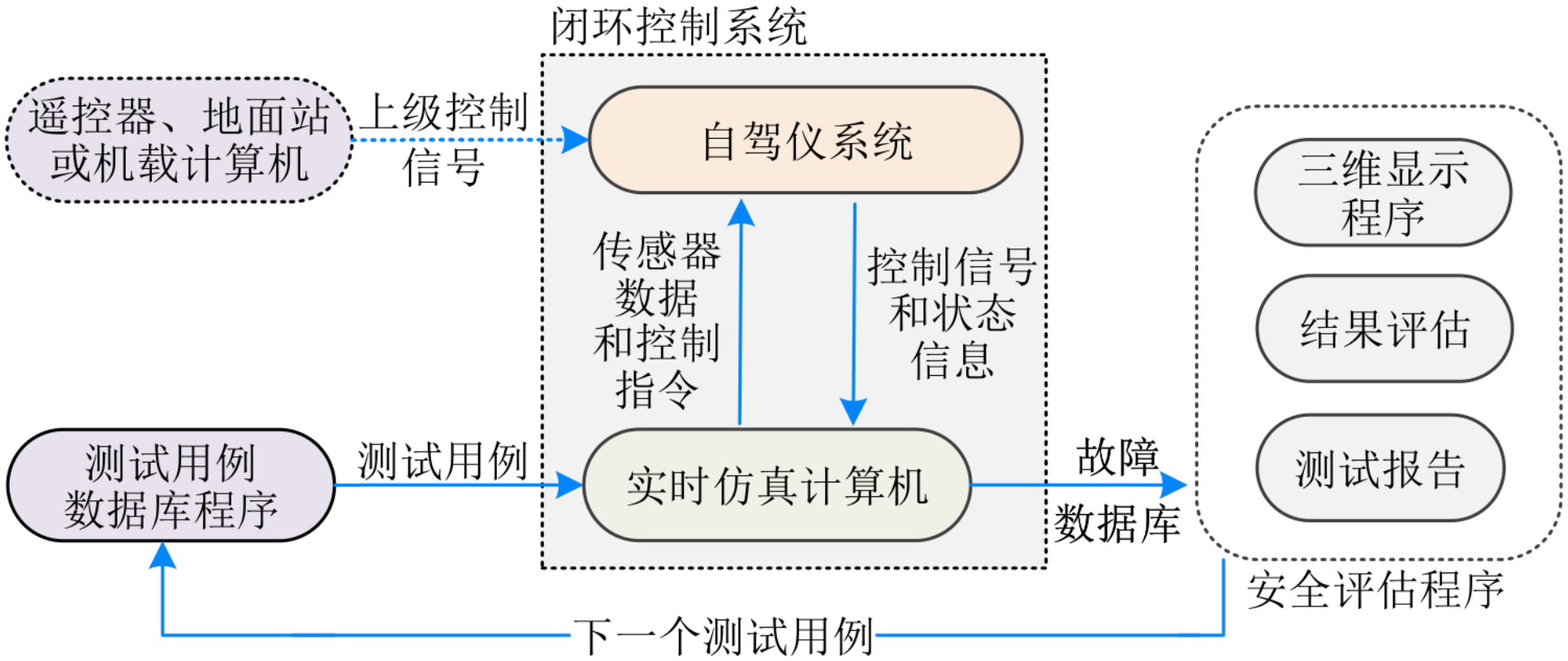
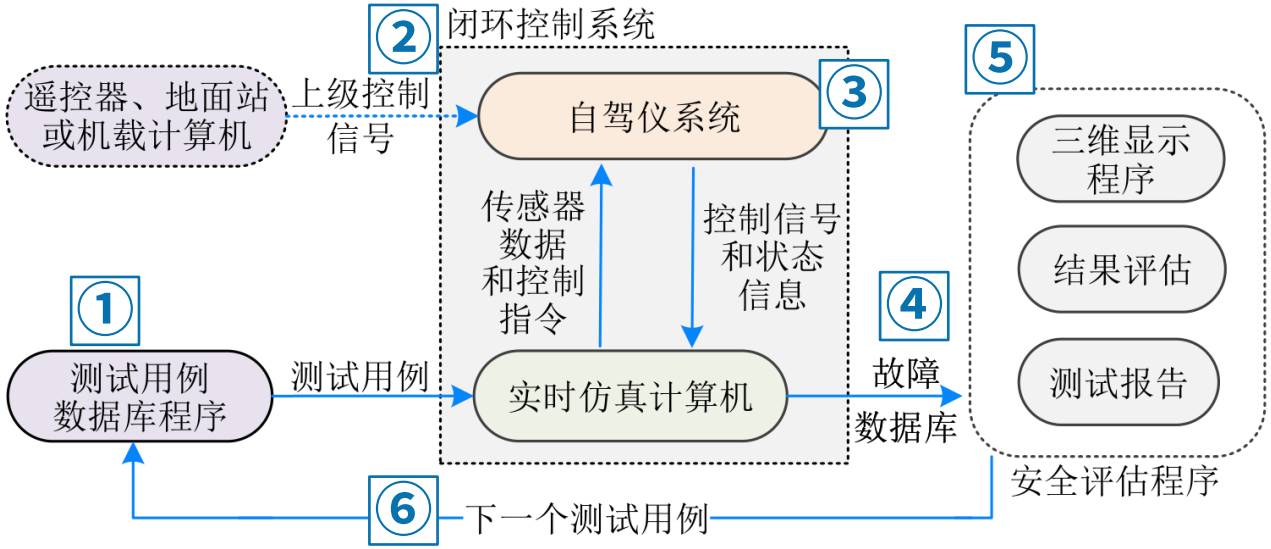


