中国商飞航电系统基于Capella的MBSA应用实践

中国商飞|上海仆勾山

2026-5-12

- 目录 -

CONTENTS

01 | 简介

Part 1.1 上海飞机设计研究院（上飞院）简介

中国商飞（COMAC）是中国实施大型客机项目的主要载体

关于上飞院	上飞院是中国商飞的设计研究中心
负责工作	中国民用飞机工程设计与技术抓总
职责	民用飞机及相关产品的研发、制造与测试

Part 1.1 上海仆勾山简介

- **上海仆勾山（PGM）**全称为上海仆勾山科技有限公司
- 上海仆勾山是中国领先的**MBSE解决方案与咨询服务**供应商
- 主要客户领域包括
  - 航空、航天、兵器、核电、汽车等领域
- 拥有多项基于**Capella**的插件产品

PGM + COMAC → **基于Capella的MBSE解决方案**

- 动态执行与系统仿真 (DESS)
- 指标体系建模管理 (PMM)
- 协同建模 (T4C)
- **基于模型的安全性分析 (COMSPEC)**
- …

02 | 背景

Part 2.1 航电系统介绍

显示告警

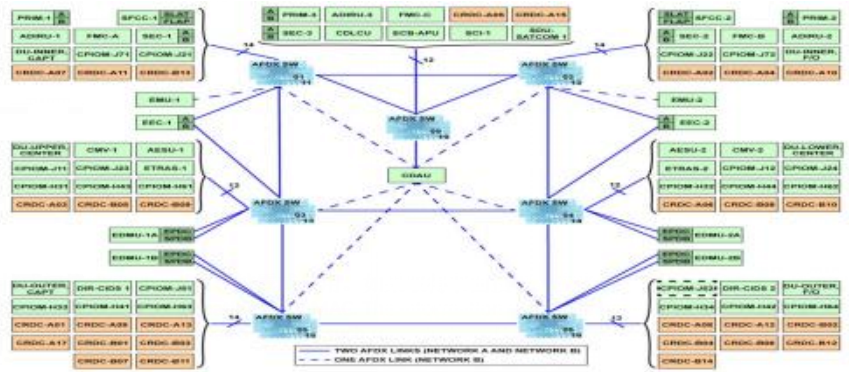
机载维护系统

通信导航

综合监视

飞行管理

航电核心处理系统



Part 2.2 航电安全性分析背景

安全性分析与系统架构设计脱节

- 故障树层级依赖于个人经验
- 难以验证系统架构的安全性需求是否被满足

故障树的定义缺乏标准化

- 对于航电公共资源的命名规范各不相同
- 难以开展对公共资源的共因失效分析

故障树无法自动创建

- 故障树手动创建
- 主要依赖设计师的个人主观经验.
- 费力且容易出错.

安全性影响分析无法自动开展

- 手动创建基于最小割集的安全性影响分析数据库
- 故障树无法自动集成，系统级联分析十分耗时费力

Part 2.3 上飞院航电安全性实践过程

1
- 航电系统的安全性分析基于安全性工程师对架构的理解建立
- 不同型号使用不同的FTA工具，包括IsoGraph,RamCommander,Medini等

2
- 2018年航电系统开始采用Capella建模
- 现已实现从系统分析到物理架构整个过程的Capella建模
- 各子系统模型可自动集成到飞机模型

3
- 基于本方法实现了基于Capella架构的失效传播和故障树自动建模
- 基于Capella模型实现安全性数据的集成，开展基于模型的级联影响分析。全机范围单点、组合、级联失效
- 能兼容其他工具的故障树模型

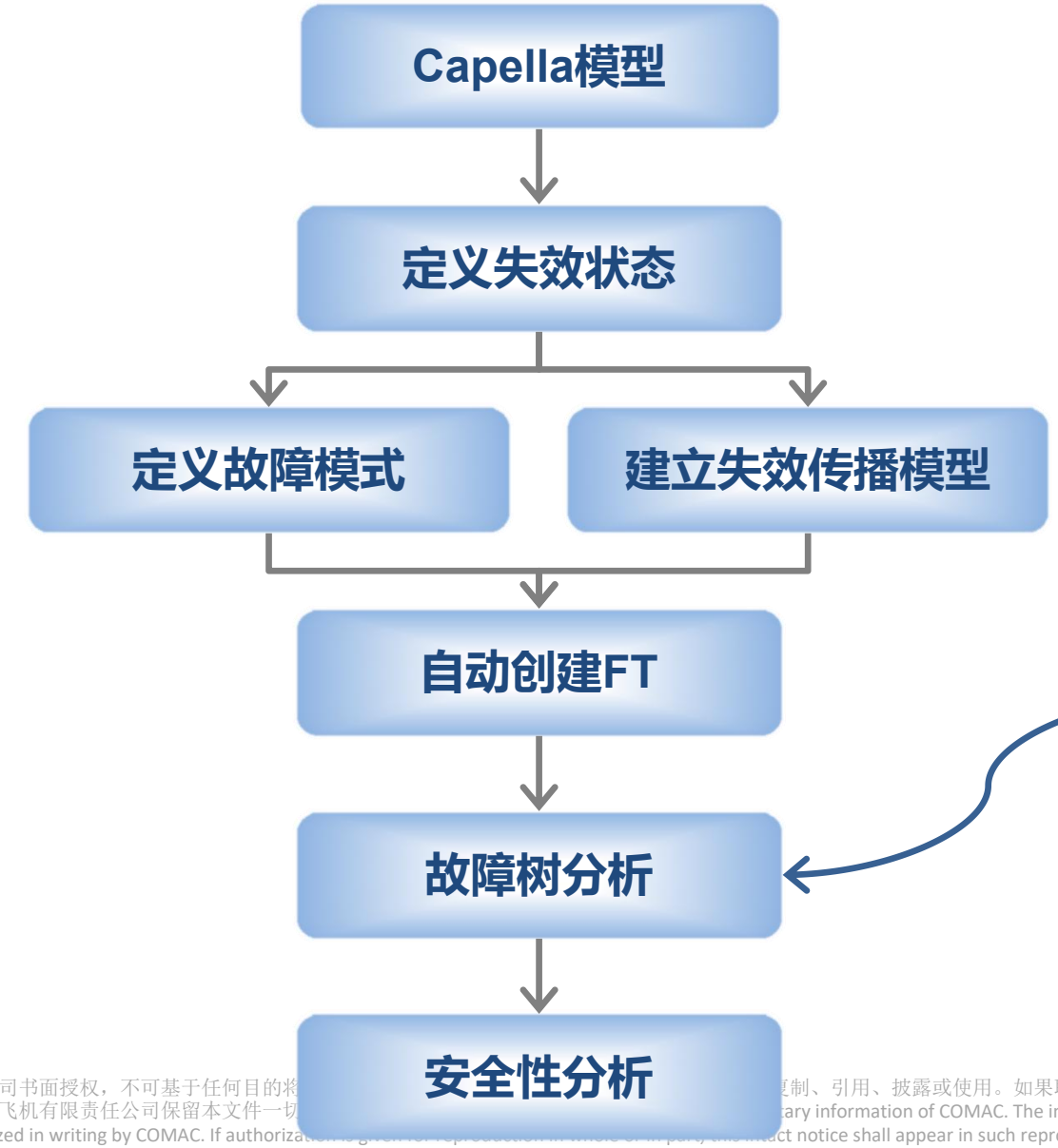
Part 2.4 MBSA技术路径

安全性分析脱离架构设计

故障树颗粒度缺乏标准化

无法自动创建故障树

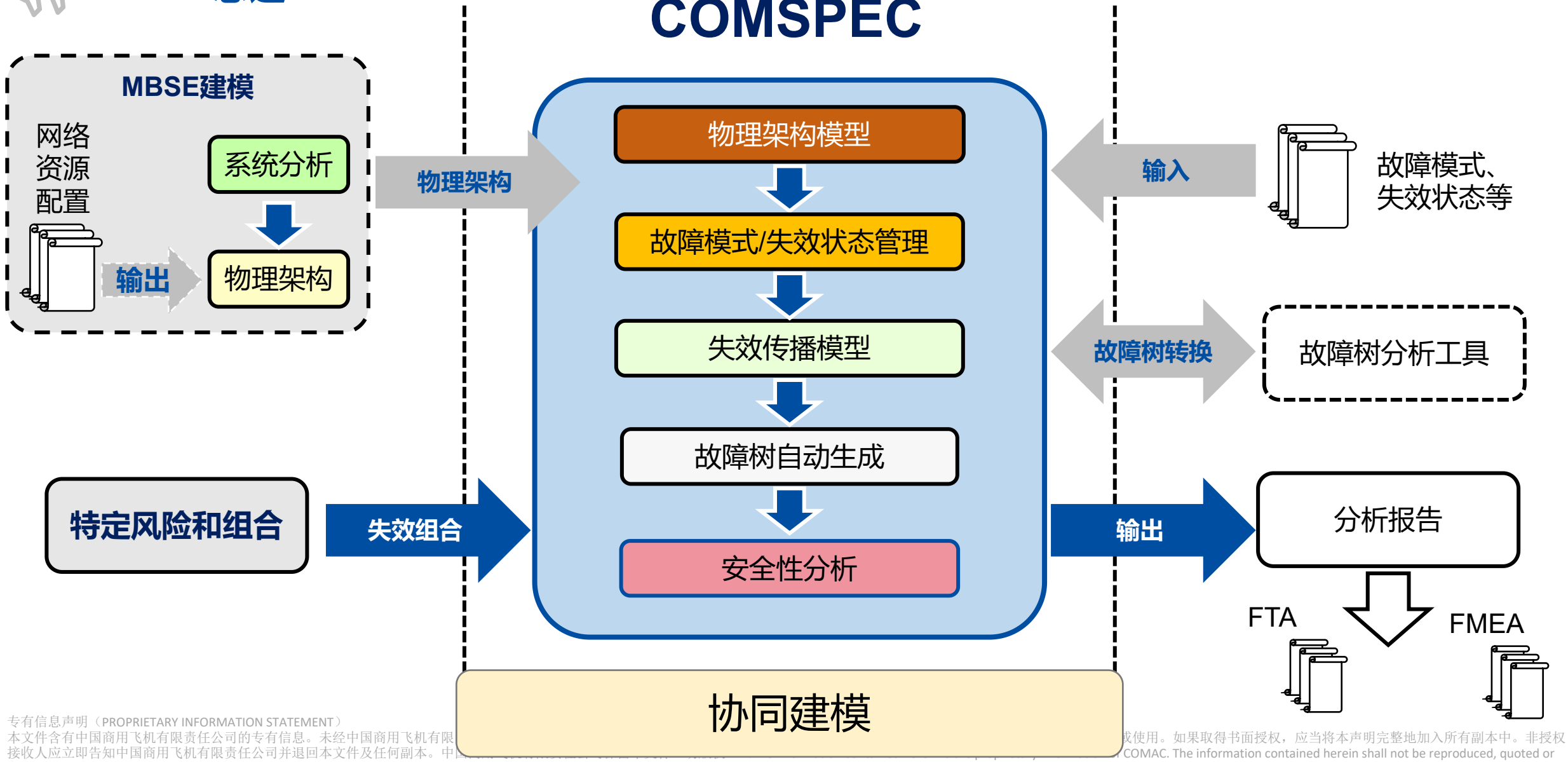
无法自动开展安全性影响分析



已有故障树模型
IsoGraph
Ram Commander
Medini
...

