第 5 章　安全目标及其编制方法

本章阐述 TOE 开发者如何使用 CC 标准化语言来编制 ST 文档，以论述实现 IT 产品安全需求的解决方案。本章内容将继续按照 ISO/IEC TR 15446:2009 技术报告的结构进行编排，并逐节讨论 CC 第 1 部分附录 A 规定的 ST 文档结构和内容编制方法和技巧，以及如何去阅读和解释其中的各部分内容。

本章包括以下内容。

(1) **ST 概述**：概述如何通过编制 ST 来响应用户对 IT 产品的安全需求，包括安全架构设计的基本概念、PP 与 ST 之间的关系、ST 的用途等。

(2) **ST 结构**：解释 ST 所提供的安全方案结构及内容，概述 ST 各部分之间的关系(安全原理编制)。

(3) **ST 编制**：按照 ST 结构，分别概述引言、符合性声明、安全问题定义、安全目的、扩展组件定义、安全要求和 TOE 概要规范的编制方法。

5.1　安全目标概述

ST 是 IT 产品开发者提供的一个响应客户安全需求(PP)的、与实现相关的安全方案，是体现某个具体 IT 产品安全规范的文档。换句话说，PP 是从 IT 产品消费者角度规定某类 IT 产品的安全功能和安全保障要求，而 ST 是 IT 产品提供者从实现的角度明确 IT 产品安全功能的实现技术与机制。这样 TOE 开发者就可依据 IT 产品生命周期的安全保障措施进行详细设计和实现，以便满足 IT 产品用户通过 PP 表达的安全需求。正如第 4 章所讨论的，PP 独立于 TOE 安全功能的具体实现，所以不同的 TOE 开发者可以编写与他们实现机制相关的，但是具备同等安全功能的 ST 来有效地响应同一个 PP。因此，在 ST 的符合性评估方面，ST 评估者将聚焦在如何验证它是 PP 所提需求的充分、完整、正确和一致的解释。

一些 CC 用户会参与 ST 的编制与使用，例如某个 TOE 开发者编制 ST，以响应用户在 PP 中表达的安全需求，由潜在 TOE 消费者阅读和确认 IT 产品开发者的 ST 是否满足其定义的 PP。当然 TOE 开发者编制的 ST 必须符合 CC 第 1 部分附录 A 定义的结构，并按照 CEM 中的 ST 评估保障要求(ASE)进行审核和评估。所以，ST 需要承担两个典型的角色。

(1) TOE 评估之前及评估期间：ST 指出“要评估什么”。在这个任务中，ST 是作为 TOE 开发者和评估者之间在 TOE 安全功能和评估范围上达成一致的基础。TOE 实现安全技术正确性和安全功能完备性是这个任务的主要挑战。

(2) TOE 测试评估后：ST 指出“被评估了什么”。在这个任务中，ST 也是作为 TOE 开发者或销售者和 TOE 潜在消费者之间达成一致的基础。ST 描述了 TOE 确切的安全功能，潜在消费者能够信赖这个描述，因为 TOE 已经过 CC 测试实验室的安全评估，证实了 TOE 实现满足 ST 定义的安全要求。

ST 的易用和易理解特性是 TOE 开发者在编制 ST 时需要考虑解决的主要问题，但是 ST 不应承担以下两个角色。

(1) 详细规范：ST 中的 TOE 概要规范(TSS)是较高抽象级别的安全功能及其实现机制的描述。ST 一般不包含 TOE 协议规范、算法或实现机制的详细描述，如冗长的 TOE 具体操作描述等。

(2) 完整规范：ST 只给出了 TOE 的安全规范，而没有包括 TOE 的通用功能规范。除非与 TOE 安全相关，否则 TOE 的兼容性、物理大小和重量、要求的电压等通用功能不应该成为 ST 概要规范的组成部分。也就是说 ST 中的概要规范通常是 TOE 完整规范的一部分，并非 TOE 的完整规范。

TOE 开发者编制的 ST 一旦被 TOE 评估者认可，就将被用作描述 TOE 安全功能及其实现的基础。被认可的 ST 一般也会发布在国家级认证产品公告栏和已评估 IT 产品列表中。注意公开发布的 ST 通常已被简化，以去除公司专有的或敏感的安全信息。因此，这些已发布的 ST 文档可能并不是“完整的”。

不同于第 4 章的 PP 结构，CC 第 1 部分附录 A 定义的 ST 文档结构中增加了 TOE 概要规范，以准确地描述 TOE 的安全功能和安全保障要求是如何被实现的。

在 IT 产品安全功能的描述方面，TOE 开发者编写的 ST 文档应当是自包含的，不应要求读者为理解 ST 去翻阅大量其他文件。ST 并非一次即可编辑成型，这是一个动态修订的过程，一旦产品还没有被最终实现，ST 的修改过程极可能被下列事件触发。

(1) 识别和应对新的威胁，例如 TOE 运行环境的变化导致 TOE 需处理新的安全攻击。

(2) 组织安全策略的改变，例如 TOE 运行环境基础设施变化需要对 TOE 的组织安全策略进行调整。

(3) IT 产品安全功能行为或预期用途的改变，例如由于 TOE 安全机制概念改变导致安全策略配置或 TSF 管理的改变。

(4) 成本或进度计划改变，例如 TOE 研发人员或研发环境的变化导致 TOE 开发成本或开发计划的变化。

(5) 出现开发成本高于预期的情况，例如使用第三方服务组件升级或使用未在预算计划中的支持工具。

(6) 在 TOE 及其运行环境之间的安全要求分配的变化，例如由于时间和资金的限制，希望由 TOE 担负与希望由 TOE 环境担负的责任划分可能发生变化。

(7) 新的 IT 技术出现，例如大数据技术、人工智能技术的采用。

(8) 出现 TOE 评估或操作过程中未覆盖的缺陷。

(9) 认证规范或活动(认证认可[C&A])要求发生变化。

正如第 4 章所述，CC 第 3 部分的生命周期保障族(ALC_LCD)定义了两个组件来评估 TOE 开发者使用的生命周期模型的恰当性、规范性及 TOE 可测试性。PP 编制、ST 编制、TOE 安全评估等涉及 CC 评估过程的相关概念可映射到软件生命周期的某阶段。ST 相当于软件生命周期的设计阶段，即开发者为响应客户在 PP 中声明安全要求生成的设计文档，并且设计的安全要求实现措施应通过 CC 第 3 部分的 ST 保障评估(ASE)活动的评估验证。

ST 是组成 IT 产品采购活动授权前所进行的招标过程的一部分，ST 应包括在潜在投标客户提交的招标响应文件中，采购方应选择合适的专家小组对其安全功能和安全保障要

求进行评估。表 5.1 列出了 ST 和通用系统生命周期阶段以及通用采购阶段相关活动的映射关系。

表 5.1 通用评估准则活动与通用系统生命周期和采购阶段的映射关系

通用评估准则活动	通用系统生命周期阶段	系统采购通用流程
无	概念	概念定义、可行性研究、需求分析、成本预算等
保护轮廓编制 PP 安全评估活动：APE	需求分析和规范说明	招标书中发布的安全要求文件
安全目标编制 ST 安全评估活动：ASE	系统设计	需求：由供应商提交技术评估和成本建议
由中标供应商开发 TOE TOE 安全评估活动：ALC_DVS、ADV	系统开发	采购招标与合同签订
TOE 评估活动：ATE、AVA	系统验证	验收交货订单物，发现不满足需求的设计或开发缺陷
TOE 评估活动：ALC、ADV、AGD	确认、安装和检验	系统安装部署和试运行
TOE 评估活动：AGD、ALC_FLR、AVA	运行和维护	系统运行，并过渡到维护合同
无	停止	合同期满

