CC 标准与 CC 认证简介

一、标准简介

1. 背景

1.1 CC 标准的发展
1.2 CC 标准的意义
1.3 CC 标准的局限性

2. CC 标准内容简介

2.1 CC 第 1 部分
2.2 CC 第 2 部分
2.3 CC 第 3 部分

二、CC 认证简介

1. CC 认证简介

1.1 第三方权威机构；
1.2 认证的主要活动：编制和修订认证文档；TOE 样品测试；现场审查。
1.3 认证的过程

2. CC 认证文档

2.1 PP 理解
2.2 ST 理解
2.3 文档编写的有关注意事项

一、标准简介

1. 背景

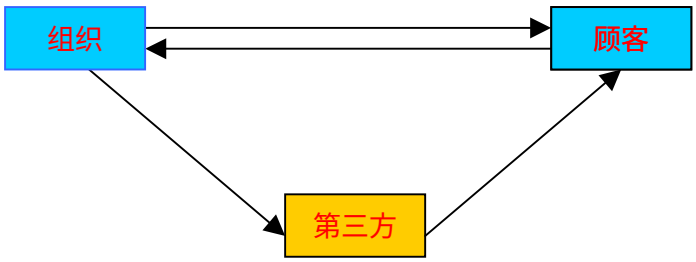
1.1 CC 标准的发展

1.1.1 背景

随着信息技术的快速发展，信息技术的应用日益渗透到政府、企业、团体、军队、家庭、个人等社会和经济的各个角落，并日益深刻的改变着人们传统的工作模式、商业模式、管理模式和生活模式。

伴随着信息技术的快速发展和全面应用，信息安全的重要性也日益凸现出来。IT 产品和系统拥有的信息资产是能使组织完成其任务的关键资源。因此，人们要求 IT 产品和系统具备充分的安全性来保护 IT 产品和系统内信息资产的保密性、完整性和可用性。

随着技术的飞速发展、社会分工的进一步细化，加剧了组织与顾客之间的信息不对称。许多 IT 用户缺乏判断其 IT 产品和系统的安全性是否恰当的知识、经验和资源，他们并不希望仅仅依赖开发者的声明。用户可借助对 IT 产品和系统的安全分析（即安全评估）来增加他们对其安全措施的信心。由此产生了对于 IT 产品和系统的安全性评估准则的需求。



1.1.2 发展

在整个安全性评估准则的发展历程中，有三个非常重要的里程碑式的标准：TCSEC、ITSEC 和 CC 标准。

1.1.2.1 TCSEC

TCSEC 是“ 可信计算机系统评估准则 ”的英文缩写。

- 是由美国国防部于 1985 年开发的，是彩虹系列丛书之一，即桔皮书；
- 主要用于军事领域，后延用至民用，主要针对保密性而言；
- 重点是通用的操作系统，为了使其评估方法适用于网络，于 1987 年出版了一系列关于可信计算机数据库和可信计算机网络等的指南（俗称彩虹系列）。

我国于 1999 年将其转化为 GB/T17859 《计算机信息系统安全防护等级划分准则》，基本等同 TCSEC。

其主要缺点在于：

1. 主要关注于保密性，不关注可用性和完整性。
2. 强调的是控制用户，没有关注于程序上的、物理上的和人员的安全措施。

3. 并没有关注网络（后续出版的书籍弥补了这一不足）。

1.1.2.2 ITSEC

ITSEC 是信息技术安全性评估准则的英文缩写。

- 1991 年，由西欧四国（英、法、荷、德）联合提出了 ITSEC；
- 比 TCSEC 更宽松，目的是适应各种产品、应用和环境的需要，试图超越 TCSEC；
- 首次提出了 C.I.A 概念；
- 将安全要求分为“ 功能 ”和“ 保证 ”两部分：
  - **功能**：为满足安全要求而采取的一系列技术安全措施；
  - **保证**：确保功能正确实现及有效性的安全措施。

1.1.2.3 CC

CC 是通用准则的英文缩写。

1996 年六国七方签署了《信息技术安全评估通用准则》即 CC1.0。1998 年美国、英国、加拿大、法国和德国共同签署了书面认可协议。后来这一标准称为 CC 标准，即 CC2.0。CC2.0 版于 1999 年成为国际标准 ISO/IEC 15408，我国于 2001 年等同采用为 GB/T 18336。

目前已经有 17 个国家签署了互认协议，即一个 IT 产品在英国通过 CC 评估以后，那么在美国就不需要再进行评估了，反之亦然。目前我国还未加入互认协议。

1.2 CC 标准的意义

CC 的意义在于：

- 通过评估有助于增强用户对于 IT 产品的安全信心；
- 促进 IT 产品和系统的安全性；
- 消除重复的评估。

1.3 CC 标准的局限性

- CC 标准采用半形式化语言，比较难以理解；
- CC 不包括那些与 IT 安全措施没有直接关联的、属于行政性管理安全措施的评估准则，即该标准并不关注于组织、人员、环境、设备、网络等方面的具体的安全措施；
- CC 重点关注人为的威胁，对于其他威胁源并没有考虑；
- 并不针对 IT 安全性的物理方面的评估（如电磁干扰）；
- CC 并不涉及评估方法学；
- CC 不包括密码算法固有质量的评估。

2. CC 标准内容简介

2.1 CC 标准的第 1 部分

介绍了 CC 标准中的一般性概念、相关的背景知识并引入了几个安全模型。CC 标准的第 1 部分的掌握程度对于标准的后续部分的理解至关重要。

2.1.1 CC 标准的内容梗概

1. 范围
2. 引用标准
3. 定义
   - 通用缩略语、术语表的范围、术语表
4. 概述
   - 引言、CC 的目标读者、评估上下文、CC 的文档组织
5. 一般模型
   - 安全上下文、CC 方法、安全概念、CC 描述材料、评估类型、保证的维护
6. 通用准则要求和评估结果
   - 引言、PP 和 ST 要求、TOE 内的要求、评估结果的声明、TOE 评估结果的应用

