ISCCC-QOG-0310-B/0

# EAL1-EAL5 级 ST 文档编写指南


**中国信息安全认证中心 制**

发布日期：二〇一七年八月十四日

# 目 录

**适用范围** ..... **1**

**术语和定义** ..... **1**

**缩略语** ..... **1**

**第一部分：EAL1 级 ST 文档编写指南** ..... **2**

1. ST 引言 ..... 3
   1.1. ST 参照号和 TOE 参照号 ..... 3
   1.2. TOE 概述 ..... 4
   1.3. TOE 描述 ..... 4
2. 符合性声明 ..... 5
   2.1. 国家标准符合性声明 ..... 5
   2.2. 评估保障级声明 ..... 5
   2.3. STR 声明 ..... 5
   2.4. 符合性基本原理 ..... 5
3. 缩略语、术语和定义 ..... 6
4. 安全目的 ..... 6
   4.1. 运行环境安全目的 ..... 6
5. 扩展组件定义 ..... 7
6. 安全要求 ..... 8
   6.1. SFR ..... 9
   6.2. SAR ..... 12
   6.3. 安全要求基本原理 ..... 14
7. TOE 概要规范 ..... 14

**第二部分：EAL2-EAL5 级 ST 文档编写指南** ..... **15**

1. ST 引言 ..... 16
   1.1. ST 参照号和 TOE 参照号 ..... 16
   1.2. TOE 概述 ..... 17
   1.3. TOE 描述 ..... 17
2. 符合性声明 ..... 18
   2.1. 国家标准符合性声明 ..... 18
   2.2. 评估保障级声明 ..... 18
   2.3. STR 声明 ..... 18
   2.4. 符合性基本原理 ..... 18
3. 缩略语、术语和定义 ..... 19
4. 安全问题定义 ..... 19
   4.1. 威胁 ..... 20
      7.3.1. 主体 ..... 20
      7.3.2. 资产 ..... 20
      7.3.3. 威胁行为 ..... 20
   4.2. 组织安全策略 ..... 21
   4.3. 假设 ..... 21

5. 安全目的 ..... 22
5.1. TOE 安全目的 ..... 23
5.2. 运行环境安全目的 ..... 25
5.3. 安全目的基本原理 ..... 27
6. 扩展组件定义 ..... 27
7. 安全要求 ..... 27
7.1. SFR ..... 28
7.2. SAR ..... 32
7.3. 安全要求基本原理 ..... 33
7.3.1. 安全要求基本原理分析 ..... 33
7.3.2. 依赖性分析 ..... 34
8. TOE 概要规范 ..... 34

# 适用范围

安全目标（ST）文档用于描述一个既定评估对象（TOE）的 IT 安全要求，并描述 TOE 为满足相关安全要求应提供的安全功能和保障措施，是评估保障级分级评估、认证的基础。

本文件依据 GB/T 18336-2015《信息技术 安全技术 信息技术安全评估准则》，概述了 ST 文档的强制性内容，可作为编制相关安全目标文档的参考。

# 术语和定义

GB/T 18336.1 确立的术语、定义适用于本指南性技术文件。

# 缩略语

| | | |
|---|---|---|
| STR | Security Technology Requirement | 安全技术要求，对应 GB/T 18336 标准中的保护轮廓。 |
| EAL | Evaluation Assurance Level | 评估保障级 |
| ST | Security Target | 安全目标 |
| TOE | Target of Evaluation | 评估对象 |
| SFR | Security Functions Requirement | 安全功能要求 |
| SAR | Security Assurance Requirement | 安全保障要求 |
| TSF | TOE Security Functions | TOE 安全功能 |
| IT | Information Technology | 信息技术 |
| OSP | Organizational Security Policy | 组织安全策略 |

# 第一部分：EAL1 级 ST 文档编写指南

EAL1 级是评估保障级分级中最低的一级，用于 EAL1 级评估的 ST 文档称为低保障级 ST 文档。

低保障级 ST 文档应包括如下内容：

a） ST 引言：用于描述 ST 和相关 TOE 的标识和必要的描述信息；

b） 符合性声明：用于说明 ST 与 GB/T 18336、评估保障级（EAL）和安全技术要求（STR）的符合性；

c） 安全目的：用于描述 TOE 的运行环境安全目的；

d） 扩展组件定义（可选）：用于定义新组件（即在 GB/T 18336.2 和 GB/T 18336.3 中不包含的组件），这些新组件用于定义扩展功能要求和扩展保障要求；

e） 安全要求：用于将 TOE 安全目的转化成组件形式表示的 TOE 安全要求标准语言形式，包括安全功能要求和安全保障要求以及安全要求基本原理；

f） TOE 概要规范：用于描述 TOE 提供的安全功能及其实现安全功能要求的机制；

g） 缩略语、术语和定义：用于描述 ST 文档中使用的缩略语、技术术语和定义。

EAL1 级 ST 的基本结构图如下图所示：

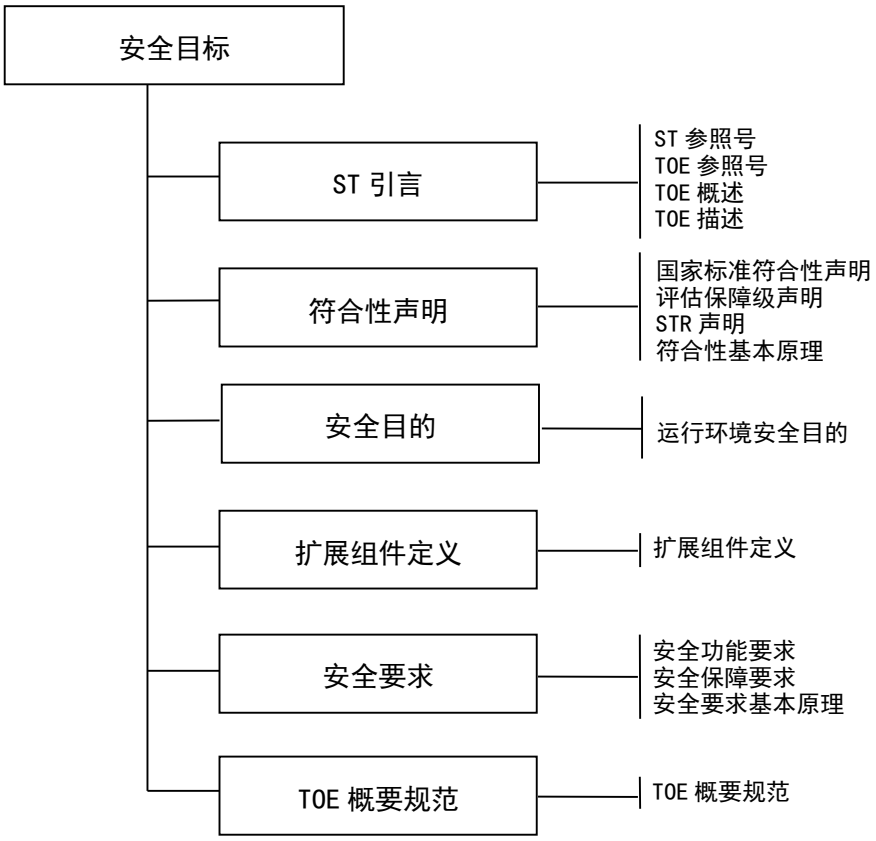


图 1-1 EAL1 级 ST 基本结构图

# 1. ST 引言

ST 引言应描述 ST 和 TOE 的标识性信息，以及与评估相关的 TOE 关键信息。

## 1.1. ST 参照号和 TOE 参照号

应在本部分描述 ST 参照号和 TOE 参照号。

1）ST 参照号，是唯一标识 ST 的标识性信息。一个典型的 ST 参照号由 ST 标题、版本号、编写日期和作者组成；

2）TOE 参照号，是用来标识与 ST 对应的 TOE。一个典型的 TOE 参照号由 TOE 名称、TOE 版本号和开发者名称组成。

## 1.2. TOE 概述

TOE 概述应简单描述 TOE 的用途和其重要安全特征、TOE 类型和 TOE 运行环境的配置信息（TOE 依赖的、非 TOE 的硬件、软件或固件）。

TOE 概述是面向潜在消费者的信息，应通过描述使消费者了解 TOE 的安全能力和用途，帮助消费者快速确定 TOE 是否能够满足他们的安全需求，是否为他们的现有资源所支持。

1）TOE 用途和重要安全特征示例：

某数据库 V2.11 是一个用于网络环境的多用户数据库，它允许 1024 个用户同时活动，允许口令/令牌和生物识别认证，提供意外数据故障保护，能够回滚 1 万个事务，其审计特征可配置程度高，以便允许对某些用户和事务执行详细审计，同时保护其他用户和事务的隐私。

2）TOE 一般类型示例：

防火墙、VPN 防火墙、智能卡、加密调制解调器、企业网、WEB 服务器、数据库、WEB 服务器和数据库、LAN、包含 WEB 服务器和数据库的 LAN 等。

3）TOE 运行环境配置示例：

- 标准 PC，处理器 1GHz 以上，内存 512MB 以上，某操作系统运行版本 3.0，更新版本 6d，带 1.0 WM 驱动套件的某图形卡 1.0；
- 智能卡 SB2067 集成电路，运行某智能卡操作系统 V2.0；
- 某局域网。

