本章目录

故障注入接口与算法开发框架

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

7.7.1 故障作用层与注入框架
教材对应：第7.2.1节

7.7.2 评估与诊断开发框架
教材对应：第7.2.2节

7.7.3 故障ID与参数接口
教材对应：第7.2.1、7.2.3节

7.7.4 注入、恢复与复位规则
教材对应：第7.1.5.2、7.2.3节

7.7.5 观测接口与生效验证
教材对应：第7.1.2.3、7.1.5.1、7.2.3节

7.7 故障注入接口与算法开发框架

7.7.1 故障作用层与注入框架：注入框架

故障首先对应一个具体作用层

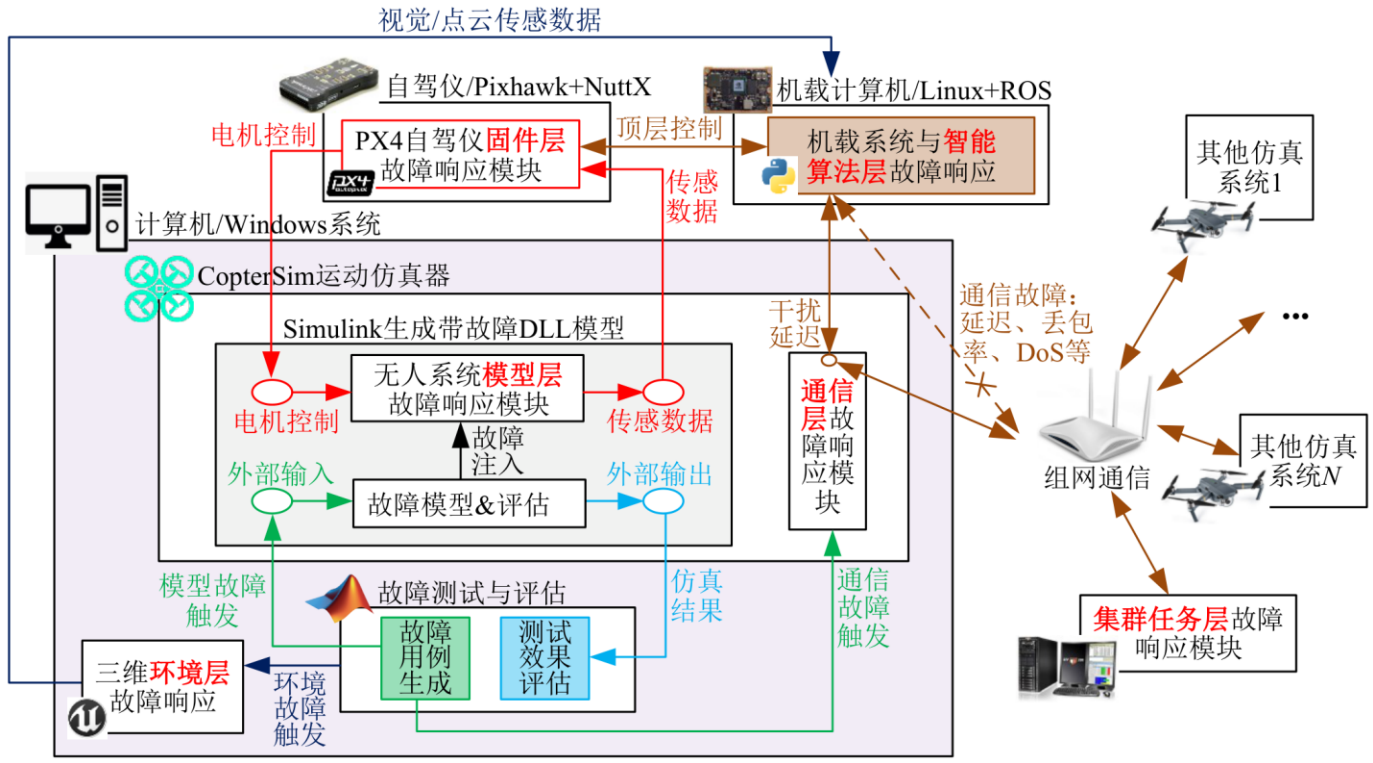


图7.13 故障建模与注入框架

模型层：改变动力或模拟测量。