附录 A：通用准则项目

附录 B：PP 规范

附录 C：ST 规范

2.1.2 安全模型（注意与 13335 中的相应图表的区别）

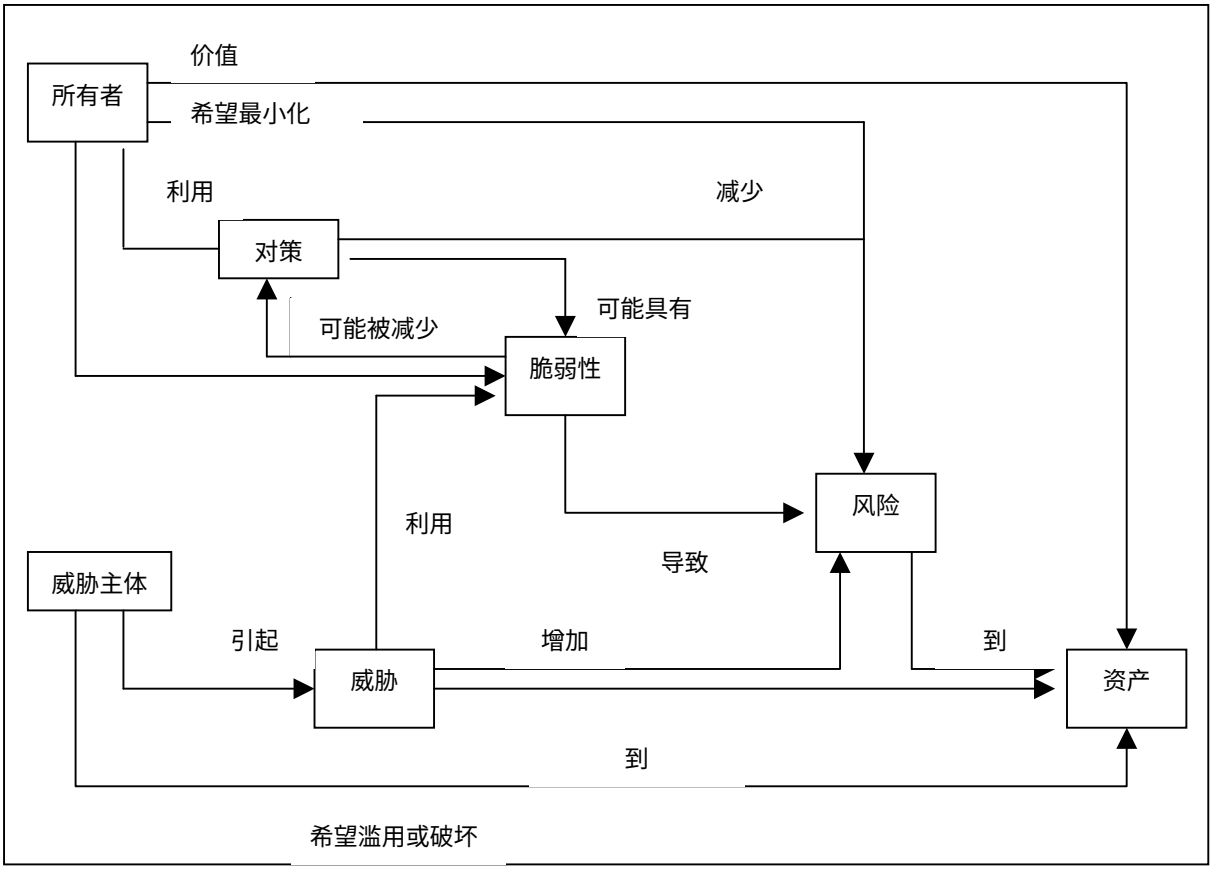


图 3 安全概念和关系

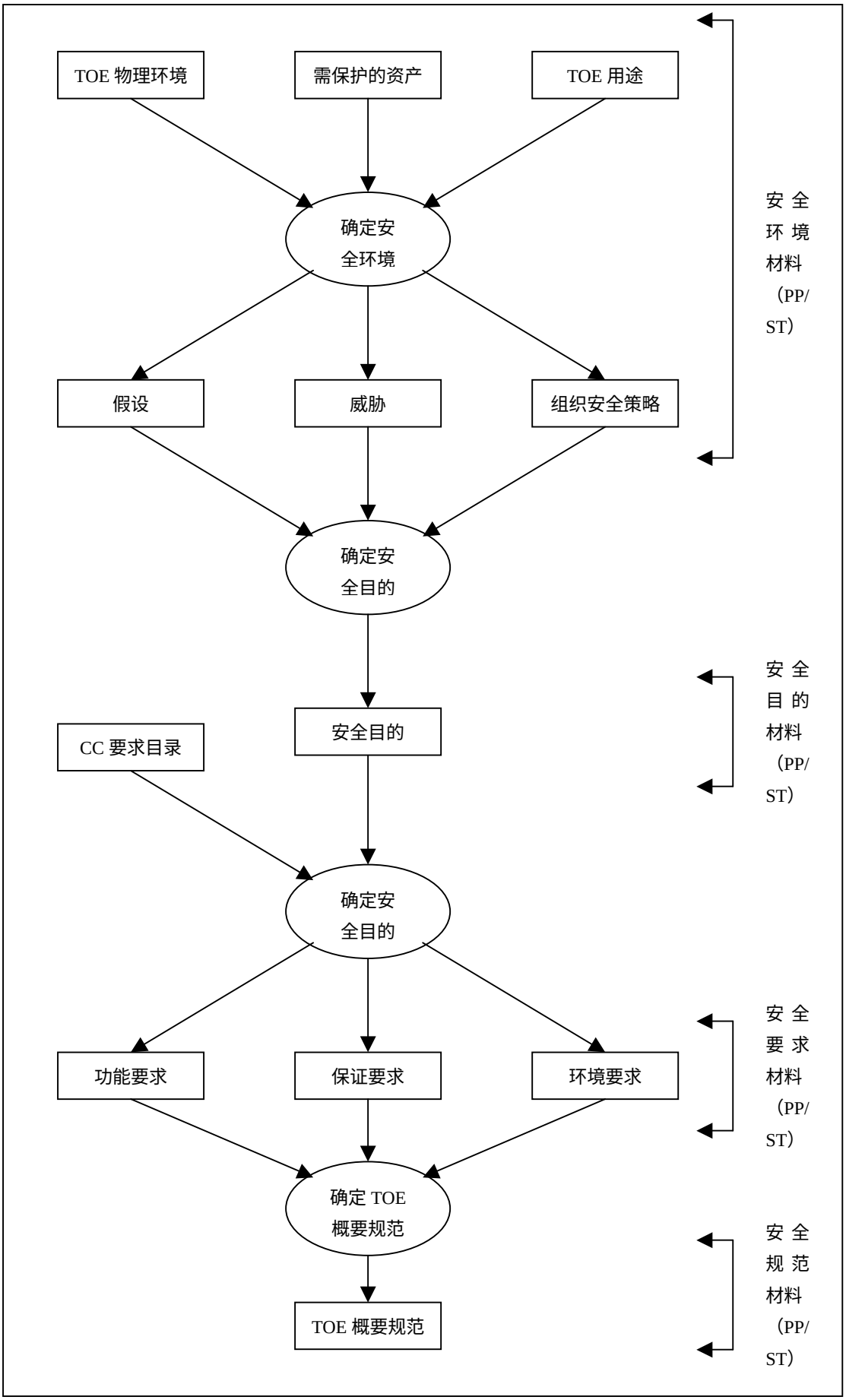

TOE 物理环境
需保护的资产
TOE 用途
确定安全环境
假设
威胁
组织安全策略