03 | COMSPEC

Part 3.1 总述



Part 3.2 方法论

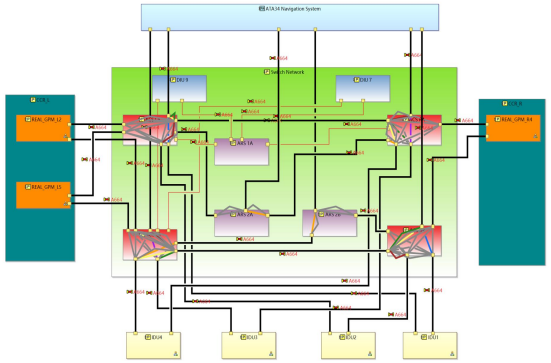
架构建模 —模型→ 架构分析 —故障传播模型→ 故障树分析 —分析结果→ 安全性评估

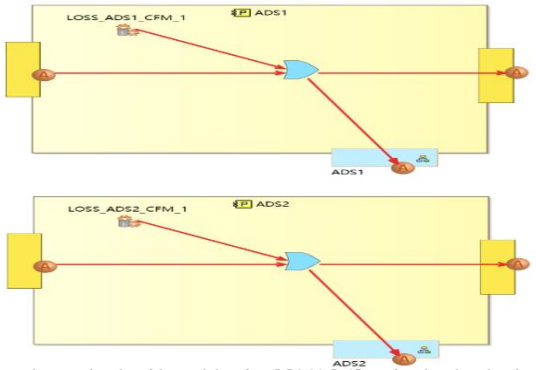
- 对每个系统的功能架构进行分层建模；
- 对功能和接口的余度进行建模；
- 对实际的物理架构进行建模。

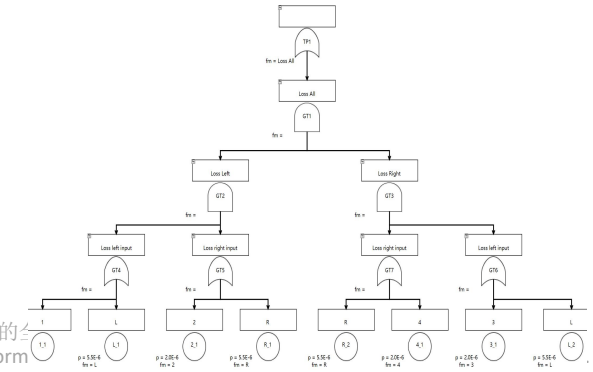
- 定义内部故障模式和接口故障模式；
- 定义每种故障模式的传播链路和逻辑关系；
- 定义失效状态并将失效状态追溯至故障模式。

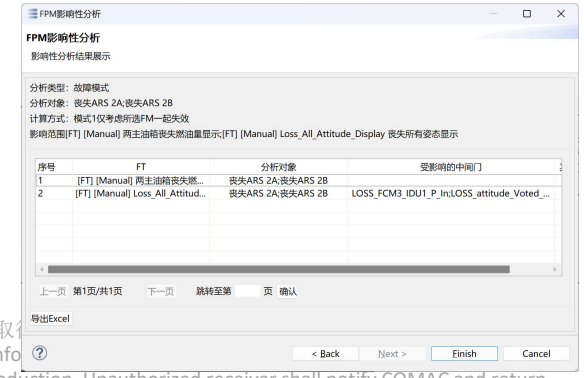
- 基于故障传播模型自动生成故障树；
- 对故障树进行定性和定量分析；
- 自动生成整架飞机的安全分析数据库。

- 对单点故障、组合故障、共因以及级联故障进行自动化分析
- 利用分析结果来确定物理架构和安全要求。









Part 3.3 架构建模——建模理念

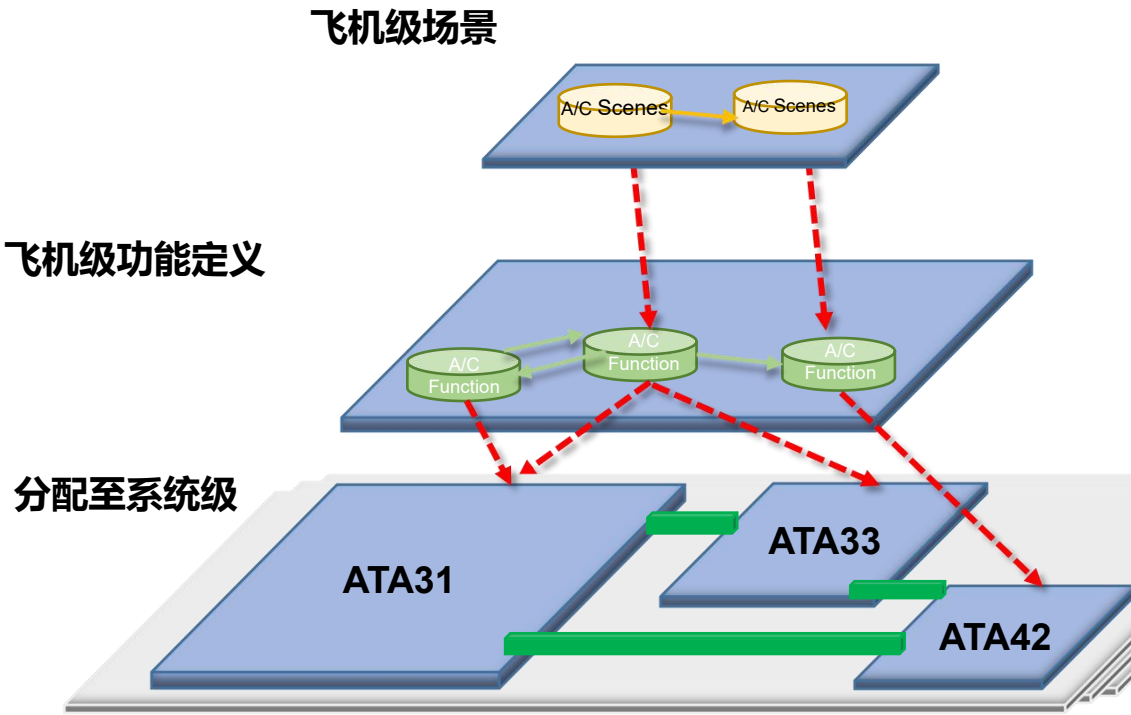
COMAC系统工程

Need需要 飞机级设计

Function功能

Requirement需求

Product产品

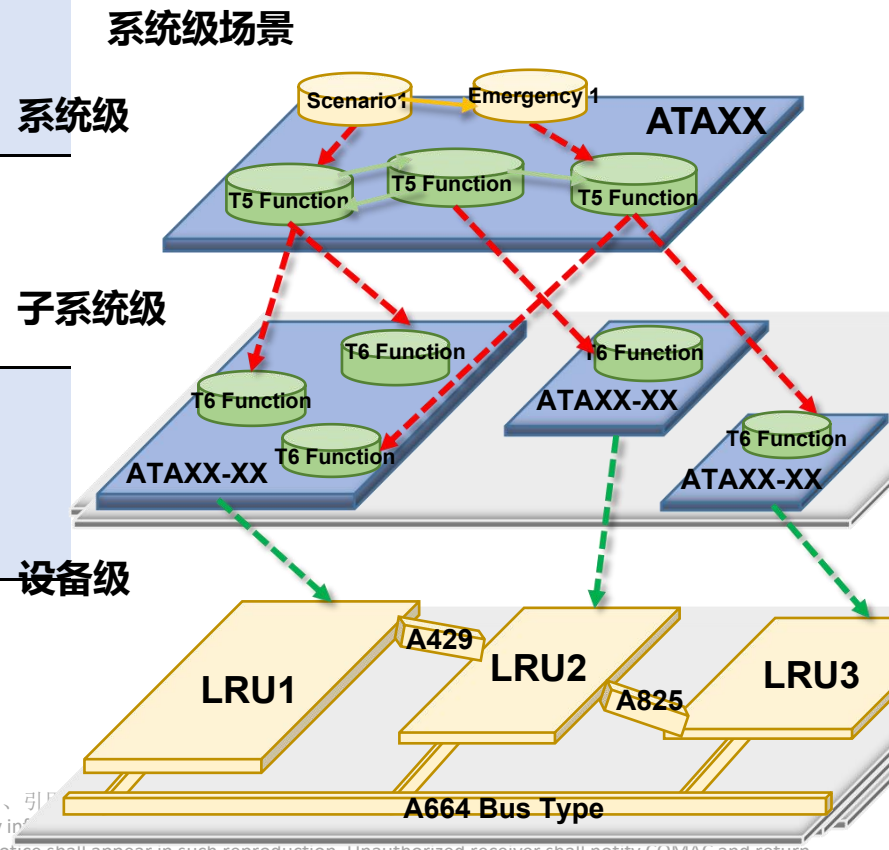


Part 3.3 架构建模——建模理念

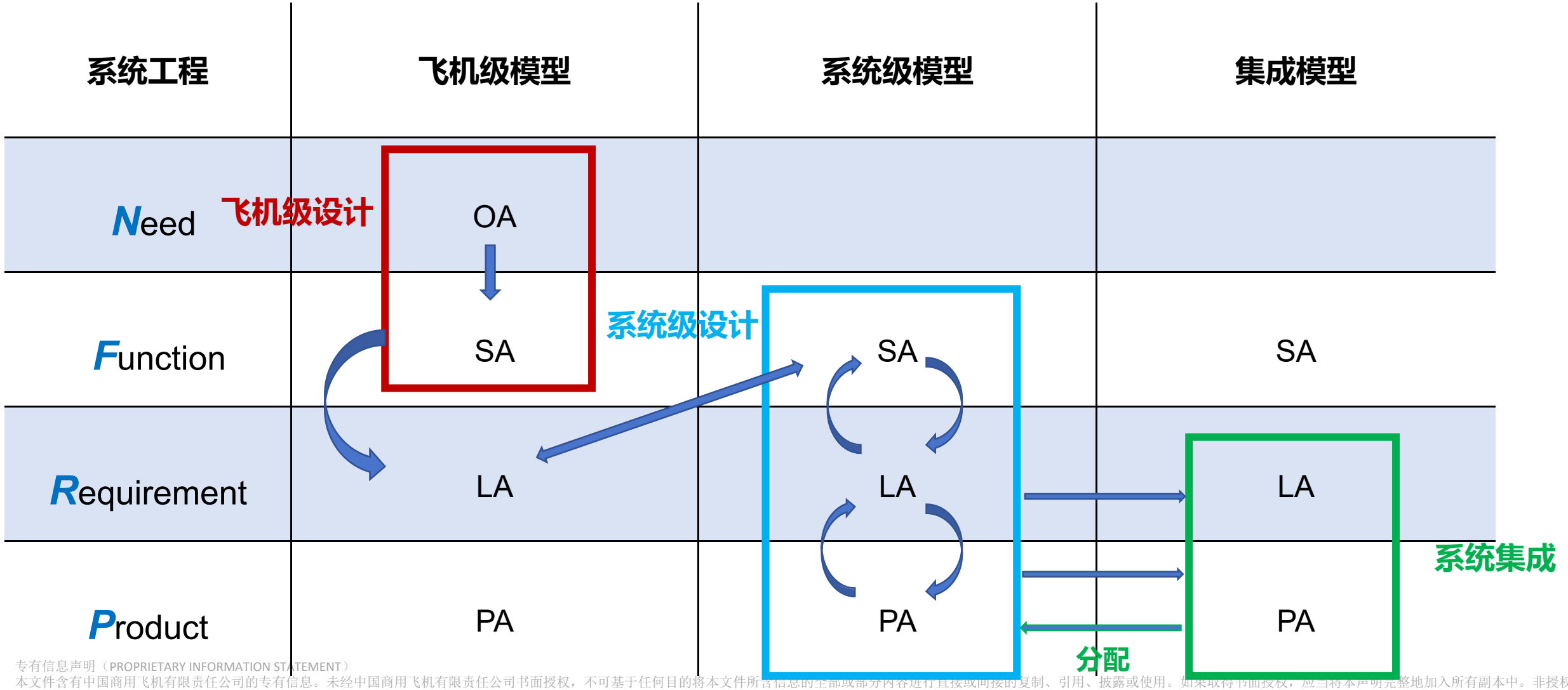
系统工程	飞机级模型	系统级模型
Need	OA	
Function	SA	SA
Requirement	LA	LA
Product	PA	PA

