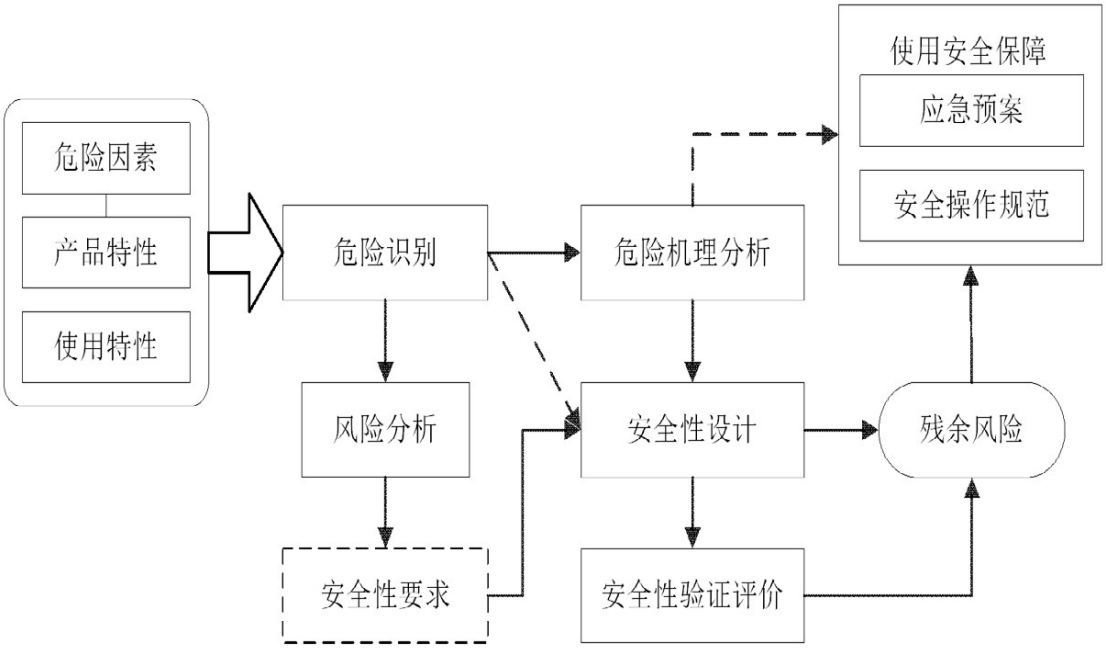
软件安全性复习

安全性核心原理



基本概念

系统

系统是由相互制约的各部分组成的具有一定功能的整体。（钱学森）
系统的基本特征：多元性、关联性、整体性。

安全性

产品具有的不导致人员伤亡、装备毁坏、财产损失 或不危及人员健康和环境的能力。（GJB900A-2012《装备 安全性工作通用要求》）

安全原理

以事故为对象、以危险为核心，阐述安全的 本质与属性，事故为何发生和如何发生的基本规律，以及 如何预防、控制事故和救援的一般原理与方法论。

基本方法

安全性要求确定
危险分析
安全性设计
安全性验证
安全性评价
危险跟踪
变更安全性保证

软件开发与管理的三维模型

现代软件工程化管理的理念为软件开发与管理构建一个全方位、全过程、多层次的三维框架，这三维是：

时间维：对软件生存期的全过程进行控制；全过程控制

空间维：对软件质量有关的关键因素实施全方位管理；

组织维：构建从软件开发个人、软件开发小组到软件开发单位的多层次的管理模式。全组织管理

事故

造成人员伤亡、职业病、设备损坏或财产损失的一个或一系 列意外事件。--GJB/Z 142-2004

危险

- 可能导致事故的状态。--GJB 900A
- 可能导致或有助于事故或灾难（人员伤亡、或系统毁坏、或 财产损失或环境破坏等）发生的实际条件或潜在条件（1 维）
- 危险可能是硬件或软件的缺陷或人的错误引起，或一个非预 期输入。