图7.9 自动化测试与训练框架

7.3.3 自动测试与事件证据：六步流程

图7.9 按六步逐条执行用例，评估后取下一条



① 用例库逐条发出用例
② 闭环自动初始化、执行任务
③ 触发故障，日志标注时刻
④ 终止时记录状态、收齐日志
⑤ 评估程序对比任务预期
⑥ 评估完请求下一条用例

图7.9（缩图）编号对应右侧六步

用例内容：启动仿真、执行任务、故障注入、参数收集与安全评估的控制序列。

评估三问：故障是否被准确诊断？安全决策是否正确触发？故障后运动是否符合预期？据此输出定量指标。

7.3.3 自动测试与事件证据：闭环与数据来源

运动真值与飞控估计值来自不同位置

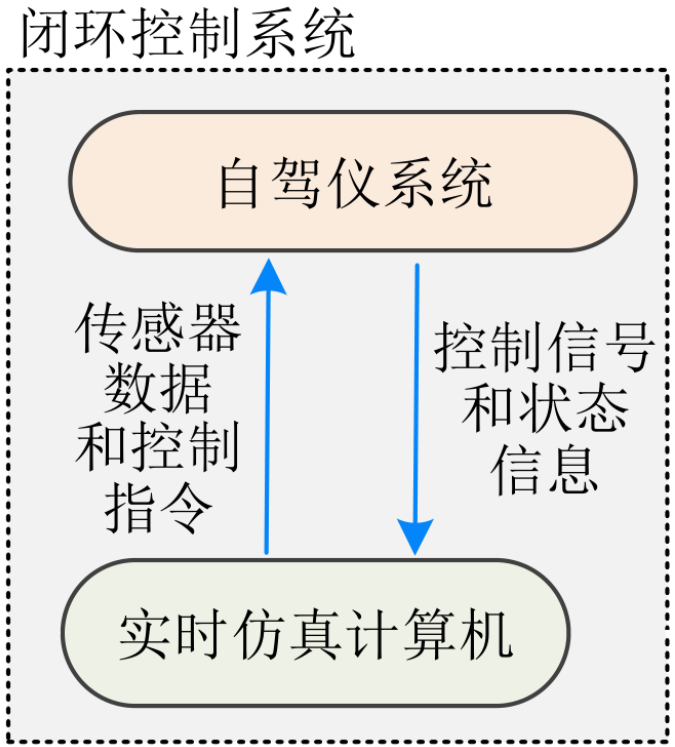


图7.9（中部）自驾仪与仿真闭环

模型真值：仿真计算机更新的位置、速度和姿态，供结果核验。

飞控估计：自驾仪依据传感数据估计状态，供控制与诊断使用。

控制输出：自驾仪给执行器的指令；不能直接当作电机实际转速。

7.3.3 自动测试与事件证据：每轮执行顺序

重置恢复初值，结束条件封存这一轮

恢复初值 → 执行任务 → 触发故障 → 结束并封存

检查时点	恢复或确认的对象	留下的证据
开始前	模型故障状态、飞控模式； 运动初值与日志缓存	运行编号、初值、模型与固件版本
触发时	时间/阶段条件与注入接收状态	命令、接收或生效标记及实际参数
结束时	到时、越界、坠地或数据中断	终止原因、完整日志及可用性状态

7.3.3 自动测试与事件证据：论文示范用例

论文 Table 1 用时序与判据定义示范用例

论文 Table 1 时点	动作	记录与示例判据
5 s	解锁	记录位置、速度、姿态和角速度
10 s	起飞至 10 m 并悬停	悬停并记录故障前基线
20 s	停止 2 号电机	姿态波动 ≤10°； 最大撞地速度 ≤5 m/s
25 s	停止仿真并记录	按所述判据分析这次测试

出处：Dai 等（2021），Aerosp. Sci. Technol.；平台为 FPGA 支持的 HITL（硬件在环）。
DOI：10.1016/j.ast.2021.106727（链接见本节学习资料）
安装版：[安装目录]/RflySimAPIs/PaperRes/0.RflySimToolChain/

7.3.3 自动测试与事件证据：故障事件标记

发出命令、故障生效和检测时刻分别标记

命令发送 控制端 → 故障生效 模型或固件 → 观测响应 日志通道 → 诊断输出 报警记录

e18 例程用 SendFaultEvent 把注入命令写入飞控日志（command=31000）。

事件字段	具体含义或示例
run_id；event_type	本次执行编号；command_sent / fault_effective / alarm
timestamp；fault_id	时刻与单位；作用层及故障编号
parameters；version	实际注入参数；模型、固件与采集配置版本