固件层：改变驱动或控制逻辑。

上层与外部：改变环境、通信、算法或任务协作。

7.7.1 故障作用层与注入框架：模型层

模型触发通道独立于飞控控制通道

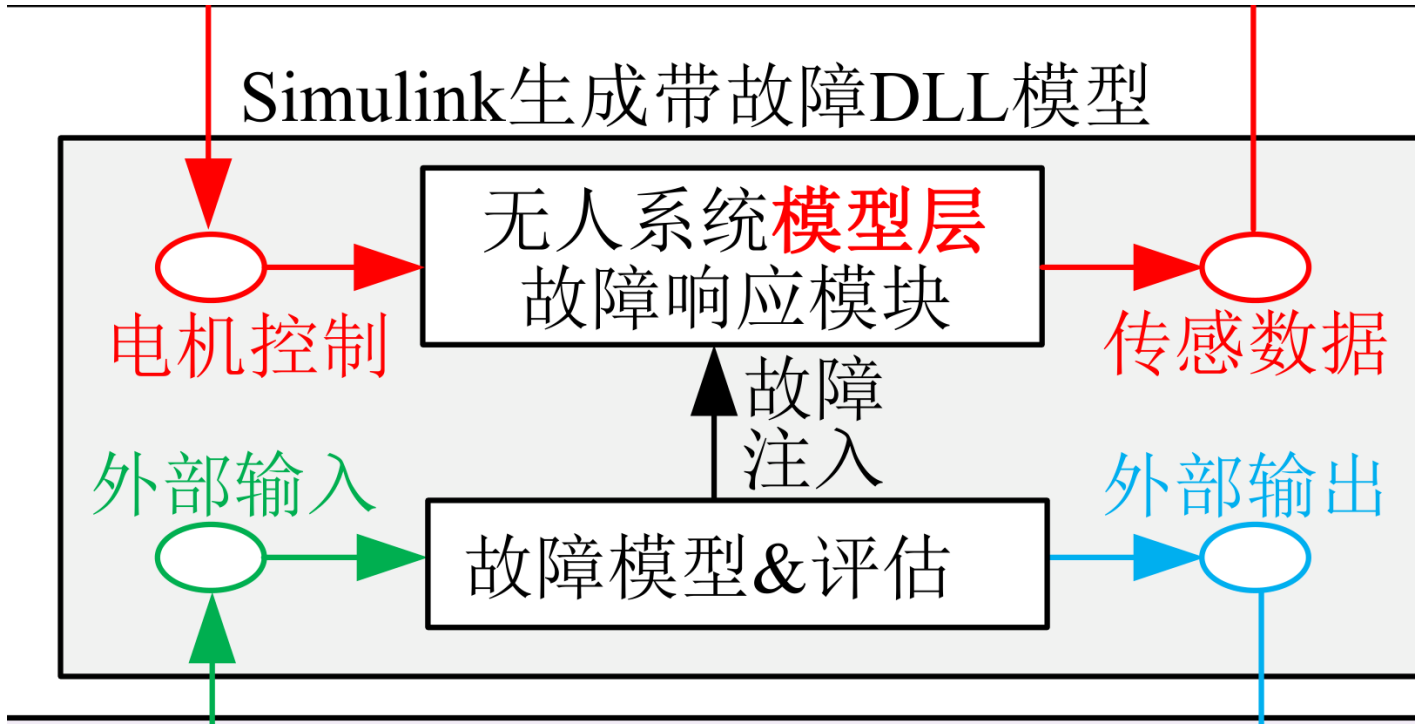


图7.13（模型层）故障触发与控制反馈

红色：控制输出与模拟传感数据。

绿色与黑色：参数进入故障模块，再作用于模型。

青色：输出用于检查的仿真结果。

7.7.1 故障作用层与注入框架：固件与智能算法层

固件与智能算法改变不同计算环节



图7.13上部：模型、飞控与机载计算三部分

固件层：在飞控固件内部改变驱动、估计或控制逻辑；
NuttX为飞控实时操作系统（见课件5.5）。
智能算法层：在机载识别、定位或决策输出中引入异常，经顶层控制影响飞控；
ROS组织机载模块通信（见课件6.1）。
数据来源：机载算法另从三维环境接收视觉/点云数据。