飞机级设计

系统级设计

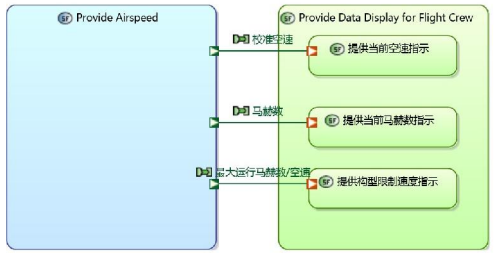


Part 3.3 架构建模——建模理念

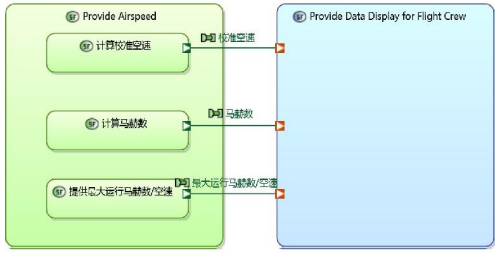


Part 3.3 架构建模

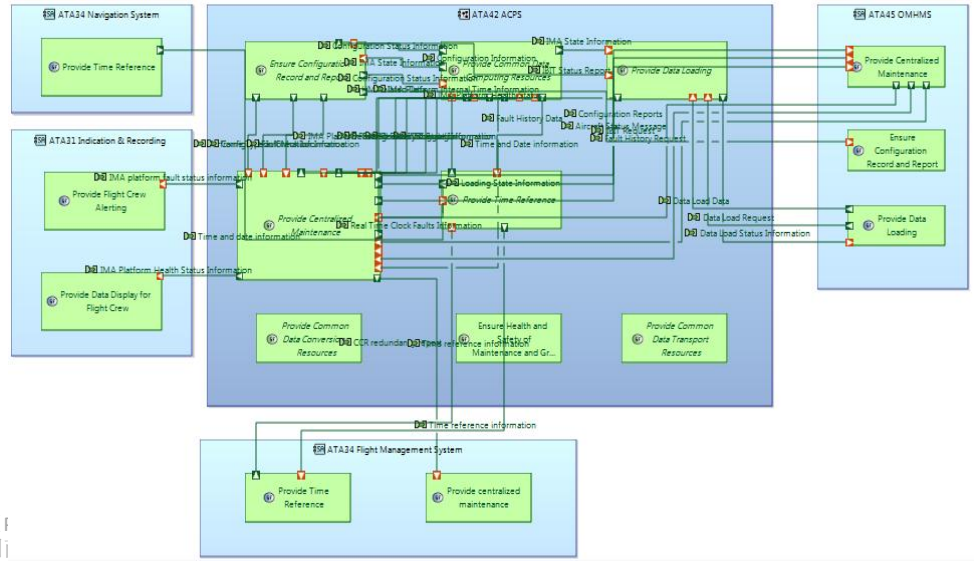
系统分析：
跨模型、实时协同建模



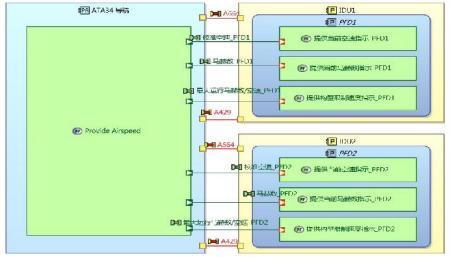
项目1：指示记录系统模型



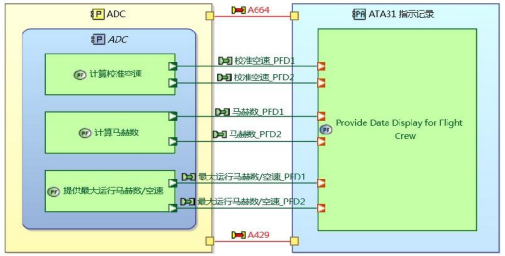
项目2：导航系统模型



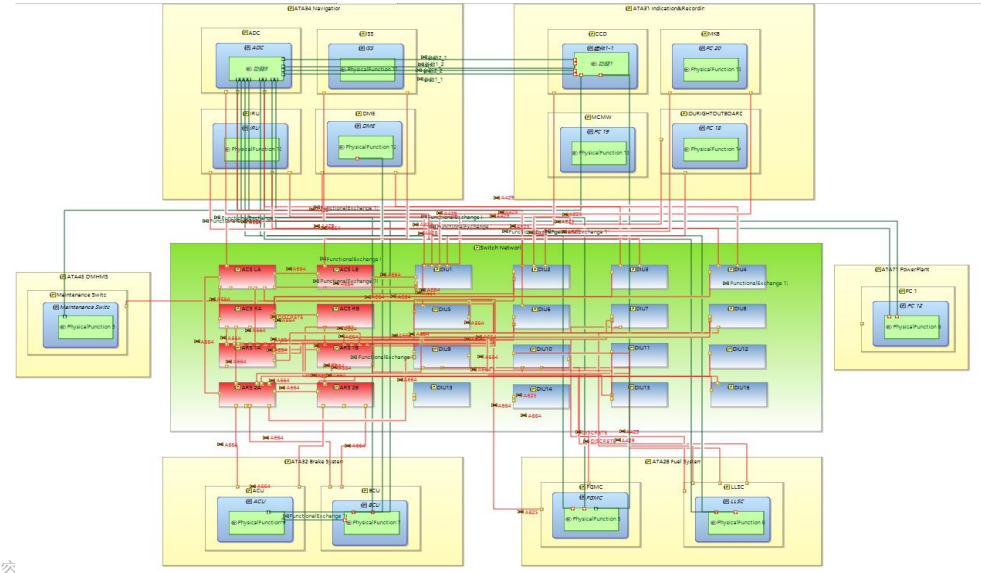
物理架构模型：
跨模型、实时协同建模



项目1：指示记录系统模型