本章目录

虚实安全强化与故障数据方法

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 5 个教学单元

7.3.1 虚实安全强化与仿真节点
教材对应：第7.1.4、7.1.5.1节

7.3.2 触发与用例设计
教材对应：第7.1.5.2节

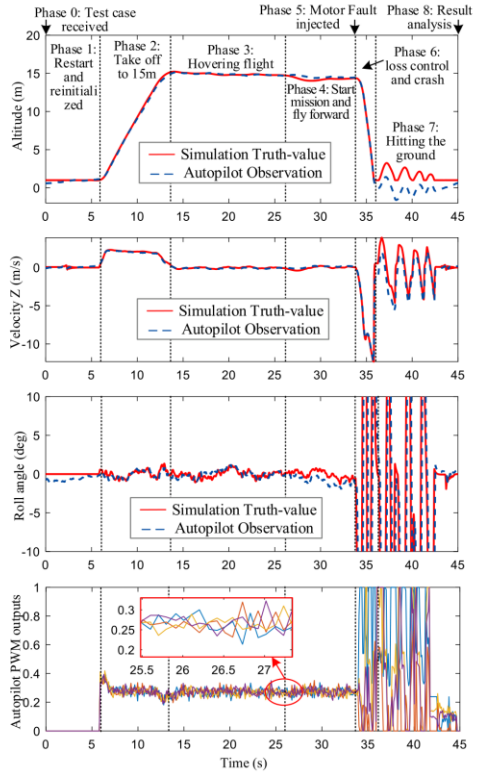
7.3.3 自动测试与事件证据
教材对应：第7.1.5.2节

7.3.4 日志同步与标签
教材对应：第7.1.5.4节（故障数据标签）

7.3.5 数据划分与质量
教材对应：第7.1.5.4节

7.3.4 日志同步与标签：论文正常与故障对照

论文 Fig.19 按事件读出一次堵转测试

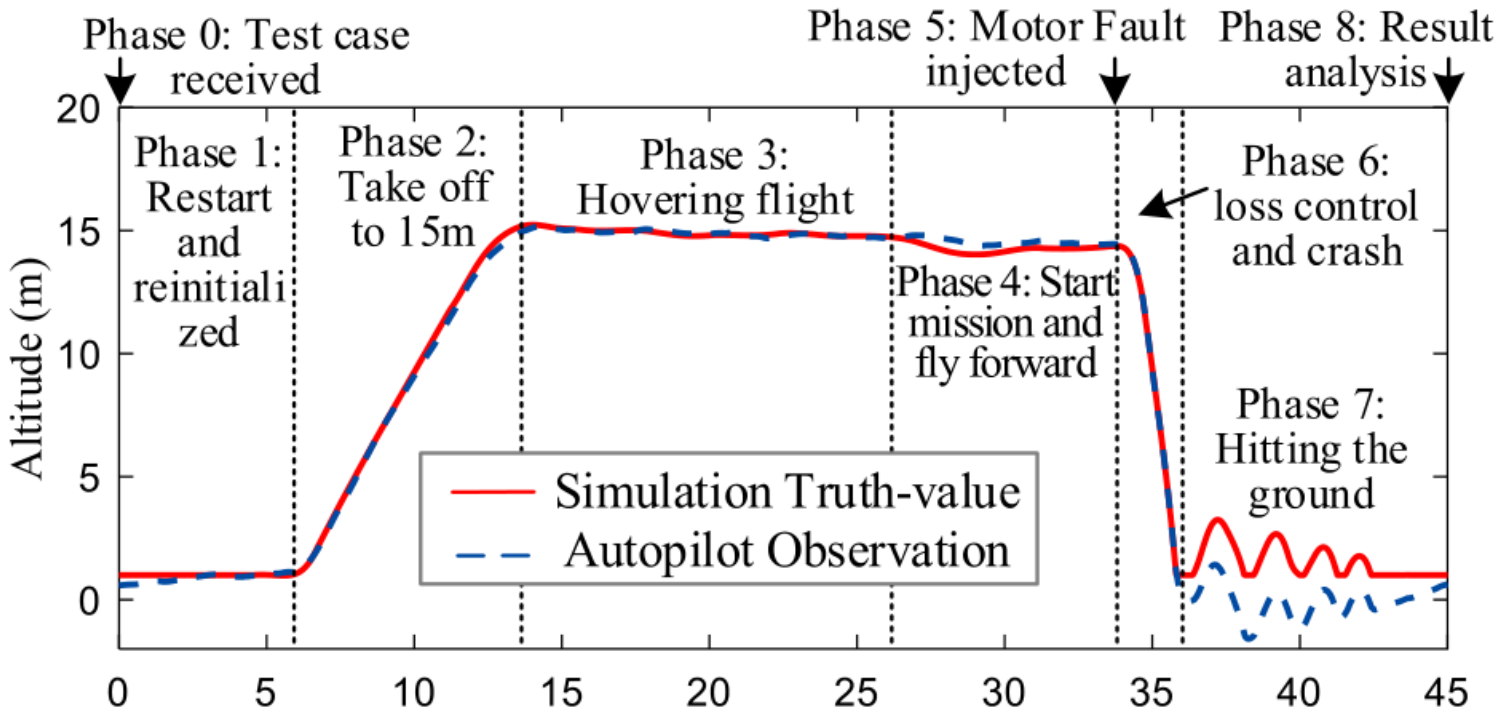


通道	正常段与故障后分别观察什么
高度（m）	悬停维持；堵转后快速降高并碰地
垂向速度（m/s）	正常任务响应；急剧下降及碰地后的振荡
滚转角（°）	小幅姿态变化；堵转后剧烈滚转
PWM 输出	正常调节；失控时剧变并触及端点