5.2 安全目标结构

作为响应客户 PP 的安全方案文档，ST 是 TOE 开发和评估的依据。CC 实施这一约束是为了确保 TOE 开发者编制的 ST 是准确的，并且能被 CC 所有用户充分、完整、正确和一致地理解和解释。

编写 ST 的前提是 TOE 开发者获取了一系列描述客户安全需求的资料。所以 TOE 开发者在编写 ST 之前通常需要与 CC 专家和安全评估人员一起分析客户认可的 PP 或可参考的 IT 产品安全需求。图 5.1 描绘了 CC 第 1 部分给出的 ST 文档结构及其内容，包括相关的格式要求。它可用作 TOE 开发者编制 ST 的结构性框架。但该结构也是允许变化的，例如，如果安全要求基本原理内容特别多，可以放在 ST 最后作为一个章节单独描述，而不放在图 5.1 所示的安全目的和安全要求章节。ST 文档的每一部分内容和应用都将在本章的 5.3 节～5.9 节中详细讨论。ST 文档包含的 7 部分内容如下。

(1) ST 引言：ST 第 1 部分在 3 个抽象层面上对 TOE 进行叙述性描述。为 ST 及其相关的 TOE 提供标识信息；通过定义 ST 功能、范围和状态来简要描述 TOE 功能；从系统类型、安全架构、逻辑及物理安全边界等来对 TOE 安全功能进行更加详细的描述。

(2) 符合性声明：表明 ST 是否声明与某些 PP 或包符合(且与哪些 PP 或包符合)。这部分阐明 ST 是用来响应哪一个 PP(如果有)、包(如果有)以及是否在 CC 第 2 部分和第 3 部分组件的基础上增加了扩展组件来响应特定的安全要求。

(3) 安全问题定义：第 3 部分声明了 TOE 安全假设，分析了 TOE 面临的安全威胁并且列出了适用于 TOE 安全运行的组织安全策略。

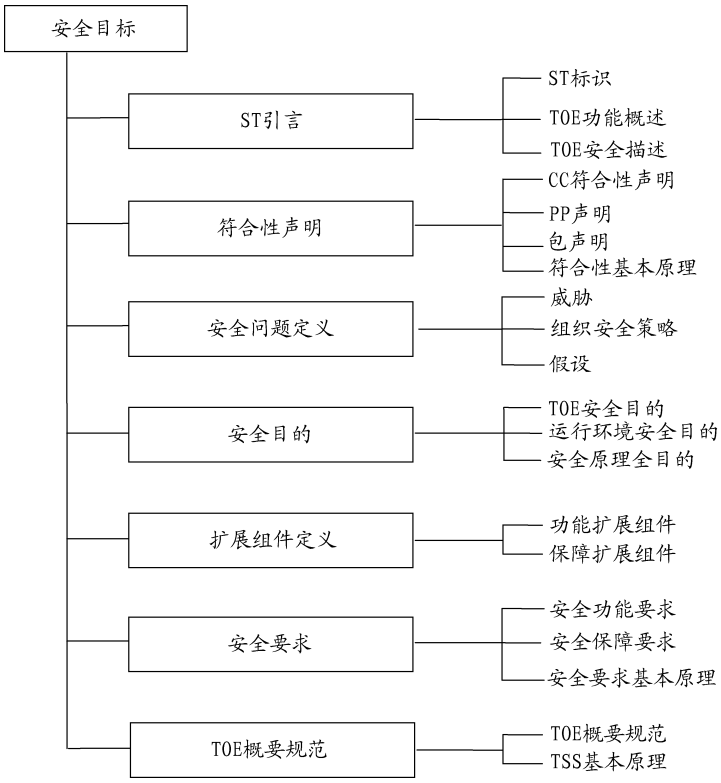

图 5.1　ST 文档结构和内容

(4) 安全目的：第 4 部分描述了 TOE 安全目的和运行环境安全目的，这些安全目的来自对第 3 部分的假设、威胁和组织安全策略的分析。因此，该部分还包括安全目的的基本原理说明。安全目的划分为 TOE 安全目的和运行环境安全目的。

(5) 扩展组件定义(可选)：第 5 部分用于描述在 ST 中 TOE 特定的安全要求没有采用 CC 第 2 部分和第 3 部分标准组件来定义，而是通过新定义组件来表达这些特殊的扩展功能要求和扩展保障要求。

(6) 安全要求：第 6 部分分别通过安全功能要求(SFR)和安全保障要求(SAR)来回答第 4 部分中描述的 TOE 安全目的是如何实施的，这些 SFR 和 SAR 来自对第 1 部分中讨论的安全架构、安全边界以及第 3 部分中描述的威胁和组织安全策略的分析。

(7) TOE 概要规范：第 7 部分描述用来实现第 6 部分所陈述的安全要求具体的功能行为及其实现技术与机制，表明安全功能要求(SFR)在 TOE 中是如何被实现的。

如果安全目的、安全要求或概要规范的基本原理内容特别多，可以放在 ST 文档的最后一并陈述。总之，ST 编制者在 ST 中陈述的基本原理包括以下几点。

(1) 第 4 部分中声明的安全目的支持所有的假设，应对所有威胁，执行第 3 部分定义的所有组织安全策略。

(2) 第 6 部分定义的安全要求满足第 4 部分声明的 TOE 所有安全目的。

(3) 第 7 部分描述的 TOE 概要规范实现了第 6 部分声明的 TOE 所有安全要求。

(4) 第 2 部分关于 PP 合规性的声明是有效的。

ST 不同章节内容之间的完整性与一致性证明来自对上面所列部分的关联分析和一致性与完整性检验。表 5.2 总结了 ST 各部分内容之间的依赖关系。

表 5.2 ST 各部分内容之间的依赖关系

章 节	目 标	源
引言	确定 ST 的性质、范围和状态，描述需要保护的 TOE 的系统类型、安全架构、通用功能，保护资产、逻辑与物理安全边界	来自 CC 第 1 部分的 PP 结构要求
PP 符合性声明	识别出可应用于 ST 的 PP，指明相关的裁剪和扩充要求	由 PP/ST 第 3 节至第 6 节内容的比较导出
安全问题定义	陈述 TOE 保护的资产，相关的假设、面临的安全威胁，并引用适用于 TSF 的组织安全策略	来自参考 PP
安全目的	描述 TOE 和 TOE 运行环境的安全目的	来自第 3 节的假设、威胁和安全策略的分析
扩展组件定义	提供 TOE 附加的安全要求	来自 TOE 的安全问题陈述及 TOE 的安全目的
安全要求	通过安全功能要求 SFR 和 SAR 的组合实现 ST，并用证据证实 TOE 的安全要求是完整而紧密的	来自系统安全架构和安全边界分析（第 2 节）和面对的安全问题风险分析（第 3 节）
TOE 概要规范	向 TOE 的潜在消费者提供 TOE 如何满足安全功能要求和安全保障要求的描述，使潜在消费者能够充分理解 TOE 的一般形态和实现	通过对第 6 节的安全要求、当前 IT 技术和工业界最佳实践分析得出