风险

用事故的可能性和事故严重性表示发生事故的可能程度（2 维）

软件安全性相关概念

软件可靠性

在规定的条件下，在规定的时间内， 软件运行不发生失效的概率。

失效

是指程序的运行偏离了软件需求规格说明文 档中的要求，是软件动态运行的输出结果。

软件安全性

软件在系统中运行而不导致系统发生 事故的能力。

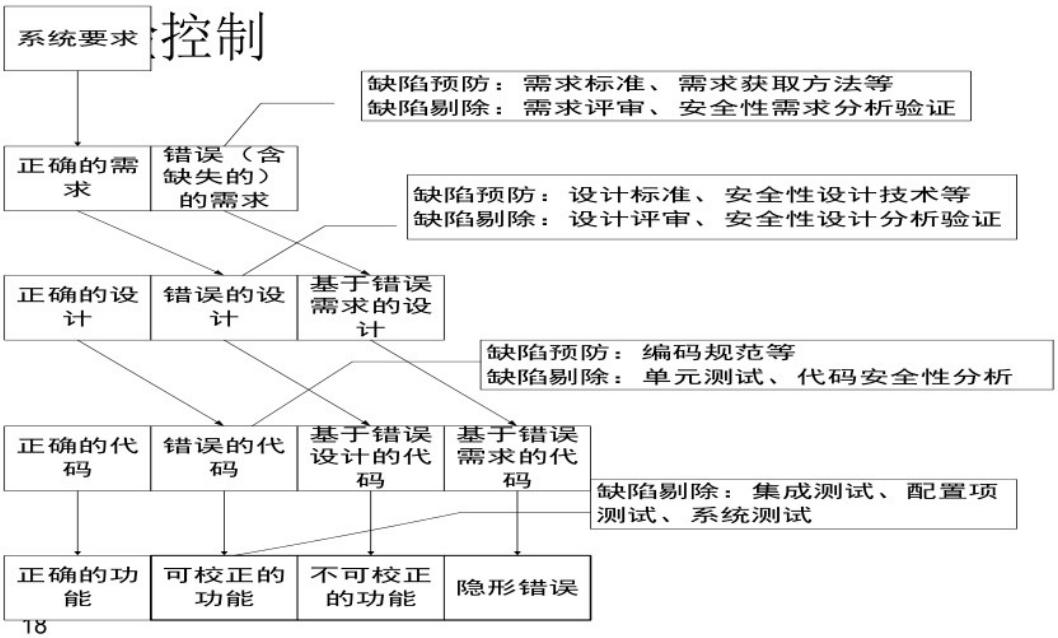
安全相关软件

软件安全性需求

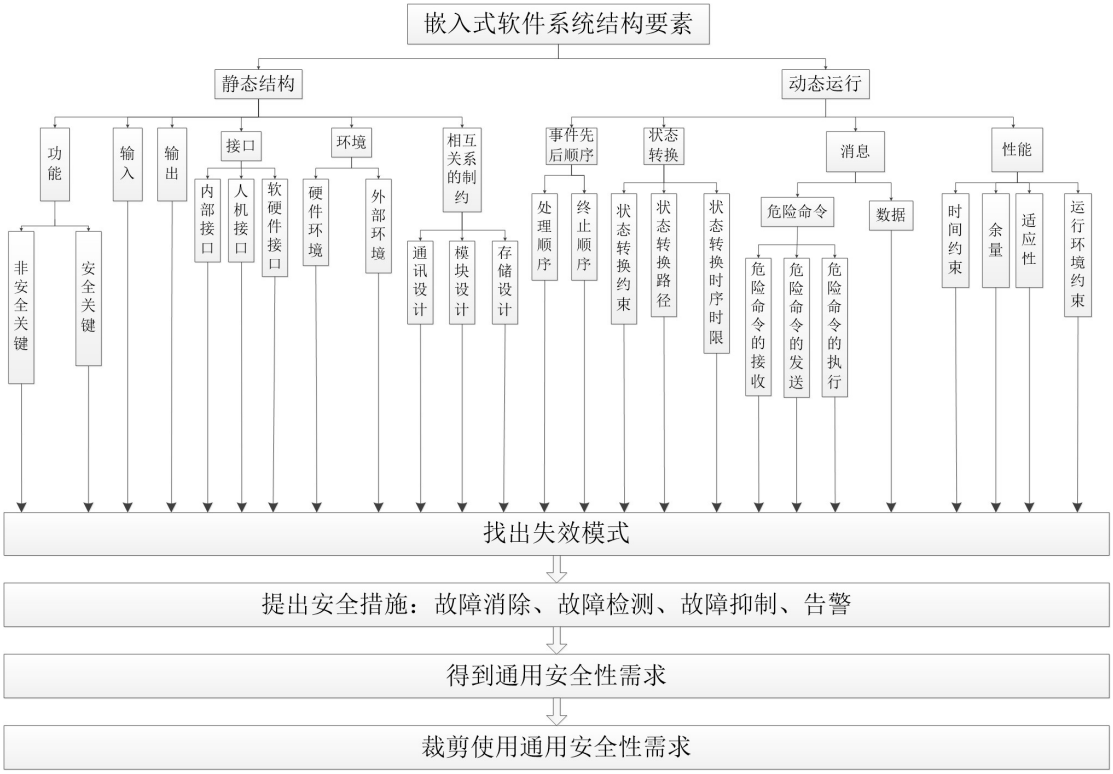
既包括安全关键的功能、性能等 用户实际需要的需求，又包括用于防止、消除、检测、处理危险的需求。