7.7.1 故障作用层与注入框架：环境层

场景扰动与动力扰动要对应起来

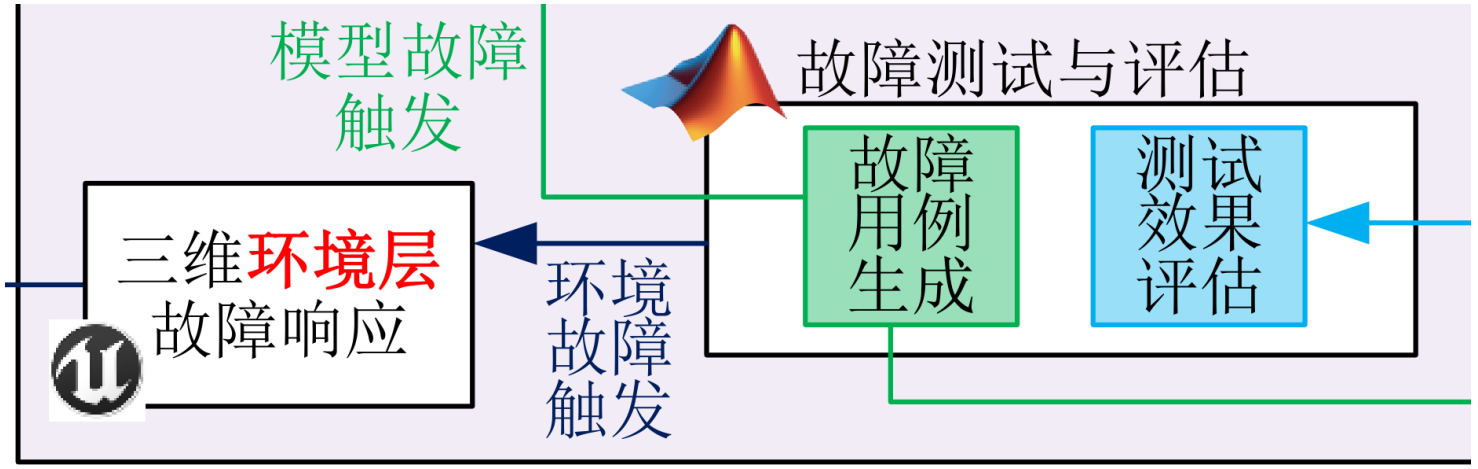


图7.13（环境与用例）场景和模型分别接收触发

视觉变化：三维场景改变相机或点云观测。

动力变化：运动模型的扰动输入改变受力与运动。

结果解释：同一用例核对两通道的参数与时间。

7.7.1 故障作用层与注入框架：通信与集群任务层

通信与集群故障影响消息和任务协作

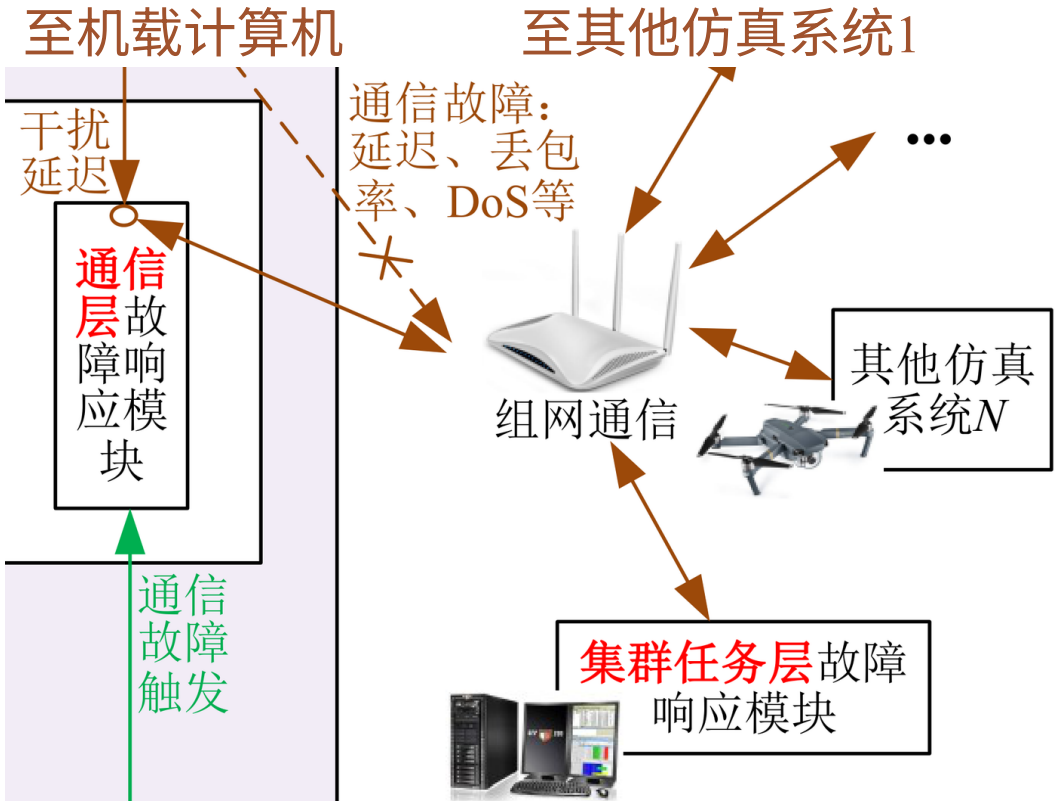


图7.13（右部）通信层与集群任务层

通信层：在链路中引入延迟、丢包或中断；DoS即拒绝服务，属于通信可用性故障。

通信检查：比较发送与接收时间、序号和丢失情况。

集群任务层：观察任务分配、各机状态和执行结果。

作用边界：电机数组不作用于这两层。

本章目录

故障注入接口与算法开发框架

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

7.7.1 故障作用层与注入框架
教材对应：第7.2.1节

7.7.2 评估与诊断开发框架
教材对应：第7.2.2节

7.7.3 故障ID与参数接口
教材对应：第7.2.1、7.2.3节

7.7.4 注入、恢复与复位规则
教材对应：第7.1.5.2、7.2.3节

7.7.5 观测接口与生效验证
教材对应：第7.1.2.3、7.1.5.1、7.2.3节

7.7 故障注入接口与算法开发框架

7.7.2 评估与诊断开发框架：算法开发框架总览

诊断模块嵌在测试与评价的数据链中

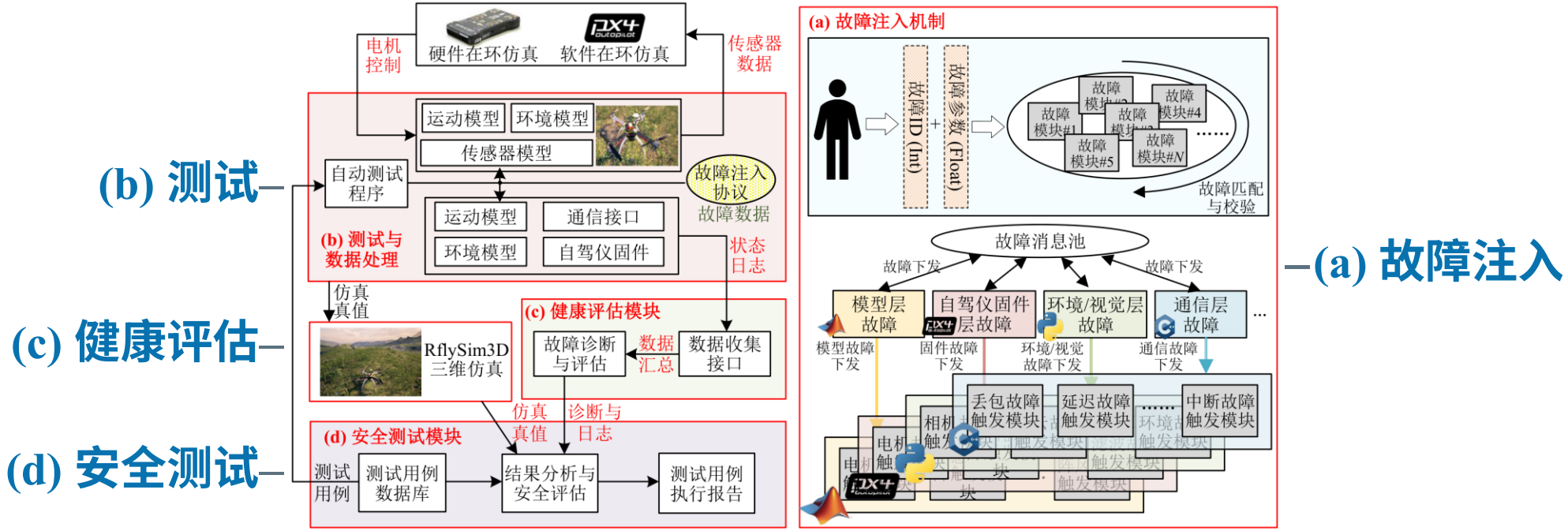


图7.14 评估与诊断算法开发框架

故障注入给条件，日志给诊断输入；结果分析还要结合真值与任务响应。

7.7.2 评估与诊断开发框架：注入接口与标签语义

故障标识、参数与作用层必须对应

(a) 故障注入机制

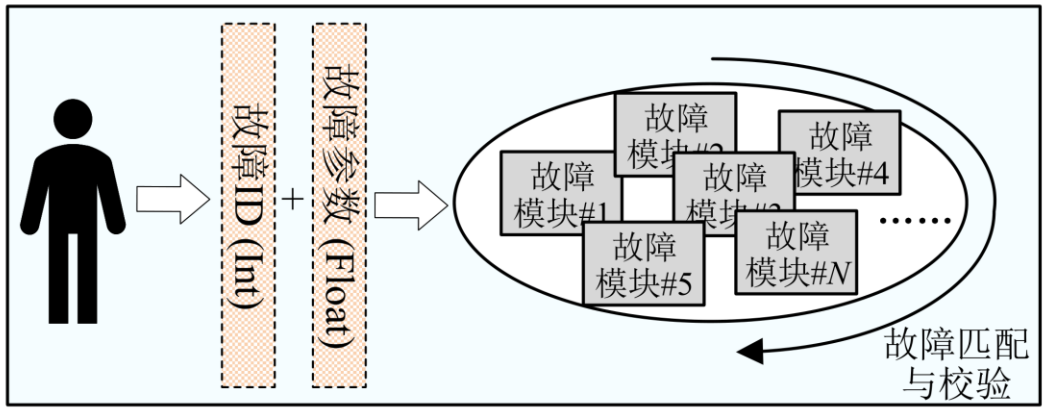


图7.14（a上部）标识与参数匹配

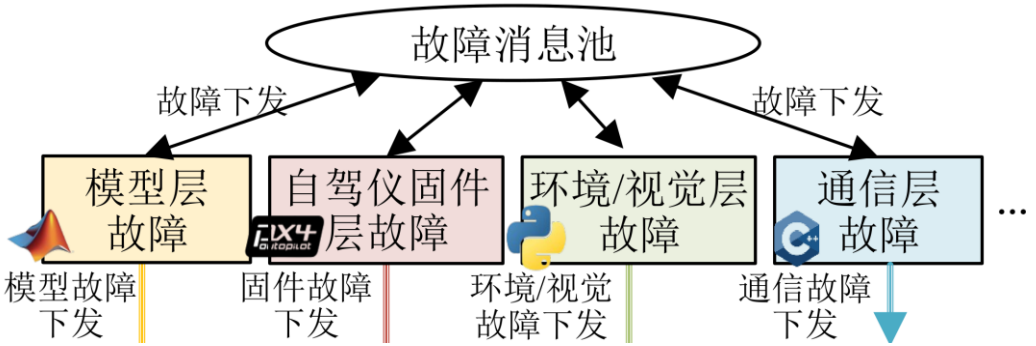


图7.14（a中部）作用层选择

故障ID（整数）＋参数（浮点）：
先匹配模型，再校验参数。