## 1.3. TOE 描述

TOE 描述是面向评估者和潜在消费者提供的信息，应描述 TOE 的物理范围和逻辑范围。还应该提供 TOE 应用环境等与 TOE 安全评估相关的背景信息，使读者能够对 TOE 安全能力有一般性理解。TOE 描述应比 TOE 概述中的描述详细。

1）TOE 物理范围

TOE 物理范围是指构成 TOE 的硬件、固件、软件及指南的所有部分，描述 TOE 物理范围时可采用结构图或列表等形式描述 TOE 的所有构成部分，并对图表中的每一项进行详细解释，同时应界定出物理评估边界，即哪些部分在评估范围之内，哪些部分在评估范围之外。

2）TOE 逻辑范围

TOE逻辑范围是指TOE提供的安全能力。在描述TOE的逻辑范围时应列出TOE提供的所有安全特征，并逐项进行详细描述。同时应界定出逻辑评估边界，即哪些安全特征在评估范围之内，哪些安全特征在评估范围之外。

# 2. 符合性声明

符合性声明用于描述ST和TOE对GB/T 18336的符合情况，以及ST对安全技术要求（STR）和评估保障级（EAL）的符合情况。

## 2.1. 国家标准符合性声明

应描述ST和TOE声明遵从的GB/T 18336的版本、ST与GB/T 18336.2的符合或扩展、ST与GB/T 18336.3的符合或扩展。

## 2.2. 评估保障级声明

应列出ST声明遵从的评估保障级级别，描述ST与评估保障级级别的符合或增强。

## 2.3. STR 声明

应列出ST声明遵从的所有STR的名称和版本。对每一个STR描述符合的方式是严格的还是可论证的。

## 2.4. 符合性基本原理

如果符合的方式是“可论证的”，则应证实ST中描述的TOE类型与符合性声明中STR定义的TOE类型是一致的，应证实ST中描述的安全问题定义、安全目的、安全要求与符合性声明中的STR中的相关陈述是一致的或者是STR中相应集合的超集。如果符合的方式是“严格的”，此处仅声明本ST严格符合对应STR。

# 3. 缩略语、术语和定义

应在本部分描述 ST 文档中使用的缩略语、技术术语和定义。

# 4. 安全目的

## 4.1. 运行环境安全目的

应在本部分描述所有运行环境安全目的。

环境安全目的包含由 IT 环境实现的技术措施或非技术措施满足的安全目的。换言之，环境安全目的包括 IT 环境安全目的和非 IT 环境安全目的。

TOE 不处理或不能处理的安全问题的环境安全目的必须被标识出来，下列环境安全目的通常是必需的：

a）用于对抗不是由 TOE 对抗的威胁的安全目的；

b）用于帮助满足那些不能由 TOE 满足的 OSP 的安全目的；

c）用于支持已标识的 TOE 安全目的去对抗威胁或满足 OSP 的安全目的；

d）用于确保满足已标识的环境假设。

识别环境安全目的可以首先通过依次对照每个未被 TOE 完全处理的威胁、OSP 和假设，编辑出一个安全目的的清单，然后对 TOE 安全环境中的每个项目作以下两步处理：

a）在清单中增加可以覆盖该项目的一个新的安全目的，或者映射一个已有的合适的安全目的到该项目，必要的时候可以修改已有的安全目的；

b）当构成安全目的基本原理时，应精练这个清单，因为这个过程可能识别出额外的安全目的，需要确保安全目的是作为整体来对抗威胁或满足 OSP 和假设的。

运行环境安全目的和 TOE 安全目的的识别过程是相互联系的。识别 TOE 及运行环境分别对应的安全需求以确定评估边界，划分责任。二者的内容构成了安全目的的整体。

（非 IT）环境安全目的的典型实例包括：

a）建立和采取适当流程，保证以安全方式使用 TOE（应与环境假设协调一致）；

b）在恰当的安全实践中，教育和培训管理员及用户类安全目的。

因此，环境安全目的陈述应包括所有与管理活动有关的目的，需要以这些活动来保证 TOE 提供有效的安全服务。某些情况下要求的管理活动是明显的，很容易以（非 IT）环境安全目的的形式表达，而另一些情况下要求的管理活动依赖于实现 TOE 安全目的的详细要求。例如，“标识与鉴别”有关的安全目的可能通过口令来实现，这意味着要求用户保证不要将自己的口令泄露给其他人，这就要作为非 IT 安全要求来适当表达，而安全要求也是对环境安全目的的提炼。

GB/T 18336 指出，当威胁或 OSP 由 TOE 和其环境部分覆盖时，不同的类别中将重复出现相关联的安全目的。对上面安全目的的识别过程，这种做法是适当的，因为，有的威胁只能在环境管理活动支持下由 TOE 来对抗。如：鉴别数据（口令）管理，该安全目的可以如下陈述：

受环境支持的 TOE 将保证用户在获准访问 TOE 之前唯一地标识每个用户，用户所声称身份是经鉴别的。

在能够明确划分 TOE 及其环境责任的情况下，不必在一类安全目的中重复另一类的相同内容。比如，对于安全审计目的，TOE 的责任是产生和采集数据，而环境的责任是支持管理活动，即对产生的数据进行分析。

IT 环境安全目的的典型例子是底层操作系统标识和鉴别 TOE 用户。这种对 IT 环境的依赖性将在对环境的 IT 安全要求中详细说明。

与 TOE 安全目的相同，建议环境安全目的使用唯一性标识以便于引用。采用的标识方法应能区别环境的安全目的和 TOE 安全目的。对所描述的环境安全目的应单独命名，唯一标识，建议由“OE.”后跟简短而有意义的英文名称或其缩写构成，以便于记忆和引用，如：OE.AUD_REVIEW、OE.RESIDUAL。

# 5. 扩展组件定义

通常情况下，ST中的安全要求选自GB/T 18336.2和GB/T 18336.3中的组件。但是，在某些情况下，为了满足安全目的，可能需要一些特殊的安全要求，这部分安全要求无法基于GB/T 18336.2和GB/T 18336.3的组件提出，这种情况下，就

需要在本部分自定义新组件，这些组件称为扩展组件。但应尽量避免在ST中定义和使用扩展组件。

定义扩展组件时，应按照GB/T 18336中现有组件的类似定义方式、类似抽象程度和相同结构进行定义。

# 6. 安全要求

在本部分应描述安全要求和安全要求基本原理。

其中安全要求包括两个方面的要求：

a）安全功能要求(SFR)：SFR 应是对 TOE 安全目的的完全转化，用于对 TOE 预期安全行为进行清晰、无歧义且定义准确的描述，SFR 以一个较详细且抽象的形式表述，且独立于任何特定的技术解决方案（实现）。

b）安全保障要求（SAR）：对 TOE 获得保障而采取的预期活动进行清晰、无歧义且规范的描述。

应尽可能使用 GB/T 18336.2 中定义的安全组件和 GB/T 18336.3 中定义的保障组件（如下图），并以组件为单位构建安全要求，即：如果在 ST 中包括某个组件，则组件中所有已定义的元素都应包括进来。

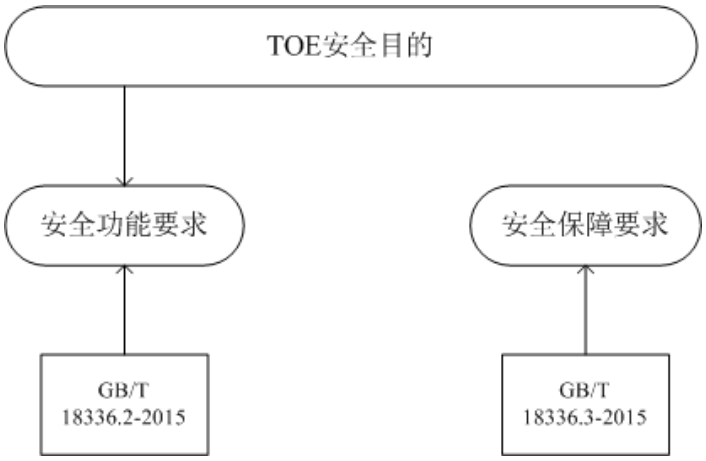


图 1-2 安全目的和安全要求之间的关系

选择安全功能组件描述 SFR 时，需要注意功能组件之间的依赖关系，这表示如果ST使用了某一SFR，那么，它一般也需要使用另外一些其依赖的SFR。因此，对于 ST 的制定，可以通过组件间的依赖关系这一机制来更好的进行功能组件的选取，以便全面包含必要的 SFR 从而提高 ST 的全面性。同时，在引用组件

时，需要遵循反复、赋值、选择、细化等对组件的操作原则。

选择安全保障组件描述 SAR 时，也需要注意保障组件之间的依赖关系，这表示如果ST使用了某一SAR，那么，它一般也需要使用另外一些其依赖的SAR。因此，对于 ST 的制定，可以通过组件的依赖关系这一机制来更好的进行保障组件的选取，以便全面包含必要的 SAR 从而提高 ST 的全面性。

同时，在选择组件时，要注意同一个类不同组件间可能存在的层次关系，即：一个组件包括所在子类内其他组件中规定的全部要求元素。例如，FAU_STG.4 是 FAU_STG.3 的从属组件，因为所有在后者中定义的功能元素都包括在前者之中，因此不可能在同一个 ST 中同时包括这两个组件。