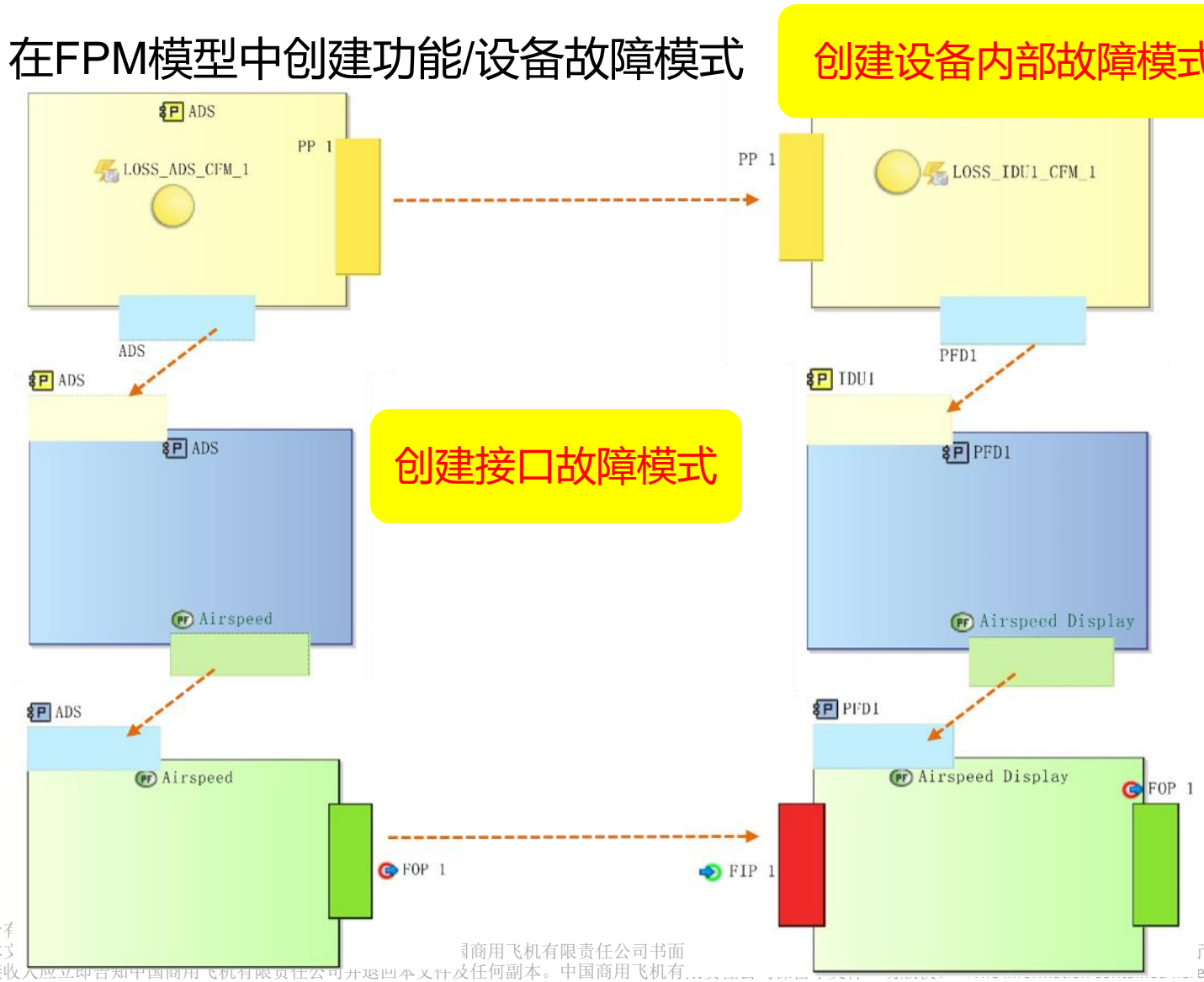


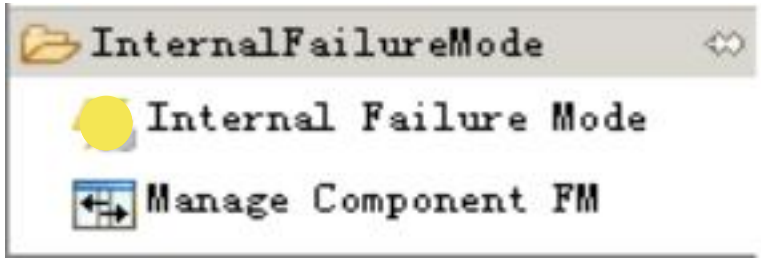
项目2：导航系统模型

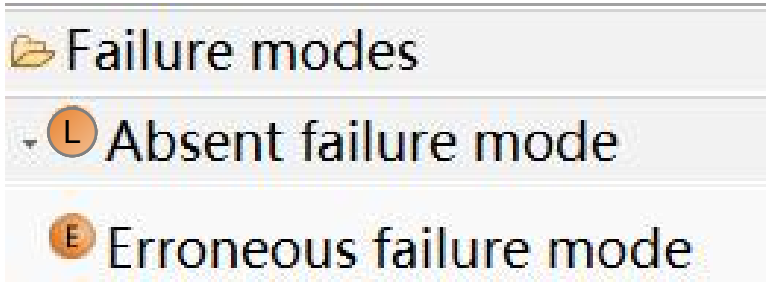


Part 3.4 架构分析——故障模式管理

- 在FPM模型中创建功能/设备故障模式



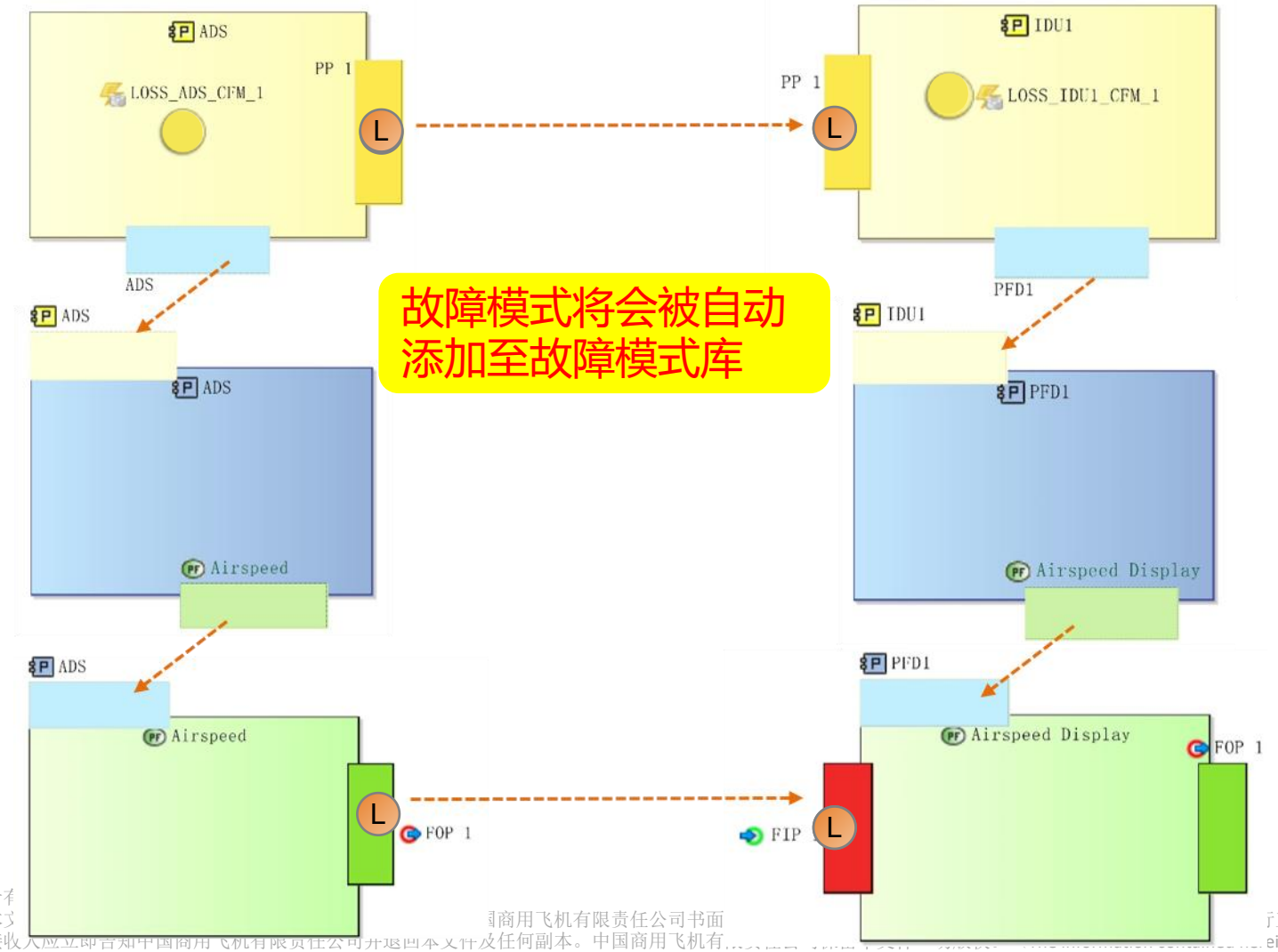




FM：Failure Modes故障模式
FPM: Failure Propagation Model故障传播模型

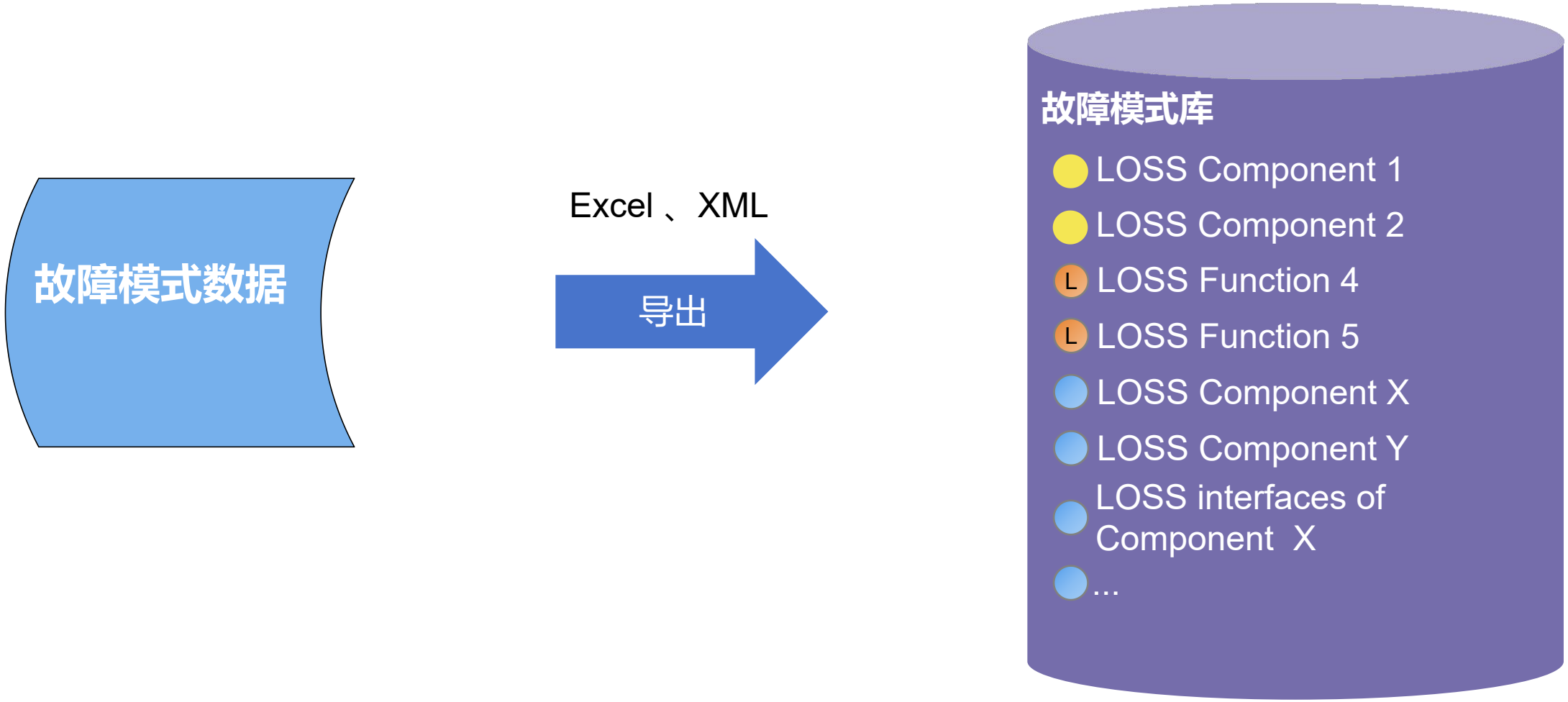
Part 3.4 架构分析——故障模式管理

- 故障模式会自动被添加到故障模式库中