模型、固件、环境/视觉、通信：
四路分别选择，作用层进入标签。

记录类别、对象、参数、有效时刻与窗口；ID格式见课件7.7.3「外部注入接口」页。

7.7.2 评估与诊断开发框架：测试与数据处理

同一测试记录要保留输入、响应和时序

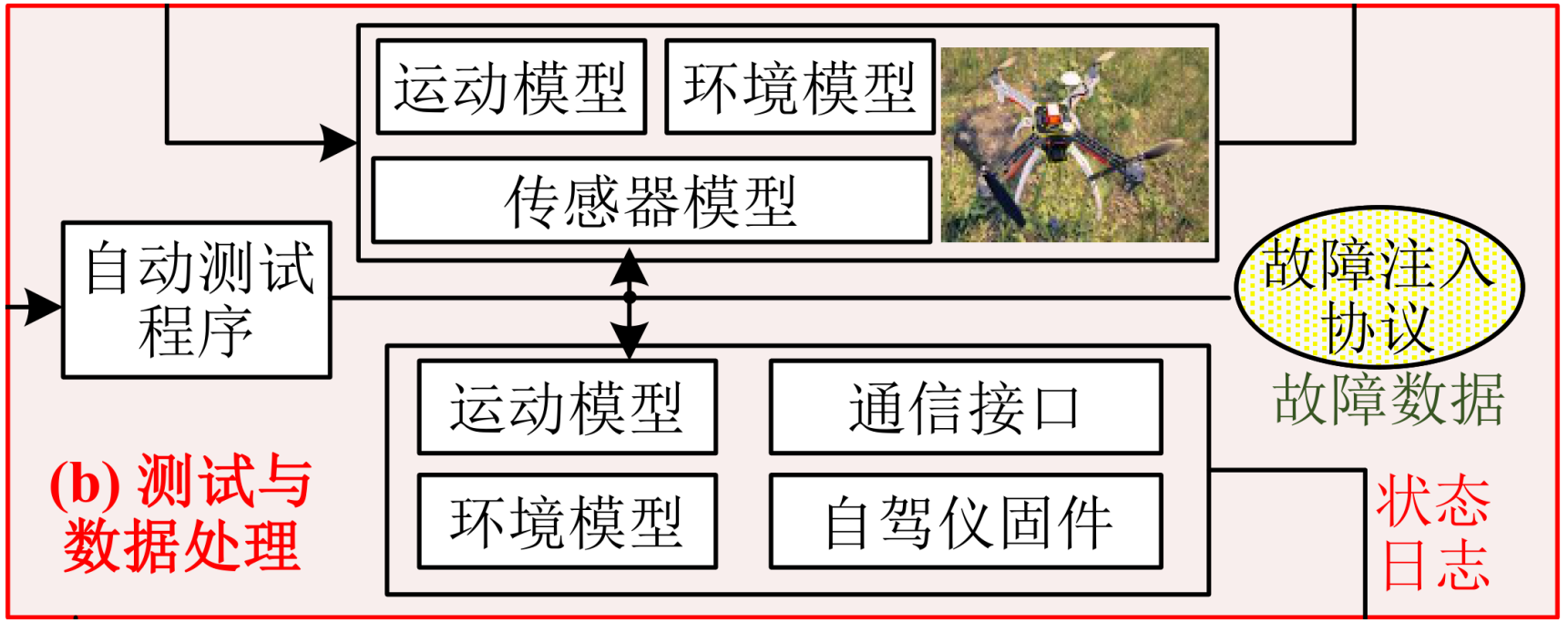


图7.14（b局部）测试调度与数据采集

上组：三维仿真侧模型；下组：含自驾仪固件的在环模型；日志同记时间戳。

7.7.2 评估与诊断开发框架：健康评估与安全测试

诊断读日志，评价另用真值和任务响应

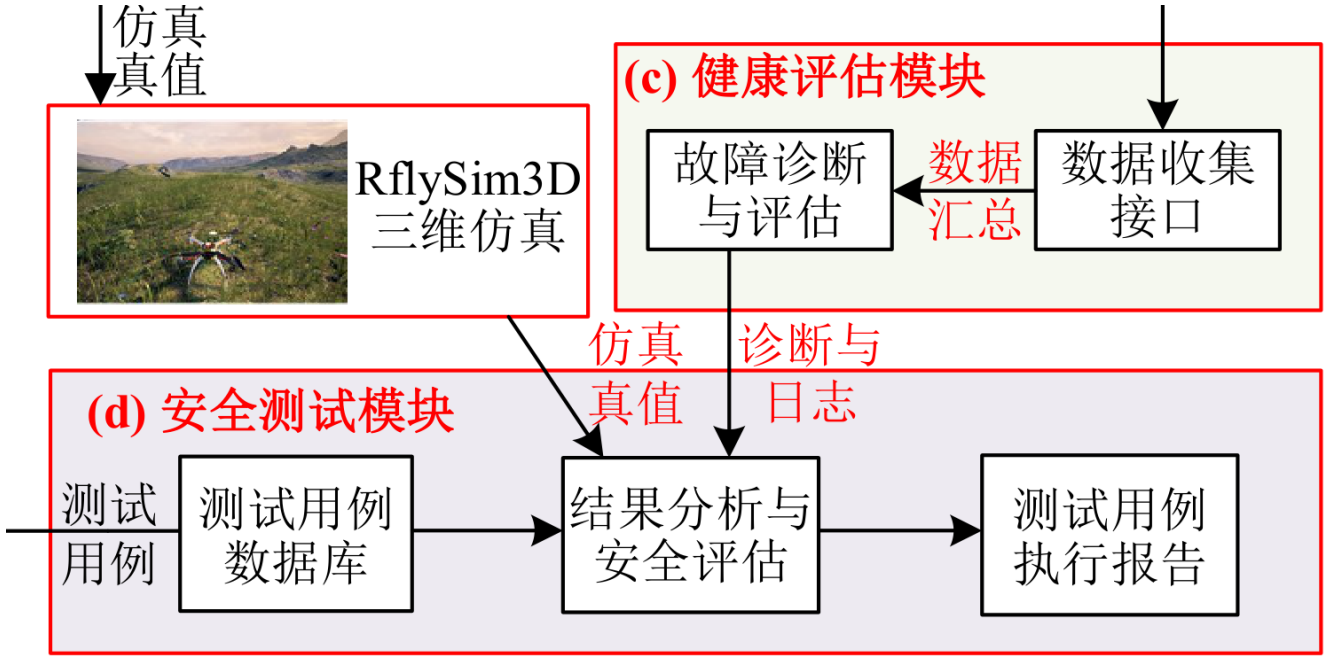


图7.14（c、d局部）诊断与评价支路

诊断输入：传感日志与状态经采集接口汇总。

评价参照：试验标签与仿真真值，只在评价时使用。

任务后果：控制响应、任务误差与安全裕度进入报告。

部署输入没有真实类别；测试报告用真值检验诊断是否正确。

本章目录

故障注入接口与算法开发框架

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

7.7.1 故障作用层与注入框架
教材对应：第7.2.1节

7.7.2 评估与诊断开发框架
教材对应：第7.2.2节

7.7.3 故障ID与参数接口
教材对应：第7.2.1、7.2.3节

7.7.4 注入、恢复与复位规则
教材对应：第7.1.5.2、7.2.3节

7.7.5 观测接口与生效验证
教材对应：第7.1.2.3、7.1.5.1、7.2.3节

7.7.3 故障ID与参数接口：外部注入接口

故障参数占8个整数槽和20个浮点槽

字段	长度 / 类型	当前实现中的用途
checkSum **CopterID**	2个整数	校验标识1234567897；目标载具编号
inSILInts	8个 int32	故障类型匹配及参数槽定位
inSILFLoats	20个 float32	故障参数；含接收模块约定的扩展槽
目标模型端口	$30100 + 2(\mathrm{ID} - 1)$	DLL：1号30100；2号30102 飞控通信另走20100系列

实际调用：mav1.sendSILIntFloat(silInt, silFloat, copterID=1)