理解 PP/ST 之间的关系是很重要的。不同于 PP，第 7 部分定义的 TOE 概要规范是 ST 特有的。相对地，ST 的前 6 个部分与 PP 结构基本相同。如果一个 ST 声明了 PP 的完全符合性要求，则相应 PP 的第 3 到第 6 部分在本 ST 中可能是被引用而不是被复制。在 CC 网站上已经发布的 ST 中，通常的做法是在 ST 相应部分中提供附加的具体实现细节。表 5.3 说明了 ST 和相符合的 PP 各部分之间的相似与不同。

表 5.3 PP 中各部分和 ST 中各部分之间的相似与不同

保护轮廓结构	交 互	安全目标结构
1. 引言	• PP/ST 标识部分基本相同 • 在 TOE 概述部分，PP 聚焦于系统资产所有者和 TOE 安全边界，而 ST 关注 TOE 的安全架构、物理和逻辑安全边界 • 在 ST 中多一个比 TOE 概述更详细的 TOE 描述小节，这样评估者和潜在消费者对 TOE 安全能力能有更清楚理解	1. 引言
2. 符合性声明	• PP 与 ST 基本相同 • PP 不一定有 PP 符合性声明，ST 一般有 PP 符合性声明	2. 符合性声明
3. 安全问题定义	• PP 与 ST 基本相同 • ST 进一步区分是 TOE 应对威胁还是由其运行支持环境应对威胁	3. 安全问题定义
4. 安全目的	• PP 与 ST 基本相同 • ST 安全原理部分可能增加 ST 概要规范原理性解释	4. 安全目的

续表

保护轮廓结构	交　互	安全目标结构
5. 扩展组件定义	• PP 与 ST 基本相同	5. 扩展组件定义
6. 安全要求	• PP 与 ST 基本相同 • ST 可能对 PP 中未完成的组件元素进一步操作 • ST 可能对 PP 中未解决的依赖关系进一步分析 • ST 可能增加新的安全要求 • ST 安全原理部分可能增加 ST 概要规范原理性解释	6. 安全要求
	• 在 PP 中没有对应内容 • 提供 TOE 用于该目的的一般性技术机制	7. TOE 概要规范

图 5.2 是 2014 年发布在 CC 官方网站上的 IBM 数据库产品 DB2 在 z/OS 平台上的 ST(DB2 11 for z/OS Security Target)结构。从目录结构(注意省去了该 ST 的三级目录)可以看出,IBM 的 DB2 数据库基本遵循了 ISO/IEC TR 15446 技术报告结构要求,只在最后添加了一个缩略语、术语和参考文献。

1　引言
　1.1　ST 参考
　1.2　TOE 参考
　1.3　TOE 概述
　1.4　TOE 描述
2　符合性声明
3　安全问题定义
　3.1　介绍
　3.2　威胁
　3.3　组织安全策略
　3.4　假设
4　安全目的
　4.1　TOE 安全目的
　4.2　运行环境安全目的
　4.3　安全目的原理
5　扩展组件定义
6　安全要求
　6.1　TOE 安全功能要求
　6.2　安全功能要求原理
　6.3　TOE 安全保障要求
　6.4　安全保障要求原理
　6.5　TOE 概要规范原理
7　TOE 概要规范
　7.1　TOE 体系结构概述
　7.2　标识与鉴别
　7.3　访问控制
　7.4　z/OS 通信安全
　7.5　安全管理
　7.6　审计
　7.7　对象重用
　7.8　TOE 自保护
8　缩写、术语和参考文献

图 5.2　DB2 ST 结构样例

关于组合 TOE,应对每个 TOE 部件都编写一个独立的 ST,被引用的 PP 都应当反映到组合 TOE。注意区分包含在 PP 里的假设、威胁、组织安全策略、安全目的、SFR、SAR 等,明确哪些部分将应用于组合 TOE 的所有 TOE 部件,哪些将应用于某一个 TOE 部件。另外注意对于不同的 TOE 部件,安全组件上的元素操作执行上可能有所不同。不论哪种情况,对 TOE 部件适用的假设、威胁、组织安全策略(OSP)、安全目的、安全功能要求(SFR)和安全保障要求都将成为 ST 的一部分内容。图 5.3 阐明了组合 TOE 与 PP/ST 之间的关系。

在 GB/T 18336—2015 版本中允许低保障级 ST 用于作 EAL1 评估(注 EAL2 及以上评估保障级不可以)。低保障级 ST 只能声明符合一个低保障级 PP(见 4.9 节讨论)。一个常规的 ST(即有 ST 规范要求的全部内容)可以声明与一个低保障级的 PP 符合。

低保障级 ST 包括常规 ST 的部分内容,但与常规 ST 相比也明显减少了一些内容,如下。

(1) 不用描述安全问题定义。

(2) 不用描述 TOE 安全目的,但运行环境安全目的仍然必须描述。

(3) 由于 ST 中没有安全问题定义,所以不用描述安全目的基本原理。

(4) 由于 ST 中没有 TOE 安全目的,所以安全要求基本原理只需要证明未被满足的组件依赖关系。

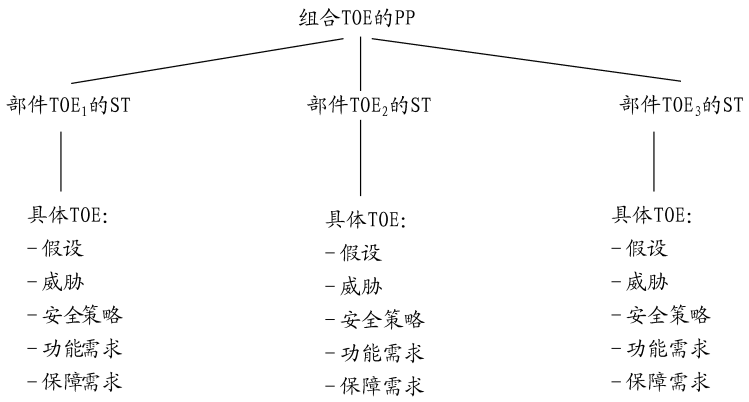

图 5.3 组合 TOE 与 ST 和 PP 之间的关系

5.3 安全目标引言

ST 引言在 3 个抽象层面上对 TOE 进行描述。

(1) ST 标识：为 ST 及其相关的 TOE 提供标识信息。

(2) TOE 功能概述：简要描述 TOE 通用功能及其运行环境。

(3) TOE 安全描述：对 TOE 安全架构及其主要安全功能进行更加详细的描述。

5.3.1 ST 标识

ST 标识用于正确地登记、索引和交叉引用由各国评估机构和 CCRA 参与者维护的 ST 相关信息。ST 标识一般由标题、版本、作者、出版日期等信息组成。因此，ST 标识部分里的第 1 个字段简单地描述 ST 名称；而第 2 部分陈述 ST 版本、发布日期、作者等字段信息；第 3 部分字段列出与 ST 相关的关键词，例如产品分类、开发或用户组织和商标名称；第 4 个字段引证编制 TOE 时参考的 CC 版本信息；最后字段指出 ST 当前评估状态。图 5.4 给出了 CC 官方网站上两个 ST 标识部分的例子和我国推荐使用的 ST 标识样例，第一个样例没有给出 ST 标识，只给出了 ST 的版本和发布日期，第二个有完整的注册信息，并包括评估认证等字段。最后一个样例是我国 GB/Z 20283 指导性文件推荐使用的 ST 和 TOE 相关标识信息。