确定安全目的
安全目的
CC 要求目录
确定安全目的
功能要求
保证要求
环境要求
确定 TOE 概要规范
TOE 概要规范
安全环境材料（PP/ST）
安全目的材料（PP/ST）
安全要求材料（PP/ST）
安全规范材料（PP/ST）

图 4 要求和规范的导出

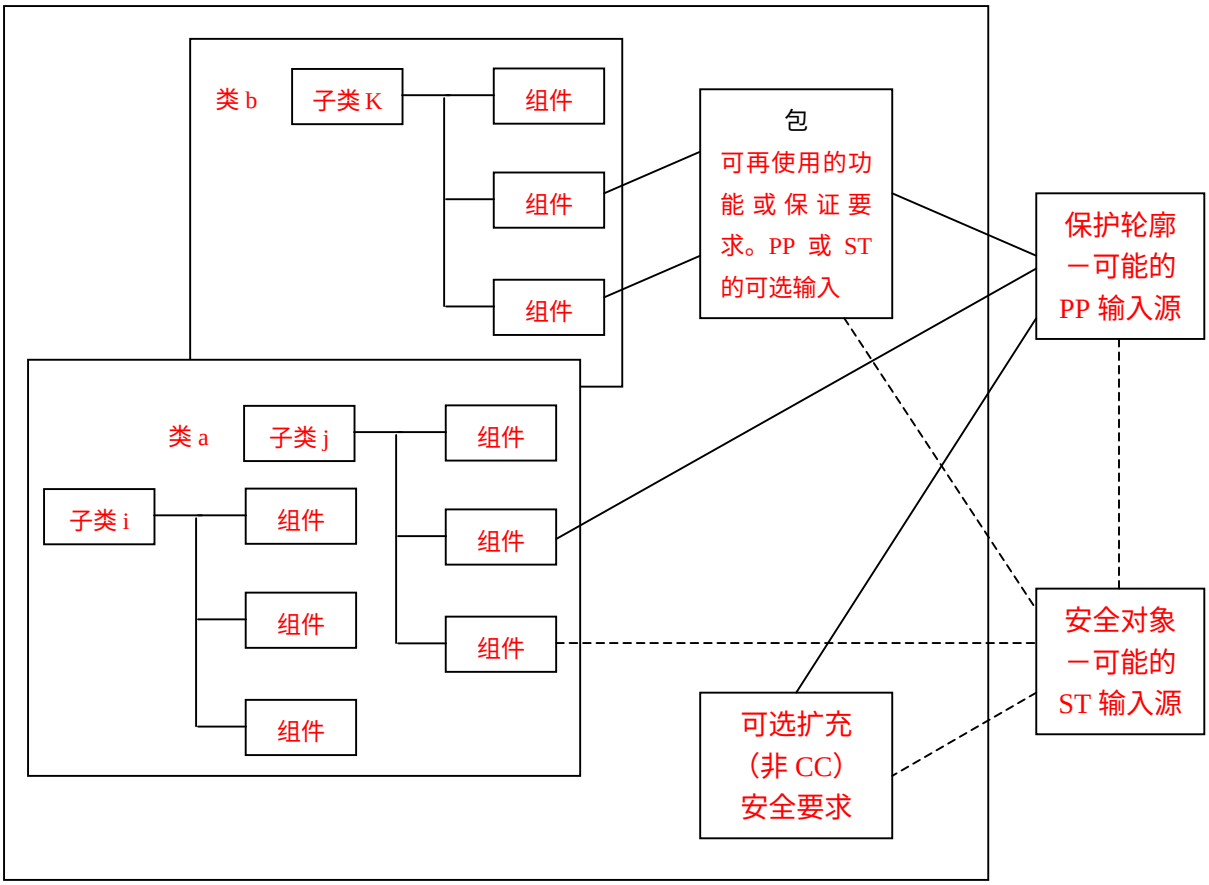
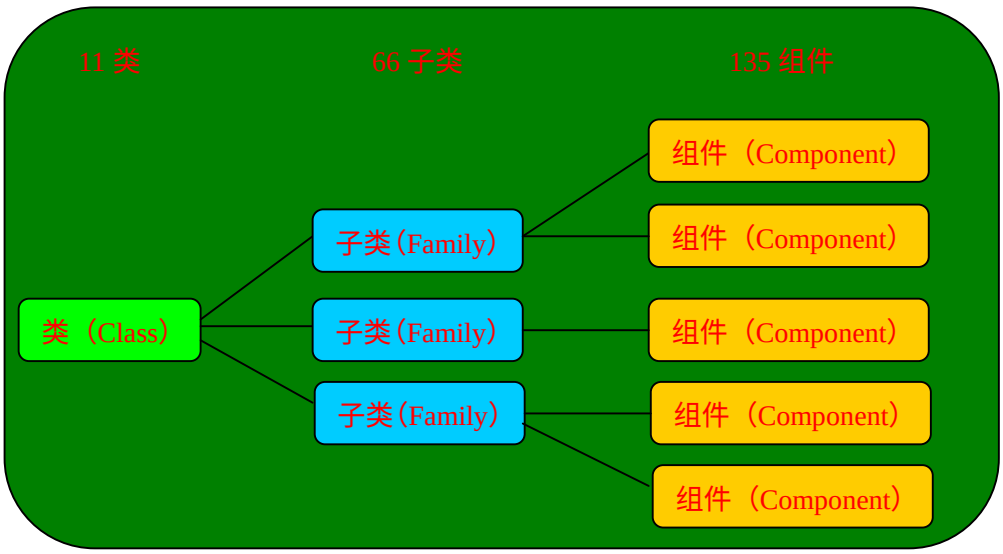