软件安全性机理和危险控制方法

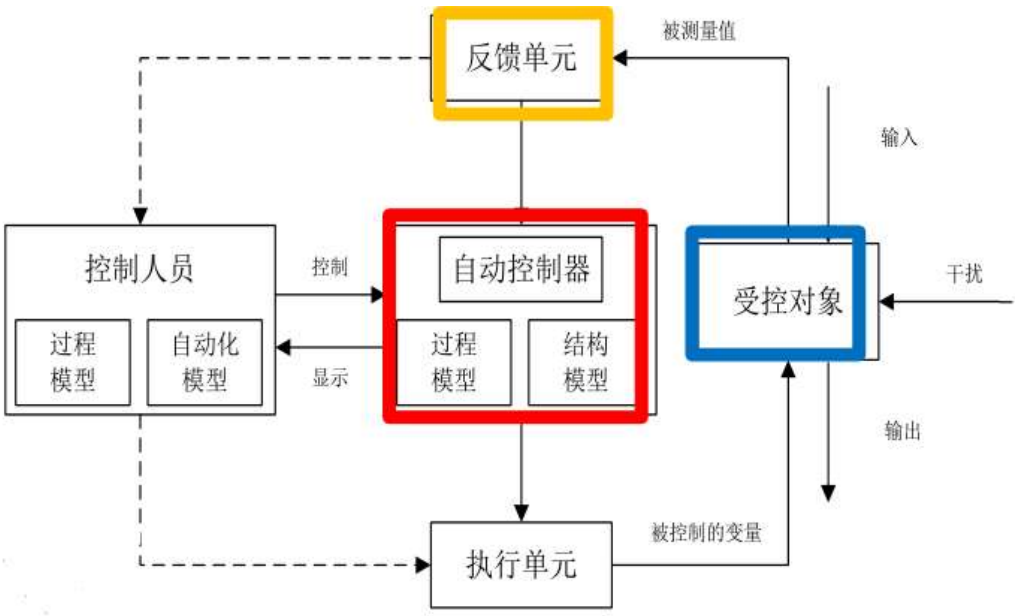
基于开发过程的软件安全性机理及危险控制



基于软件产品的软件安全性机理及危险控制

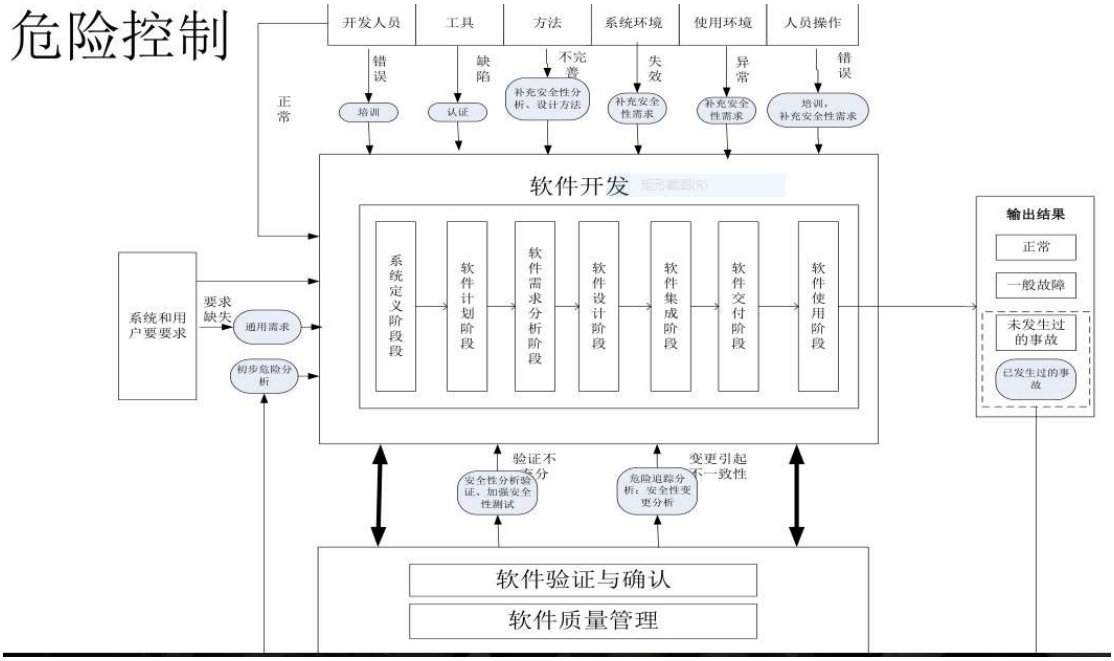


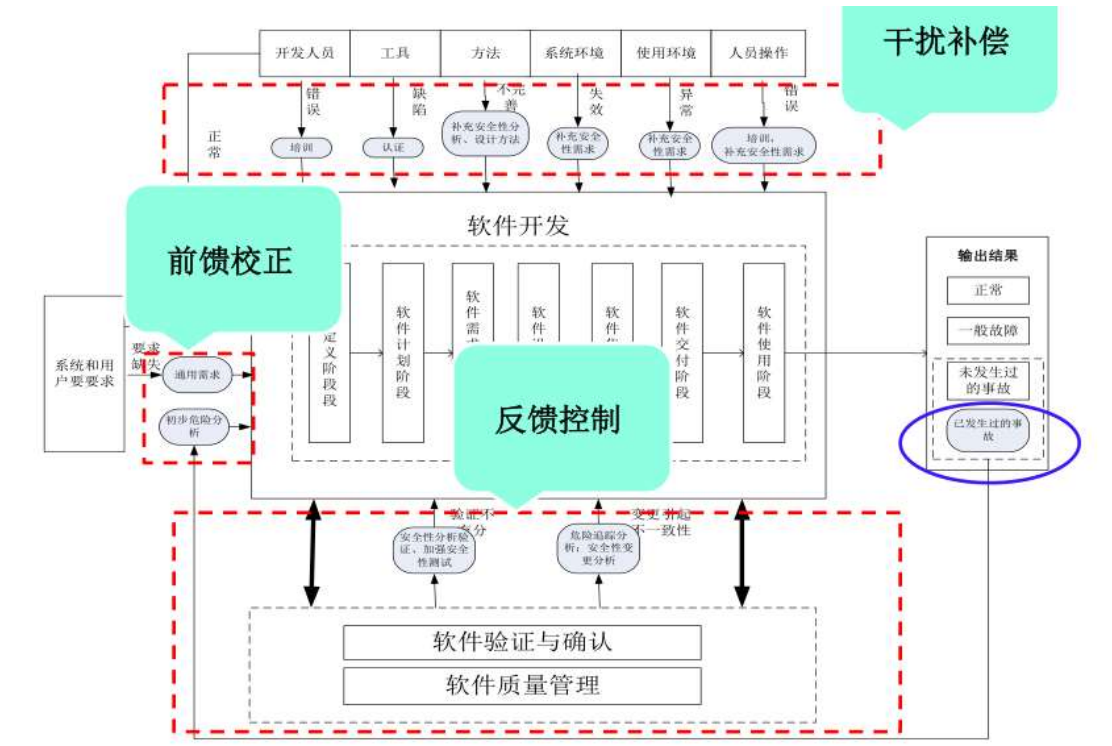
基于系统交互的软件安全性机理及危险控制



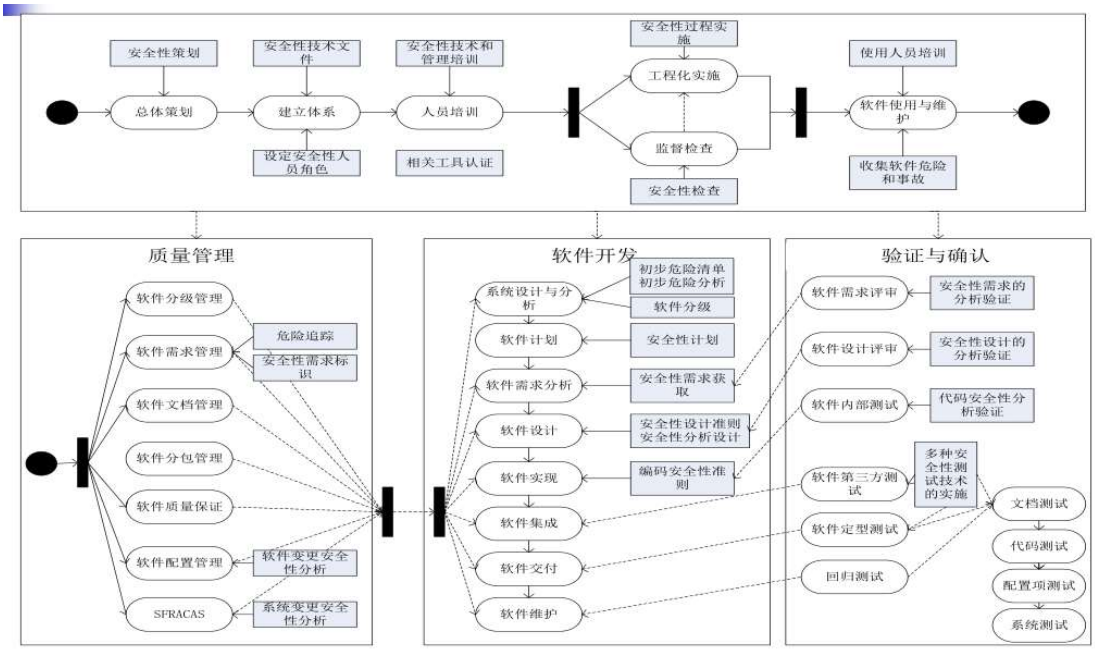
基于开发和使用环境的软件安全性机理及危险控制

危险控制



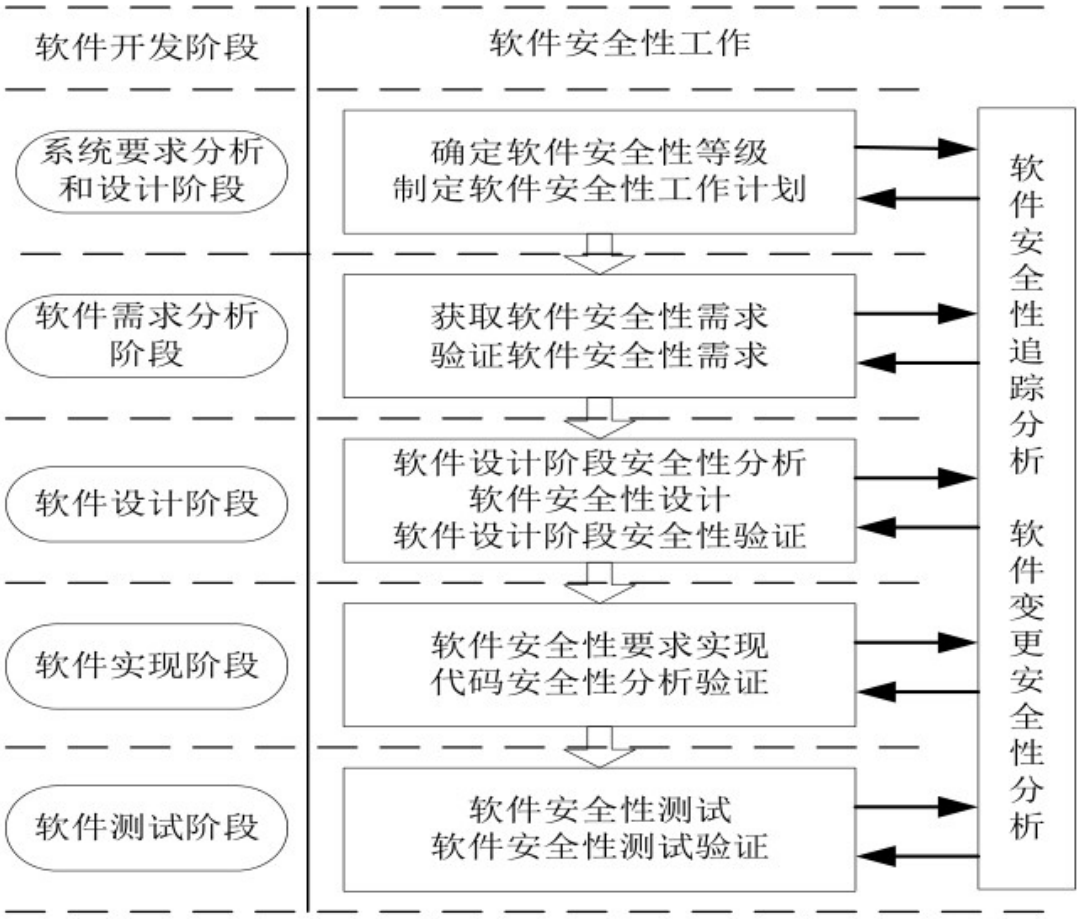


软件安全性工程的框架



技术、过程、管理

软件开发各阶段的主要安全性工作



■分级方法

确定软件安全性等级是软件安全性工作的重要内容之一，是在软件开发过程中的第一步工作。确定软件等级是开展后续安全性计划和安全性技术活动的基础。

表 1 危险严重性等级定义

等级	描述
Ⅰ（灾难的）	导致或促使系统功能失效，从而妨碍飞机安全飞行与着陆。
Ⅱ（严重的）	降低飞机能力或机组处理不利运行条件能力，包括1、导致安全裕度或航空器操纵能力大幅度下降，2、使机组人员无法精确和完整地完成任务的身体压力或过重的工作负担3、对乘客的不利影响，包括对少量成员严重的或潜在致命的伤害。