总体来说，TOE 标识需包括 TOE 名称、开发者名称和 TOE 版本号。TOE 标识的例子："某数据库 v2.11"。由于真实的 IT 产品处于不断发展中(如 Oracle 数据库已经有 14 个大版本)，同一个 IT 产品可能因版本升级需要多次评估。因此某个 IT 产品会有多个 ST(TOE)。即使是同一版本的 IT 产品，由于安全选件不同，或满足不同消费者的需求，同一版本 IT 产品可能有多个 ST(TOE)。因此，面向不同消费者进行评估的 IT 产品会有多个 ST，TOE 标识不必是唯一的。例如 Oracle 数据库分标准版和企业版，企业版又分为基础版、标签版和数据库仓库版，表 5.4 给出了 Oracle 公司 Oracle 11g 不同数据库版本的认证情况(https://www.oracle.com/technetwork/topics/security/security-evaluations-099357.html)，从表中的 Oracle 不同安全选件看出，Oracle 针对不同功能的版本发布了相应的 ST。

样例 1：TOE for IBM DB2 11 for z/OS Version 1 Release 13

1.1　ST 标识

标题：IBM z/OS 平台 DB2 11 安全目标

版本：1.9

状态：最终版本

发布日期：2014-03-28

发起人：IBM 公司

开发者：：IBM 公司

关键字：IBM DB2 for z/OS；关系数据库管理系统(DBMS)

样例 2：TOE for Mobile PayPass 1.0.13vA.2.4 on Orange NFC V2 G1

1.1　ST 标识

标题：Mobile PayPass 1.0.13vA.2.4 on Orange NFC V2 G1

参考文献：D1321203

版本：1.0p

发表日期：October 20th,2014

作者：Gemalto

安全评估机构：THALES CEACI

认证主体：ANSSI

CC 版本：CC v3.1 r3

状态：发布

样例 3：基于 GB/T 的评估对象技术要求标识

ST 标识信息

ST 标题：×××安全目标

ST 文档编号：×××

ST 文档版本：×××

发行时间：×××

作者：×××公司

TOE 标识信息

TOE 名称：××××××芯片(以下简称×××)

TOE 版本：×××

发布：×××公司

图 5.4　ST 标识样例

表 5.4　Oracle 11g 数据库不同版本、不同组合选件的 ST 列表样例

安 全 目 标	保障级别	认 证 日 期
Oracle Database 11g Release 2 Enterprise Edition, version 11.2.0.2, with all critical patch updates up to and including July 2011 via the July 2011 PSU as well as the October 2011 CPU	EAL 4+ ALC_FLR.3	2012-01-17
Oracle Database 11g Release 2 Standard Edition and Standard Edition 1, version 11.2.0.2, with all critical patch updates up to and including July 2011 via the July 2011 PSU as well as the October 2011 CPU	EAL 4+ ALC_FLR.3	2012-01-17
Oracle Database 11g Enterprise Edition, Release 11.1.0.7 with Critical Patch Updates up to and including July 2009	EAL 4+ ALC_FLR.3	2009-09-16

续表

安 全 目 标	保障级别	认证日期
Oracle Database 11g Enterprise Edition with Oracle Label Security, Release 11.1.0.7 with Critical Patch Updates up to and including July 2009	EAL 4+ ALC_FLR.3	2009-09-16
Oracle Database 11g Standard Edition and Standard Edition One Release 11.1.0.7 with Critical Patch Updates up to and including July 2009	EAL 4+ ALC_FLR.3	2009-10-12
Oracle Database 11g Enterprise Edition with Oracle Database Vault Release 11.1.0.7 with Critical Patch Updates up to and including July 2009	EAL 4+ ALC_FLR.3	2009-10-12

对于组合 TOE 来说，如果它是由一个或多个已评估 IT 产品（TOE 部件）构成，那么允许在 TOE 标识中引用已评估的 TOE 部件名称，但 TOE 标识信息不应该用来误导组合 TOE 消费者：不允许在标识中出现 TOE 部件评估中没有考虑的重要部件或安全功能，同样也不允许在 TOE 标识中出现没有反映出组合 TOE 的安全功能要求的情况。

前面提到，ST 标识和 TOE 标识便于在已评估的 TOE 或产品列表中检索和标识 ST 和 TOE。因此，ST 作者在标识 ST 和 TOE 时可参照国家评估体制或 IT 厂商产品名称等标识规范。

5.3.2 TOE 功能概述

TOE 功能概述的目的是帮助 TOE 潜在消费者通过阅读已评估 TOE 功能概述信息，以找到可能满足他们功能需求的 IT 产品，且是他们的硬件、软件和固件等 TOE 运行环境支持的 IT 产品。

如果 ST 是符合某个 PP 的，则相应 PP 引言的第 2 部分已经包含用作开发 TOE 功能概述的输入信息，如：TOE 通用功能描述、TOE 资源类型和敏感资源列表、TOE 资源的访问控制权限和特权、TOE 安全边界定义等。

TOE 开发者可能在 ST 中简单地重申 PP 中的这些 TOE 功能概述信息。然而，最好的方式是通过分析 TOE 实现技术与机制对 PP 中的 TOE 功能概述提供一些增量的说明，尤其是当 ST 是为一个组合 TOE 编写时。重述 PP 中的信息只是告知 TOE 消费者和评估者 PP 信息的准确适用。相反，在 ST 中进行增量分析表示 PP 中 TOE 功能概述信息已经被开发者分析和评估，并且已经被 ST 编制人员理解。

TOE 功能概述一般包括三部分内容。

（1）TOE 用途：简单描述 TOE 的使用场景和它的重要功能。

（2）TOE 类型：标识 TOE 类型。

（3）TOE 运行环境：标识 TOE 运行所依赖的硬件、软件和固件。

TOE 功能概述为 ST 文档其余部分设置了评估语境。因此，TOE 功能概述通常需要用几个段落对上述 3 部分内容进行描述。TOE 功能概述部分可能列出与这一部分或任一在 ST 中引用的文档相关的 PP/ST。相关的 ST 可能包含同一 TOE 部件部分的其他安全

组件，引用的文档可能包含组织安全规范和安全策略、国家法律法规和 CC 出版物。当然 TOE 功能概述部分应阐述 ST 的内容和结构，包括在 ST 中使用的缩略词、术语等。

1. TOE 用途

ST 编制者需要定义 TOE 的预期用途，包括与外部 IT 实体的依赖关系。这些信息的有些部分可能来自对 PP 里的通用功能描述的分析和 TOE 特定功能行为的组合。

TOE 用途是为 TOE 潜在的消费者编写的，所以 ST 编制人员应依据消费者业务功能需求，使用消费者理解的语言描述 TOE 的用途和重要安全功能。

例如："某数据库 v12.01 是一个用于网络环境的多用户数据库，它允许百万用户同时并发操作数据库中的数据，提供口令、令牌和生物识别等数据库用户认证方式，提供系统宕机、磁盘介质故障等意外故障的数据库恢复功能，提供细粒度访问控制以支持基于标签策略的授权控制，其数据库审计特征可支持一般的数据库安全审计及细粒度安全审计，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 类型

TOE 类型一般通过 TOE 的信息技术来区分不同的 TOE。对于单一的 TOE 或商用现货产品(COTS)产品，业界已经建立了 TOE 类型列表，例如应用级别防火墙、流量过滤防火墙、入侵检测系统、数据库管理系统等。对于组合 TOE 以及 TOE 部件应提供更多的实现机制及相关技术细节，例如 TOE 部件中的技术类型和组合 TOE 框架中执行的具体技术。