图 5　要求的组织和结构

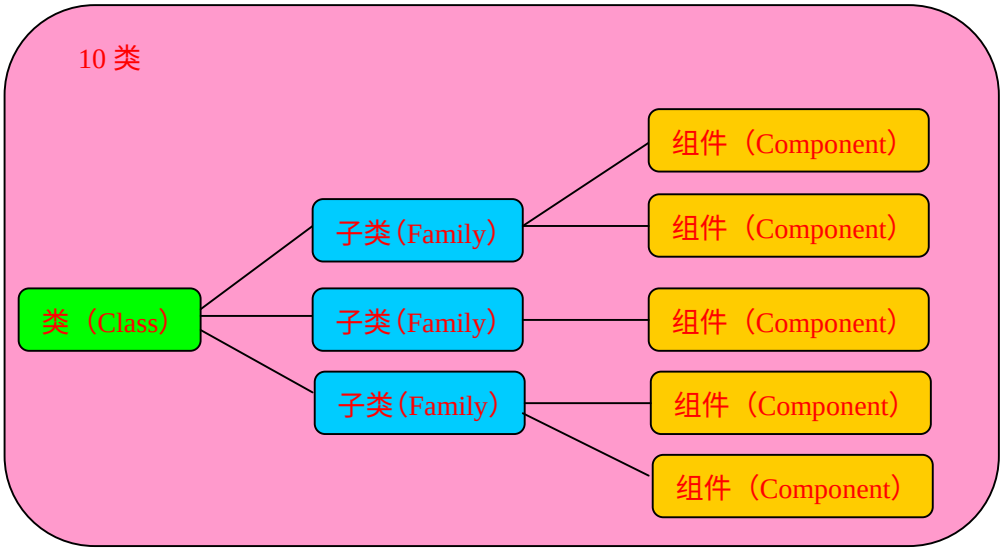
2.2 CC 标准的第 2 部分

第二部分定义了 CC 的安全功能要求。安全功能要求分为 11 类包括：审计（FAU）、密码支持（FCS）、通信（FCO）、用户数据保护（FDP）、识别和鉴权（FIA）、安全管理（FMT）、隐私（FPR）、TSF 保护（FPT）、资源利用（FRU）、TOE 访问（FTA）和可信路径/通道（FTP）。



2.3 CC 的第 3 部分

定义了 CC 的安全保证要求。安全保证要求分为 10 类，保护轮廓评估（APE）、安全目标评估（ASE）、配置管理（ACM）、交付和运行（ADO）、开发（ADV）、指导性文档（AGD）、生命周期支持（ALC）、测试（ATE）、脆弱性评估（AVA）和保障维护（AMA）。



1. CC 认证简介

1.1 第三方权威机构；

为了确保认证过程的公正、公开，目前国家的认证认可机构为中国国家信息安全产品测评认证中心。预计于 2005 年，国际认证认可监督委员会将认证权上收，中国国家信息安全产品测评认证中心将仅仅履行评估和测评任务。

1.2 认证的主要活动

- 编制和修订认证文档：

  认证活动中最主要的一项工作就是提交并修订各类认证文档。认证文档所需的文档会根据所申请的 EAL 级别的不同而略有不同。但是一些常见的文档，如，功能规范、高层设计、低层设计等文档还是需要的。