Ⅲ（轻度的）	降低航空器性能或机组处理不利运行条件能力，导致安全裕度或航空器操作性能显著下降，显著地增加机组工作量或降低其工作效率，或使机上乘员感到不适，甚至受伤。
Ⅳ（轻微的）	不会显著降低航空器安全，且需要机组采取的动作完全能在其能力范围之内，包括：安全裕度或航空器操作能力轻微下降、稍微增加了机组的工作量。

软件控制类别

表 2 软件控制类别定义

软件控制类别	控制程度
Ⅰ	软件部分或者完全控制安全性关键功能
	具有多个子系统、交互式并行处理器或者多个接口的复杂系统
	某些或者全部安全性关键功能都是时间关键的
Ⅱ	控制危险，但其他安全性关键系统能够部分的缓解，或者检测危险，通报安全员需要采取安全性措施。
	适复杂性，具有很少子系统和/或少数接口，没有并行处理
	某些危险控制措施可能是时间关键的，但不超过操作员或者系统自动响应的时间
Ⅲ	如果软件存在故障，存在若干缓解系统以防止危险，或者是冗余的安全性关键信息来源
	稍微复杂的系统，有限的接口数
	缓解系统能够在任何关键时间段内响应
Ⅳ	不控制危险的硬件且不为操作员产生安全性关键数据
	仅有2-3个子系统和少量接口的简单系统
	不是时间关键的

！等级划分过程

1) 确定软件所在系统的危险严重性等级

根据 **FHA** 确定的各个危险的影响，选择所有危险中最严重的影响