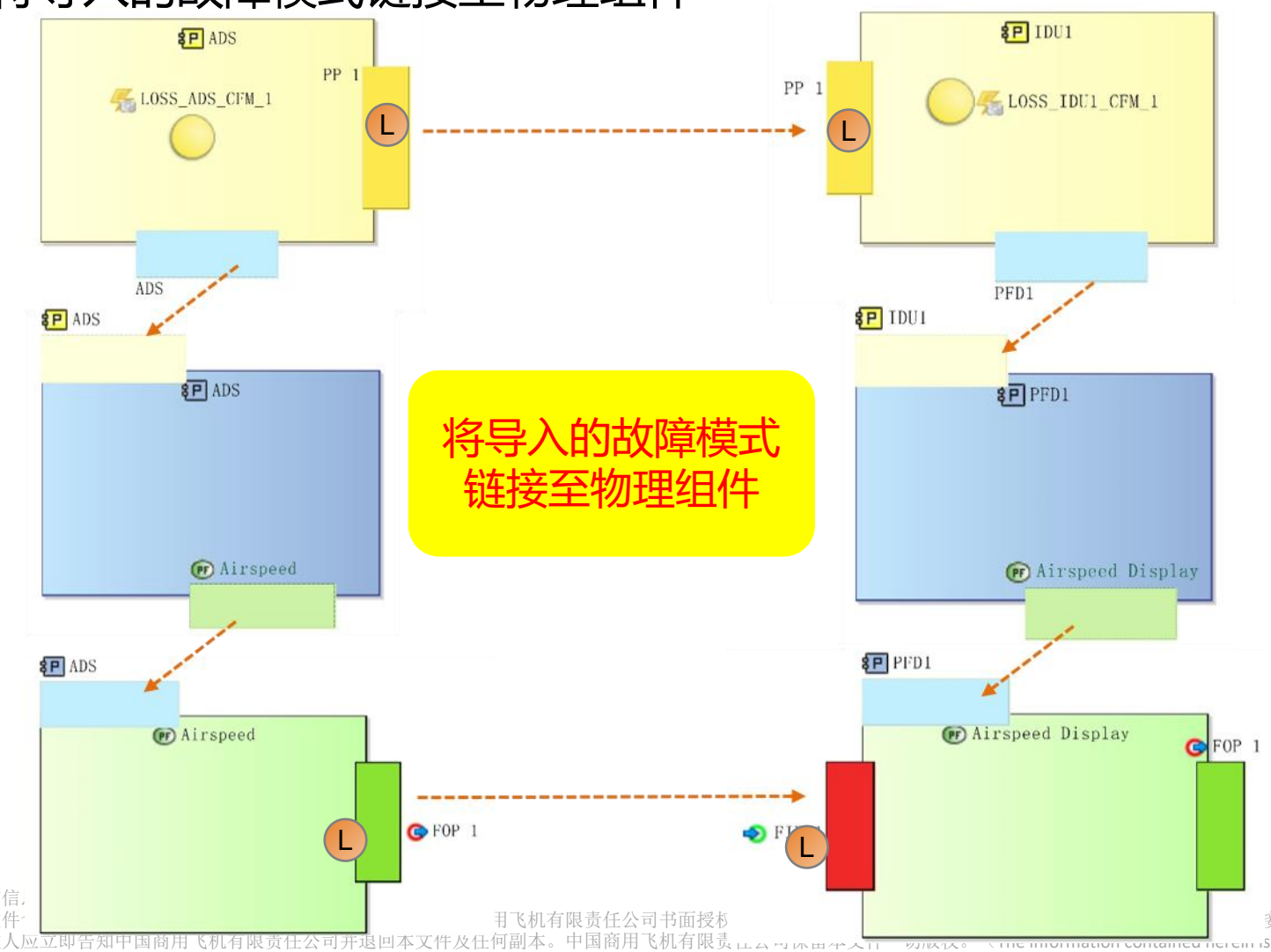
Part 3.4 架构分析——故障模式管理

- 导入设备故障模式



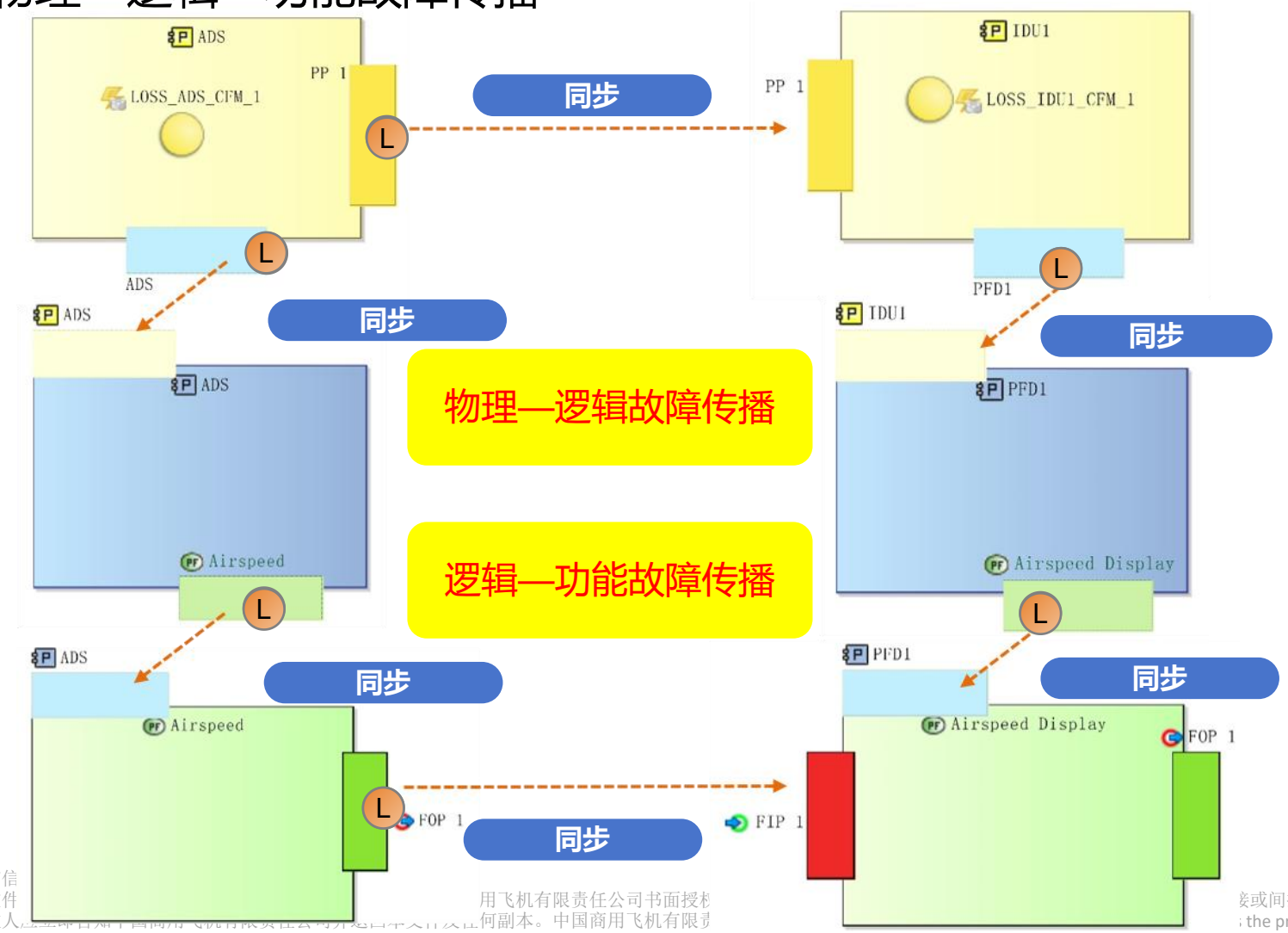
Part 3.4 架构分析——故障模式管理

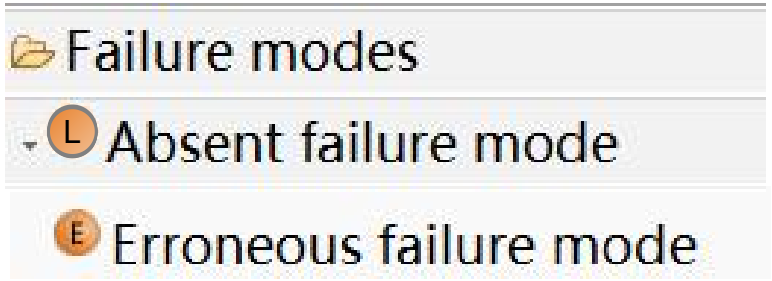
- 将导入的故障模式链接至物理组件



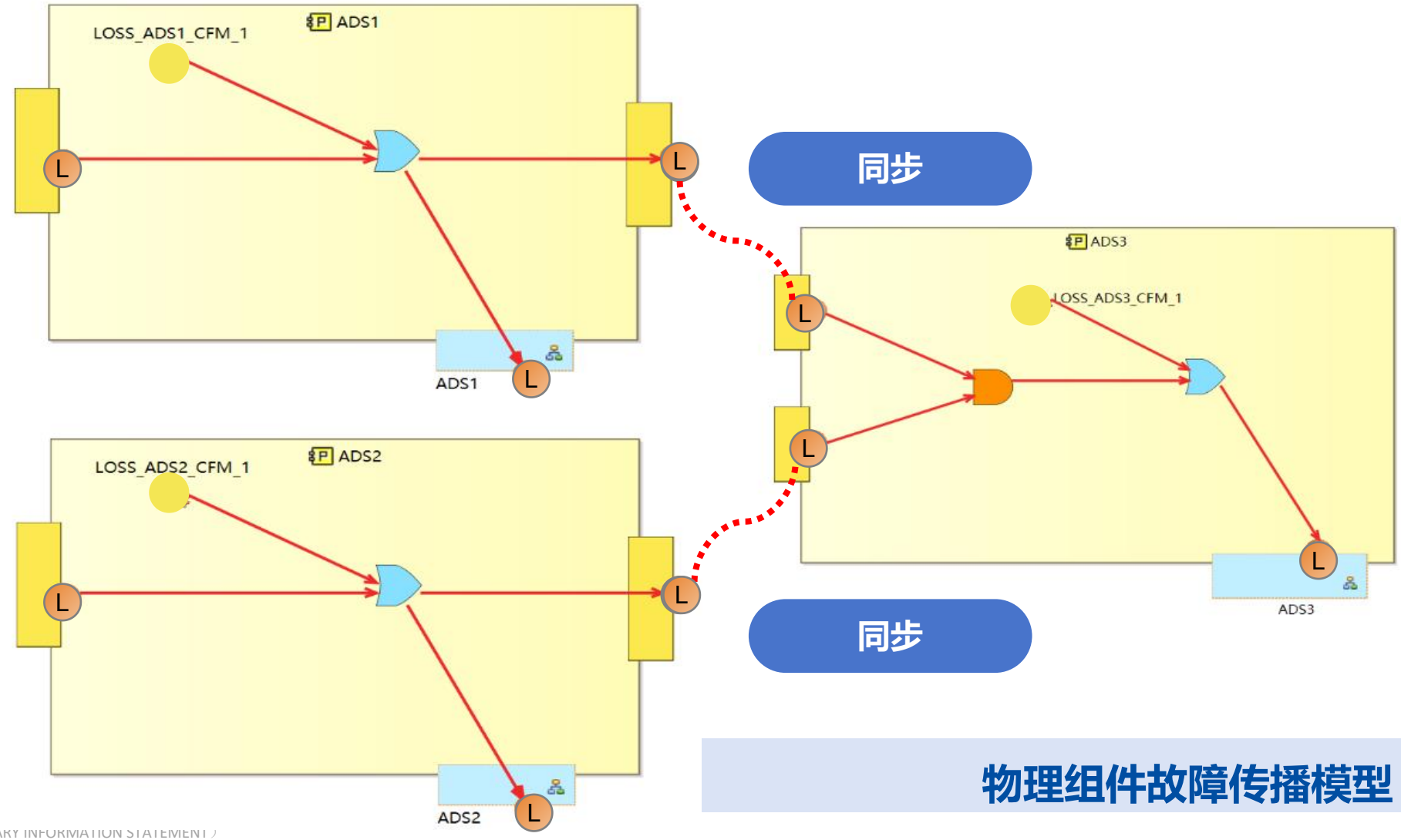
Part 3.4 架构分析——故障传播模型

- 物理—逻辑—功能故障传播



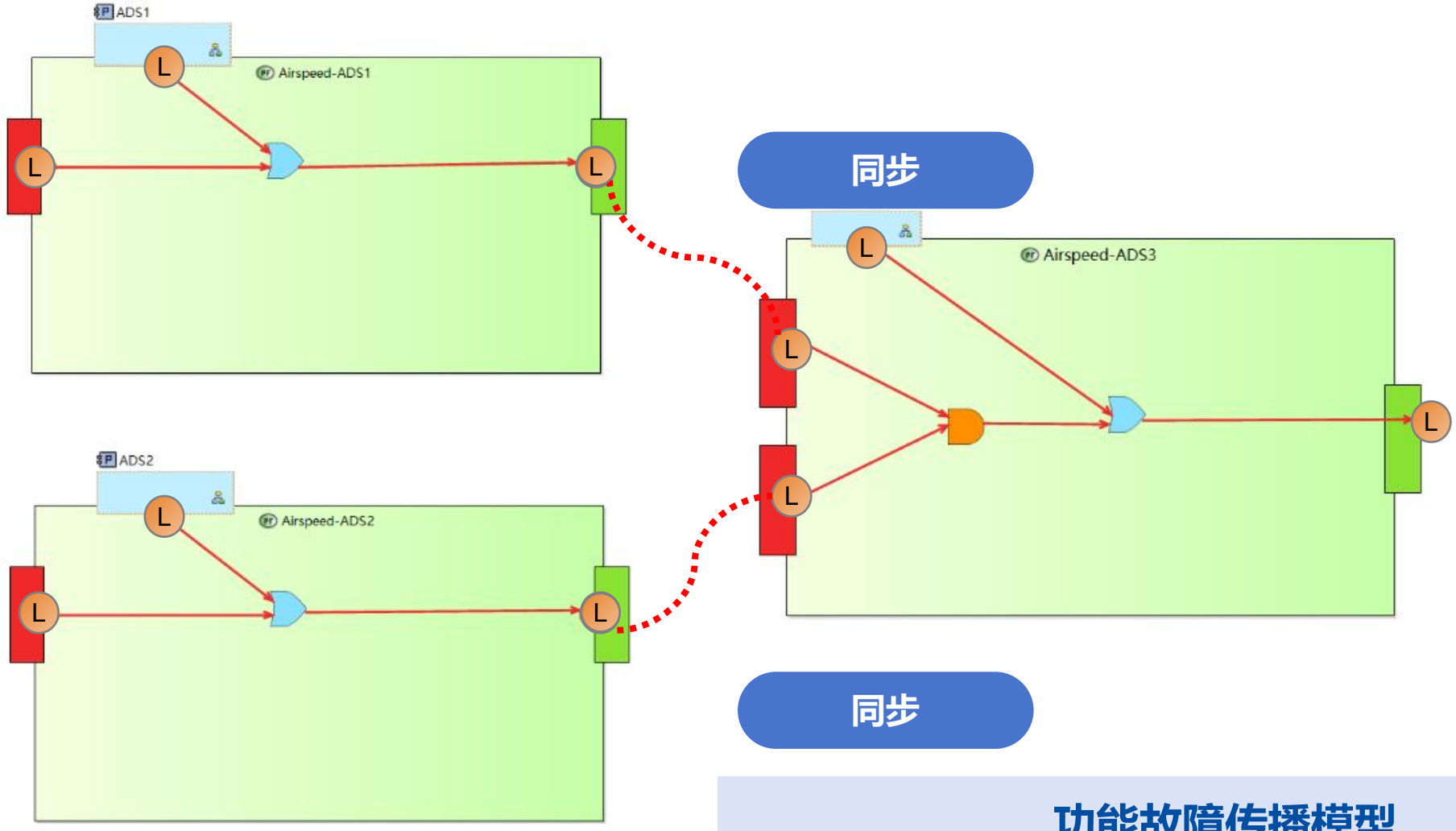


Part 3.4 架构分析——故障传播模型



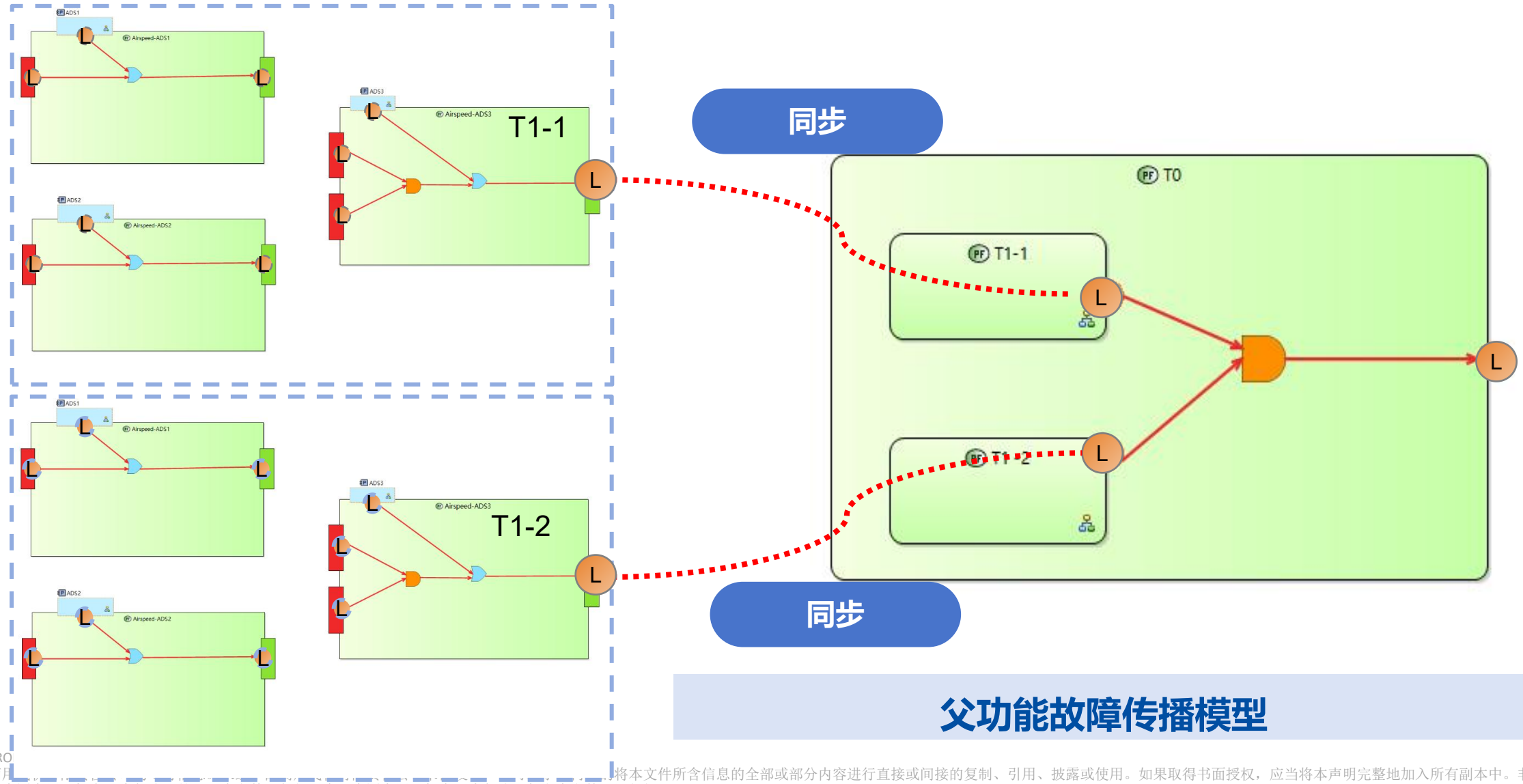