- TOE 样品测试

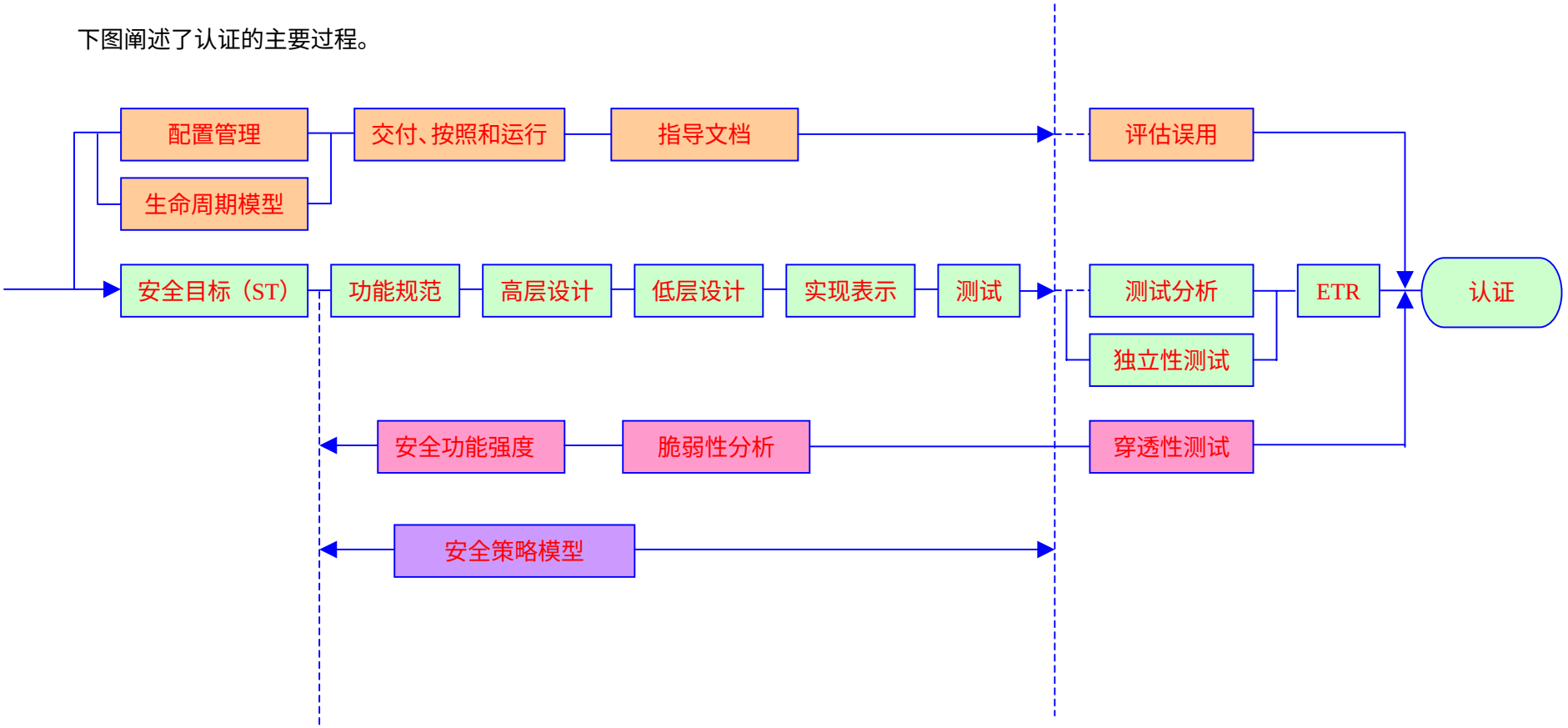
  TOE 的样品测试也需要较长的时间。测试的依据就是提交的各类文档。

- 现场审查。

  通过查阅文件和记录、现场观察和询问等方式进行现场审核。

1.3 认证的过程

下图阐述了认证的主要过程。



2. CC 认证文档

2.1 PP 理解

－PP ：An implementation-independent set of security requirements for a category of TOEs that meet specific consumer need.

－满足特定用户需求、与一类 TOE 实现无关的一组安全要求。

其含义可以理解为：

- ✧ 为既定的一类产品和系统提出安全功能和保证要求的完备的组合，表达了一类产品和系统的用户要求；
- ✧ PP 与某个具体的 TOE 无关，它定义的是用户对这类 TOE 的安全要求；
- ✧ 主要内容包括：需要保护的对象；确定安全环境；TOE 的安全目的；IT 安全要求；基本原理；
- ✧ 在标准体系中 PP 相当于产品标准，也有助于过程规范性标准的开发；
- ✧ 国内外已经对应用级防火墙、包过滤防火墙、智能卡、IDS、PKI 等开发了相应的 PP。

