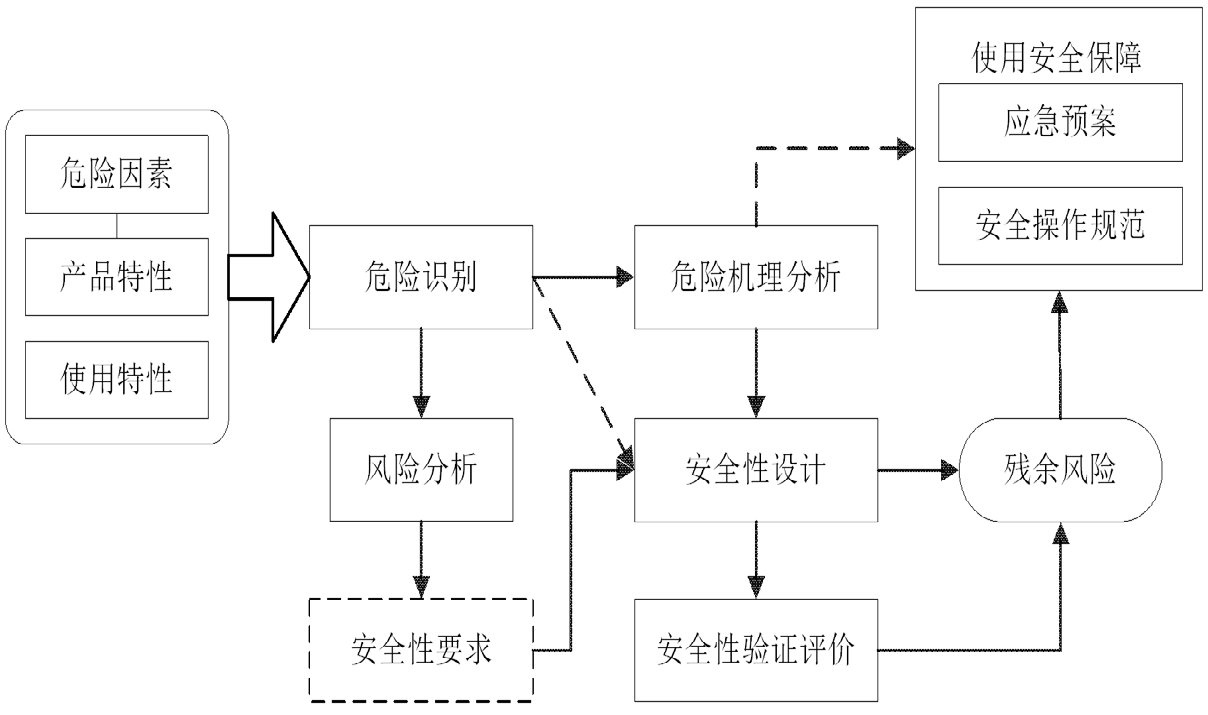
软件安全性复习

# 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。

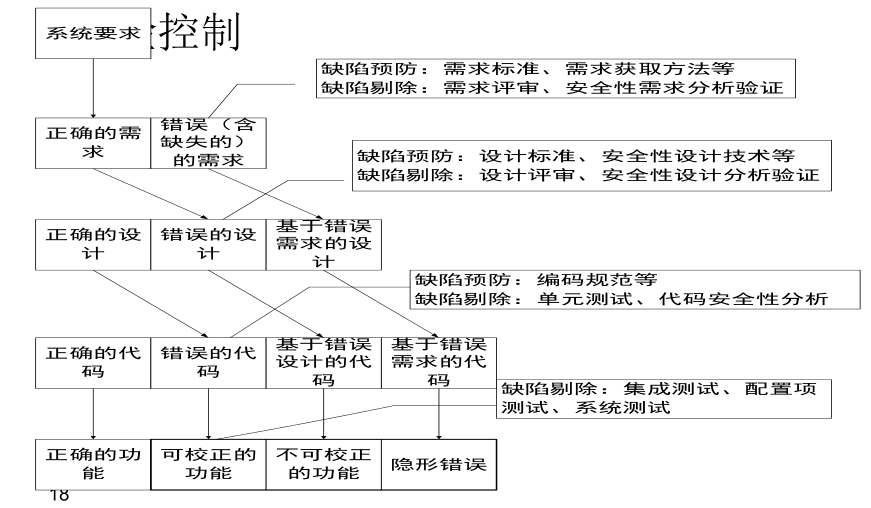