物理组件故障传播模型

Part 3.4 架构分析——故障传播模型



功能故障传播模型

Part 3.4 架构分析——故障传播模型

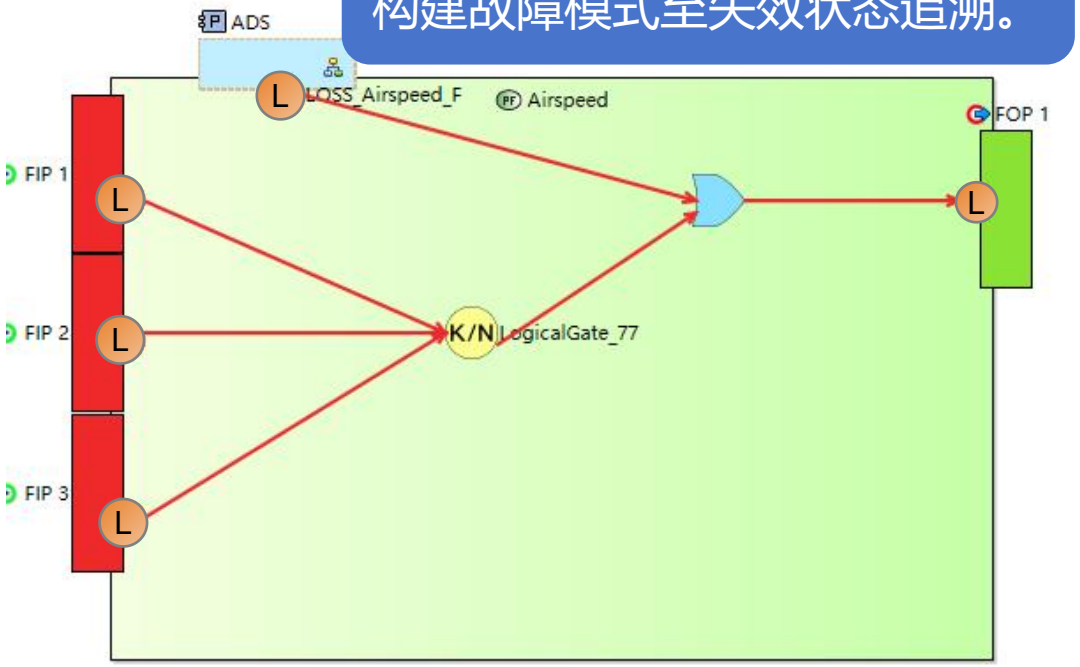


父功能故障传播模型

Part 3.4 架构分析——失效状态管理

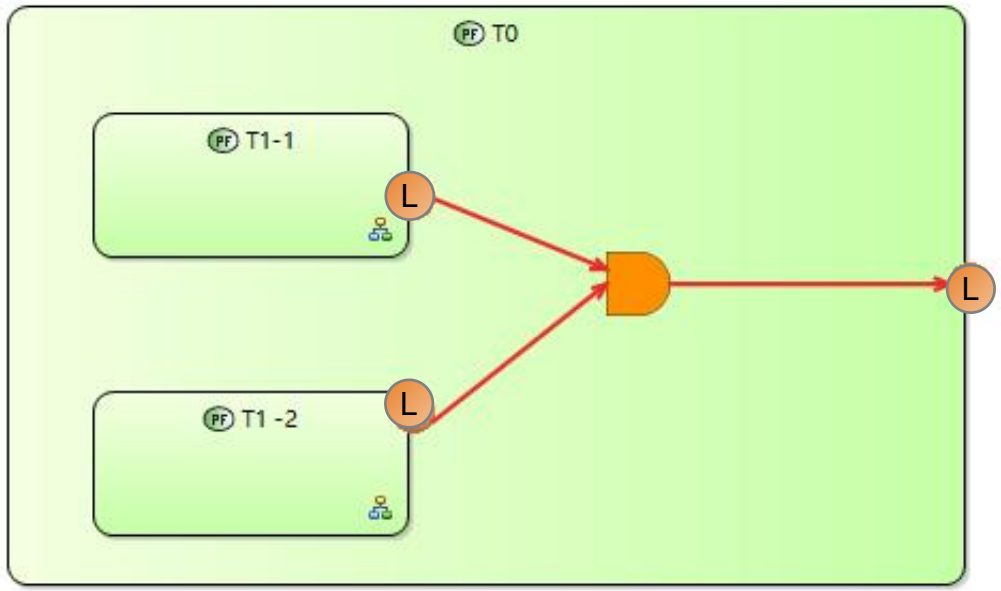
- 定义失效状态触发条件

在功能故障传播图中，
构建故障模式至失效状态追溯。



[FC]LOSS the Left Redundancy

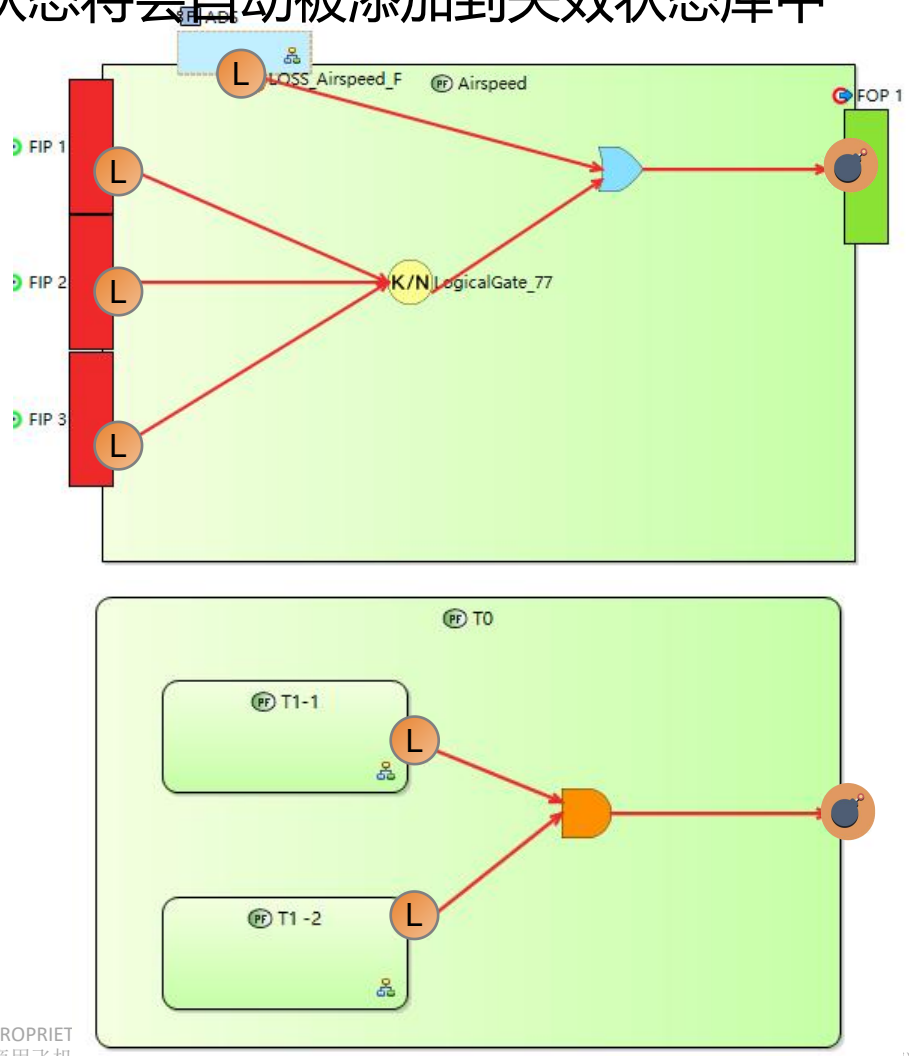
在父功能故障传播模型图中，
构建故障模式至失效状态追溯。



[FC]LOSS All Redundancies

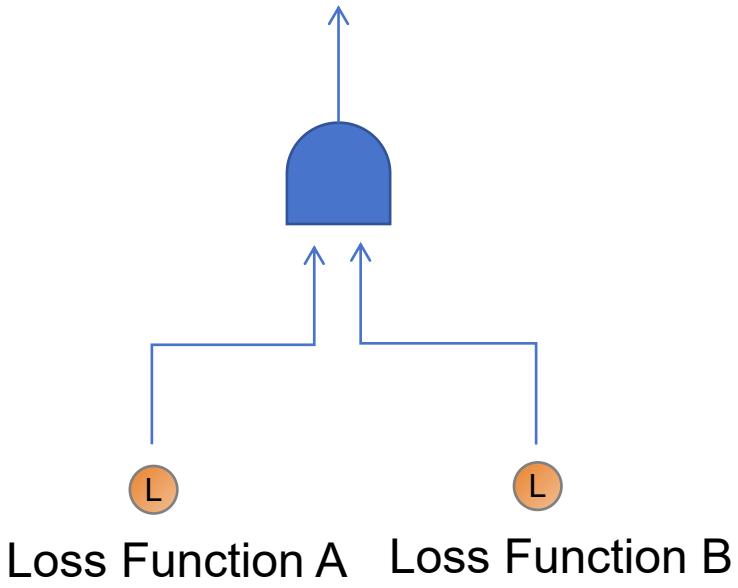