图：Dai 等（2021）Fig.19 全图，同一次 HITL 堵转测试的正常段与故障段

7.3.4 日志同步与标签：论文高度与阶段

正常悬停与堵转后的降高由事件分开



图：同上论文 Fig.19 高度与阶段局部

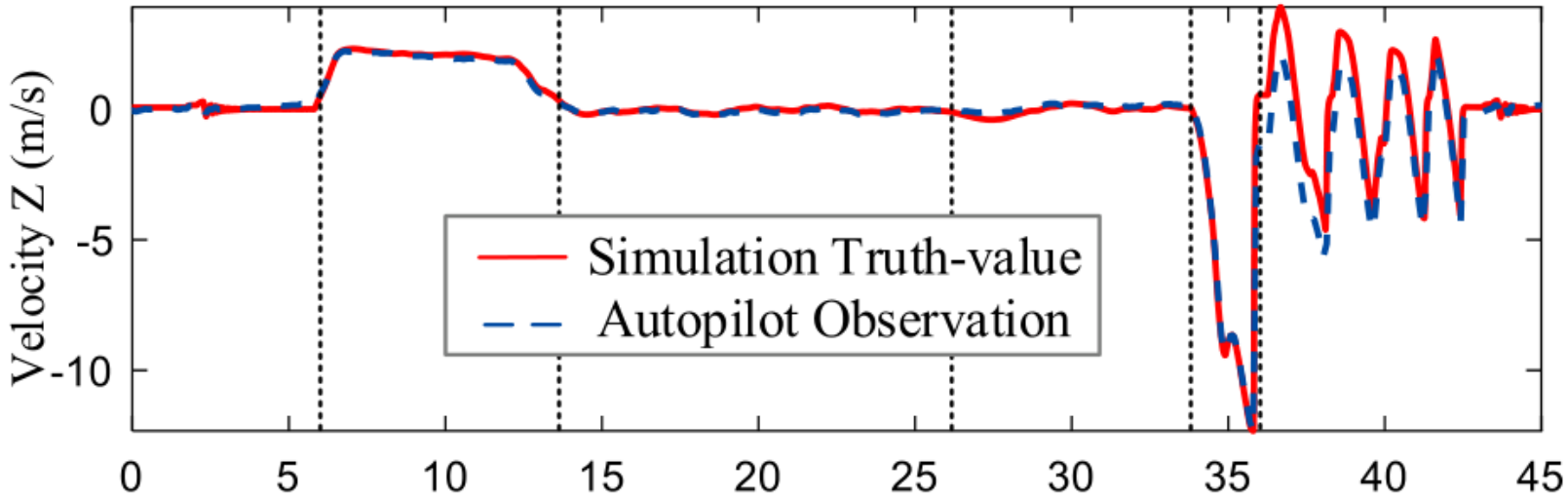
正常段：
约 15 m 悬停。

事件：
约 34 s 堵转。

响应：
降高后碰地。

7.3.4 日志同步与标签：论文垂向速度

碰地前后同时核对速度与状态来源



红实线
仿真真值

蓝虚线
飞控估计

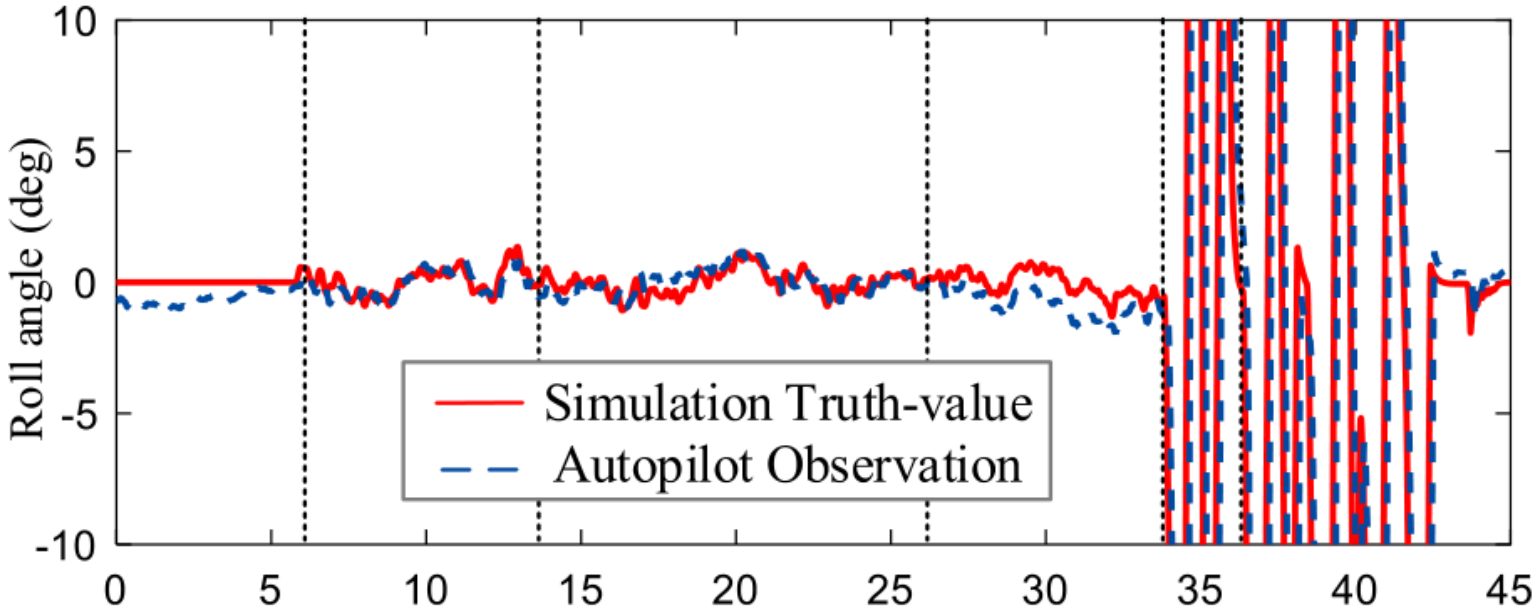
图：同上论文 Fig.19 垂向速度局部

符号： 原图 z 速度向上为正；NED（北东地）向下为正，比较前先变号。

证据： 撞地前的下降速度与碰地后的振荡分别读；峰值以原始数值记录核验。

7.3.4 日志同步与标签：论文姿态响应

剧烈滚转说明姿态约束已被破坏



图：同上论文 Fig.19 滚转角局部（纵轴 ±10°）

事件给出分段依据；姿态与高度、速度共同解释运动后果。

正常段：小幅滚转。　　**堵转后：**剧烈滚转。　　**读数：**边界非峰值。

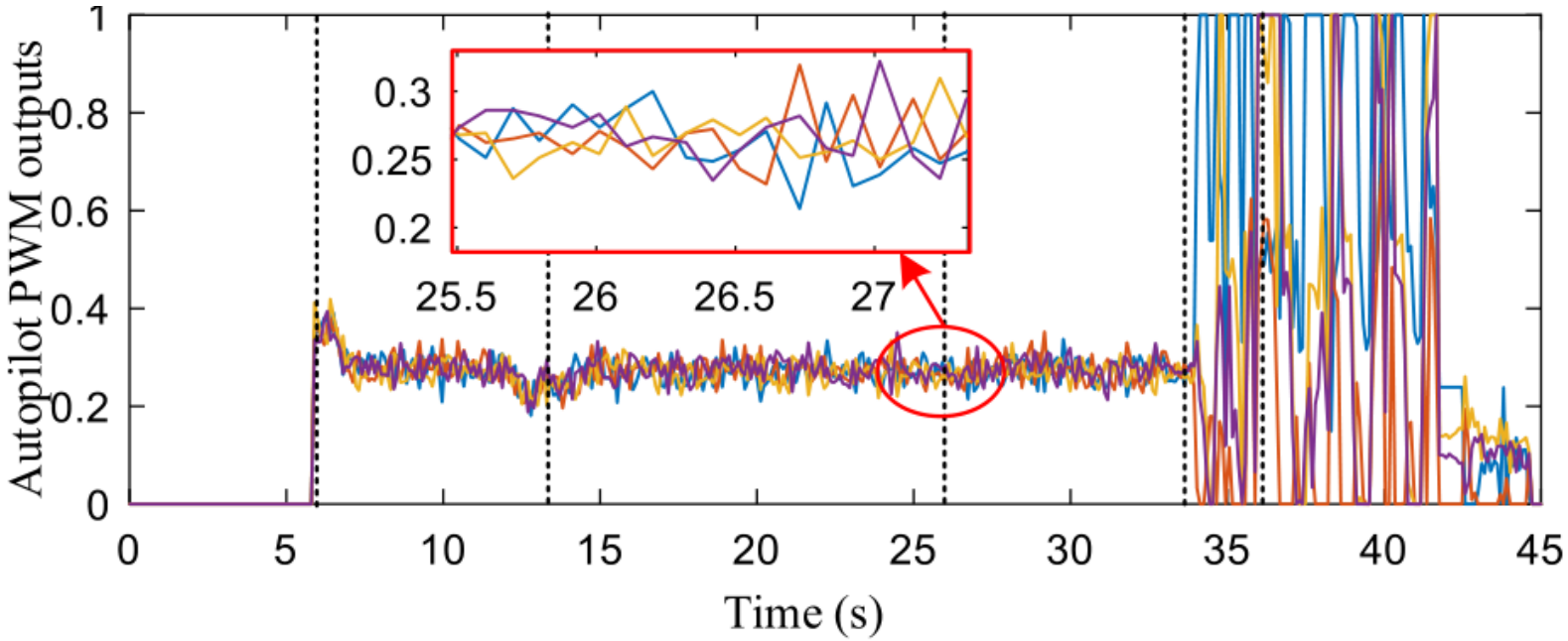
7.3.4 日志同步与标签：论文执行器输出

控制输出触及端点，仍要看实际运动

PWM：
脉宽调制输出。

端点：
0 或 1。

后果：
运动失控。



图：同上论文 Fig.19 四路电机 PWM 输出；红框为 25.5–27 s 局部放大