有关 TOE 类型可参照 CC 官方网站和各国安全认证体系对 IT 产品的分类进行标识。例如我国针对 IT 产品和信息服务分别发布了 GB/T 25066—2010《信息安全技术 信息安全产品类别与代码》和 GB/T 30283—2013《信息安全技术 信息安全服务 分类》。当然如果不易确定 TOE 所说的类型，此时也可在 ST 中不明确指定 TOE 类型。

在某些情况下，TOE 类型可能误导消费者，示例如下。

(1) 某些 TOE 因为其类型而被预期认为具备某种功能，但是 TOE 却不具有该功能，例如：

① ATM 卡类型的 TOE，但该 TOE 却不支持任何标识和鉴别功能；

② 防火墙类型的 TOE，但该 TOE 却不支持用户使用的各种网络协议；

③ 公钥基础设施(PKI)类型的 TOE，但该 TOE 却没有证书撤销功能。

(2) TOE 因为其类型而被预期运行在某些运行环境中，但该 TOE 达不到这样的要求，例如：

① 个人计算机操作系统型 TOE，该 TOE 要求除非 PC 没有网络连接、软盘驱动器和 CD/DVD 播放器，否则就不能安全工作；

② 防火墙类型的 TOE，该 TOE 要求除非所有能够连接防火墙的用户都是善意的，否则防火墙不能认为是安全工作的。

图 5.5 给出了两个 TOE 类型定义示例：一个是 SQL Server 数据库的，另一个是面向商用现货产品(COTS)的。注意 TOE 类型描述一般不会超过几个段落。

样例 1：SQL Server 2012

1.3.1 产品类型(Product Type)

The product type of the TOE described in this ST is a database management system (DBMS) with the capability to limit TOE access to authorized users, enforce Discretionary Access Controls on objects under the control of the database management system based on user and/or role authorizations, and to provide user accountability via audit of users' actions.

The TOE, which is described in this ST, is the database engine and therefore part of SQL Server 2012. It provides a relational database engine providing mechanisms for Access Control, Identification and Authentication and Security Audit.

样例 2：COTS Security Product

2.1.5 系统类型(System Type)

The XYZ Guard is a network security device that uses the National Security Agency's (NSA) cards to provide multi-level secure(MLS) services to legacy networks, i. e. Internet Protocol (IP) networks that operate in system high mode. XYZ Guard protects enclaves or individual hosts. With in a network, XYZ Guard is in-line between the host and the network. XYZ Guard operates on standard IP datagrams. The XYZ Guard can also serve as a firewall or an in-line encryptor.

图 5.5 TOE 类型定义样例

3. TOE 运行环境

某些 TOE 可能不会依赖其他 IT 系统，但常见的 IT 产品(特别是软件产品)的安全运行需依赖 TOE 外部的硬件、软件或固件。在此情况中，ST 编制者需要在 TOE 功能概述中标识出 TOE 运行环境相关的 IT 硬件、软件或固件。尽管 CC 不要求 ST 编制者完整地，且充分详细地标识出 IT 运行环境信息，但是 CC 还是建议在 ST 中应完整并尽量详细地描述这些信息，以便 TOE 潜在消费者能确定他们使用该 TOE 需要的硬件、软件或固件。

TOE 运行环境所需的硬件、软件、固件等标识示例如下。

(1) 标准 PC，处理器 1GHz 以上，内存 8G 以上，某操作系统运行版本 10.0，更新版本 10b、10c 或 10d，或者版本 11.0。

(2) 标准 PC，处理器 1GHz 以上，内存 512MB 以上，某操作系统运行版本 7.0，更新版本 7d，带 1.0 WM 驱动套件的某图形卡 1.0。

(3) 智能卡 SB2067 集成电路。

(4) 智能卡 SB2067 集成电路，运行某智能卡操作系统 v2.0。

(5) 某办公室局域网等。

5.3.3 TOE 描述

TOE 描述包括 TOE 安全架构及其相关的安全功能行为叙述。TOE 描述是为使评估者和消费者理解 TOE 的安全能力的，它应比第 1 部分引言中的 TOE 功能概述的描述更详细，且 TOE 描述需要说明 TOE 在未来部署中可适用的各种应用环境。CC 建议 TOE 描述需包含体系架构、安全边界与接口、安全功能概述等内容。

1. 体系架构

体系架构代表了 TOE 的组织结构、组成构件和构件间的相互关系，以及构件与外部环

境间的交互关系。TOE 通过对其体系架构的描述，界定各组成部分之间的连接、确定它们不同组件之间的交互机制，并且为后续的 TOE 设计和开发提供指南类的原则。图 5.6 示例了一个关系数据库管理系统体系架构图，它包括一组内存结构组件、后台进程组件以及各组件之间的交互关系，将数据库管理系统的不同功能单元通过这些组件之间定义良好的接口和契约联系起来，对外提供高效的数据组织、存储和检索服务。

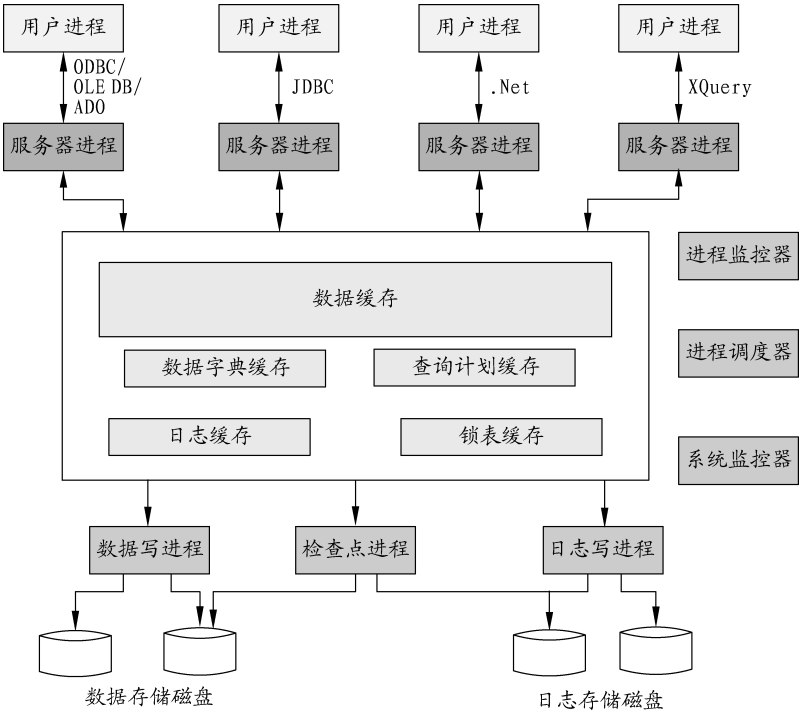

图 5.6　TOE 体系架构样例

不同于 TOE 安全架构(ADV_ARC.1)，TOE 体系架构主要是帮助用户理解资产在 TOE 中的位置及其数据流向。TOE 安全架构定义 TOE 安全功能(TSF)正常运转的语境，是 TSF 展示自保护、域分离、不可旁路等安全属性的集合。

(1) **自保护**是 TSF 用于保护自身的能力，以抵御外部实体可能导致 TSF 改变的操作。没有这些属性，TSF 可能无法执行安全服务。常常有这种情况，TOE 使用其他 IT 实体提供的服务或资源来实现它的功能(例如数据库管理系统的存储依赖它的下层操作系统)。在这些情况中，TSF 不完全凭借自身保护自己，因为它依赖于其他 IT 实体保护其使用的服务。