如果 ST 声明了严格符合的 STR，可复制该 STR 文档的安全要求部分的内容作为 ST 文档安全要求的一部分。

## 6.1. SFR

SFR 是 TOE 安全目的的细化和规范表示。应使用 GB/T 18336.2 中或扩展组件定义部分定义的功能组件进行描述。

应该在满足 TOE 安全目的的 TOE 总体安全功能模型的基础上选择 SFR。GB/T 18336.2 中的安全功能范例，提供了开发 SFR 抽象模型的基础，如：

a） 对资源和对象的访问和使用控制：定义相关的主体、客体、操作、安全属性、访问控制规则和相关的管理行为规则等；

b） 用户管理：定义用户类型、安全属性、用户标识和鉴别规则及相关的管理行为规则等；

c） TOE 自我保护：定义故障检测、响应规则及相关的管理行为等；

d） 安全通信：定义相关的连接属性、连接建立规则及相关的管理行为等；

e） 安全审计：定义被审计事件、事件响应、审计规则及相关的管理行为等；

f） 结构化要求：定义和确定满足安全目的所需要的支持性要求和规则，如审计迹保护、密码运算功能、失效安全、安全时间戳等。

为 ST 选择 SFR 的过程分几个阶段，在选择过程中要注意区别以下两种类型的 SFR：

a）主要的 SFR，它直接满足已知的 TOE 安全目的；

b）支持性的 SFR，它不直接满足 TOE 安全目的，但对主要的 SFR 提供支持，从而间接帮助支持相关 TOE 安全目的。

GB/T 18336 没有明确区别这两种类型的 SFR，但其差别暗含在对功能组件间的依赖性，或对 SFR 间的相互支持的表现这两方面的考虑当中。因此，没有必要在 ST 中明确按主要的或支持性的分列 SFR。当编写 ST 基本原理时，认识到存在这两种类型 SFR 是非常有益的。

在 SFR 选择的第一步，识别出能够满足 TOE 一个安全目的的主要的 SFR，一旦建立了一组完整的主要 SFR，重复上面过程识别出一组完整的支持性 SFR。如前所述，所有 SFR（不论主要的或支持性的）应该用适当的 GB/T 18336.2 中的功能组件来表达。当从 GB/T 18336.2 中选择功能组件时，也应参考包括在 GB/T 18336.2 的附录中有关组件的指导意见。

两种 SFR 类型之间的关系如下图所示，注意这种关系与 ST 基本原理相关，应体现 SFR 的相互支持，统一有效，从而保证了 TOE 安全目的得到满足。

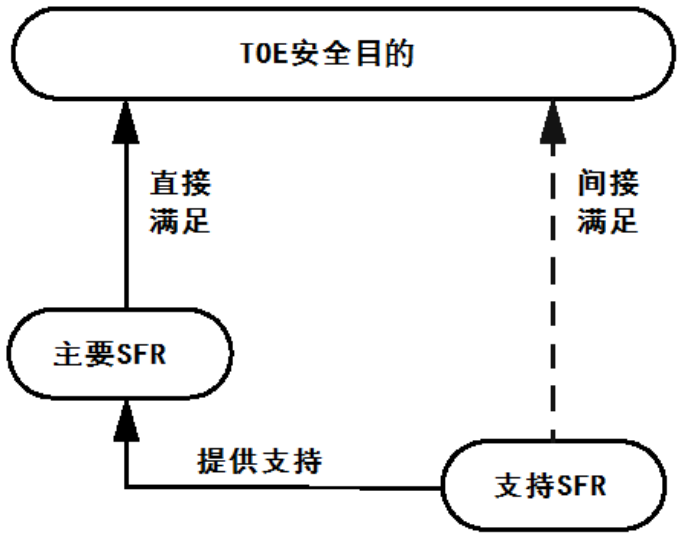


图 1-3 SFR 类型之间的关系

识别完整的支持性 SFR 的过程分 3 个阶段：

a）识别出所需的用于满足所有主要 SFR 依赖性的补充 SFR，它包括本步骤识别的支持性 SFR 的所有依赖性；

b）识别所有为确保达到 TOE 安全目的所需的补充 SFR,它包括保护主要 SFR 免受组合攻击所需的 SFR；

c）识别所需的补充 SFR，以满足这些在第 2 步和第 3 步中选择的支持性 SFR

的依赖性。

对满足 GB/T 18336.2 中确定依赖的支持性 SFR 的识别可能是一个迭代过程，例如：

a）假设ST要包括要求TOE在检测到即将发生安全事故时作出响应的安全目的，这会导致将基于FAU_ARP.1组件(安全警告)的主要SFR包含进来；

b）根据GB/T 18336.2，FAU_ARP.1依赖于FAU_SAA.1,那么该组件要作为支持性SFR应被包含进来；

c）FAU_SAA.1依赖于FAU_GEN.1（审计数据产生）；

d）FAU_GEN.1依赖于FPT_STM.1（可靠时间戳）；

e）FPT_STM.1则不需要引入别的功能组件。

应注意 GB/T 18336 允许部分不满足依赖性要求，但要解释为什么不要求相关SFR满足安全目的（从而满足安全需求）。

依赖性应以一致地方式被使用，例如，对于 FAU_ARP.1 而言，其一致性是由该组件的性质决定的（即：FAU_ARP.1依赖于对可能发生的安全违规的预测，这种违规是用FAU_SAA.1.2来定义的）。

对另外一些组件来说，保证一致性可能比较困难。例如，对于组件FDP_ACC.1，ST将识别出与之相关的特定访问控制类SFP，为满足FDP_ACC.1对FDP_ACF.1 的依赖性，必须确保相同的访问控制 SFP 作用于 FDP_ACF.1 和FDP_ACC.1。如果迭代操作应用在 FDP_ACC.1 并使用了不同的访问控制 SFP，那么作为依赖，FDP_ACF.1就需要满足每一个这样的SFP。

对额外的支持性 SFR（即那些在 GB/T 18336.2 中未被识别的依赖性）的识别包括识别人们认为必要的、用来支持TOE安全目标实现的其它任何SFR，这样的 SFR 一般通过减少攻击者可利用的选择或机会提供支持，或增强攻击者要实施成功攻击所需达到的专业知识水平或资源。应根据安全需求和安全目的考虑下述问题：

a）基于 GB/T 18336.2 中同类相关组件的 SFR。比如，如果包括组件FAU_GEN.1（审计数据产生），那就需要创建并维护一个安全审计追踪来存储生成的数据（需要一个或多个FAU_STG族安全组件）并需要用来检查生成的审计数据的工具（需要一个或多个FAU_SAR族安全组件），或

者将所产生的审计数据输出到其他系统去审查。

b）基于 FPT 类（TOE 安全功能的保护）相关组件的 SFR。这类 SFR 一般保护其他 SFR 所依赖的 TSF 或 TSF 数据的完整性和可用性。以 FPT_AMT.1（抽象机测试）和 FPT_SEP（域分离）子类的组件为例，当有确定的需求要保护 TSF 免受诸如 TSF 失败、崩溃或可能恶意的修改，可能需要上述组件支持相应的安全目的。

c）基于 FMT 类（安全管理）相关组件的 SFR。这些组件用于规定所有需要支持的安全管理 SFR，以处理取消安全属性的 FMT_REV.1 组件为例，在含有处理安全属性（如访问控制）的 SFR 时，可以考虑使用这类相关组件。

应根据安全目的选择支持性的 SFR，尤其要考虑 SFR 应该是相互支持的、紧密结合的、有效的一个整体。构建基本原理的过程对支持性 SFR 的选择具有重要作用，因为原理需要证明 SFR 是相互支持的、完整的、有效的整体。强烈建议不要包含与安全目的无关的支持性 SFR，因为这样会让 ST 不易被接受，其原因是：

a）某些 TOE 可能不满足这样的 SFR；

b）增加 SFR 的数量会增加评估过程中的成本和不必要的要求的维护。

如果 ST 以相关 PP 为基础编写，那么选择 SFR 的过程会大大简化。如果 ST 和 PP 包括不同的 SFR，应考虑 TOE 中的安全问题定义和（或）安全目的之间的差异。

## 6.2. SAR

在选择 SAR 时，应综合考虑下述几个因素：

a）受保护的资产价值及其面临的已知风险；

b）技术可行性；

c）可能的开发和评估费用；

d）TOE 评估和开发所需的时间表；

e）观察到的市场需求（如果是产品的话）；

f）功能组件对保障组件的任何已知的依赖性。

需要保护的资产价值越高，面临的风险越大，用于保护资产的安全功能要求的保障级别就越高，这些应反映在安全目的描述中。任何组织可通过定义其自身的策略和规则来确定保障级别，以确保把其资产面临的风险降到可以接受的水平。然后再定义组织中所用到的产品所需的保障级别。

其他如费用和时间等因素也可能制约实际上可达到的保障级别。技术可行性将成为考虑产生特定保障组件所需证据是否现实的一个因素。尤其是针对已有的系统（没有可供参考的设计文档），或者理论上要求一个高保障级别，从技术上来说无法在规定时间内得到半形式化或形式化的证据，所能达到的最高保障要求会低于理论上的要求。这种接受风险的举措，应当在安全目的中陈述。