论文该控制配置未识别并处置这一堵转；结论受机型、模型与控制策略条件限制。

7.3.4 日志同步与标签：离线数据入口

e10 留存 ULG、四个通道表和处理结果

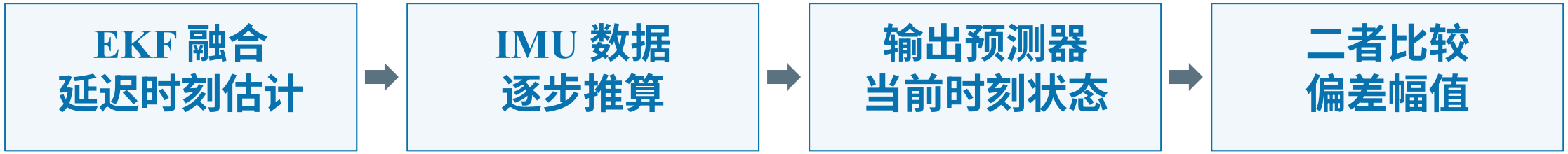
目录：[安装目录]/RflySimAPIs/7.RflySimPHM/0.ApiExps/e10_data_process/

data/ 下的真实文件	可读内容
09_23_59.ulg	原始二进制日志；保留采集上下文
09_23_59_actuator_outputs_0.csv	4 路输出指令（非实测转速）
09_23_59_estimator_status_0.csv	输出预测器误差：姿态/速度/位置 单位依次：rad、m/s、m
09_23_59_sensor_combined_0.csv	三轴角速度、三轴加速度
09_23_59_vehicle_magnetometer_0.csv	三轴磁场

入口：dataProcess.py → processed_data.csv；按各表 timestamp 对齐。

7.3.4 日志同步与标签：输出预测器误差

输出预测器把延迟的 EKF 估计推到当前时刻



输出预测器：用 IMU 数据把延迟融合时刻的 EKF 估计逐步推算到当前时刻。

跟踪误差：输出预测器状态与 EKF 估计之差的幅值；
三项依次为姿态（rad）、速度（m/s）、位置（m）。

区分：它反映估计器内部推算的一致性，与控制器跟踪目标轨迹的误差不同；