(2) **域分离**是指 TSF 为每个操作其资源的不可信主动实体创建各自的安全域，并维持域之间彼此分离的机制，防止某个域中的实体在其他实体域中运行。例如，操作系统 TOE 为每个与不可信实体相关的过程提供一个域(地址空间、进程环境变量)。对有些 TOE 来说这样的域是不存在的，因为所有不可信实体的行为都由 TSF 来代理。包过滤防火墙就是此类 TOE 的一个例子，TSF 只维护相关的数据结构，没有不可信实体域这个概念。TOE 安全域依赖于 TOE 类型以及 TOE 的安全功能要求。TOE 若提供针对不可信实体的域，本族要求拥有不可信实体的域要与其他域隔离，以免受其他不可信实体域的干扰(不受 TSF 控制的影响)。

(3) **不可旁路性**是 TSF 安全功能经常调用的一个属性，要求 TOE 特定机制不能被绕过。例如，如果对文件的访问控制被安全功能要求规定为 TSF 的一种功能，那么 TOE 不能存在可直接访问文件的接口(例如原始磁盘访问文件这样的接口)。TSF 自保护使有些 TOE 很自然地依赖它们所处的环境，在 TSF 的不可旁路性中发挥作用。例如，某安全应用 TOE 要求它仅被底层操作系统调用。类似地，防火墙的安全性依赖于这样一个事实，即不存在内部网络和外部网络的直接连接通路，所有它们之间的通信必须通过防火墙。

对 TOE 安全架构的描述解释了 TSF 如何展示以上描述的这些属性。具体地说，它描述安全域如何定义，TSF 之间如何保持隔离，怎么阻止不可信进程获得 TSF 并修改它，怎样确保 TSF 控制之下的所有资源得到充分的保护，以及 TSF 所要满足的安全功能要求相关的所有行为都表现正常。它还会解释所有情况下(例如，假定它的底层环境调用正确，它的安全功能如何被调用?)环境应扮演的角色等。

TOE 安全架构定义了由 TOE 体系架构约束下的 TSF 特性、PP/ST 定义的资源类型和敏感性。如果 ST 是为一个特定安全商业化产品编写，则 TOE 体系架构和安全架构可能是相同的。相对地，如果 ST 是为某个系统的 TOE 部件编写的，则 TOE 体系架构和安全架构之间可能存在区别。

描述 ST 中的系统架构应包括主要硬件和软件(系统和应用)平台、其中的组件和模块及其之间层次结构依赖关系。系统架构应列出这些组件具体的版本号和配置，并且在补充的图表中阐明这些关系。例如在安全目标-SQL Server 架构最后，给出了表 5.5 所示的软硬件配置需求。

表 5.5 软件与硬件配置需求

项 目	配 置 需 求
中央处理器	AMD Opteron, AMD Athlon 64, Intel Xeon with Intel EM64T support, Intel Pentium IV with EM64T support at 1.4 GHz or faster
内存	1GB
硬盘	Approx. 1500 MB of free space
其他	DVD ROM drive, display at Super VGA resolution, Microsoft mouse compatible pointing device, keyboard
操作系统	Windows Server 2008 R2 Enterprise Edition(English) or Windows Server 2012 Standard Edition(English)
支撑软件	.NET Framework 3.5.1SP1/4

2. 安全边界

TOE 安全边界包括 TOE 逻辑和物理两个层面的安全边界描述。评估者使用这一部分信息来决定 TOE 安全配置的范围和边界。因此，需要保证有哪些内容包含在或不包含在 TOE 边界里的精确而简洁的边界描述。

物理安全边界表示应该将构成 TOE 的所有硬件、固件、软件及指南部分在 ST 中进行列表展示。该列表应该在一定程度上使读者对 TOE 物理安全边界有一般性理解：边界内的 IT 实体是在 TSF 控制范围(TSC)内，并且以指定的方式在一定程度上被保护；边界外

的 IT 实体则不在 TSC 里，即不在 TOE 安全评估范围。换句话说物理安全边界是通过确切地声明哪些硬件、固件、软件平台、组件和模块包含与 TSF 实现独立的实例来定义的。版本号、配置选项、交互接口、系统应用、初始化参数、应用程序模块等都应该通过列表方式给出。另外，应描述 TSF 接口（TSFI）——通过什么接口［人机界面或应用程序接口（API）］访问 TOE 保护的各种资源或者以什么方式获取相关的信息。实质上，TOE 安全描述中的物理安全边界定义附加了在 TOE 体系架构部分里提供信息的其他层次的交互细节。

逻辑安全边界的定义与 TOE 安全服务或安全功能相关。通过对 TOE 提供的安全功能描述，使读者获得对 TOE 安全服务的一般性理解。该描述应该比 TOE 功能概述中描述的重要安全功能更加详细。通常包含以下内容。

（1）讨论哪些安全服务会被物理安全边界内的 IT 实现提供。

（2）按照与功能类名相同的标准给这些功能或服务分组，例如安全审计、用户数据保护、鉴别与认证、安全管理等。

TOE 物理边界和逻辑边界需要以一种无歧义的方式描述 TOE 安全功能，明确哪些组成部件或安全功能在 TOE 之内，哪些部件或功能在 TOE 之外。当 TOE 与非 TOE 实体联系在一起并且不能轻易将它们分离时这显得尤其重要。

界定 TOE 与非 TOE 实体的特殊示例如下。

（1）TOE 是智能卡 IC 的密码协处理器，而不是整个 IC。

（2）TOE 是除了密码处理器之外的智能卡 IC。

（3）TOE 是某防火墙 v18.5 的网络地址转换部件。

本部分的最后，一般会给出哪些内容不包含在 TOE 安全边界里的一个声明。例如：

在 TSF 定义范围外的软件和硬件安全功能不会被评估，包括：［由开发者提供的列表］。

表 5.6 举例说明了物理和逻辑安全边界的部分定义。

表 5.6　TOE 安全边界定义

例 1：物理安全边界

2.3　安全边界

2.3.1　物理边界

表 1 里描述的条目是在 TOE 物理安全边界内。

表 1：TOE 物理安全边界定义

TOE	组件/模块
工作站	• 英特尔 I7 处理器 • 8GB RAM • 2T 硬盘 • CD-RW 驱动器 • 键盘 • 鼠标 • 串行端口 • 2 个 USB 端口

续表

TOE	组件/模块
工作站	• 15 英寸，高分辨率平板彩色监视器 • 电源线 • 2 个 1000Mb/s 以太网接口 • 微软 Windows Server 操作系统专业版 • 文件系统 • 安全子系统 • 事件日志服务 • 注册表服务 • Office 2017

例 2：逻辑安全边界

2.3 安全边界

2.3.2 逻辑边界

2.3.2.1 用户数据保护

FTP 和 Telenet 安全服务器向不正确的服务请求提供认证和保护，而 HTTP 和 SMTP 安全服务器提供应用级别保护。模块 A 确保一旦会话完成，前一会话里的数据包包含的信息不再可以访问。管理数据包存储和处理来确保没有残留信息会被传入之后的会话。模块 B 通过应用 TSP 规则执行检验过程。模块 C 作出关于每个包是否应当被接受、拒绝或放弃的决定。