Part 3.4 架构分析——失效状态管理

- 失效状态将会自动被添加到失效状态库中



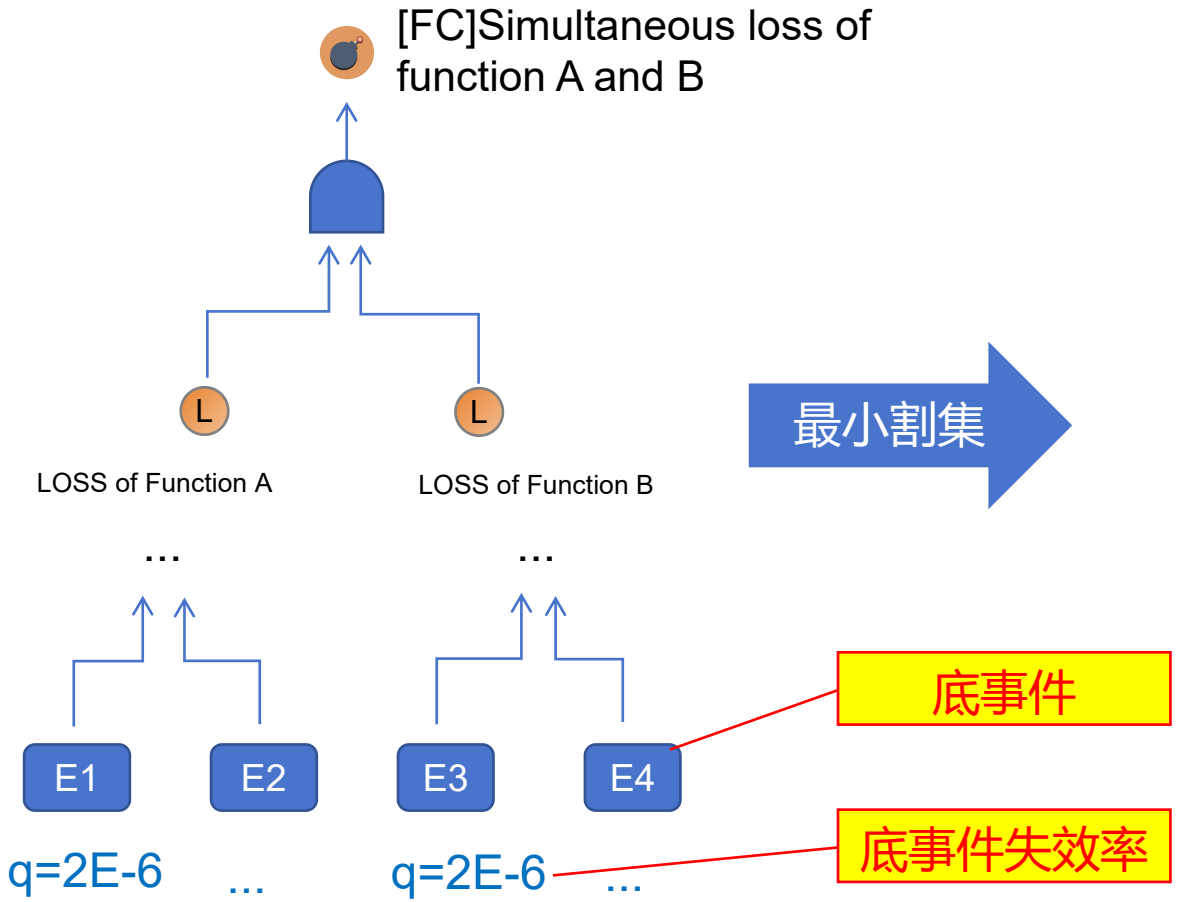
Part 3.4 架构分析——失效状态管理

- 一个失效状态可能与多个飞机功能相关
  - 工具提供失效状态自定义定义功能



Part 3.5 故障树分析

- 根据对应失效状态的故障传播模型自动生成故障树
- 计算该失效状态的最小割集

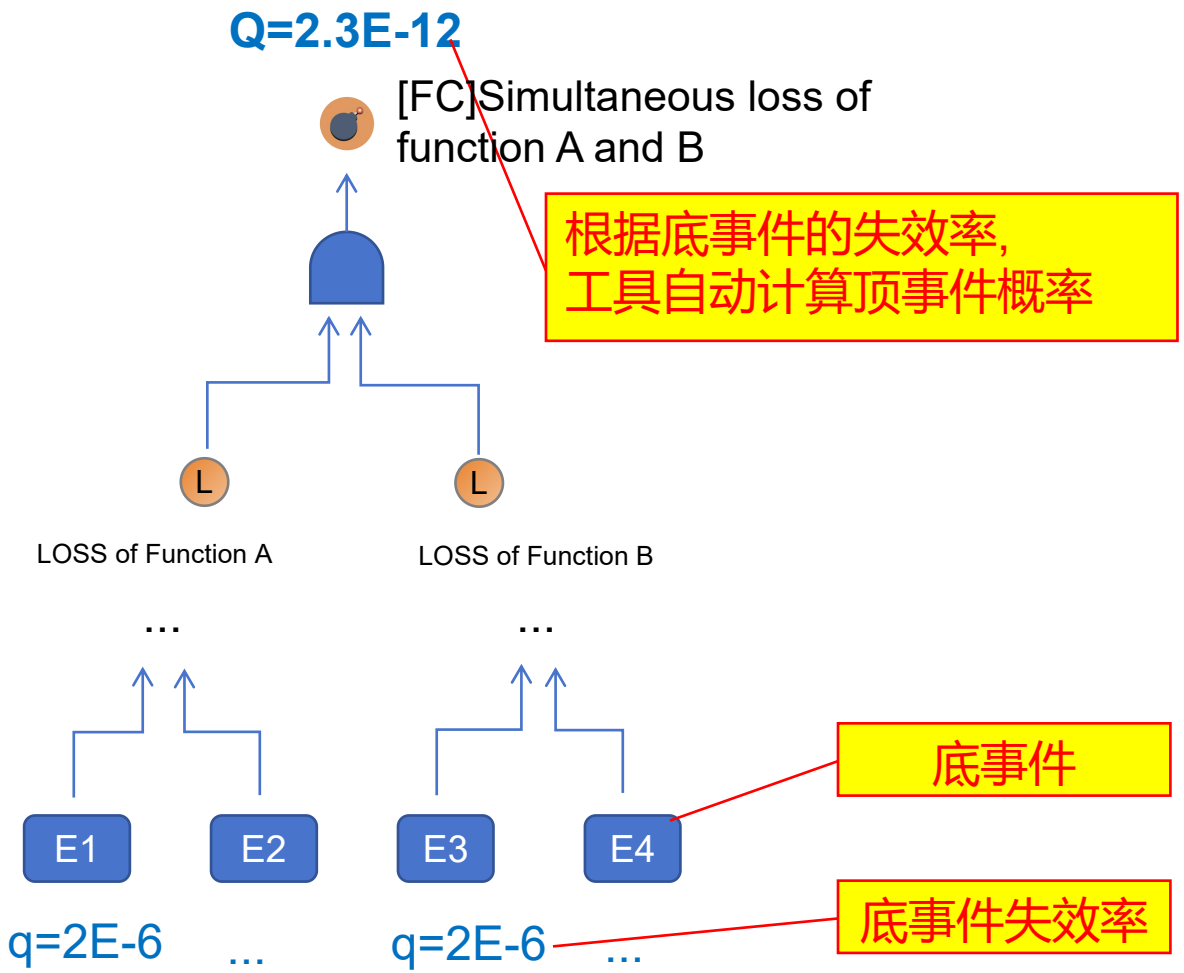


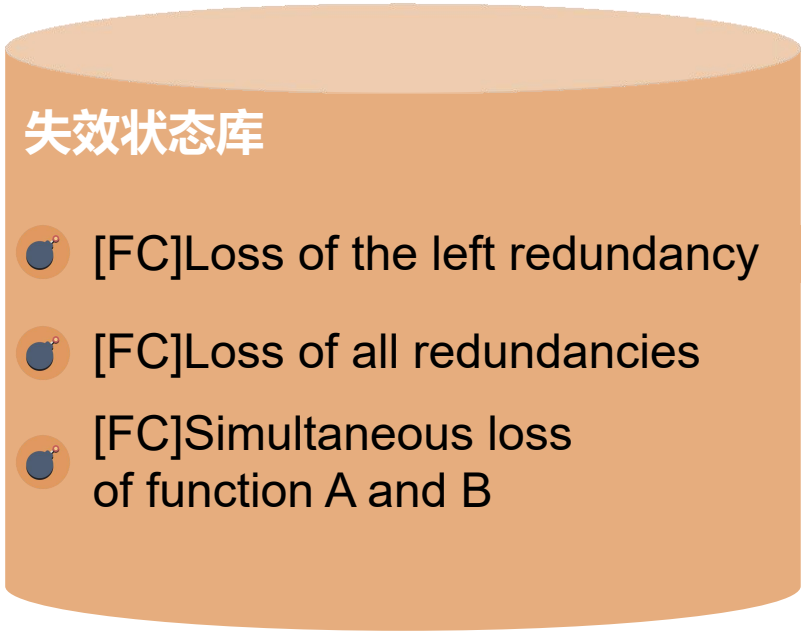
失效状态库

No.	MCS	Q
1	E1，E3	2E-6
2	E1，E4	2.1E-7
3	E2，E4	3E-8
...	...	...