其内容见下图：

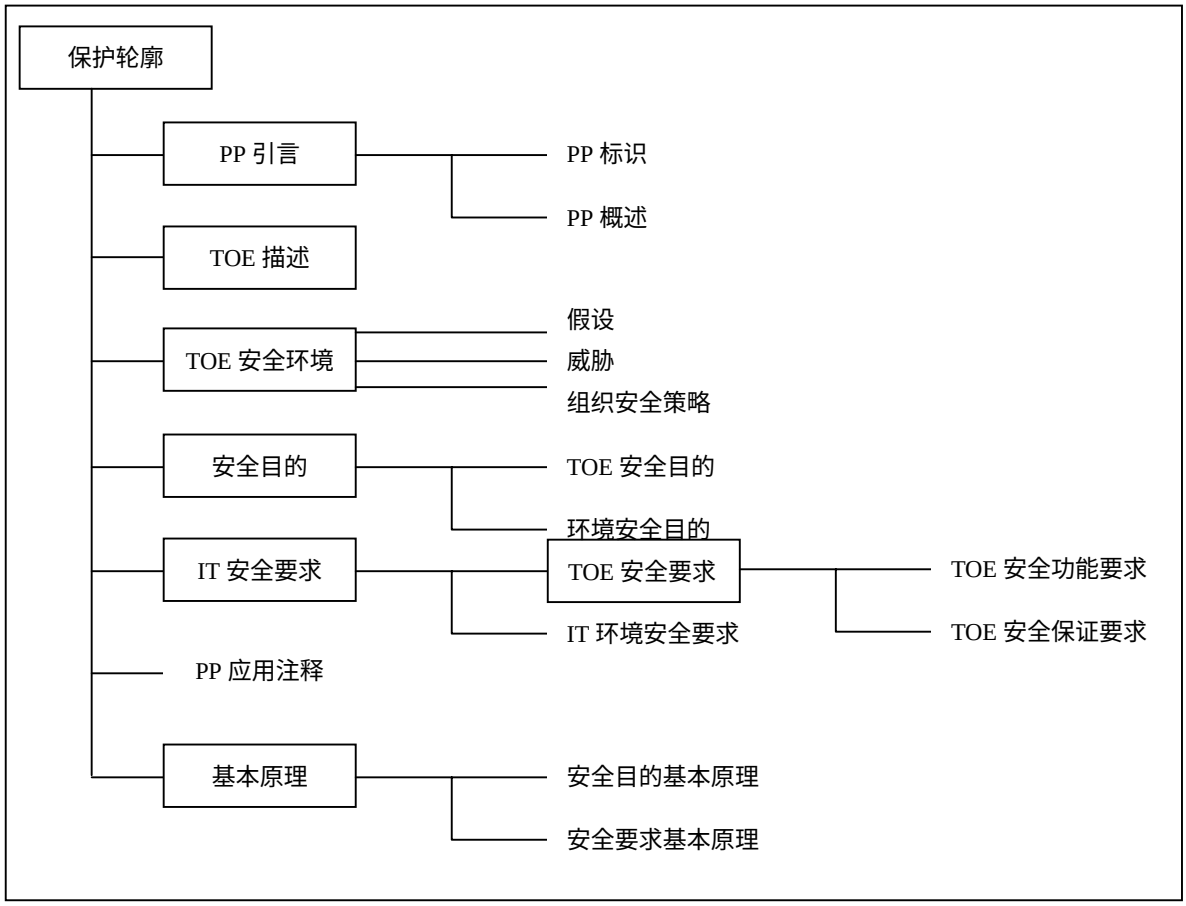


图 保护轮廓内容

PP 内容简述

注：该 PP 内容简述只是针对一般性 PP 而言，具体的 PP 可能会对内容略有变更。为了便于理解，增加了目前国内某一类 TOE 的 PP 作为索引。

<table>
<tr><th>项目</th><th>内容</th><th>对应的索引内容</th></tr>
<tr><td>1. PP 引言</td><td></td><td></td></tr>
<tr><td>1.1 PP 标识</td><td>标识 PP</td><td rowspan="2">1.1 范围
1.2. 引用标准
1.3 术语和定义</td></tr>
<tr><td>1.2 PP 概述</td><td>叙述性概括 PP</td></tr>
<tr><td>2. TOE 描述</td><td></td><td></td></tr>
<tr><td>2.1 TOE 描述</td><td>概述 TOE</td><td>2.1 TOE 概述
2.2 其他方面的概述</td></tr>
<tr><td>3. TOE 安全环境</td><td></td><td></td></tr>
<tr><td>3.1 假设</td><td>描述环境的安全问题</td><td rowspan="3">3.1 资产：
资产包括 TOE 本身所涉及的资产，也包括 TOE 被预期用来保护的资产
3.2 假设 ：
从多个方面阐述存在于 TOE 的使用环境中的特定条件。
3.3 威胁
3.3.1 对 TOE 的威胁
3.3.1.1 在使用环境中对 TOE 的威胁
3.3.1.1.1 对 TOE 的物理攻击威胁
3.3.1.1.2 对 TOE 的逻辑攻击威胁
3.3.1.1.3 与不充分说明相关的威胁
3.3.1.1.4 与不可预测的相互作用相关的威胁
3.3.1.1.5 有关密码功能的威胁
3.3.1.1.6 监视信息的威胁
3.3.1.1.7 其他各种威胁
3.3.1.2 在使用环境中对 TOE 的威胁
3.3.1.2.1 与信息泄漏相关的威胁
3.3.1.2.2 对象窃取相关的威胁
3.3.1.2.3 与信息修改相关的威胁
3.3.2 对 TOE 使用环境的威胁
3.4 组织安全策略</td></tr>
<tr><td>3.2 威胁</td><td>描述对资产的威胁</td></tr>
<tr><td>3.3 组织安全策略</td><td>TOE 必须遵守的组织安全策略</td></tr>
<tr><td>4. 安全目的</td><td></td><td></td></tr>
<tr><td>4.1 TOE 安全目的</td><td>说明 TOE 安全目的</td><td rowspan="2">4.1 TOE 安全目的
4.2 环境安全目的</td></tr>
<tr><td>4.2 环境安全目的</td><td>说明环境安全目的</td></tr>
</table>

项目	内容	对应的索引内容
5. IT 安全要求		
5.1 TOE 安全要求 5.1.1 TOE 安全功能要求 5.1.2 TOE 安全保证要求	陈述安全要求，包括功能和保证安全要求； 从 GB/T18336 的第 2 部分中提取适当的功能组件； 从 GB/T18336 的第 3 部分中提取适当的保证组件。	5.1 信息技术安全要求 5.1.1 信息技术的安全功能要求 列出从 GB/T18336 的第 2 部分中提取的适当的功能组件，并予以解释 5.1.2 信息技术的安全保证要求 列出从 GB/T18336 的第 3 部分中提取的适当的保证组件，并予以解释 5.2 信息技术环境安全要求 列出了应用到信息技术环境中的安全功能组件，并予以解释。
5.2 IT 环境安全要求	陈述 IT 环境安全要求	
6. PP 应用注释		
6.1 PP 应用注释	额外的支持信息	6.1 TOE 的特点 6.2 安全功能管理
7. 基本原理		
7.1 安全目的基本原理	阐明安全目的可追溯到在 TOE 安全环境里指明的所有方面，并且能够覆盖所有方面	7.1 安全目的基本原理： TOE 的安全目的能够对付所有可能的威胁、假设和组织的安全策略，即每一种威胁、假设和组织的安全策略都至少有一个或一个以上的安全目的与之对应，因此是**完备**的； 没有一个安全目的没有相应的威胁、假设和组织安全策略与之对应，这证明每一个安全目的都是**必要**的； 没有多余的安全目的不对应威胁、假设和组织的安全策略，因此说明了安全目的是**充分**的。 7.2 安全要求基本原理 说明了安全要求的充分必要性基本原理，即每一个安全目的都至少有一个安全要求（包括功能要求或保证要求）组件与其对应，每一个安全要求都至少解决了一个安全目的，因此，安全保证要求对安全目的而言是充分和必要的。 7.3 满足依赖关系的基本原理 在选取安全要求组件时，必须满足所选组件之间的相互依赖关系，列出所选安全功能要求组件和安全保证要求组件之间的依赖关系。
7.2 安全要求基本原理	阐明系列安全环境的功能和保证要求组件相结合，能满足所述的安全目的	