7.7.3 故障ID与参数接口：参数提取规则

一个整数槽关联两个浮点参数槽

checkSum	CopterID

头部2个整数：校验标识1234567897与目标载具编号

silInt[0] = 123450	**silFloat[0]**	1号电机效能系数
	silFloat[1]	2号电机效能系数
silInt[1] = 123450	**silFloat[2]**	3号电机效能系数
	silFloat[3]	4号电机效能系数
silInt[2:8] = 0	silFloat[4:20] = 0	本案例未使用

123450是电机故障的FaultID（故障类型号），每槽带2个参数，故写两次。
电机号由接收模块的连接决定，不按画面左右猜测。

7.7.3 故障ID与参数接口：电机效能模型

当前电机模块缩放归一化控制量

```
if hasFault
    y(i) = inPWMs(i) * FaultParams(i);
end
```

$$u_{i,\text{out}} = h_i u_{i,\text{in}} = 0.6 \times 0.5 = 0.3$$

$u_{i,\text{in}}$、$u_{i,\text{out}}$：归一化电机控制量，无量纲。
h_i：控制效能系数；1保持原输出，0令该通道输出为0。
缩放的是控制量，不能直接推出推力下降相同比例。

7.7.3 故障ID与参数接口：两层接口

模型与固件的故障ID各有接收规则

比较项	模型层电机案例	配套固件源码注入
接收端	CopterSim加载的故障DLL	修改过的PX4驱动或控制模块
发送接口	sendSILIntFloat	高级例程e3_PX4FailureGenerator：SendHILCtrlMsg
同数异义例	123456：载荷漂移	配套v1.12.3源码：GPS输入修改
复现条件	模型含接收逻辑 数组与模块匹配	指定固件、消息布局 与硬件链路匹配

7.7.3 故障ID与参数接口：固件接口扩展

官方固件注入还受组件支持范围限制

```
failure gps off
failure gps ok
```

前置条件：参数SYS_FAILURE_EN设为启用；v1.12.3已含failure命令。

命令含义：off停止GPS数据发布；ok恢复正常发布。

核对方式：看命令回应、GPS数据恢复与飞控状态；组件支持范围按所用版本查表。