output_tracking_error 的三项不是 x、y、z 分量。

7.3.4 日志同步与标签：多源时间同步

时间戳与单位先统一，再插值到公共时刻

通道 A 原样本	通道 B 目标时刻	对齐结果（教学例）
32.0 s → 0	32.1 s	A 在目标时刻取插值 1
32.2 s → 2	32.2 s	A 保留原样本 2

x 是被对齐的连续量，两端读数使用同一单位。

$$x(32.1) = 0 + \frac{32.1 - 32.0}{32.2 - 32.0}(2 - 0) = 1$$

连续量可插值；离散事件按区间标记；跨设备的时间偏移先由共同事件校准。

PX4 通道时间戳以微秒记录；秒制时间为 $t_s = t_{us}/10^6$。

7.3.4 日志同步与标签：e10 对齐方式

e10 使用时间戳并集，采样间隔并不固定

32–36 s 开区间内的通道	原样本数	相邻时间差中位数
执行器输出	40	100 ms
估计器状态	467	8 ms
惯性传感器	658	4 ms
磁场	59	70 ms

合并后的时刻：712 个；相邻间隔为 3–13 ms，中位数为 4 ms。

插值边界：端点之外代码延用端值（np.interp）；使用前核对缺口与有效时间范围。

7.3.4 日志同步与标签：标签阈值与曲线

标签分界来自代码阈值，事件分界来自注入记录

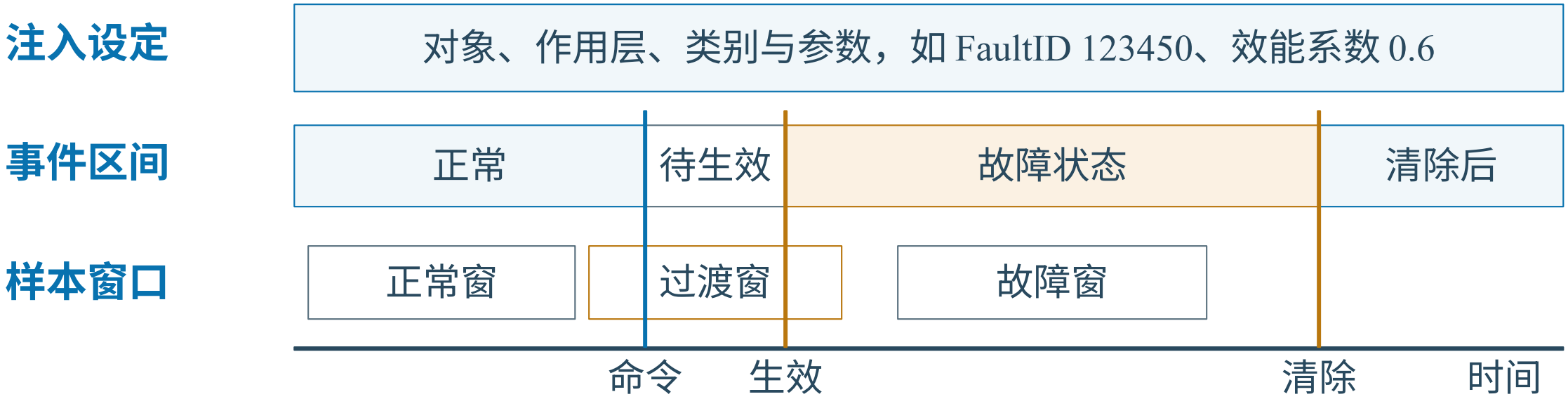
机体 x 轴角速度；虚线是代码阈值；此日志无注入事件记录（command=31000）。