2.2 ST 理解

－作为指定的 TOE 评估基础的一组安全要求和规范。

－ST：A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

其含义包括：

✧ ST 是针对具体 TOE 而言，它包括该 TOE 的安全要求和用于满足安全要求的特定安全功能和保证措施。

✧ ST 包含的技术要求和保证措施可以直接引用该 TOE 所属产品和系统类的 PP；

✧ ST 是开发者、评估者和用户在 TOE 安全性和评估范围之间达成一致的基础；

✧ ST 相当于是产品和系统的实现方案。

其具体内容见下图：

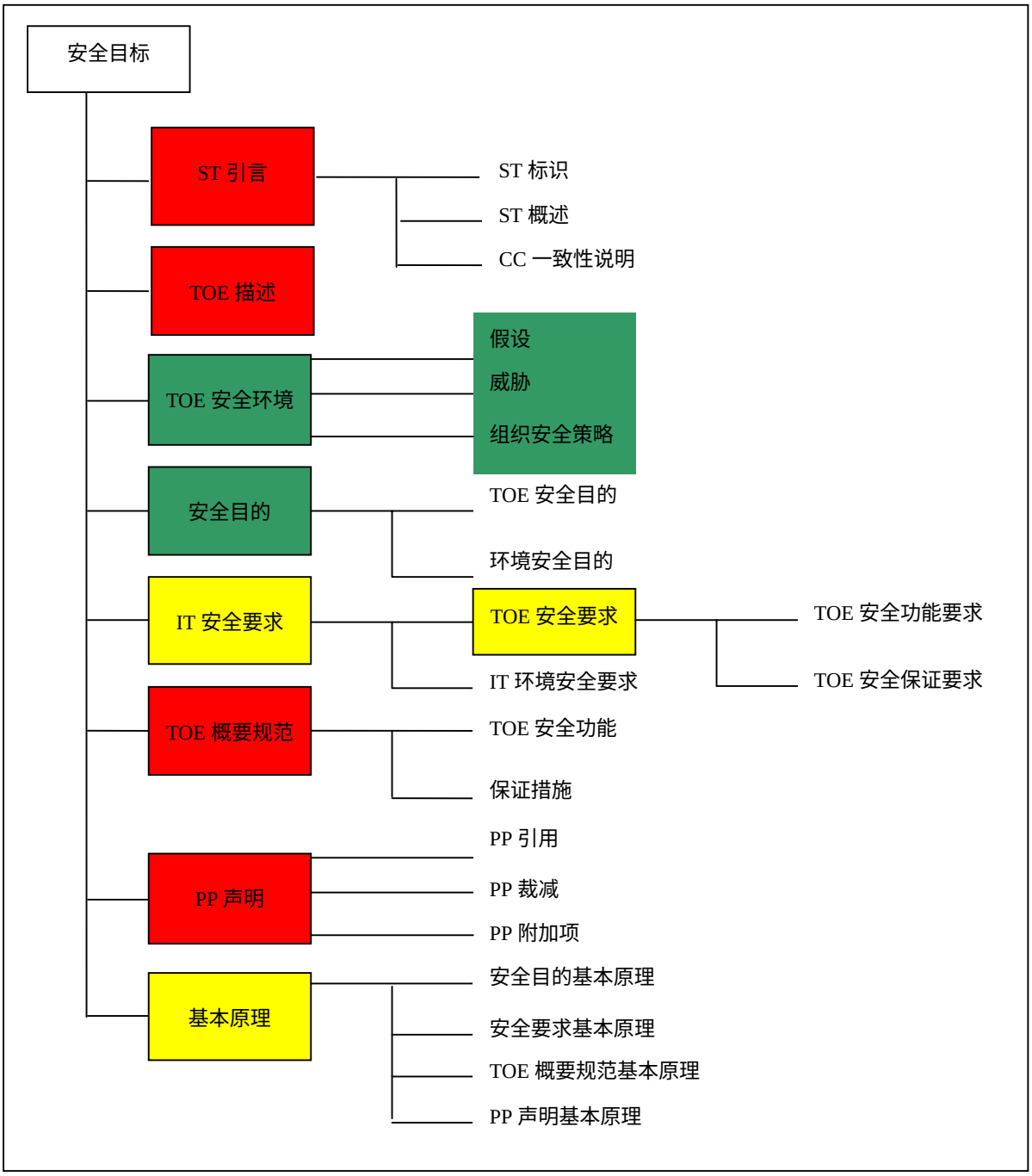


图 2 安全目标内容

1. ST 引言

1.1 ST 和 TOE 标识

1.1.1 ST 标识：

ST 标题：

版本号：

编制日期：

校对日期：

审核日期：

批准日期：

1.1.2 TOE 标识：

TOE 名称：

其他相关信息

1.2 ST 概述：对 ST 文档的概要描述。

本 ST 是 TOE 的安全目标，描述了 TOE 的系统结构、物理以及逻辑的范围和边界，分析了 TOE 预期用法和使用环境，标识并解释了已知的或假定的对于 TOE 及其环境保护的资产的威胁和必须遵循的组织安全策略。为了达到针对 TOE 及其环境所定义的安全目的，提出了一组安全要求，包括 TOE 安全功能要求和安全保证要求，以及 IT 环境安全要求。在概要规范中描述了 TOE 提供的安全功能和实现安全功能的保证措施。本文最后阐述了 TOE 的安全环境、安全目的、安全要求和安全功能之间相互对应的的基本原理，从而证明满足本 ST 陈述的 TOE 提供的安全功能和保证措施是 PP 中确定的完整的、紧密结合的安全要求集合的实现。保证措施与 PP 中的 EALX 级的要求相一致。

1.3 CC 一致性声明

a) TOE 符合 GB/T 18336.1-2001《信息技术 安全技术 信息技术安全性评估准则 第 1 部分：简介和一般模型》的一般模型的要求。

b) TOE 的安全功能要求子集遵循 GB/T 18336.2-2001 《信息技术 安全技术 信息技术安全性评估准则 第 2 部分：安全功能要求》。

c) TOE 在安全保证要求上符合 GB/T 18336.3-2001 《信息技术 安全技术 信息技术安全性评估准则 第 3 部分：安全保证要求》中的安全评估保证 X 级的要求。

d) TOE 与 PP 是一致的。

1.4 术语和缩略语定义

2. TOE 描述

2.1 概述

2.1.1 TOE 概述

2.1.2 TOE 应用环境

2.2 TOE 的范围和边界

2.2.1 物理范围和边界

2.2.2 逻辑范围和边界

2.3 应用环境：TOE 应用环境的概要描述。

2.4 TOE 的生命周期

2.4.1 TOE 的生命周期

2.4.2 TOE 的各个生命周期所涉及的角色

3.TOE 安全环境（基本可以完全引用 PP）

3.1 资产

3.2 TOE 预期使用环境的假设

3.3 TOE 可能遭受的威胁

3.3.1 对 TOE 的威胁
3.3.2 对 TOE 使用环境的威胁
3.4 组织安全策略
4. 安全目的（基本可以完全引用 PP）
4.1 TOE 的安全目的
4.2 环境安全目的
5. IT 安全要求
5.1 TOE 安全要求
5.1.1 TOE 安全功能要求（框架与 PP 一致，需要根据组织的实际情况予以确定各个参数）
5.1.2 TOE 安全保证要求（框架与 PP 一致，需要根据组织的实际情况予以补充完善）
5.2 IT 环境安全要求（与 PP 基本一致）
6．TOE 概要规范
6.1 TOE 安全功能
6.2 TOE 安全功能要求的实现（即对 TOE 安全功能的解释）
6.3 安全保证措施的实现
6.4 环境安全功能
7. PP 声明：TOE 符合 PP 要求的程度
8. 基本原理（从 PP 而来）
8.1 安全目的基本原理
8.2 安全要求基本原理
8.3 TOE 概要规范基本原理
8.3.1 安全功能基本原理
8.3.2 安全保证要求的基本原理
8.4 满足依赖关系的基本原理

8.1 安全目的基本原理（从 PP 而来）

下面的表 8.1、表 8.2、表 8.3、表 8.4 说明了 TOE 的安全目的能对付所有可能的威胁、假设和组织安全策略，即每一种威胁、假设和组织安全策略都至少有一个或一个以上安全目的与其对应，因此是完备的。没有一个安全目的没有相应的威胁、假设和组织安全策略与之对应，这证明每一个安全目的都是必要的；没有多余的安全目的不对应威胁、假设和组织安全策略，说明了安全目的是充分的。

表 8.1 与目的相关的威胁

威胁	对应的目的

表 8.2 与目的相关的组织安全策略

策略	对应的目的

表 8.3 与目的相关的假设

假设	对应的目的

表 8.4 与环境考虑相关的安全目的

环境	对应的目的

8.2 安全要求基本原理（从 PP 而来）

下面的表 8.5、表 8.6、表 8.7 说明了安全要求的充分必要性基本原理，即每一个安全目的都至少有一个安全要求（包括功能要求或保证要求）组件与其对应，每一个安全要求都至少解决了一个安全目的，因此安全要求对安全目的而言是充分和必要的。