安全目的中也可能需要表明 SAR 中特定的保障要求,例如：

a）TOE 安全目的可以声明 TOE 应能抵抗高攻击潜力者的攻击。这就明确指明要包含 AVA_VAN.5 组件；

b）安全目的可以表示要关注自我保护、域分离、不可旁路性，这种情况就必须包含 ADV_ARC.1 组件，注意 ADV_ARC 尽管只含有一个组件，但架构描述的级别依赖从 ADV_TDS 族中选择的组件；

c）安全目的可能提醒 TOE 的安全很大程度依赖于开发环境的安全。这就强烈建议 SAR 应包含 ALC_DVS 族中的组件，该族确保检查开发环境的安全被检测。

SAR 的选择是相对简单的，只需要简单地选择一个合适的保障包，例如 GB/T 18336 的 EAL。保障包的定义和描述应经过商议以确保这些包能够恰当地描述安全目的。存在这种可能，已有保障包大体可以提供所需的保障级，但对应安全目的在特定方面是缺乏的。这种情况下适合引入增强的保障要求（即在包中增加额外的要求）来确保安全目的被满足。

对于增强的保障要求，ST 作者应确保附加的要求也要满足保障组件的依赖关系。例如，如果 ST 用 AVA_VAN.3 增强 EAL3，就应增加 ADV_TDS.3 和 ADV_IMP.1，这些都是不包含在 EAL3 中的。另外也需要包括 ADV_FSP.4，因为 ADV_TDS.3 依赖 ADV_FSP.4。

### 6.3. 安全要求基本原理

EAL1 级中安全要求基本原理仅需论证依赖关系基本原理，以表格等方式说明安全要求之间满足依赖关系，或者证明不需要满足某个依赖关系。

## 7. TOE 概要规范

应在本部分描述 TOE 实现的安全功能及其如何实现相关安全要求。

TOE 概要规范是对 TOE 实现的安全功能的高层抽象描述，目的是向消费者解释 TOE 如何满足 SFR，使消费者理解 TOE 实现的安全功能，理解 TOE 安全功能满足 SFR 的实现机制。因此 TOE 概要规范应该在 TOE 的整体功能和架构的背景下描述 TOE 的安全功能，提供 TOE 整体的抽象视图和 TOE 实现 SFR 的充分的。

TOE 概要规范因此提出了一个以整体 TOE 安全为中心的抽象模型，模型中 SFR 定义的主体、客体、安全属性和规则在 TOE 的架构及其整体功能的上下文中进行描述。如果这些功能和 TOE 的安全功能实现无关,该模型仍然可以从 TOE 提供的大量的非安全功能中抽象出来。TOE 概要规范表述的详细程度应该高于 TOE 描述的详细程度，并应重点描述 SFR 是如何被满足的。同时，TOE 概要规范还应描述 SFR 与安全功能的对应关系映射，说明 SFR 是如何通过安全功能被满足的。可参考下述过程描述 TOE 概要规范：

a）概述 TOE，包括描述 TOE 的结构和 TSF 边界，描述 TSF 如何自我保护免遭篡改和旁路；

b）在导出 SFR 的 TOE 功能模型的基础上描述 TOE 的安全功能；

c）在描述每一个安全功能的同时，描述其所实现的、功能模型所导出的 SFR，描述安全功能所满足的 SFR 的实现机制。由此可构造出安全功能和 SFR 之间的映射关系。重点在通过用文本描述将功能模型代入到整个 TOE 所有功能和架构中进行描述，使读者能理解为什么要选择这些安全功能或细节，它们如何支持了 TOE 的整体功能。

# 第二部分：EAL2-EAL5 级 ST 文档编写指南

用于 EAL2-EAL5 级评估的 ST 文档应包括如下内容：

a） ST 引言：用于描述 ST 和相关 TOE 的标识和必要的描述信息；

b） 符合性声明：用于说明 ST 与 GB/T 18336、评估保障级（EAL）和安全技术要求（STR）的符合性；

c） 安全问题定义：用于描述 TOE 及其运行环境要解决的安全问题，包括威胁、组织安全策略和假设；

d） 安全目的：用于描述安全问题的高层解决方案，包括 TOE 安全目的和运行环境安全目的以及安全目的基本原理；

e） 扩展组件定义（可选）：用于定义新组件（即在 GB/T 18336.2 和 GB/T 18336.3 中不包含的组件），这些新组件用于定义扩展功能要求和扩展保障要求；

f） 安全要求：用于将 TOE 安全目的转化成组件形式表示的 TOE 安全要求标准语言形式，包括安全功能要求和安全保障要求以及安全要求基本原理；

g） TOE 概要规范：用于描述 TOE 提供的安全功能及其实现安全功能要求的机制；

h） 缩略语、术语和定义：用于描述 ST 文档中使用的缩略语、技术术语和定义。

EAL2-EAL5 级 ST 的基本结构图如下图所示：

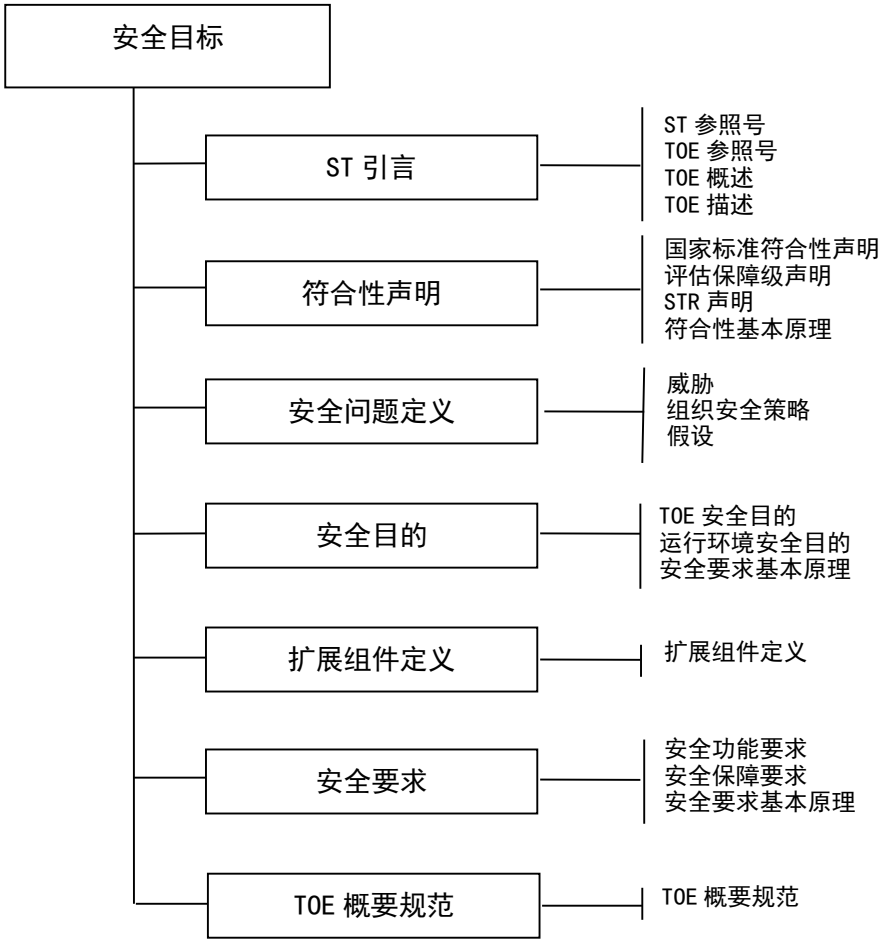


图 2-1 EAL2-EAL5 级 ST 基本结构图

# 1. ST 引言

ST 引言应描述 ST 和 TOE 的标识性信息，以及与评估相关的 TOE 关键信息。

## 1.1. ST 参照号和 TOE 参照号

应在本部分描述 ST 参照号和 TOE 参照号。

1）ST 参照号，是唯一标识 ST 的标识性信息。一个典型的 ST 参照号由 ST 标题、版本号、编写日期和作者组成；

2）TOE 参照号，是用来标识与 ST 对应的 TOE。一个典型的 TOE 参照号由 TOE

名称、TOE 版本号和开发者名称组成。

## 1.2. TOE 概述

TOE 概述应简单描述 TOE 的用途和其重要安全特征、TOE 类型和 TOE 运行环境的配置信息（TOE 依赖的、非 TOE 的硬件、软件或固件）。

TOE 概述是面向潜在消费者的信息，应通过描述使消费者了解 TOE 的安全能力和用途，帮助消费者快速确定 TOE 是否能够满足他们的安全需求，是否为他们的现有资源所支持。

1）TOE 用途和重要安全特征示例：

某数据库 V2.11 是一个用于网络环境的多用户数据库，它允许 1024 个用户同时活动，允许口令/令牌和生物识别认证，提供意外数据故障保护，能够回滚 1 万个事务，其审计特征可配置程度高，以便允许对某些用户和事务执行详细审计，同时保护其他用户和事务的隐私。

2）TOE 一般类型示例：

防火墙、VPN 防火墙、智能卡、加密调制解调器、企业网、WEB 服务器、数据库、WEB 服务器和数据库、LAN、包含 WEB 服务器和数据库的 LAN 等。

3）TOE 运行环境配置示例：

- 标准 PC，处理器 1GHz 以上，内存 512MB 以上，某操作系统运行版本 3.0，更新版本 6d，带 1.0 WM 驱动套件的某图形卡 1.0；
- 智能卡 SB2067 集成电路，运行某智能卡操作系统 V2.0；
- 某局域网。

## 1.3. TOE 描述

TOE 描述是面向评估者和潜在消费者提供的信息，应描述 TOE 的物理范围和逻辑范围。还应该提供 TOE 应用环境等与 TOE 安全评估相关的背景信息，使读者能够对 TOE 安全能力有一般性理解。TOE 描述应比 TOE 概述中的描述详细。