图：e10 留存 sensor_combined 数据，机体 x 轴角速度，32–36 s

7.3.4 日志同步与标签：故障数据标签

故障类别、参数与时间区间一起构成标签



e10 第13列 flag 只按 34 s 阈值生成：0/1 为 343/369 行，首个 1 在 34.004 s；
日志无同步标志，类别需由事件确认。

天然标签：注入时写入同步标志，注入参数直接成为标签，免去人工标注。

7.3.4 日志同步与标签：统计特征预处理

滚动特征提取局部水平与波动

e10 流程：16 个原始量 ×（原值、滚动均值、样本标准差）＋1 标签＝49 列。

教学一步：角速度样本为 0、0.01、0.02 rad/s，取 3 行窗口。

$$\bar{x} = \frac{0 + 0.01 + 0.02}{3} = 0.01\,\text{rad/s} \qquad s = \sqrt{\frac{\sum_{i=1}^{3}(x_i - \bar{x})^2}{3-1}} = 0.01\,\text{rad/s}$$

实际循环：e10 用 10 行滚动窗口；行间隔不固定，窗口时长也不固定。

复算方法：按同一窗口重算，结果应与 processed_data.csv（712×49）一致。

后续处理：特征多时可再降维；过渡窗、起始短窗与常量通道分别登记。

本章目录

虚实安全强化与故障数据方法

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 5 个教学单元

7.3.1 虚实安全强化与仿真节点
教材对应：第7.1.4、7.1.5.1节

7.3.2 触发与用例设计
教材对应：第7.1.5.2节

7.3.3 自动测试与事件证据
教材对应：第7.1.5.2节

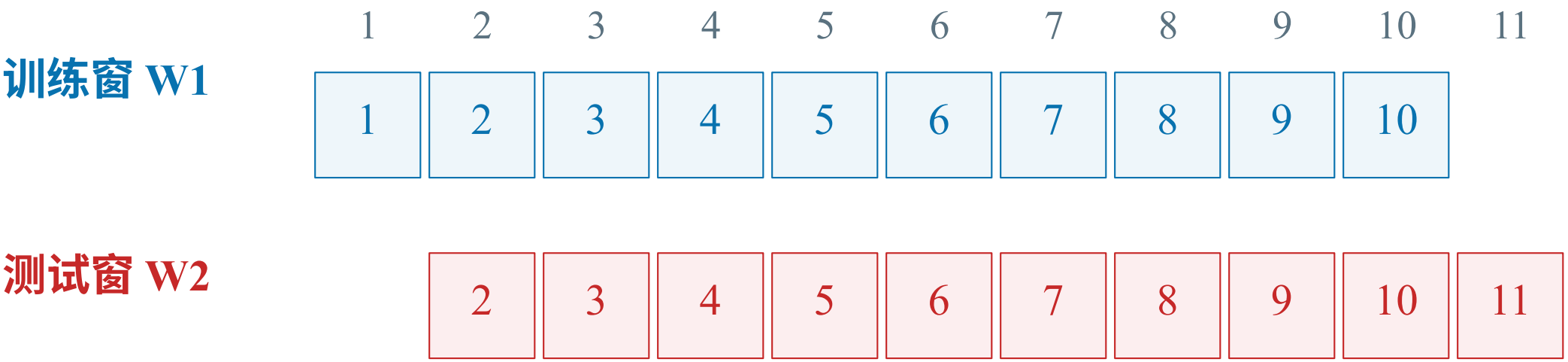
7.3.4 日志同步与标签
教材对应：第7.1.5.4节（故障数据标签）

7.3.5 数据划分与质量
教材对应：第7.1.5.4节

7.3.5 数据划分与质量：滑窗数据泄漏

相邻窗口共享 9 行，会把同一记录带进测试

数据泄漏指测试信息进入训练。例：窗长 10 行、步长 1，窗口随机分给训练和测试。



共同原样本：第 2–10 行，共 9 行，占每窗 90%。

随机分窗口可能只测到记忆，独立飞行才能检验对新数据的泛化。

7.3.5 数据划分与质量：训练验证测试划分

先分完整飞行，再在组内生成窗口

完整飞行列表 → 按飞行/工况分组 → 组内切窗口

组别（教学例）	完整飞行	用于什么决定
训练组	F01、F02 的全部记录	学习模型；算归一化均值与尺度
验证组	F03 的全部记录	选模型、阈值与超参数 （超参数在训练前设定）
测试组	F04 的全部记录	最终报告；评价前固定模型和阈值