组件、故障类型与支持范围：PX4官方主分支文档

https://docs.px4.io/main/en/debug/failure_injection

本章目录

故障注入接口与算法开发框架

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

7.7.1 故障作用层与注入框架
教材对应：第7.2.1节

7.7.2 评估与诊断开发框架
教材对应：第7.2.2节

7.7.3 故障ID与参数接口
教材对应：第7.2.1、7.2.3节

7.7.4 注入、恢复与复位规则
教材对应：第7.1.5.2、7.2.3节

7.7.5 观测接口与生效验证
教材对应：第7.1.2.3、7.1.5.1、7.2.3节

7.7.4 注入、恢复与复位规则：一次注入示例

单台效能下降保留其余电机为1

```
import PX4MavCtrlV4 as PX4MavCtrl
mav1 = PX4MavCtrl.PX4MavCtrler(1)
silInt = [123450, 123450] + [0] * 6
silFloat = [0.6, 1.0, 1.0, 1.0] + [0.0] * 16
mav1.sendSILIntFloat(silInt, silFloat, copterID=1)
```

模型电机号	1号	2号	3号	4号
效能系数	0.6	1.0	1.0	1.0

配置SDK模块路径后导入；单电机教学设置，后三项为健康值1。

7.7.4 注入、恢复与复位规则：触发与时序

触发条件把正常段和故障段分开



原脚本条件：主机经过20 s且flag==1；发送后flag=2，只发一次。

状态触发设计：相同任务状态、估计有效、指定持续时间；条件和阈值写入用例。

时刻证据：主机发送时刻与接收/生效时刻分别记录，统一时基后比较。

7.7.4 注入、恢复与复位规则：撤销效能下降

恢复输出要再次发送同ID健康参数

```
silInt = [123450, 123450] + [0] * 6
silFloat = [1.0, 1.0, 1.0, 1.0] + [0.0] * 16
mav1.sendSILIntFloat(silInt, silFloat, copterID=1)
```