3. 安全功能

TOE 描述的第 3 部分是安全功能概述，概述的目的是向 TOE 的潜在消费者提供 TOE 预期的安全行为描述。本部分应该提供 TOE 安全功能实现技术与机制，描述的详细程度应该使潜在消费者能够充分理解 TOE 安全功能的一般行为及其运行机制。

5.4 符合性声明

符合性声明编制的基本要求是保证 ST 内容是完整的、清晰的和无歧义的，以使 ST 的评估符合 CC 相关要求。ST 是支撑 TOE 评估的基础材料，对 ST 中任一指定的符合性声明其追溯过程应该清楚。

符合性声明包括：

- CC 版本；
- PP(如果有)；
- 包(如果有)。

ST 与 CC 符合性描述由两项组成：使用的 CC 版本以及 ST 是否包含扩展安全要求。在包含扩展安全组件情况下，新组件(扩展组件)必须在 ST 的第 5 部分明确定义，必须使用类似于 CC 第 2 部分和第 3 部分标准组件结构的方式定义扩展组件：保证其清晰、明确和可以评估。

PP 和包符合性声明应说明和解释一个 ST 和被引用的 PP 和包之间的符合程度，可以是无，也可以是完全符合。所有的 PP 和包符合性声明必须通过充分解释，说明并论证其原理。

ST 读者，不管是 TOE 消费者还是 TOE 评估者，都需要在 ST 的第 3 部分之前先对引用的 PP 和包有一定认识才能正确地理解和解析 ST 所包含的全部内容。因此，把 PP 和包符合性声明作为 ST 的第 2 部分是合理的。表 5.7 是两种主流商业化数据库管理系统安全目标的符合性声明示例。

表 5.7　ST 符合性声明样例

样例 1：SQL Server 2012

2　符合性声明

2.1　CC 符合性声明

本安全目标符合

- CC 标准第 2 部分(版本 3.1，修订 3)扩展，原因是使用了 FAU_STG_EXP.5 扩展组件。
- CC 标准第 3 部分(版本 3.1，修订 3)EAL 4＋，原因是增强了 ALC_FLR.2 保障组件。

2.2　PP 符合性声明

本保护轮廓符合严格符合：

- 美国政府数据库管理系统保护轮廓(BR-DBMSPP)，版本 1.3，2010 年 12 月 24 日。

样例 2：**DB2**

2　符合性声明

本安全目标符合 CC 标准第 2 部分(版本 3.1，修订 4)扩展和 CC 标准第 3 部分(版本 3.1，修订 4)EAL 4＋＋，增加了 ALC_FLR.3 保障组件。

本安全目标符合下列保护轮廓和扩展包：

- [OSPP]：操作系统保护轮廓，版本 2.0，2010 年 6 月 1 日；严格符合。
- [OSPP-EIA]：OSPP-标识和鉴别扩展包，版本 2.0，2010 年 5 月 28 日。
- [OSPP-LS]：OSPP-标签安全扩展包，版本 2.0，2010 年 5 月 28 日。

这些保护轮廓及其扩展包可从 BSI Web 站点下载（认证标识 ID BSI-CC-PP-0067-2010）。

对 PP 符合性声明一般包含 4 个子部分：PP 引用、PP 裁剪、PP 增加和符合性说明。

5.4.1　PP 引用

PP 引用部分列出了 ST 参考的 PP 信息，包括 PP 全称、版本号、发布日期等信息。ST 中的 PP 符合性声明可能有 5 种场景。

(1) **无参考 PP**：没有声明 PP 符合性。ST 编制者必须在 ST 的第 3 到第 6 部分明确定义安全问题、安全目的和安全要求；相应地，有关 PP 符合性声明的 PP 裁剪(5.4.2 节)和 PP 增加部分(5.4.3 节)将在本部分省略掉。

(2) **完全符合**：也称为严格符合。ST 编制者应列出安全符合的 PP，并在 ST 的第 3 到第 6 部分仅引用符合性声明 PP 中的部分安全问题、安全目的和安全要求，而不一定需要在 ST 中重新定义这些内容。对于完全符合的 PP，有关 PP 符合性声明的该引用 PP 裁剪(5.4.2 节)和该 PP 增加部分(5.4.3 节)将在本部分省略掉。

(3) **仅对 PP 进行裁剪**：列出符合的 PP，并对引用 PP 的安全问题、安全目的或安全要求进行部分裁剪。ST 编制者应重点突出对 PP 引用第 3 到第 6 部分的裁剪内容。PP 符合

性声明的5.4.2子部分被包含并用来阐述和证明裁剪合理性。

(4) **仅对PP进行增加**：列出符合的PP，并列出增加的安全问题、安全目的或安全要求。ST编制者应重点突出对PP引用第3到第6部分增加的内容。PP符合性声明的5.4.3子部分被包含来阐述和证明增加内容的合理性。

(5) **部分操作**：列出符合的PP，并对PP组件元素操作的符合性进行说明。这一场景仅在PP是针对某个组合TOE和ST反映的某个TOE部件时有效。为组合TOE的个体或TOE部件声明部分符合性是无效的。注意，部分操作中对PP所有裁剪和增加都应当被重点突出概述，PP符合性声明的5.4.2和5.4.3子部分应当被包含来阐述和证明裁剪或增加的合理性。

“无参考PP”和“完全符合”的PP引用场景互相排斥，但“仅对PP进行裁剪”和“仅对PP进行增加”这两个场景不互相排斥。“部分”场景也可能不包含“仅对PP进行裁剪”和“仅对PP进行增加”。例如SQL Server 2012 EAL 2＋安全目标没有引用任何PP，而SQL Server 2012 EAL 4＋明确指出它严格符合U.S. Government Protection Profile for Database Management，Version 1.3(BR-DBMSPP)。

5.4.2 PP裁剪

这一部分指明引用PP第3部分的安全问题，第4部分的安全目的或第6部分的安全要求在ST中被裁剪或客户化定制的情况，包括第5部分扩展组件定义裁剪或自定义情况。ST中安全要求的有效裁剪选项主要是对PP里安全组件元素没有执行过元素操作的进行操作，例如“赋值”“选择”“细化”“反复”。ST编制者应在这部分提供执行了哪些组件元素的裁剪以及为什么执行这些裁剪的说明。

5.4.3 PP增加

这一部分指明了ST里包含但不在引用PP里所包含的安全问题、安全目的或安全要求。ST编制者应在这部分解释考虑了PP中未包括的哪些安全问题，衍生出了哪些新的安全目的，并增加了什么要求以及为什么做这些增加。表5.8介绍了一个PP符合性声明示例。

表5.8 PP符合性声明示例

2.2 PP符合性声明 这一部分介绍了PP符合性声明 2.2.1 PP引用 这一安全目的符合以下的PP： • 针对低-风险环境，U.S. DoD，版本1.d.1(草案)9，1999的应用级别防火墙PP。 声明的符合性程度： • 部分操作 2.2.2 PP裁剪 下表所列的SFR和SAR从引用的PP裁剪而来。

续表

裁剪的项	裁剪动作	证　明
FAU_GEN.1	细化	需要指明(1)审计需求是最小、基本、详细还是未指明；(2)审计里包含的项
FAU_SAR.3+1 FAU_SAR.3+2	细化和反复	需要阐明 TOE 应当能够：(1)进行用户身份、推测对象、日期范围、时间范围和 IP 地址范围的检索；(2)基于时间顺序或发生排序审计数据
AVA_VAN.1	细化	需要指明必须进行分析的被评估 TOE 的最小已识别漏洞
7.3 PP 增加 以下所列的 SFR 被添加到引用的 PP 里进行声明。		
增加的项	证　明	
FIA_UAU.5	引用的 PP 指明了两个验证机制(重用和单用)需求的一些特殊性，这两个验证机制可能通过 FIA_UAU.1 和 FIA_UAU.4 SFR 来要求。然而，不能仅提供一个 SFR 来指明可能被使用的验证机制的类型，或者需要使用它们的条件	