1）TOE 物理范围

TOE 物理范围是指构成 TOE 的硬件、固件、软件及指南的所有部分，描述 TOE 物理范围时可采用结构图或列表等形式描述 TOE 的所有构成部分，并对图表中的

每一项进行详细解释，同时应界定出物理评估边界，即哪些部分在评估范围之内，哪些部分在评估范围之外。

2）TOE 逻辑范围

TOE 逻辑范围是指 TOE 提供的安全能力。在描述 TOE 的逻辑范围时应列出 TOE 提供的所有安全特征，并逐项进行详细描述。同时应界定出逻辑评估边界，即哪些安全特征在评估范围之内，哪些安全特征在评估范围之外。

# 2. 符合性声明

符合性声明用于描述 ST 和 TOE 对 GB/T 18336 的符合情况，以及 ST 对安全技术要求（STR）和评估保障级（EAL）的符合情况。

## 2.1. 国家标准符合性声明

应描述 ST 和 TOE 声明遵从的 GB/T 18336 的版本、ST 与 GB/T 18336.2 的符合或扩展、ST 与 GB/T 18336.3 的符合或扩展。

## 2.2. 评估保障级声明

应列出 ST 声明遵从的评估保障级级别，描述 ST 与评估保障级级别的符合或增强。

## 2.3. STR 声明

应列出 ST 声明遵从的所有 STR 的名称和版本。对每一个 STR 描述符合的方式是严格的还是可论证的。

## 2.4. 符合性基本原理

如果符合的方式是“可论证的”，则应证实 ST 中描述的 TOE 类型与符合性声明中 STR 定义的 TOE 类型是一致的，应证实 ST 中描述的安全问题定义、安全目的、安全要求与符合性声明中的 STR 中的相关陈述是一致的或者是 STR 中相应集合的超集。如果符合的方式是“严格的”，此处仅声明本 ST 严格符合对应 STR。

# 3. 缩略语、术语和定义

应在本部分描述 ST 文档中使用的缩略语、术语和定义。

# 4. 安全问题定义

安全问题定义用于描述 TOE 及其运行环境将要负责处理的安全问题，是 ST 文档的重要部分，安全问题定义包括威胁、组织安全策略、假设。

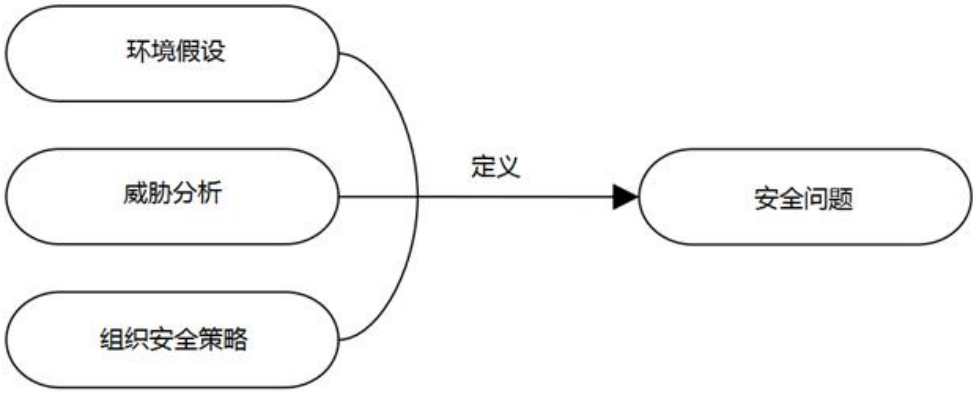


图 2-2 安全问题定义

可参考下述过程完成安全问题定义：

a） 通过获取来自用户需求的安全功能要求、风险评估、威胁评估等方式识别对 IT 产品的非正式的安全功能要求，形成基本安全问题；

b） 将基本安全问题中必须由 IT 产品对抗的潜在攻击识别为威胁；

c） 将基本安全问题中 IT 产品必须具有的安全属性和安全特征识别为组织安全策略；

d） 将基本安全问题中 IT 产品不必具有的安全属性和安全特征识别为假设；

e） 根据已经识别的威胁、组织安全策略和假设编写形成安全问题定义的具体内容，并进行相关检查，确保清晰和明确。

如果 ST 声明了严格符合的 STR，可复制该 STR 文档的安全问题定义部分的内容作为 ST 文档安全问题定义的一部分。

## 4.1. 威胁

威胁表明了资产遭受攻击的可能途径。应分别列出并简单描述已经识别的威胁。

可通过获取来自用户需求的 IT 产品安全功能要求、对该 IT 产品进行安全风险评估和威胁评估等方法识别必须由 TOE 或其 IT 环境对抗的威胁。

描述每一个安全威胁时，应包括威胁主体、需要保护的资产和威胁主体对该资产的侵害行为。

### 7.3.1. 主体

威胁主体指的是可能对资产实施侵害行为的实体。如黑客、用户、计算机进程等，可通过限定威胁主体相关专业技能、资源、机会和动机等来进一步明确描述威胁主体。

### 7.3.2. 资产

资产是有可能遭受威胁主体通过某种方法侵害但具有价值的实体，与 TOE 相关的资产可考虑信息资产、过程资产和物理资产三个类别：

信息资产是对其拥有组织有价值的数据，如普通数据、系统数据、专家数据库等，其中由 TOE 安全功能（TSF）使用的系统数据称为 TSF 数据，如 TSF 配置数据、鉴别数据、审计记录等，需要与其他数据进行区别。

过程资产指的是传输和分析数据的应用程序，如金融应用、办公自动化应用等，一般需要标识受保护的实际过程资产的名称和特征。

物理资产指的是用来支持信息和过程资产的信息处理设备，如便携 PC、关键网络基础设施等。

### 7.3.3. 威胁行为

关于侵害行为，建议尽量简单明确的加以描述，如：不适当的访问、不适当的传送访问权限等。

每个威胁都应单独标识以方便引用，建议用“T.”后跟简短而有意义的英文

名称或其缩写作为威胁的唯一标识。例如 T.ADMIN_ERROR、T.TSF_FAILURE、T.UNAUTHORIZED_ACCESS 等。

## 4.2. 组织安全策略

组织安全策略（OSP）是指组织为保障其运转而采用的若干安全规则、程序、规范和指南。应列出并简单描述已识别的 OSP。

组织安全策略可能需要由 TOE 或其环境或由两者一起实施。

可将 IT 安全控制措施等组织的管理策略、法律法规要求、客户提出合同条款等作为起点考虑 OSP，也可从未来的市场需求或 IT 产品预期实现的 IT 安全控制措施的愿望出发规定 OSP，也可参考类似组织或产品已经实现的 OSP。

一般的规则是：当 TOE 预期由特定组织或一类组织使用时，或当 TOE 需要实现一组明显不包含或仅隐含在威胁描述中的规则时，指定出 OSP 才是适当的。如：标识所使用的信息流控制规则；标识所使用的访问控制规则；定义有关安全审计的组织策略；使用组织强制的解决技术，例如使用特别批准的密码算法，或与认定的指南相一致的密码算法。

同威胁一样，应单独标识 OSP 以方便引用，建议用“P.”后跟简短而有意义的英文名称或其缩写作为 OSP 的唯一标识。例如 P.AUTHORIZED_USERS、P.PWD&CRT 等。

## 4.3. 假设

应列出并简单描述有关 TOE 运行环境和预期用法的所有假设。

假设主要用于限制或排除 TOE 内部的安全特性，表示特定的控制措施或控制措施类型由 TOE 运行环境提供，而不是由 TOE 提供；或者已经识别的威胁在运行环境中不存在或者不重要。通常采用陈述事实的描述方式。

假设可以是关于运行环境的物理、人员和连通性方面的。

运行环境物理方面的假设示例：

- 假设 TOE 放在经过电磁辐射最小化设计的房间中；
- 假设 TOE 的管理员控制台放在受限访问区域中。

运行环境人员方面的假设示例：

- 假设为了操作 TOE，TOE 的用户经过了充分的培训；
- 假设 TOE 的用户被批准为允许接触国家涉密信息；
- 假设 TOE 的用户不会写下他们的口令。

运行环境连通性方面的假设示例：

- 假设 PC 工作站至少具有 10GB 可用磁盘空间运行 TOE；
- 假设 TOE 是该工作站上运行的唯一的非 OS 应用；
- 假设 TOE 不会连接到不可信网络。