恢复参数： 模型中的四个效能系数回到1，输出回到输入比例。

核对响应： 比较故障前后控制量、姿态、速度；运动惯性和控制状态仍会延续。

恢复模型参数与恢复飞行状态是不同过程。

7.7.4 注入、恢复与复位规则：复位机制

全零ID不会清除当前模型的锁存

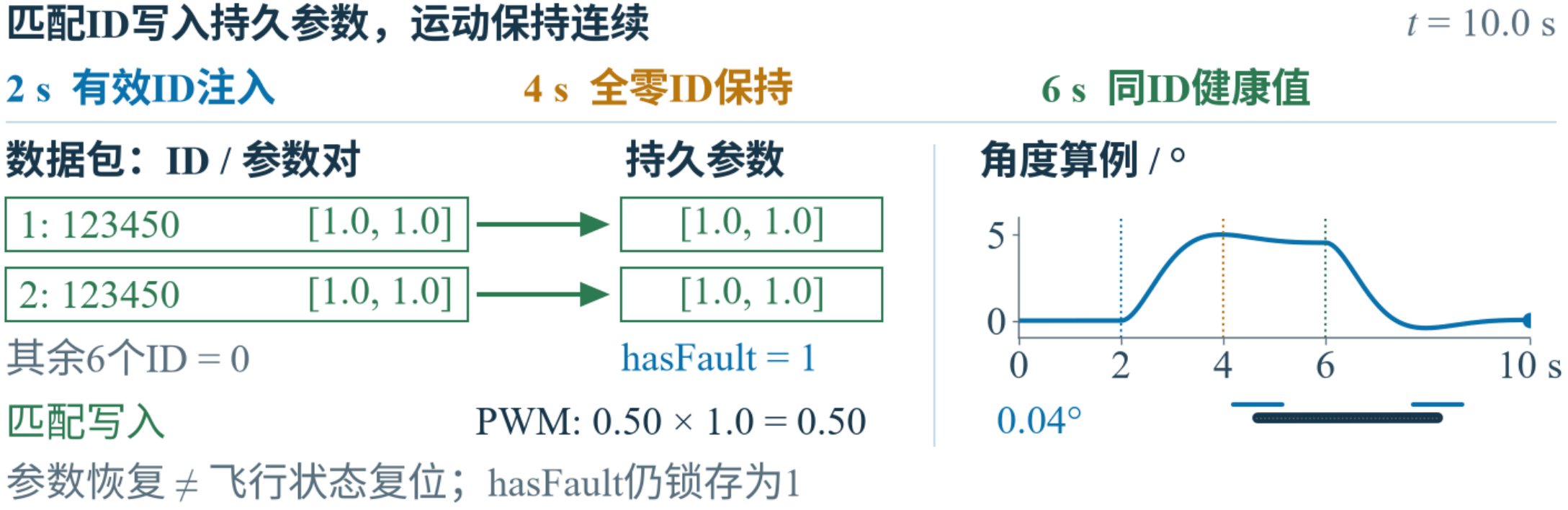
```
persistent hFault;
persistent fParam;
if hFaultTmp
    hFault = hFaultTmp;
    fParam = fParamTmp;
end
hasFault = hFault;
```

只有ID匹配时才更新；全零ID使本次匹配失败，旧状态继续保留。
独立下一轮：重新初始化模型，再确认效能系数、机体初态和正常基线。

7.7.4 注入、恢复与复位规则：锁存与连续运动

锁存状态按包更新，机体运动保持连续

有效包保留两个123450；全零ID不更新，健康参数恢复输出比例。



图：参数接收与锁存逻辑；右侧为独立二阶角度响应算例。

7.7.4 注入、恢复与复位规则：结束与重复运行

接收线程退出后还要完成实验复位

结束当前用例：停止任务更新；恢复纯效能参数，并记录最终机体与飞控状态。

结束清理：endMavLoop()可请求强制上锁并结束Offboard；EndTrueDataLoop()停接收，不复位模型。

新用例复位：重新初始化模型，恢复机体/控制初态、任务flag和时间基准。

重跑自检：正常系数、输入输出一致、估计有效、日志新起点，随后再触发故障。

本章目录

故障注入接口与算法开发框架

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

7.7.1 故障作用层与注入框架
教材对应：第7.2.1节

7.7.2 评估与诊断开发框架
教材对应：第7.2.2节

7.7.3 故障ID与参数接口
教材对应：第7.2.1、7.2.3节

7.7.4 注入、恢复与复位规则
教材对应：第7.1.5.2、7.2.3节

7.7.5 观测接口与生效验证
教材对应：第7.1.2.3、7.1.5.1、7.2.3节

7.7.5 观测接口与生效验证：证据分层

命令、模型状态、观测和估计分开记录

记录层	最小内容	它能说明什么
命令	载具ID与FaultID 参数、发送时刻	发送端要求施加的异常
模型有效状态	匹配状态与效能系数 模型输入/输出	接收端实际使用的异常
观测与控制	传感数据、执行器量、飞控模式	闭环如何响应异常
估计与真值	飞控估计；DLL运动参考	估计与模型运动是否一致

7.7.5 观测接口与生效验证：坐标核对

位置比较先统一参考原点

SDK字段	坐标 / 单位	参考原点
uavPosNED	NED：北、东、下；m	飞控估计器本地原点
truePosNED	NED运动真值；m	CopterSim / 三维地图中心

$$p_{\text{true,local}}(t) = p_{\text{true,map}}(t) - p_{\text{origin,map}}$$

origin：估计器本地原点在地图中的位置，可能不同于起飞点。
例：原点北向10 m、起飞点12 m、真值13 m，本地位置为3 m；
误减起飞点得1 m，这2 m是原点偏差而非估计误差。