2) 确定软件对系统的控制类别

根据软件系统需求文档提供的信息，确定软件对系统功能行使的控制程度，继而确定软件所属的控制类别。

3) 确定软件等级

按照建立的矩阵，可以确定软件等级，并据此决定软件后续的安全性工作开展程度。

！FHA

FHA 定义

对产品的功能进行系统而全面的检查，以识别各种功能故障状态，并根据故障影响的严重程度对其进行分类的一种安全性分析方法。

目的

识别危险，确定安全性关键部位；
评估各种危险的风险，确定危险影响等级；
确定危险控制建议。

！分析等级

飞机级（整机级）

飞机研制开始时对所规定的飞机基本功能进行的高层次定性评估，应识别与飞机级功能相关的故障状态并进行分类。

系统级

实质上是 FHA 的迭代过程。在设计过程中将飞机功能分配到系统后，综合了多重飞机功能的每个系统必须使用系统级 FHA 过程重新被检查。

实施流程

总体流程

- 在方案阶段，开展飞机级 FHA。
- 以飞机 FHA 得到的故障状态为根节点，开展飞机 FTA，得到系统级可能存在的各类故障状态。
- 在初步设计阶段，开展系统级 FHA，此时各系统的故障状态应充分考虑飞机 FTA 的分析结果。
- 对系统级的故障模式开展 FTA，得到低层次的故障原因。
- 飞机和系统 FTA 相结合可以进行定量计算。