表 8.5 与安全目的相关的安全要求组件

安全目的	对应的安全要求组件

表 8.6 与安全功能要求相关的安全目的

安全功能要求	对应的安全目的

表 8.7 与安全保证要求相关的安全目的

安全保证要求	对应的安全目的

8.3 TOE 概要规范基本原理

8.3.1 安全功能基本原理

下面的表 8.8、表 8.9 说明了 TOE 概要规范安全功能基本原理。即每一个安全功能至少有一个安全功能要求组件与其对应，每一个安全功能要求至少对应于一个安全功能，因此 TOE 卡实现的安全功能完全满足安全功能的要求。

表 8.8 与安全功能要求相关的安全功能

安全功能要求	安全功能要求名称	对应的安全功能

表 8.9 与安全功能相关的安全功能要求

TOE实现的安全功能	对应的安全功能组件

8.3.2 安全保证要求的基本原理

表 8.10 说明了 TOE 概要规范安全保证基本原理。即每一个安全保证要求组件都至少有一个安全保证措施与其对应，因此 TOE 的安全保证措施完全满足安全保证要求。

表 8.10 与安全保证要求相关的保证措施

保证要求组件	组件名称	保证措施（见下列文档）

8.4 满足依赖关系的基本原理（从 PP 而来）

在选取安全要求组件时，TOE 必须满足所选组件之间的相互依赖关系，表 8.11、表 8.12 分别列出了所选安全功能要求组件和安全保证要求组件的依赖关系。

表 8.11 安全功能组件依赖关系表

功能组件	依赖关系

表 8.12 安全保证组件依赖关系表

保证组件	依赖关系

2.3 关于认证文档编写的有关注意事项

CC 认证非常重要的一份工作就是编制并修订各类文档。在编制和修订文档过程中，应注意以下事项：

1、文档的符合性：符合性包含两个含义，第一，文档要符合 CC 标准的要求；第二，文档要符合实际情况。

2、文档的一致性：一致性也包含两个含义，第一，文档前后之间要保持一致，不能前后矛盾或者前言不搭后语；第二，文档与文档之间要保持一致，不能出现互相矛盾的现象。

3、文档的详细性：认证的文档要求详细到能够让评估者和 TOE 的用户清晰理解的程度，因为提交文档的目标读者是认证中心的评估人员和 TOE 用户而不是相关领域的专家学者，他们通常不具备相关领域的专业知识和技能，因此要求在编制文档时要保证文档的详细和易懂。

《功能规范》：功能规范是《ST 文档》中**概要规范**的精确和完备的实例化。其主要内容包括两个部分：一，以 UIM 卡安全功能为主线，注重安全机制的介绍；二，标识外部接口（如，所有详细的命令信息）。功能规范部分内容（如命令解释、命令意义）需要进行补充完善。

《高层设计》：高层设计是**《功能规范》**的精确和完备的实例化。其主要内容包括两个部分：一，以子系统的方式来描述安全功能；二，标识子系统的接口（尤其是外部接口）

《低层设计》：低层设计是高层设计的精确和完备的实例化。其主要内容包括两个部分：一，以模块的形式描述安全功能；二，标识模块接口。

《配置管理计划》的主要内容是：如何使用 CM 系统来保存 TOE 每个配置项的完整性。

《配置项清单》的主要内容是：阐述 TOE 所有配置项的标识。

《接受计划》的主要内容是：新创建的或修订后的配置项是如何被 CM 系统接受的。

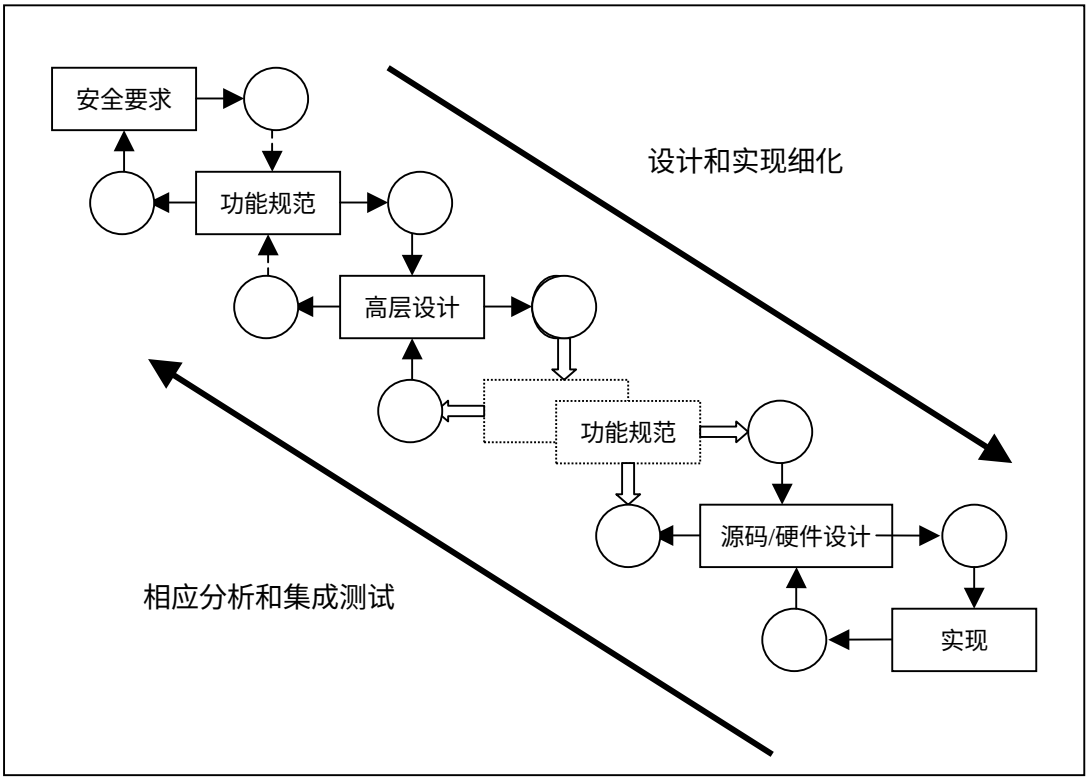


图 评估对象开发模型

2.3 功能规范
2.4 高层设计
2.5 低层设计
2.6 其他文档（交付运行、CM 文档、安装生成和启动文档、生命周期支持文档等）