同一飞行、相邻窗口和配对的正常/故障片段保持在同一组。

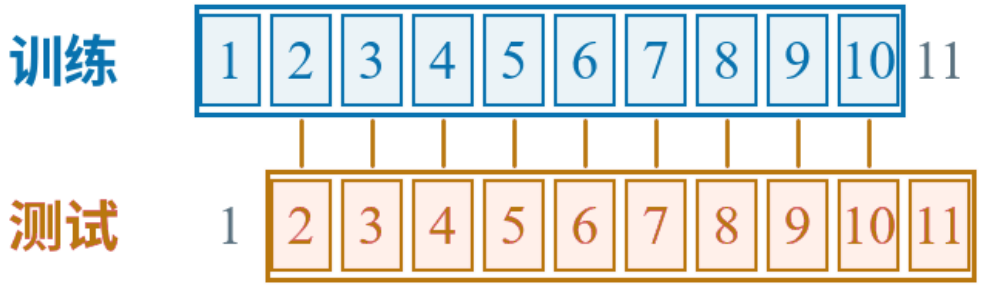
7.3.5 数据划分与质量：移动窗口对比

移动窗口共享采样点，完整飞行隔离组别

窗长10行、步长1行；先按完整飞行分组，再在各组内部生成窗口。

先开窗，再随机分组

原始行号 F01

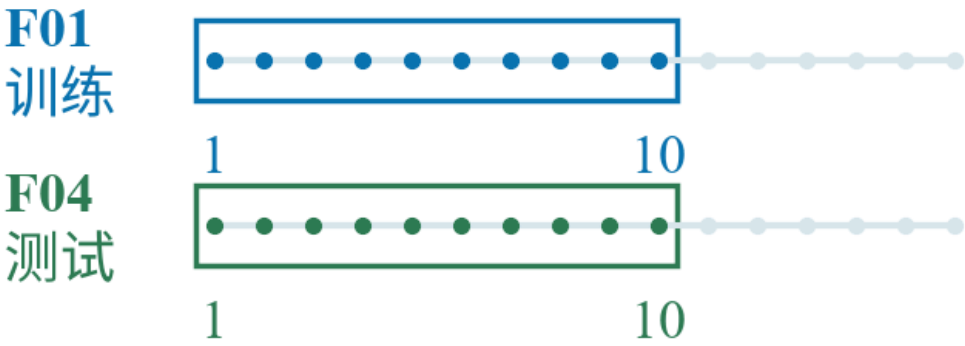


共享 9 / 10

同一飞行内可重叠；跨组保留完整飞行边界

先分飞行，再开窗

F01 / F02 → 训练　F04 → 测试



跨组共享 0

图：行索引与窗口示意；归一化和特征选择只在训练侧拟合。

7.3.5 数据划分与质量：数据质量检查

数据可用性先于诊断模型分数

检查对象	判断依据	处理与记录
时间与采样	排序、重复、间隔分布、缺口	限制插值缺口； 剔除采样频率异常的记录
数值与语义	单位、坐标、缺失、常量或饱和	e10 本段 x 轴加速度全0；核对通道
事件与标签	类别、参数、生效标记、过渡窗	追溯原事件；登记标签规则
类别与划分	各类独立飞行数、工况及组别	先分组； 批量仿真防类别失衡

质量报告写清有效飞行数、排除原因和处理规则，才能解释诊断结果的适用范围。

本节学习资料

数据与方法都有可定位的原始入口

已有故障数据：RflyMAD 作者项目

https://rfly-openha.github.io/documents/4_resources/dataset.html

日志结构与时间戳：PX4 ULog 格式

https://docs.px4.io/v1.13/en/dev_log/ulog_file_format

数据泄漏与预处理：scikit-learn 官方文档

https://scikit-learn.org/stable/common_pitfalls.html

自动测试原论文：Dai 等（2021），Table 1 / Fig.19

https://doi.org/10.1016/j.ast.2021.106727

练习与讨论

把本节方法用到新数据与新用例

问题 1：要把 e10 的 flag=1 命名为某类故障，还需要哪些记录？平台用什么写入？

问题 2：窗口 20 行、步长 5，相邻两窗共享多少行、占每窗几成？应怎样划分？

问题 3：为陀螺仪噪声故障设计一对正常/故障用例，写出触发条件和事件字段。

作答要求：写出依据的记录或计算过程，以及可检验的处理规则。

参考要点

每题落到具体记录、数值或用例字段

1. 标签含义： flag=1 只表示 34 s 之后；补 FaultID、参数、注入事件与时钟映射；e18 的 SendFaultEvent 写入 command=31000 记录。

2. 重叠窗口： 共享 20−5＝15 行，占每窗 75%；
先分完整飞行，组内切窗；预处理只拟合训练组。

3. 用例设计： 同任务同环境；故障组 15 s 注入 FaultID 123543（陀螺仪噪声）；
正常组不注入；记录 run_id、FaultID、噪声增益、命令与生效时刻。

合格交付能从每个样本追回原始记录、事件、处理规则和数据组别。

本节小结

可信数据来自可比较、可追溯和独立检验

用例：任务、初值、故障、触发、结束、记录和判据共同定义一次测试设计。

证据：命令（e18 写入 command=31000）、生效、观测和诊断分别标记；真值与飞控估计同时核对。

数据：先统一时间和通道语义，再切片、提取特征；标签保留物理含义与来源。

检验：先分完整飞行再切窗；检查事件、缺口、无效值、类别与组间重复。

易错点：用例条数不等于已测次数；34 s 阈值不是已确认故障；
命令时刻不是生效时刻；堵转不是渐进退化。