  注意：此时的 FTA 同样只是对功能的分析。

FHA 实施流程

1. 识别与分析等级相关的所有功能

内部功能和交互功能：

内部功能

对于整机级，内部功能即飞机的主要功能和飞机内部系统间的交互功能。

对于系统级，内部功能是指所分析系统的功能和系统内部设备间的交互功能。

交互功能（外部功能）

对于整机级，外部功能是指与其它飞机或地面系统的接口功能；

对于系统级，外部功能是指所分析系统为其它系统（包括其它飞机系统或地面系统）提供的功能或从其它系统获得的功能。

2. 识别和说明故障状态

3. 确定故障状态的影响

4. 确定故障状态影响的分类

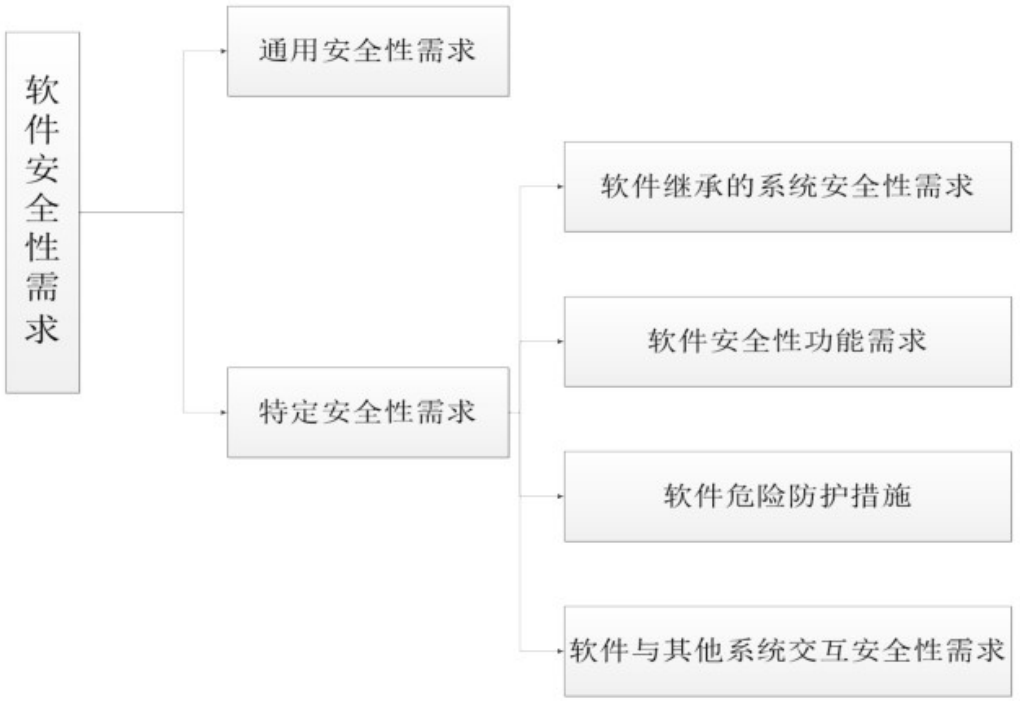
5. 对于较低层次的故障状态分配概率要求

6. 识别对故障状态的验证方法

7. 给出控制建议

■软件安全性需求获取方法流程、验证

软件安全性需求是从系统安全性需求中分解而来，保证系统维持在一个安全状态，同时可以对潜在失效做出充分的反应的软件需求。
需求开发（获取需求）+需求分析（验证需求）

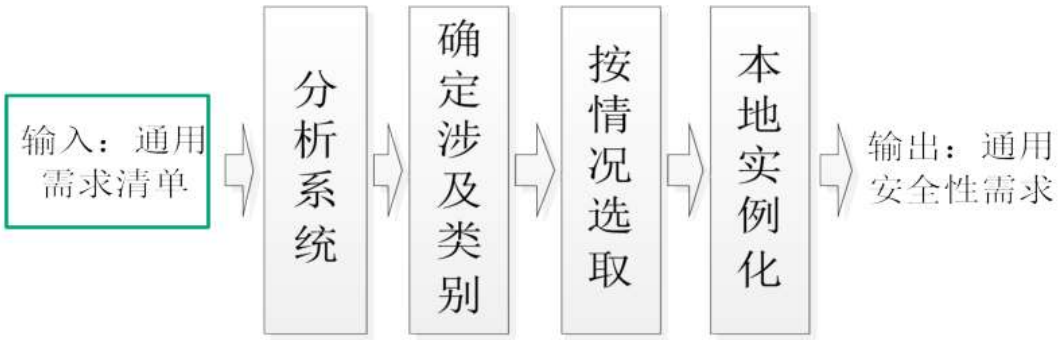


获取过程