同威胁和 OSP 一样，应单独标识假设以方便引用，建议用“A.”后跟简短而有意义的英文名称或其缩写作为假设的唯一标识。例如：A.PHYSICAL、A.USER。

# 5. 安全目的

安全目的是应对安全问题的对策表达形式。安全目的的作用包括三个方面：

a）为安全问题提供高层的、以自然语言描述的解决方案；

b）将该解决方案划分为 TOE 安全目的和运行环境安全目的两个局部方式的解决方案，以反映出每个不同实体都必须处理一部分问题；

c）采用安全目的基本原理形式论证这些局部方式的解决方案，构成了一个对安全问题的完整解决方案。

在安全问题定义部分中已经陈述了安全问题，在本部分应以安全目的的陈述形式明确地界定出：安全问题是由 TOE 还是由环境来满足或处理的，如下图所示。

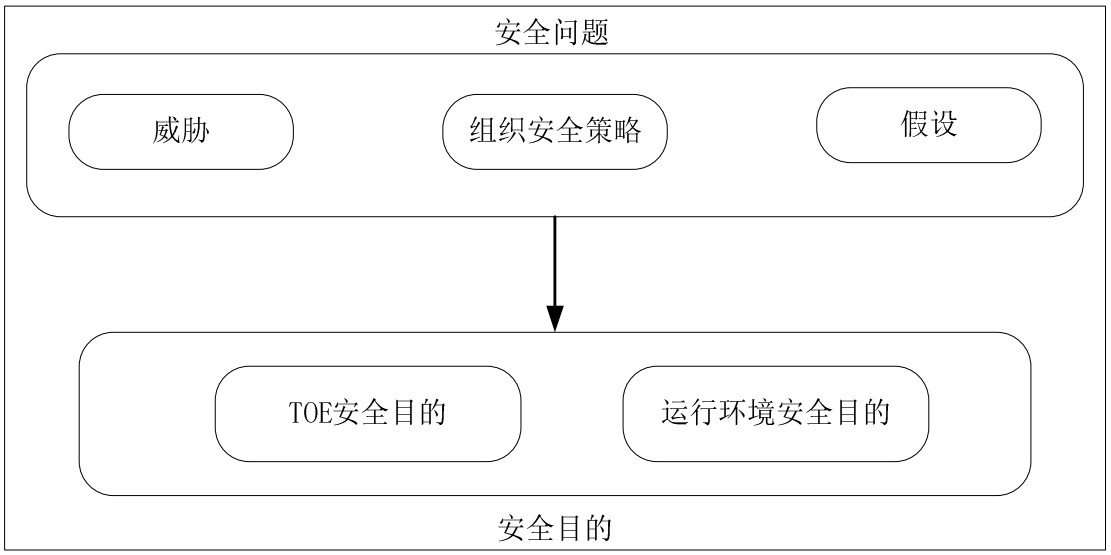


图 2-3 安全目的类型

在描述安全目的之前，应将安全问题定义中定义的安全问题划分为非 IT 环境相关、IT 环境相关和 TOE 安全功能相关 3 个类别，以便于区分处理安全问题的安全目的类别。

为确定安全目的定义的详细程度，需要遵循如下原则：

a）安全目的应能帮助读者理解由 TOE 处理的安全需求的范围，而不必深入到实现的细节，TOE 安全目的最好独立于实现。因此，应重点说明预计达到的结果而不是达到结果的方法；

b）应确保已定义的安全目的不是对包含在威胁和 OSP 中内容的重述，或只是形式稍有差异的重述。

实际上，当确定安全目的和安全要求之间的关系时，需要考虑安全目的的详细程度是否适当，不宜过于复杂或者简略抽象。

如果 ST 声明了严格符合的 STR，可复制该 STR 文档的安全目的部分的内容作为 ST 文档安全目的的一部分。

## 5.1. TOE 安全目的

TOE 安全目的是指由 TOE 实现的技术措施来满足的安全目的，用于处理与 TOE 安全功能相关的威胁和策略。应列出并简练精确的描述 TOE 安全目的。

可根据 GB/T 18336 中划分为类、族的安全功能组件，构建大范围的安全功

能集合，在此基础上确定需要解决的安全问题和相关安全服务，设定 TOE 的安全目的并予以描述。可参照下述功能类型构成的集合：

a）访问控制（对象、属性、操作、访问规则）

b）用户管理（用户类型、标识、鉴别）

c）TOE 自我保护（故障检查、可信恢复等）

d）安全通信（建立通信连接、连接属性、规则）

e）审计类（事件日志、响应、事件管理，分析）

f）结构化要求（所要求的属性和限制）

g）其他功能（如可信时间源、随机数生成等）

也可考虑将适合自己要求的其他安全功能类型集合作为建立 TOE 安全目的的基础。

可根据准备采用的控制措施类型进一步细化所确定的安全目的。

通常这些控制措施分为以下三种类型：

a） 预防性目的，预防将要发生的威胁或限制威胁实施的途径；

b） 检测性目的，提供手段检测和监视与 TOE 安全操作相关的事件；

c） 纠正性目的，要求 TOE 采取行动响应可能的安全违规或其他不希望的事件，从而保护或恢复 TOE 到安全状态，或限制危险的发生。

**预防性安全目的的例子如下，**它定义了对 TOE 用户标识和鉴别的需求：

TOE 确保用户在获准访问 TOE 之前唯一地标识每个用户，用户所声称身份是经过鉴别的。

访问控制和信息流控制类安全目的往往属预防性安全目的。TOE 应执行多个访问控制和信息流控制策略，建议识别每个不同的安全目的对应的策略，这有助于简化安全要求基本原理。

**检测性安全目的的例子如下，**它识别了 TOE 要提供源发抗抵赖能力的需求：

TOE 应提供办法使信息的接收者能够产生用于证明信息来源的证据。

**纠正性安全目的的例子如下，**它识别了对 TOE 检测到的入侵作出响应的需求：

当 TOE 检测到即将发生的安全违规事件时，采取适当措施遏制攻击，最小化因服务中断可能带来的破坏。

如果可能，安全目的应非正式地量化有效性的最低期望，可以采取以下方法描述：

a）相对而言，比如环境条件或已有的状态；

b）在绝对数值方面。

指定绝对数值表达精确，但有效性很难评估。应特别注意，安全目的中不应包括不必要的实现细节。

同样，对所描述的 TOE 安全目的也应单独命名，唯一标识，建议由“O.”后跟简短而有意义的英文名称或其缩写构成，以便于记忆和引用。如：O.PHYSICAL PROTECTION、O.LIFECYCLE CONTROL。

## 5.2. 运行环境安全目的

应在本部分描述所有运行环境安全目的。

环境安全目的包含由 IT 环境实现的技术措施或非技术措施满足的安全目的。换言之，环境安全目的包括 IT 环境安全目的和非 IT 环境安全目的。

TOE 不处理或不能处理的安全问题的环境安全目的必须被标识出来，下列环境安全目的通常是必需的：

a）用于对抗不是由 TOE 对抗的威胁的安全目的；

b）用于帮助满足那些不能由 TOE 满足的 OSP 的安全目的；

c）用于支持已标识的 TOE 安全目的去对抗威胁或满足 OSP 的安全目的；

d）用于确保满足已标识的环境假设。

识别环境安全目的可以首先通过依次对照每个未被 TOE 完全处理的威胁、OSP 和假设，编辑出一个安全目的的清单，然后对 TOE 安全环境中的每个项目作以下两步处理：

a）在清单中增加可以覆盖该项目的一个新的安全目的，或者映射一个已有的合适的安全目的到该项目，必要的时候可以修改已有的安全目的；

b）当构成安全目的基本原理时，应精练这个清单，因为这个过程可能识别出额外的安全目的，需要确保安全目的是作为整体来对抗威胁或满足 OSP 和假设的。

运行环境安全目的和 TOE 安全目的的识别过程是相互联系的。识别 TOE 及运

行环境分别对应的安全需求以确定评估边界，划分责任。二者的内容构成了安全目的的整体。

（非 IT）环境安全目的的典型实例包括：

a）建立和采取适当流程，保证以安全方式使用 TOE（应与环境假设协调一致）；

b）在恰当的安全实践中，教育和培训管理员及用户类安全目的。

因此，环境安全目的陈述应包括所有与管理活动有关的目的，需要以这些活动来保证 TOE 提供有效的安全服务。某些情况下要求的管理活动是明显的，很容易以（非 IT）环境安全目的的形式表达，而另一些情况下要求的管理活动依赖于实现 TOE 安全目的的详细要求。例如，“标识与鉴别”有关的安全目的可能通过口令来实现，这意味着要求用户保证不要将自己的口令泄露给其他人，这就要作为非 IT 安全要求来适当表达，而安全要求也是对环境安全目的的提炼。

GB/T 18336 指出，当威胁或 OSP 由 TOE 和其环境部分覆盖时，不同的类别中将重复出现相关联的安全目的。对上面安全目的的识别过程，这种做法是适当的，因为，有的威胁只能在环境管理活动支持下由 TOE 来对抗。如：鉴别数据（口令）管理，该安全目的可以如下陈述：

受环境支持的 TOE 将保证用户在获准访问 TOE 之前唯一地标识每个用户，用户所声称身份是经鉴别的。

在能够明确划分 TOE 及其环境责任的情况下，不必在一类安全目的中重复另一类的相同内容。比如，对于安全审计目的，TOE 的责任是产生和采集数据，而环境的责任是支持管理活动，即对产生的数据进行分析。

IT 环境安全目的的典型例子是底层操作系统标识和鉴别 TOE 用户。这种对 IT 环境的依赖性将在对环境的 IT 安全要求中详细说明。

与 TOE 安全目的相同，建议环境安全目的使用唯一性标识以便于引用。采用的标识方法应能区别环境的安全目的和 TOE 安全目的。对所描述的环境安全目的应单独命名，唯一标识，建议由“OE.”后跟简短而有意义的英文名称或其缩写构成，以便于记忆和引用，如：OE.AUD_REVIEW、OE.RESIDUAL。

### 5.3. 安全目的基本原理

定义安全目的基本原理是为了将安全目的追溯到安全问题定义中的威胁、组织安全策略和假设，以此说明所定义的安全目的是必要的，而且这些威胁、组织安全策略和假设已经全部由安全目的所覆盖，或者不再给予考虑。