#### 安全相关软件

#### 软件安全性需求

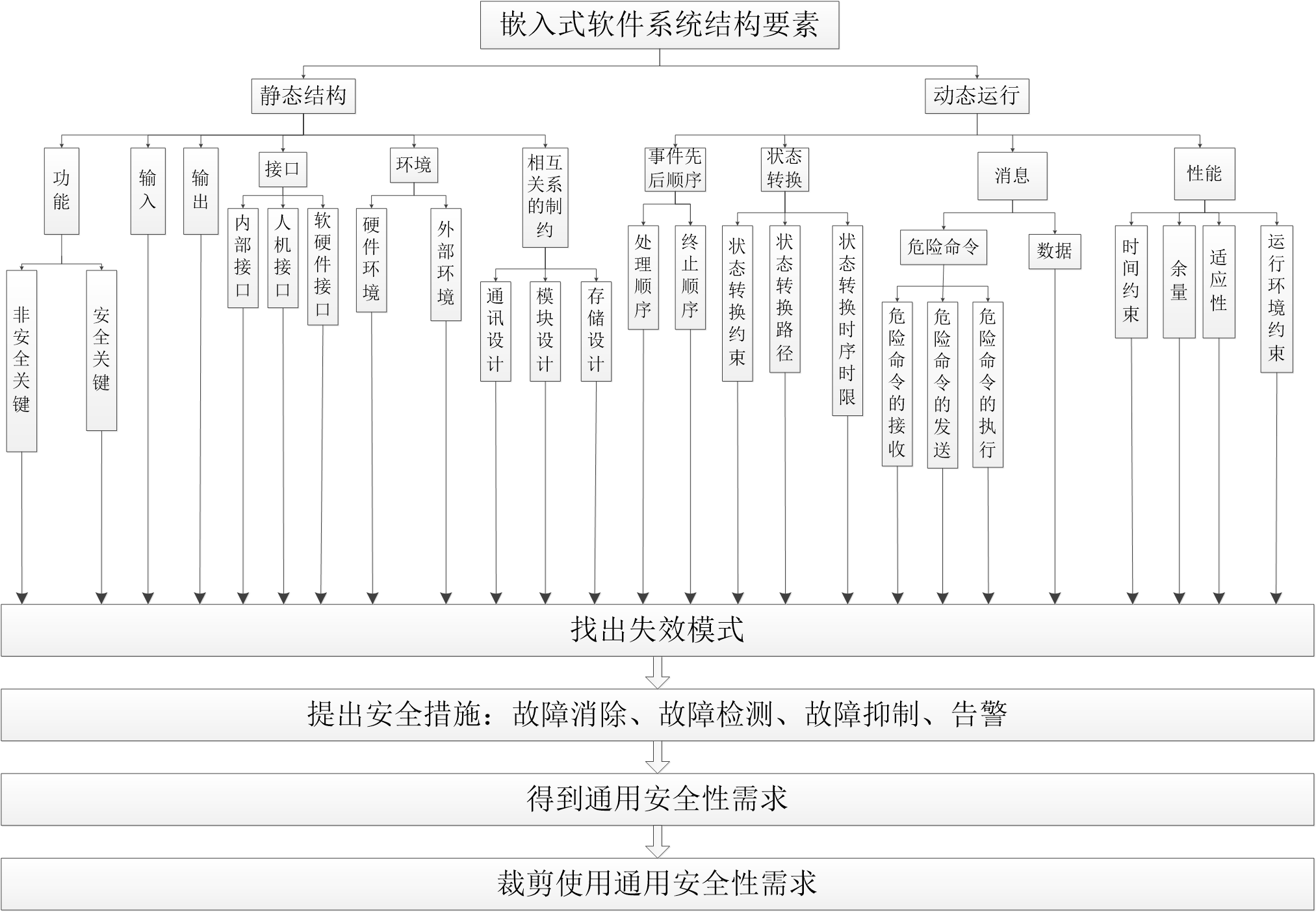
既包括安全关键的功能、性能等 用户实际需要的需求，又包括用于防止、消除、检测、处理危险的需求。