7.7.5 观测接口与生效验证：接收信号核对

状态打印要配合数据新鲜度和时基

```
mav1.InitMavLoop()
mav1.InitTrueDataLoop()
print(mav1.uavPosNED, mav1.truePosNED)
```

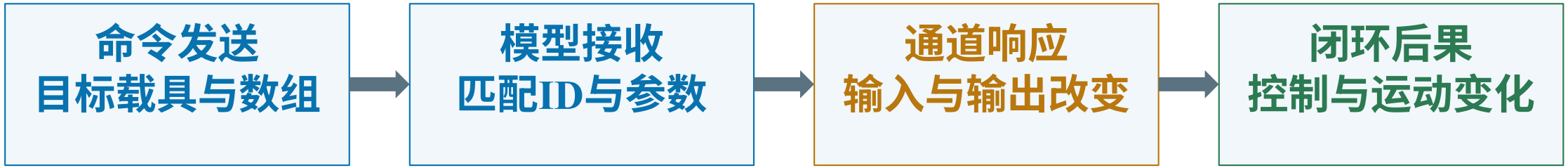
数据更新：时间戳递增、接收标志有效；禁止用启动时的默认零值判断。

时间对应：核对来源、单位和起点；用事件或已知偏移映射到公共时轴。

端口条件：InitTrueDataLoop与InitDllLogLoop占用同一30101系列端口，二选一。

7.7.5 观测接口与生效验证：注入成功判据

生效证据分默认飞行记录与模型内部两级



默认证据：脚本打印的uavPosNED与truePosNED；
PX4飞行日志中的执行器输出、姿态与位置。

进阶证据：在源模型增加效能系数与PWMIn/PWMOut日志，
生成配对DLL后按同一模型时刻比较。

判读顺序：先看其余电机的补偿与饱和，再看姿态和位置；
三维画面的提示文字只反映发送端。

7.7.5 观测接口与生效验证：常见失败

按消息路径定位“发了却没变化”

观察到的现象	优先检查	能解除疑问的证据
发送结束；参数未变	载具ID与模型端口 所加载的故障DLL	接收字段与ID匹配 实际有效参数
参数已变；通道未变	电机顺序与模型连接 实际参数取值	通道输入/输出 模块实际连接
通道已变；仍悬停	控制补偿与输出限幅 剩余控制能力	同工况正常/故障 控制量对照
第二轮开局异常	锁存、机体/控制初态 任务flag	新实例正常基线 新日志起点

7.7.5 观测接口与生效验证：最小验证用例

正常、故障和恢复采用同一核对表

阶段	效能系数应核对为	应保存的信号与关系
正常对照	1、1、1、1	保存估计、真值与执行器输出； 进阶：效能系数与电机输入/输出
单台故障	0.6、1、1、1	1号通道缩放；控制补偿与运动响应
参数恢复	1、1、1、1	输入/输出比例恢复；观察后续运动
下一独立用例	锁存复位；相同初态	新正常基线；新时间原点与任务标志

7.7.5 观测接口与生效验证：版本与二次开发

复现实验记录绑定模型和接口快照

文档入口：[安装目录]/RflySimAPIs/RflySimSDK/html/index.html
查阅Python控制接口与Simulink PHM模块。

接口核对：sendSILIntFloat的签名、消息类型、接收ID、参数索引与模型连接。

源与DLL配对：登记SDK、库源、模型与DLL快照。
源码规则须由对应DLL的构建记录或信号核对确认。

方法回顾：课件7.3组织触发与记录；课件7.5从观测推断故障。

练习与讨论

一次单电机注入怎样形成完整证据

条件：载具ID=2；3号电机效能0.4，其余为1；3号归一化输入0.55。

问题1： 写出8维整数与20维浮点数组，指出3号参数所在的浮点槽。

问题2： 计算3号故障后控制量；能否据此断言推力也只剩40%？

问题3： 怎样恢复输出、怎样完整复位？为什么全零ID不够？

问题4： 程序无异常且界面显示故障，还缺哪些证据才能确认注入生效？

参考要点

参数、恢复与生效各有独立答案

```
silInt = [123450, 123450] + [0] * 6
silFloat = [1.0, 1.0, 0.4, 1.0] + [0.0] * 16
```

$$u_{3,\mathrm{out}} = 0.4 \times 0.55 = 0.22$$

参数与推力：3号参数为silFloat[2]，由silInt[1]读取；端口30102。0.22是控制量，推力比例另查电机与旋翼模型。

恢复与复位：同ID＋四个1恢复输出；全零ID匹配失败、锁存保留旧故障，独立用例须重新初始化模型并恢复相同初态。

生效证据：目标ID正确、有效参数已更新、指定通道变化、闭环响应有记录。

本节小结

可复现的注入包含接收、恢复和复位

节点与作用层：SITL、HITL、真机覆盖不同链路；模型与固件协议不能混用。

接口与参数：8个整数槽、20个浮点槽；每个123450带两台电机参数，四旋翼写两次。

触发与结束：状态条件与时间分别记录；健康参数恢复输出，新实例复位锁存。

关键易错点：发送不等于生效；零系数清零输出。
停接收或全零ID不清除模型锁存。