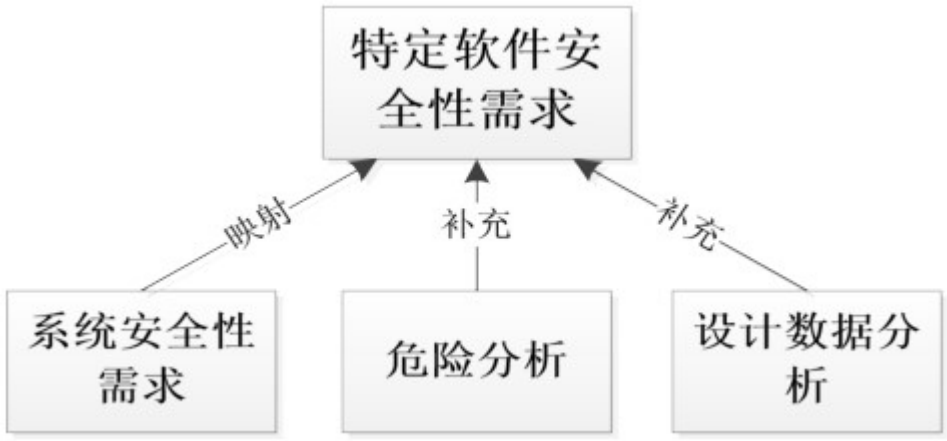
1）获取系统及软件信息

软件安全性工作的主线：软件安全性需求的获取和验证以及软件安全性需求在各开发阶段的实现和验证。

2）剪裁通用机载软件安全性需求



3）获取特定软件安全性需求



（1） 系统安全性需求映射

获取系统需求追踪矩阵；
将系统需求追踪矩阵中的安全性关键需求映射到软件，得到软件安全性关键需求。

（2）危险分析

FHA-SFTA 法
SFMEA 法
基于系统理论的危险分析方法
需求关键性分析

（3）设计数据分析

■软件安全性设计

软件安全性设计包括广义和狭义的概念
软件安全性设计阶段的工作包括针对设计的分析、设计、验证。
是软件安全性需求的具体落实
对于安全性关键软件，安全性设计的目标是实现最小风险设计，其中的风险包括软件缺陷产生的风险、用户操作产生的风险、费用风险和进度风险。

避错设计原理、准则

软件避错设计原理

简单原理
同型原理
对称原理
层次原理
线型原理
易证原理
安全原理

定义

根据所标识的信息域的软件需求，以及功能和性能需求，进行数据设计、系统结构设计、过程设计、界面设计

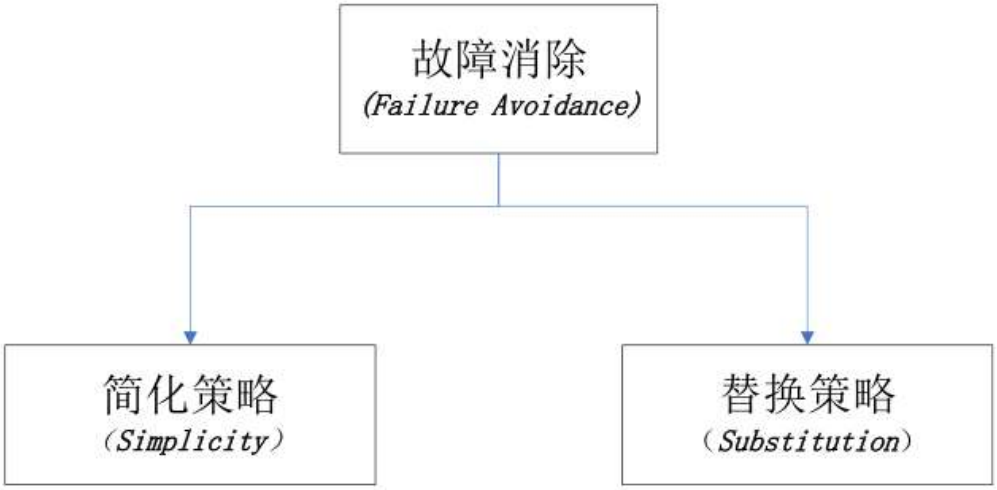
避错设计的四个方面:

程序结构化设计

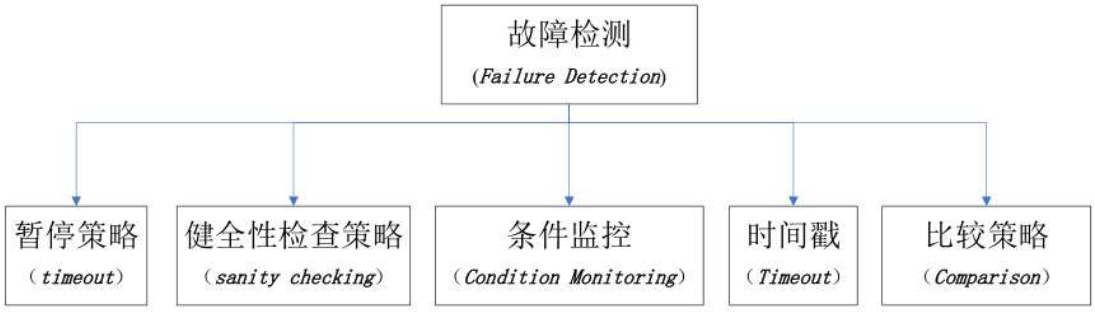
软件简化设计
软件健壮性设计
软件冗余设计

安全性三种设计策略和方法、验证

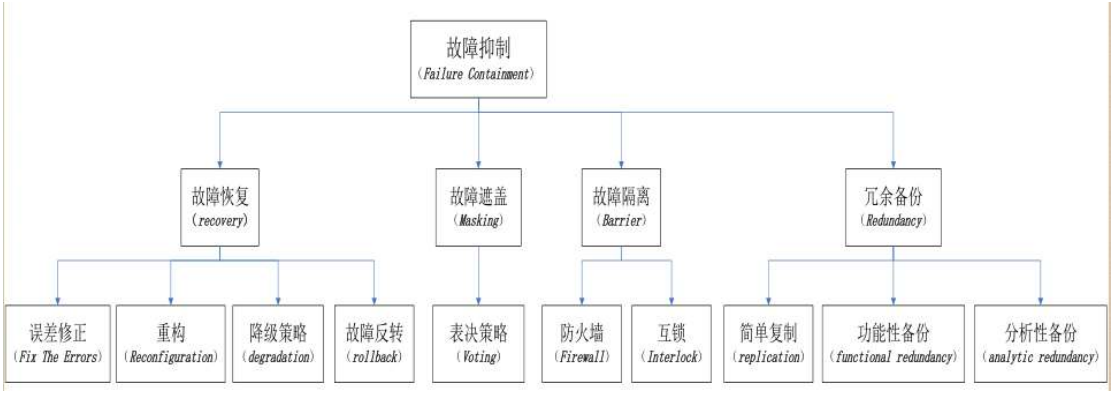
a. 故障消除



b. 故障检测



c. 故障抑制



■软件安全性测试

定义

软件测试

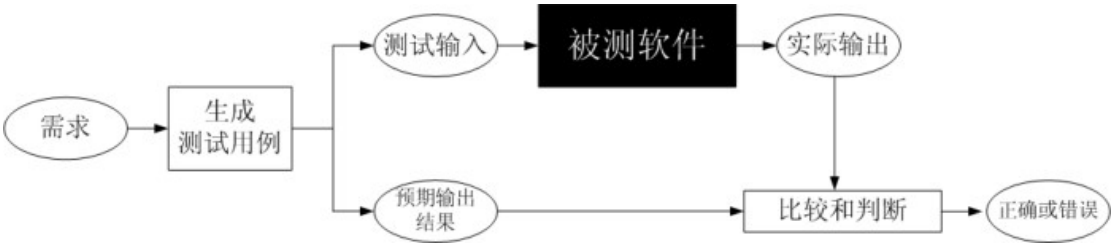
软件测试以检验是否满足需求（或设计）为目标。
重点是发现问题

软件安全性测试

软件安全性测试是为了验证软件获得的安全性而进行的测试。

安全性测试方法

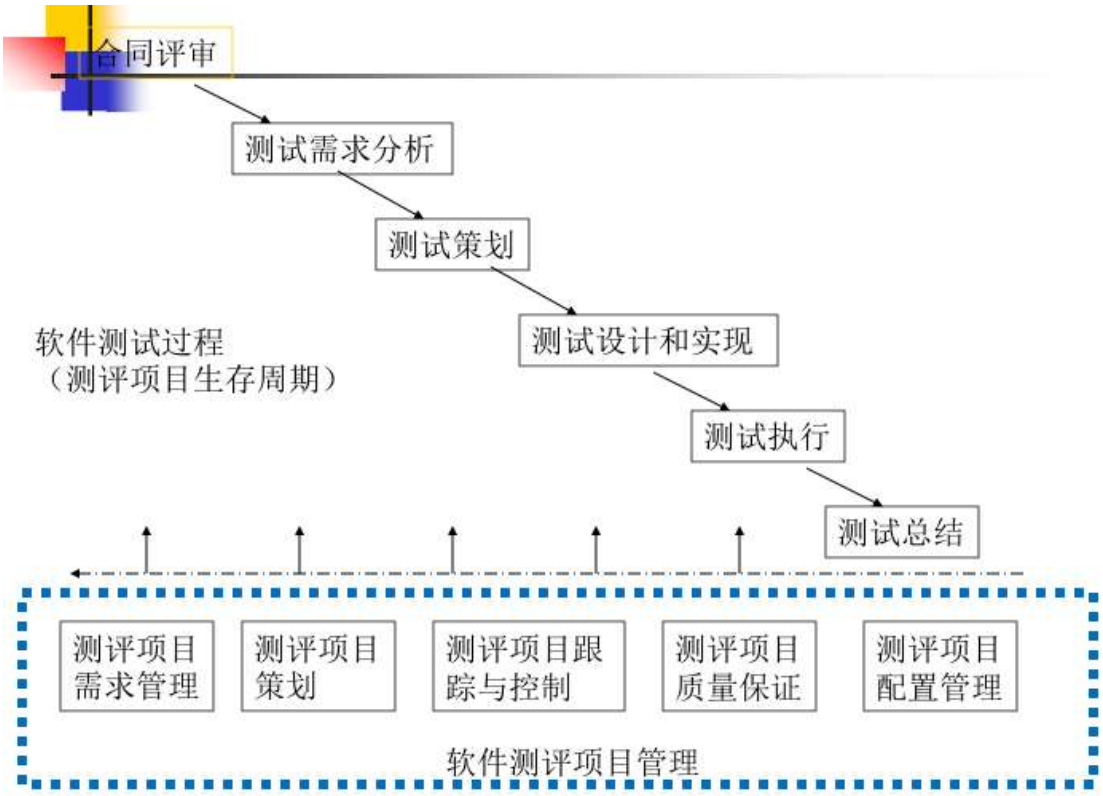
黑盒测试



（生成测试用例、各种可能的异常输入）

测试用例主要包括测试的输入和预期结果。
等价类划分方法产生异常测试

系统测试过程



1）软件测试过程包括：

测试需求分析
测试策划
测试设计和实现
测试执行
测试总结（包括评价过程和总结）

2）软件测评项目管理包括：

测评项目需求管理

测评项目策划管理
测评项目跟踪与控制
测评项目质量保证
测评项目配置管理

测试充分性验证

应验证所有的安全性需求项都经过了充分的测试，可采取的方法有**测试覆盖度量**和**需求追踪矩阵**等方法；可采用**检查单**的方法检查是否进行了足够异常模式的测试。

- 其他因素