# 软件安全性机理和危险控制方法

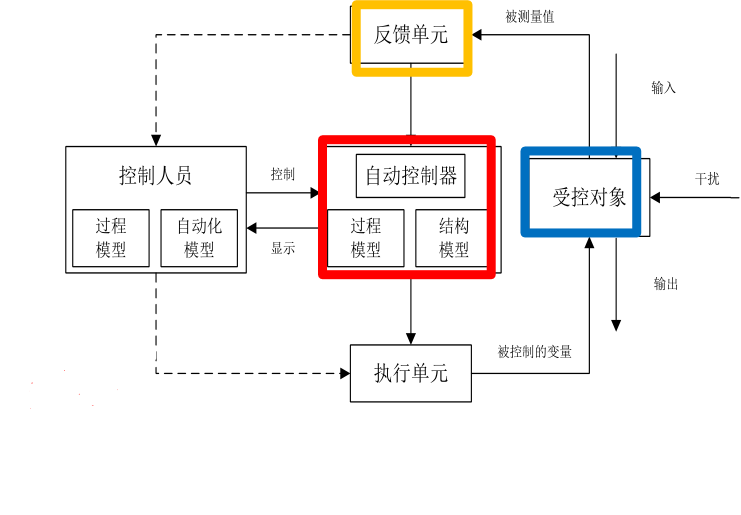
## 基于开发过程的软件安全性机理及危险控制



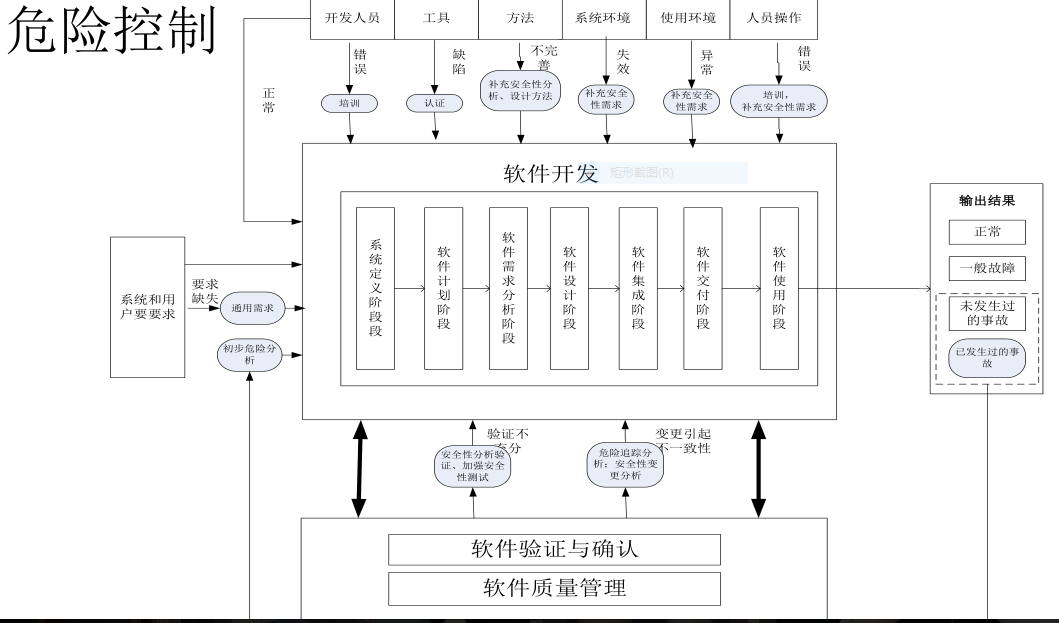
## 基于软件产品的软件安全性机理及危险控制

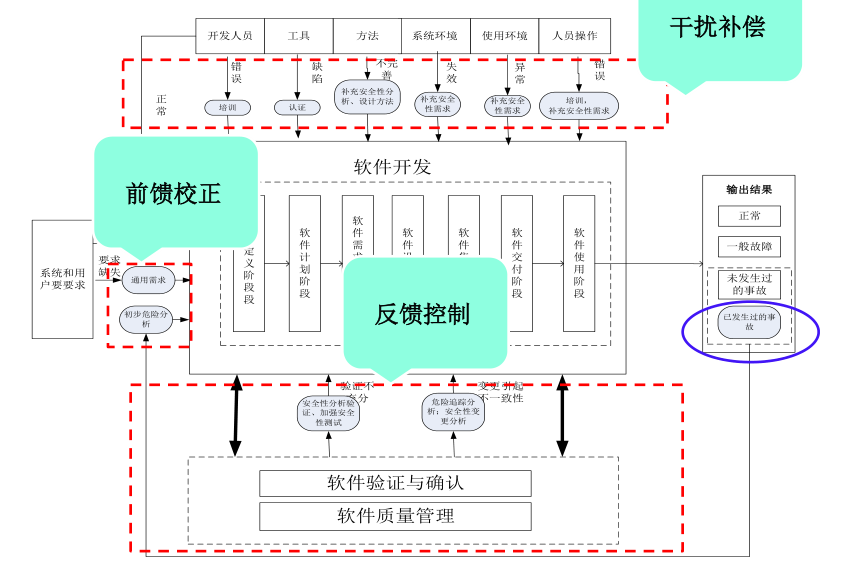


## 基于系统交互的软件安全性机理及危险控制

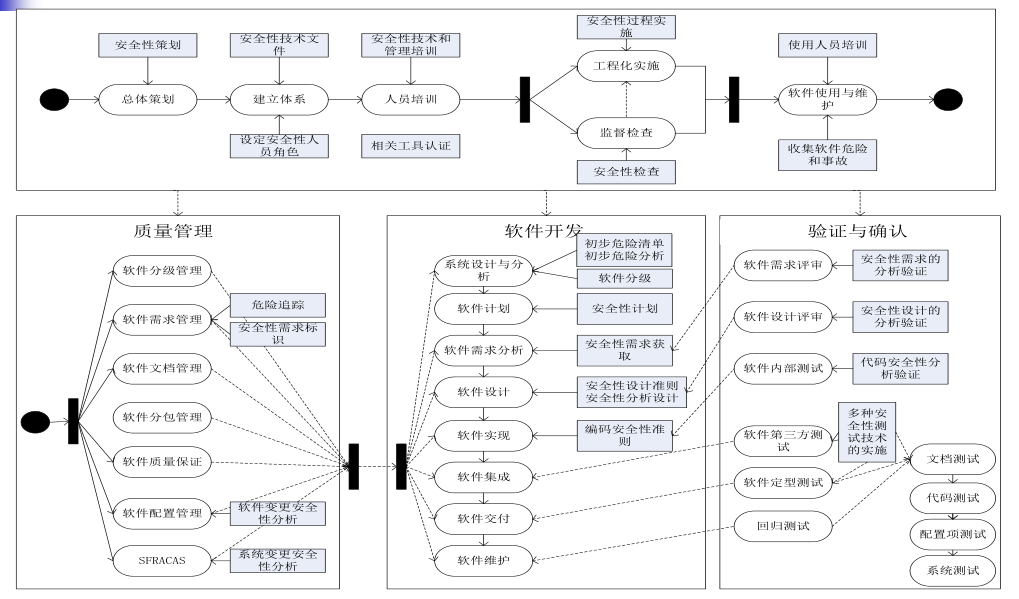