Part 3.5 故障树分析

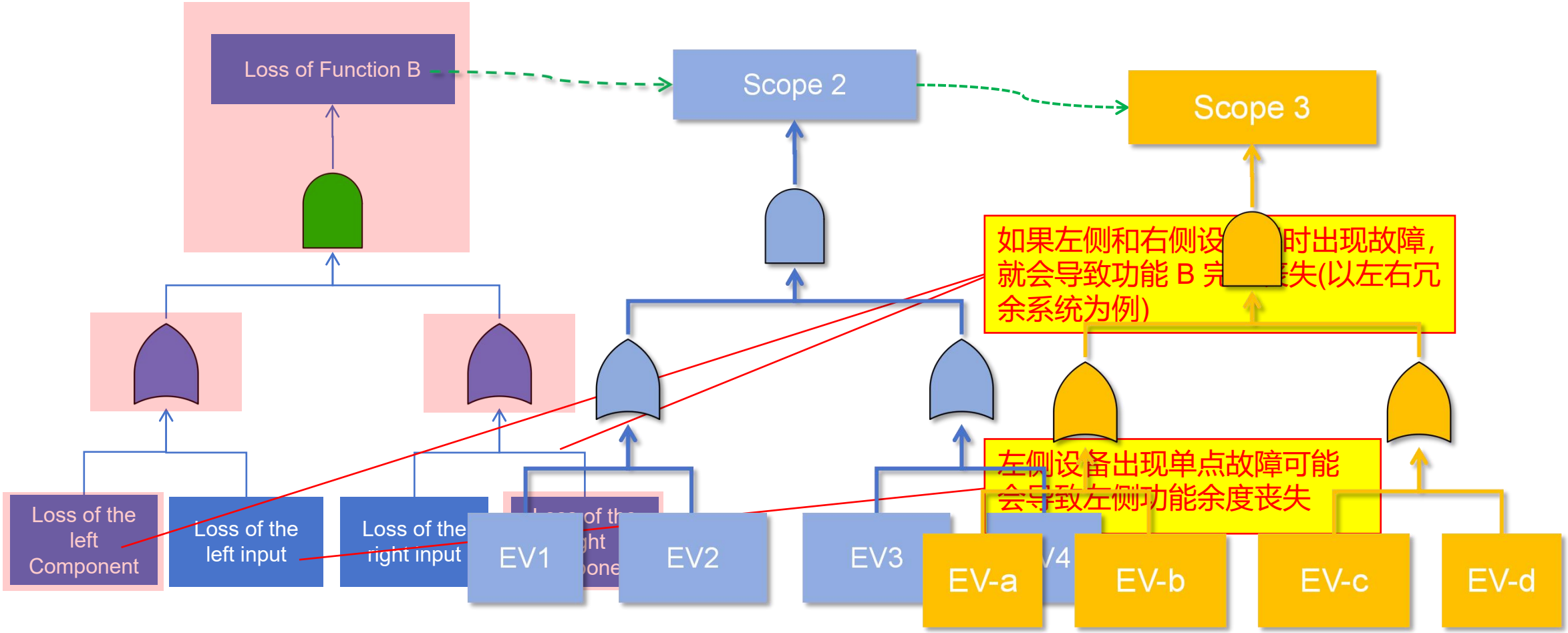
- 计算顶事件发生概率，并验证是否符合该失效状态的安全影响等级要求





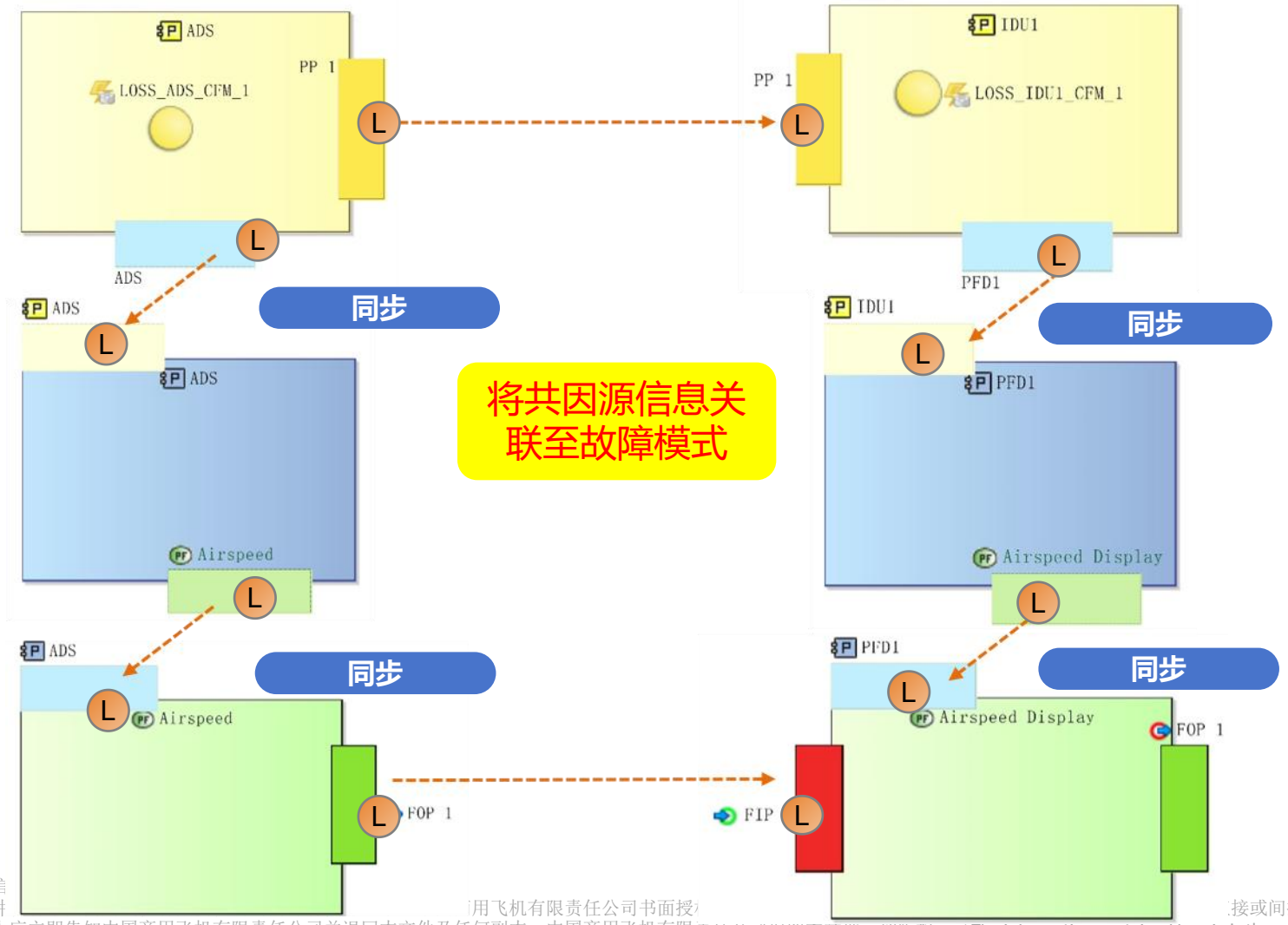
Part 3.6 安全性评估

- 在具体范围下分析特定风险产生的影响



Part 3.6 安全性评估

- 将供应源信息关联至物理组件



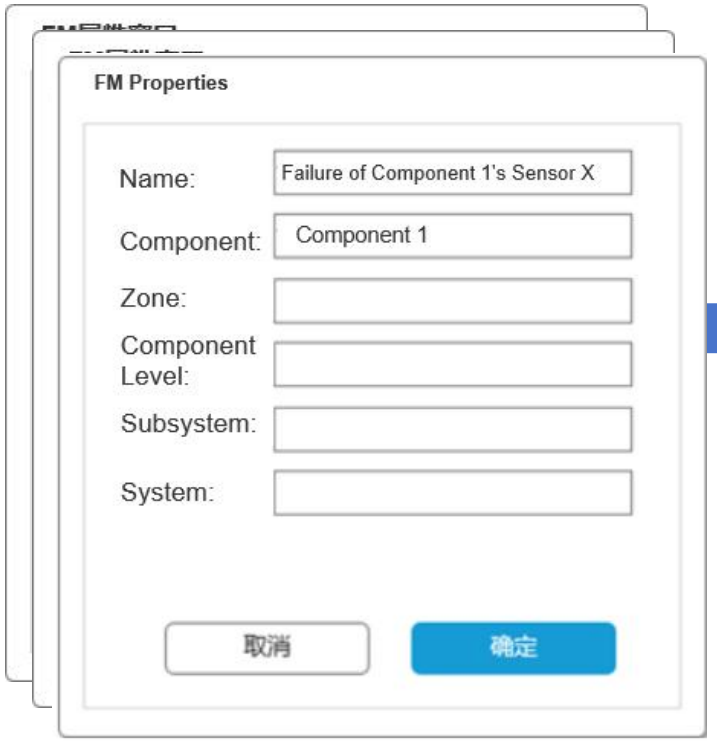
定义共因分析

共因源

- C 相同供应商
- C 相同制造商
- C …
- C …

Part 3.6 安全性评估

- 填写物理组件的属性
- 通过属性管理故障模式



筛选故障区域：左侧

FM	Zone	Device	Level	System	Sub-system
FM1	Left	Device 1	2	System A	Display
FM2	Right	Device 2	2	System A	Display
FM3	Left	Device 5	3	System A	Alerting
...	...	...	...	...	...

故障传播模型分析

安全性分析数据库

飞机左侧出现故障将会导致：FM1 和 FM3 将同时出现故障。
若 FM1 和 FM3 同时出现故障，则会导致左侧冗余系统失效。

特定风险分析

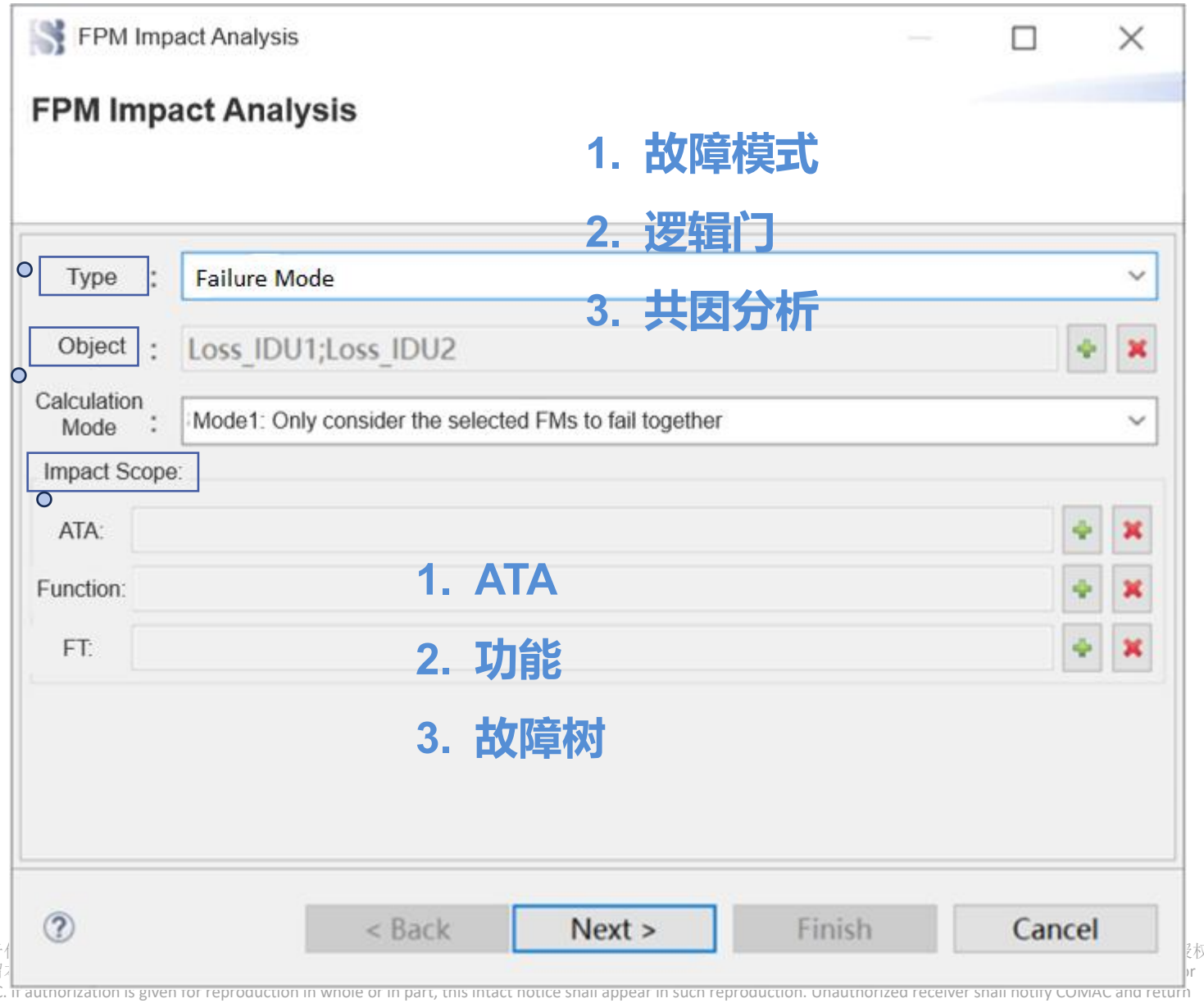
区域安全性分析

Part 3.6 安全性评估

选择分析模式

选择分析对象

选择分析范围

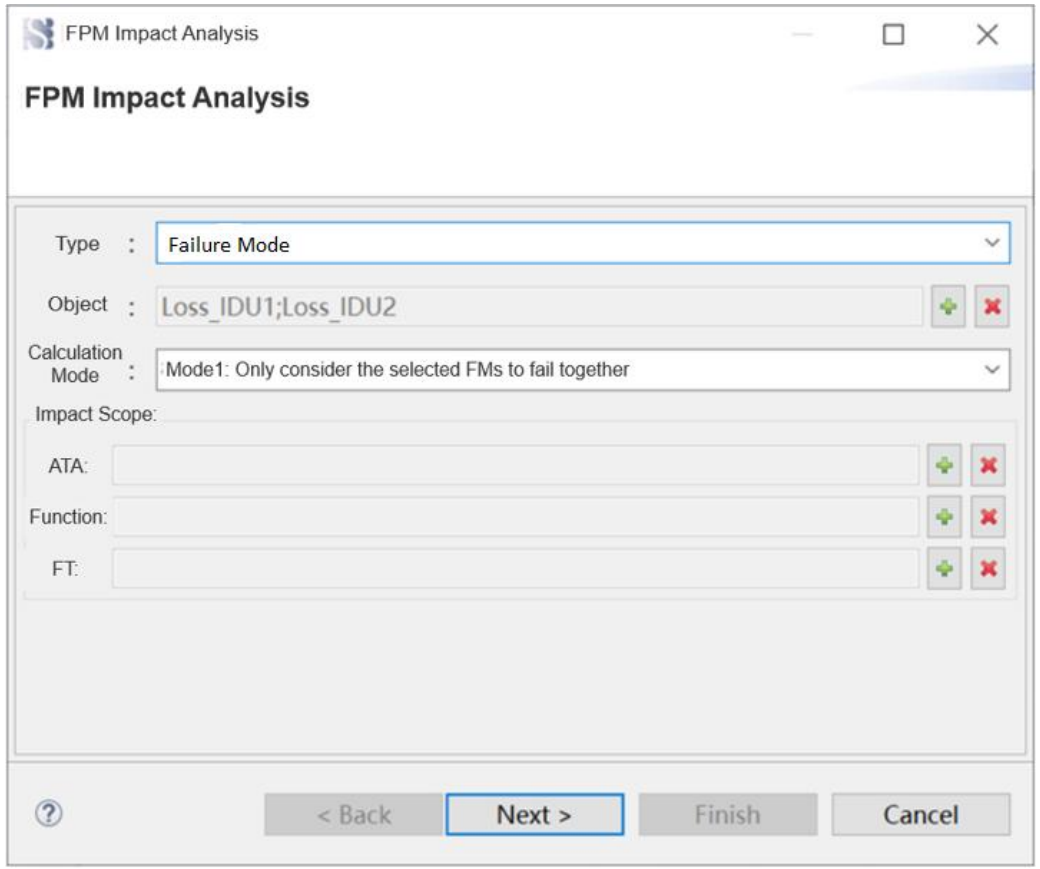


1. 故障模式
2. 逻辑门
3. 共因分析

1. ATA
2. 功能
3. 故障树

Part 3.6 安全性评估

基于整个飞机安全性数据库对复杂系统架构进行分析



单点故障分析

航电核心系统系统、供电系统以及其他公共资源系统能够从不同的功能角度进行安全性分析。

组合故障分析

特定风险分析、区域安全性分析以及共因分析可以从不同的功能层面进行。

共因和级联分析

明确评估整个架构各层级出现故障所产生的影响，包括冗余功能的丧失以及接口故障等情况。

生成标准报告

支持符合 4761A 标准的 FHA/FMEA 数据库管理，并能够导出 FHA/FMEA 报告。

Part 3.6 安全性评估

示例 :丧失A交换机和B交换机

某飞机的手动分析结果

手动分析报告结论：

燃油系统：为仪表盘显示单元（IDU）减少的燃油数据冗余量；

显示报警系统：向左侧 IDU 的数据传输出现冗余丢失的情况，但并未影响其功能。

COMSPEC工具分析结果

序号	功能	层级	失效模式
1	燃油显示	功能层级	丧失IDU2燃油量显示功能
2			丧失IDU2燃油显示功能的燃油信息输入
3		接口层级	丧失IDU2燃油显示信息接口输入
4	空速显示	功能层级	丧失IDU2计算空速显示功能
5			丧失IDU1计算空速显示功能
6			丧失IDU2空速显示功能的空速信息输入
7			丧失IDU1空速显示功能的空速信息输入
8		接口层级	丧失IDU2空速显示信息接口输入
9			丧失IDU1空速显示信息接口输入

结论

- ✓ 无详细细节
- ✓ 30多个系统同时分析一轮并汇总

≤

- ✓ **准确性:** 与人工分析结论一致
- ✓ **效率**：每次分析仅需数秒/分钟
- ✓ **便利性**：分析结果更详尽、客观且标准化
- ✓ **完整性**：分析结果涵盖了功能层面和物理接口层面。

04 | Demo演示

05 | 总结

Part 5.1 总结

复杂系统架构解析

- 能够对复杂架构模型进行解析
- 基于物理架构自动建立失效传播逻辑
- 安全性分析结果可确认与改进架构模型

故障树自动创建

- 复杂架构功能/设备定义失效传递逻辑
- 自动创建故障树，节省设计师精力
- 确保故障树层级一致

公共设备一致性

- 复杂系统公共设备故障模式模型化、标准化
- 复杂系统的公共资源可开展安全性影响分析

安全性分析自动化

- 故障树计算结果自动形成安全性数据库
- 自动开展ARP4761规定的共因分析、特定风险分析等安全性分析内容

突破创新

- 可兼容其他FTA工具的故障树模型
- 拥有该套建模方法的知识产权，不受到外部环境变化的影响

Part 5.1 总结

应用场景广阔

- 复杂系统的设计和验证工作
- 高度复杂的集成系统
- 高可靠性与高安全性系统


COMAC
中国商飞
谢　谢！
THANK YOU