应建立安全问题定义中各元素和安全目的各元素之间的关系表描述安全目的基本原理，并说明满足基本原理的合理理由:每一个威胁可由相关联的安全目的对抗、每一个组织安全策略可由相关联的安全目的实施、每一个假设可由相关联的安全目的支持。

## 6. 扩展组件定义

通常情况下，ST 中的安全要求选自 GB/T 18336.2 和 GB/T 18336.3 中的组件。但是，在某些情况下，为了满足安全目的，可能需要一些特殊的安全要求，这部分安全要求无法基于 GB/T 18336.2 和 GB/T 18336.3 的组件提出，这种情况下，就需要在本部分自定义新组件，这些组件称为扩展组件。但应尽量避免在 ST 中定义和使用扩展组件。

定义扩展组件时，应按照 GB/T 18336 中现有组件的类似定义方式、类似抽象程度和相同结构进行定义。

## 7. 安全要求

在本部分应描述安全要求和安全要求基本原理。

其中安全要求包括两个方面的要求：

a）安全功能要求(SFR)：SFR 应是对 TOE 安全目的的完全转化，用于对 TOE 预期安全行为进行清晰、无歧义且定义准确的描述，SFR 以一个较详细且抽象的形式表述，且独立于任何特定的技术解决方案（实现）。

b）安全保障要求(SAR)：对 TOE 获得保障而采取的预期活动进行清晰、无歧义且规范的描述。

应尽可能使用 GB/T 18336.2 中定义的安全组件和 GB/T 18336.3 中定义的保障组件（如下图），并以组件为单位构建安全要求，即：如果在 ST 中包括某个

组件，则组件中所有已定义的元素都应包括进来。

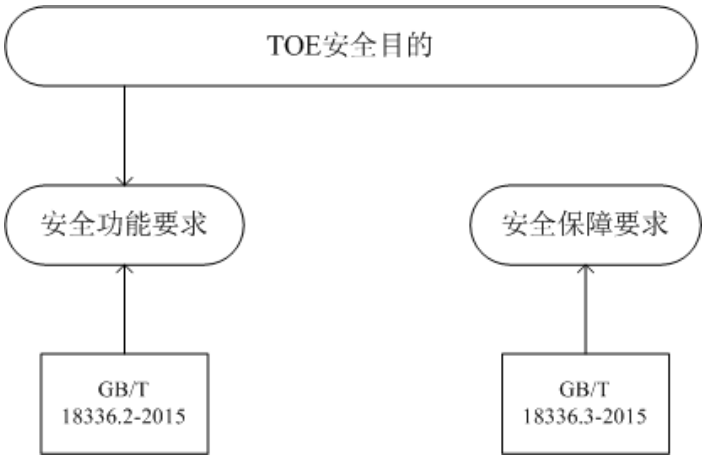


图 2-4 安全目的和安全要求之间的关系

选择安全功能组件描述 SFR 时，需要注意功能组件之间的依赖关系，这表示如果ST使用了某一SFR，那么，它一般也需要使用另外一些其依赖的SFR。因此，对于 ST 的制定，可以通过组件间的依赖关系这一机制来更好的进行功能组件的选取，以便全面包含必要的 SFR 从而提高 ST 的全面性。同时，在引用组件时，需要遵循反复、赋值、选择、细化等对组件的操作原则。

选择安全保障组件描述 SAR 时，也需要注意保障组件之间的依赖关系，这表示如果ST使用了某一SAR，那么，它一般也需要使用另外一些其依赖的SAR。因此，对于 ST 的制定，可以通过组件的依赖关系这一机制来更好的进行保障组件的选取，以便全面包含必要的 SAR 从而提高 ST 的全面性。

同时，在选择组件时，要注意同一个类不同组件间可能存在的层次关系，即：一个组件包括所在子类内其他组件中规定的全部要求元素。例如，FAU_STG.4 是 FAU_STG.3 的从属组件，因为所有在后者中定义的功能元素都包括在前者之中，因此不可能在同一个 ST 中同时包括这两个组件。

如果 ST 声明了严格符合的 STR，可复制该 STR 文档的安全要求部分的内容作为 ST 文档安全要求的一部分。

## 7.1. SFR

SFR 是 TOE 安全目的的细化和规范表示。应使用 GB/T 18336.2 中或扩展组件定义部分定义的功能组件进行描述。

应该在满足 TOE 安全目的的 TOE 总体安全功能模型的基础上选择 SFR。GB/T 18336.2 中的安全功能范例，提供了开发 SFR 抽象模型的基础，如：

a） 对资源和对象的访问和使用控制：定义相关的主体、客体、操作、安全属性、访问控制规则和相关的管理行为规则等；

b） 用户管理：定义用户类型、安全属性、用户标识和鉴别规则及相关的管理行为规则等；

c） TOE 自我保护：定义故障检测、响应规则及相关的管理行为等；

d） 安全通信：定义相关的连接属性、连接建立规则及相关的管理行为等；

e） 安全审计：定义被审计事件、事件响应、审计规则及相关的管理行为等；

f） 结构化要求：定义和确定满足安全目的所需要的支持性要求和规则，如审计迹保护、密码运算功能、失效安全、安全时间戳等。

为 ST 选择 SFR 的过程分几个阶段，在选择过程中要注意区别以下两种类型的 SFR：

a）主要的 SFR，它直接满足已知的 TOE 安全目的；

b）支持性的 SFR，它不直接满足 TOE 安全目的，但对主要的 SFR 提供支持，从而间接帮助支持相关 TOE 安全目的。

GB/T 18336 没有明确区别这两种类型的 SFR，但其差别暗含在对功能组件间的依赖性，或对 SFR 间的相互支持的表现这两方面的考虑当中。因此，没有必要在 ST 中明确按主要的或支持性的分列 SFR。当编写 ST 基本原理时，认识到存在这两种类型 SFR 是非常有益的。

在 SFR 选择的第一步，识别出能够满足 TOE 一个安全目的的主要的 SFR，一旦建立了一组完整的主要 SFR，重复上面过程识别出一组完整的支持性 SFR。如前所述，所有 SFR（不论主要的或支持性的）应该用适当的 GB/T 18336.2 中的功能组件来表达。当从 GB/T 18336.2 中选择功能组件时，也应参考包括在 GB/T 18336.2 的附录中有关组件的指导意见。

两种 SFR 类型之间的关系如下图所示，注意这种关系与 ST 基本原理相关，应体现 SFR 的相互支持，统一有效，从而保证了 TOE 安全目的得到满足。

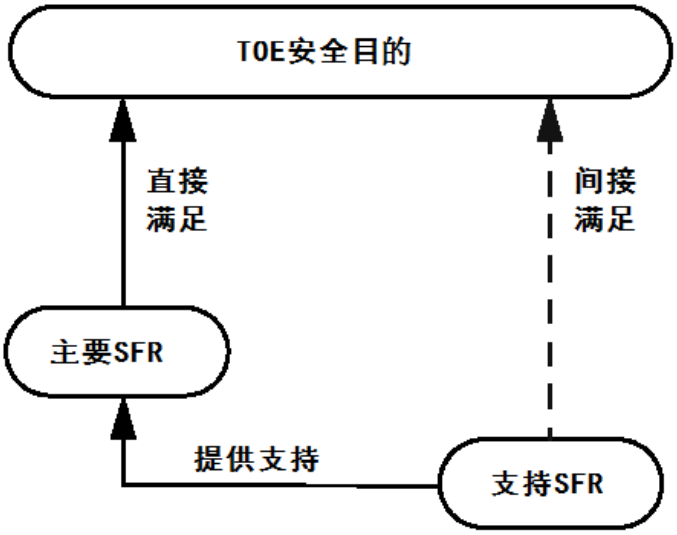


图 2-5 SFR 类型之间的关系

识别完整的支持性 SFR 的过程分 3 个阶段：

a）识别出所需的用于满足所有主要 SFR 依赖性的补充 SFR，它包括本步骤识别的支持性 SFR 的所有依赖性；

b）识别所有为确保达到 TOE 安全目的所需的补充 SFR,它包括保护主要 SFR 免受组合攻击所需的 SFR；

c）识别所需的补充 SFR，以满足这些在第 2 步和第 3 步中选择的支持性 SFR 的依赖性。

对满足 GB/T 18336.2 中确定依赖的支持性 SFR 的识别可能是一个迭代过程，例如：

a）假设 ST 要包括要求 TOE 在检测到即将发生安全事故时作出响应的安全目的，这会导致将基于 FAU_ARP.1 组件（安全警告）的主要 SFR 包含进来；

b）根据 GB/T 18336.2，FAU_ARP.1 依赖于 FAU_SAA.1,那么该组件要作为支持性 SFR 应被包含进来；

c）FAU_SAA.1 依赖于 FAU_GEN.1（审计数据产生）；

d）FAU_GEN.1 依赖于 FPT_STM.1（可靠时间戳）；

e）FPT_STM.1 则不需要引入别的功能组件。

应注意 GB/T 18336 允许部分不满足依赖性要求，但要解释为什么不要求相关 SFR 满足安全目的（从而满足安全需求）。

依赖性应以一致地方式被使用，例如，对于 FAU_ARP.1 而言，其一致性是

由该组件的性质决定的（即：FAU_ARP.1 依赖于对可能发生的安全违规的预测，这种违规是用 FAU_SAA.1.2 来定义的）。

对另外一些组件来说，保证一致性可能比较困难。例如，对于组件 FDP_ACC.1，ST 将识别出与之相关的特定访问控制类 SFP，为满足 FDP_ACC.1 对 FDP_ACF.1 的依赖性，必须确保相同的访问控制 SFP 作用于 FDP_ACF.1 和 FDP_ACC.1。如果迭代操作应用在 FDP_ACC.1 并使用了不同的访问控制 SFP，那么作为依赖，FDP_ACF.1 就需要满足每一个这样的 SFP。