## 基于开发和使用环境的软件安全性机理及危险控制



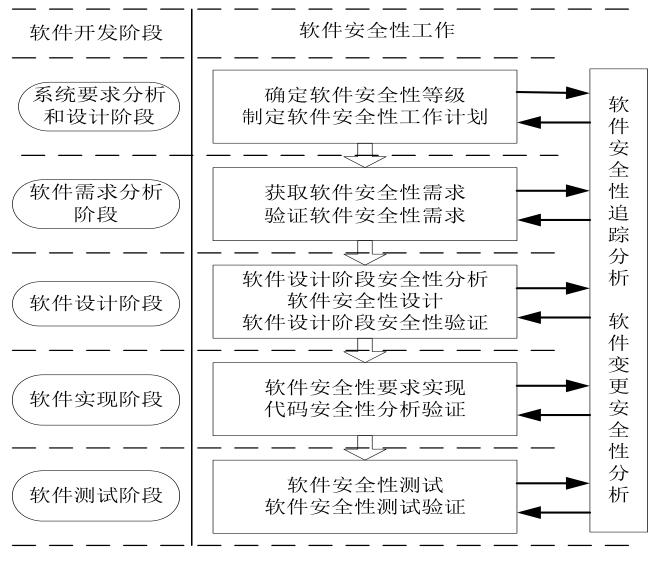


# 软件安全性工程的框架



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

## ◼软件安全性需求获取方法流程、验证

# ◼软件安全性设计

## 避错设计原理、准则

## 安全性三种设计策略和方法、验证

# ◼软件安全性测试

## 安全性测试方法

（生成 测试用例、各种可能的异常输入）

## 系统测试过程

## 测试充分性验证

◼其他因素