对额外的支持性 SFR（即那些在 GB/T 18336.2 中未被识别的依赖性）的识别包括识别人们认为必要的、用来支持 TOE 安全目标实现的其它任何 SFR，这样的 SFR 一般通过减少攻击者可利用的选择或机会提供支持，或增强攻击者要实施成功攻击所需达到的专业知识水平或资源。应根据安全需求和安全目的考虑下述问题：

a）基于 GB/T 18336.2 中同类相关组件的 SFR。比如，如果包括组件 FAU_GEN.1（审计数据产生），那就需要创建并维护一个安全审计追踪来存储生成的数据（需要一个或多个 FAU_STG 族安全组件）并需要用来检查生成的审计数据的工具（需要一个或多个 FAU_SAR 族安全组件），或者将所产生的审计数据输出到其他系统去审查。

b）基于 FPT 类（TOE 安全功能的保护）相关组件的 SFR。这类 SFR 一般保护其他 SFR 所依赖的 TSF 或 TSF 数据的完整性和可用性。以 FPT_AMT.1（抽象机测试）和 FPT_SEP（域分离）子类的组件为例，当有确定的需求要保护 TSF 免受诸如 TSF 失败、崩溃或可能恶意的修改，可能需要上述组件支持相应的安全目的。

c）基于 FMT 类（安全管理）相关组件的 SFR。这些组件用于规定所有需要支持的安全管理 SFR，以处理取消安全属性的 FMT_REV.1 组件为例，在含有处理安全属性（如访问控制）的 SFR 时，可以考虑使用这类相关组件。

应根据安全目的选择支持性的 SFR，尤其要考虑 SFR 应该是相互支持的、紧密结合的、有效的一个整体。构建基本原理的过程对支持性 SFR 的选择具有重要作用，因为原理需要证明 SFR 是相互支持的、完整的、有效的整体。强烈建

议不要包含与安全目的无关的支持性 SFR，因为这样会让 ST 不易被接受，其原因是：

a）某些 TOE 可能不满足这样的 SFR；

b）增加 SFR 的数量会增加评估过程中的成本和不必要的要求的维护。

如果 ST 以相关 PP 为基础编写，那么选择 SFR 的过程会大大简化。如果 ST 和 PP 包括不同的 SFR，应考虑 TOE 中的安全问题定义和（或）安全目的之间的差异。

## 7.2. SAR

在选择 SAR 时，应综合考虑下述几个因素：

a）受保护的资产价值及其面临的已知风险；

b）技术可行性；

c）可能的开发和评估费用；

d）TOE 评估和开发所需的时间表；

e）观察到的市场需求（适用于产品）；

f）功能组件对保障组件的任何已知的依赖性。

需要保护的资产价值越高，面临的风险越大，用于保护资产的安全功能要求的保障级别就越高，这些应反映在安全目的描述中。任何组织可通过定义其自身的策略和规则来确定保障级别，以确保把其资产面临的风险降到可以接受的水平。然后再定义组织中所用到的产品所需的保障级别。

其他如费用和时间等因素也可能制约实际上可达到的保障级别。技术可行性将成为考虑产生特定保障组件所需证据是否现实的一个因素。尤其是针对已有的系统（没有可供参考的设计文档），或者理论上要求一个高保障级别，从技术上来说无法在规定时间内得到半形式化或形式化的证据，所能达到的最高保障要求会低于理论上的要求。这种接受风险的举措，应当在安全目的中陈述。

安全目的中也可能需要表明 SAR 中特定的保障要求,例如：

a）TOE 安全目的可以声明 TOE 应能抵抗高攻击潜力者的攻击。这就明确指明要包含 AVA_VAN.5 组件；

b）安全目的可以表示要关注自我保护、域分离、不可旁路性，这种情况就

必须包含 ADV_ARC.1 组件，注意 ADV_ARC 尽管只含有一个组件，但架构描述的级别依赖从 ADV_TDS 族中选择的组件；

c）安全目的可能提醒 TOE 的安全很大程度依赖于开发环境的安全。这就强烈建议 SAR 应包含 ALC_DVS 族中的组件，该族确保检查开发环境的安全被检测。

SAR 的选择是相对简单的，只需要简单地选择一个合适的保障包，例如 GB/T 18336 的 EAL。保障包的定义和描述应经过商议以确保这些包能够恰当地描述安全目的。存在这种可能，已有保障包大体可以提供所需的保障级，但对应安全目的在特定方面是缺乏的。这种情况下适合引入增强的保障要求（即在包中增加额外的要求）来确保安全目的被满足。

对于增强的保障要求，ST 作者应确保附加的要求也要满足保障组件的依赖关系。例如，如果 ST 用 AVA_VAN.3 增强 EAL3，就应增加 ADV_TDS.3 和 ADV_IMP.1，这些都是不包含在 EAL3 中的。另外也需要包括 ADV_FSP.4，因为 ADV_TDS.3 依赖 ADV_FSP.4。

## 7.3. 安全要求基本原理

安全要求基本原理用于展示安全要求适合满足的 TOE 安全目的。对安全目的，要说明这些安全要求不仅是必要的而且是充分的，并进行安全要求依赖关系分析。

### 7.3.1. 安全要求基本原理分析

安全功能要求基本原理用于展示安全功能要求适合满足的 TOE 安全目的。对安全目的，要说明这些安全功能要求不仅是必须的而且是充分的。建议采用下面推荐的方法分析安全功能要求的必要性和充分性：

首先要提供安全目的与 SFR 对应的交叉引用表。该表要提供如下信息：

a）每一 SFR 至少对应一个安全目的；

b）每一安全目的也至少要对应一个 SFR。

前一条要充分说明每一 SFR 是必须的（即不存在冗余的 SFR）。

其次要根据交叉引用表，非形式化论证 SFR 的充分性。这些非形式化的论

证应围绕 TOE 安全目的展开。对于每个安全目的，在显式的需求和导出的需求都满足的情况下，都应提供非形式化的论证证明 SFR 是充分满足安全目的的。这些论证应涵盖 ST 中的所有 SFR，这些 SFR 不仅直接满足安全需求，还起支持作用。在讨论时，应考虑以下方面：

a）为什么以及如何应用 GB/T 18336 中的操作；

b）TOE 安全要求如何与 IT 环境安全要求相适应。

对于安全保障要求需要注意以下几个方面：

a）用清晰连贯的语言陈述选择 SAR 的理由；

b）SAR 及其选择理由应与 ST 的其他部分保持一致。如，安全问题定义中描述的威胁主体能力很强，而所选 SAR 中的 AVA_VAN 并不能够对抗这样的威胁主体，这样安全问题定义和 SAR 之间就产生了不一致。

### 7.3.2. 依赖性分析

当一个组件无法独自充分表达安全功能性或保障性而依赖于另一个组件的存在时，就产生依赖关系。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，此处需以表格等方式说明安全要求之间满足依赖关系，或者证明不需要满足某个依赖关系。

组件依赖关系的描述可通过参考 GB/T 18336.2-2015《信息技术 安全技术 信息技术安全评估准则 第 2 部分：安全功能组件》和 GB/T 18336.3-2015《信息技术 安全技术 信息技术安全评估准则 第 3 部分：安全保障组件》的组件定义来确定。

## 8. TOE 概要规范

应在本部分描述 TOE 实现的安全功能及其如何实现相关安全要求。

TOE 概要规范是对 TOE 实现的安全功能的高层抽象描述，目的是向消费者解释 TOE 如何满足 SFR，使消费者理解 TOE 实现的安全功能，理解 TOE 安全功能满足 SFR 的实现机制。因此 TOE 概要规范应该在 TOE 的整体功能和架构的背景下描述 TOE 的安全功能，提供 TOE 整体的抽象视图和 TOE 实现 SFR 的充分的。

TOE 概要规范因此提出了一个以整体 TOE 安全为中心的抽象模型，模型中SFR 定义的主体、客体、安全属性和规则在 TOE 的架构及其整体功能的上下文中进行描述。如果这些功能和 TOE 的安全功能实现无关,该模型仍然可以从 TOE 提供的大量的非安全功能中抽象出来。TOE 概要规范表述的详细程度应该高于 TOE 描述的详细程度，并应重点描述 SFR 是如何被满足的。同时，TOE 概要规范还应描述 SFR 与安全功能的对应关系映射，说明 SFR 是如何通过安全功能被满足的。可参考下述过程描述 TOE 概要规范：

a）概述 TOE，包括描述 TOE 的结构和 TSF 边界，描述 TSF 如何自我保护免遭篡改和旁路；

b）在导出 SFR 的 TOE 功能模型的基础上描述 TOE 的安全功能；

c）在描述每一个安全功能的同时，描述其所实现的、功能模型所导出的 SFR，描述安全功能所满足的 SFR 的实现机制。由此可构造出安全功能和 SFR 之间的映射关系。重点在通过用文本描述将功能模型代入到整个 TOE 所有功能和架构中进行描述，使读者能理解为什么要选择这些安全功能或细节，它们如何支持了 TOE 的整体功能。