5.4.4　符合性原理

符合性声明列出了 ST 声称符合的 CC 组件包(如 PP)。这方面的解释见 CC 第 1 部分的符合性要求。因此，在 ST 符合性声明的最后应陈述 ST 符合性声明的论据，并应通过第三方机构按照 CEM 对 ST 声明的有效性进行评估。ST 和引用的 PP 之间的符合性通过以下列表来证明。

(1) 所有的 PP 安全目的都包含在 ST 里。

(2) 所有的 PP 安全目的的细化和增加都是有效的。

(3) 所有的 PP 安全要求都包含在 ST 里。

(4) 所有的安全功能和安全保障组件元素的“赋值”“选择”“细化”“反复”操作都是有效的。

如果 ST 中第 8 部分的 TOE 概要规范(TSS)对 PP 声明是“无参考 PP”，PP 符合性声明的 5.4.4 这一部分被标记为“不适用”(即 ST 中没有这一节)。如果 TSS 对 PP 声明是“完全符合”，PP 原理应是准确的并且 TOE 开发者在 ST 中响应了第 1 和第 3 项。如果 TSS 的 PP 声明是“仅对 PP 进行裁剪”、“仅对 PP 进行增加”或“部分操作”，那么需要更多细节进行说明，并且 TOE 开发者在 TSS 中要对上述 4 项要求进行解释。

5.5　安全问题定义

安全问题定义描述 TOE 安全功能和安全控制范围。ST 安全问题定义应反映其所引用的 PP 所提及的安全应用环境。PP 与 ST 这两个文件之间的安全问题内容差异来自于这样的事实：一般来讲 TOE 消费者主导编制的 PP 是独立于 IT 产品的具体实现；而 TOE 开发者主导编制的 ST 却是依赖于 TOE 实现技术与机制的。

和 PP 安全问题定义结构一样，ST 中安全问题定义包括假设、威胁和组织安全策略。

注意，按照 CC 第 1 部分附录 A 的 ST 结构，并不是 PP 中所列的所有安全问题均需再次陈述。对于物理上是分布式部署的 TOE，ST 作者最好是针对 TOE 运行环境的不同 TOE 部件，分开讨论相关威胁、组织安全策略和假设。

如同第 4 章 PP 中的安全问题定义一样，涉及 TOE 安全问题的定义是领域相关的，也就是说面向 TOE 安全问题定义的推理过程超出了 CC 的范围。所以安全问题的定义应该借助领域专家在 TOE 威胁分析方法与技术的经验，基于 5.3.3 节 TOE 描述的安全架构和安全边界定位资产面临的安全风险进行分析。当然我们应该注意到，安全评估结果的有效性对 ST 依赖性很强，且 ST 的有效性对安全问题定义的依赖性也很强。因此，ST 作者应花费有效资源并使用良好定义的过程分析推导出 TOE 安全问题。

安全问题开头部分应解释 TOE 管理的资产。表 5.9 是数据库领域两个 ST 引言部分的样例，SQL Server 数据库直接以威胁主体和数据资产介绍数据库面临的安全问题，而 DB2 数据库则概括了 ST 及其所引用的 PP 第 3 部分之间的相互关系。

表 5.9 ST 安全问题定义引言部分样例

样例 1：SQL Server 2012

3.1 资产

与 TOE 交互的下列外部实体：

- 管理员：管理员被授权来完成管理操作和使用管理功能。
- 用户：使用 TOE 的人员。
- 攻击者：攻击者是任何试图破坏 TOE 操作，以便非法获得受 TOE 保护的资产访问权限的人员。

TOE 维护两种类型的数据资产：用户数据和 TSF 数据。作为主要资产的用户数据包括以下几部分：

- 作为数据对象存储的用户数据；
- 由 DBMS 维护的用户开发的查询(各种视图)和存储过程/函数。

次要资产包括 TSF 数据和 TOE 自身运行所需维护和使用的数据。这种类型的数据称为元数据，具体包括：

- 用户数据库和数据库对象定义；
- DBMS 配置参数；
- 用户安全属性；
- 安全审计指令和记录等。

样例 2：DB2

3.1 引言

安全问题定义描述 TOE 预期使用和部署方式的安全环境。为此，TOE 安全环境需标识包括物理和程序性规范、产品预期使用方法等假设，定义产品设计面临的威胁和组织计划采用的安全策略。

本安全目标符合基本操作系统保护轮廓[OSPP]，包括其标识和鉴别扩展包[OSPP-EIA]和标签安全扩展包[OSPP-LS]。这个保护轮廓资产、假设、威胁和组织安全策略被假设适用于本安全目标，包括 z/OS 安全目标[ZOSST]在 3.1 节至 3.4 节定义的扩展部分。在下列章节，只有不同于上述这些章节的扩展被列出。引用没有扩展的章节也是为了保证本安全目标的完整性。

5.5.1 假设

在一个 ST 里，开发者需要向 TOE 消费者和评估者证实 ST 符合性声明里的 PP 假设(或它们的一个变种)。一般来讲，假设是关于 TOE 预期用途、运行环境和 TOE 连通性，包

括预定义的角色和责任等方面的内容。所有与 TOE 运行环境约束和操作限制相关的内容都应通过假设被指明。因此,假设一般通过 IT 环境因素来保证。

像 PP 一样,ST 中的假设不能被用来减轻 TOE 威胁。ST 编制者有 4 个关于使用 PP 中假设的选项。

(1) PP 中假设可能只是简单地被逐字重申。

(2) PP 中假设可能被修改或裁剪来反映 TOE 实现细节。

(3) 新的假设可能被添加至 ST。

(4) 如果 PP 中假设不合适或不适用,那么它们可能不被采用。

表 5.10 展示了 SQL Server 数据库和 Oracle 数据库示例 ST 假设。SQL Server 数据库直接引用 PP 中的假设;但 Oracle 数据库示例 ST 在引用 PP 的假设的基础上,只是明确了添加的几个特定假设。

表 5.10　ST 假设

样例 1:SQL Server 2012

3.2　假设

下表列出了 TOE 环境的所有假设。这些假设直接采用参考的 PP,而没有做任何修改。

假　　设	描　　述
A. NO_EVIL	管理员是诚实的、经过培训的,并且遵循所有管理指南
A. NO_GENERAL_PURPOSE	在数据库服务器上没有安装其他获得通用的计算或存储能力的程序或服务(例如:编译器、编辑器或应用程序)
A. PHYSICAL	数据库服务器运行环境应提供与其所管理的数据价值相一致的物理安全。例如存储在数据库之外的评估对象相关数据(如配置参数、归档日志等)以一种安全的方式存储和管理

样例 2:Oracle 11g r2

3.2　假设

除了[BR-DBMSPP]第 3.3 节假设,本 ST 增加了下列假设,以反映 TOE 体系结构:

A. MIDTIER 在多层应用环境中为了确保评估对象的安全问责制,任意中间层次的评估对象运行环境组件服务都应将原始的授权用户标识发送给 TSF(ST 作者应根据数据库管理系统针对的具体应用解决方案解释"多层应用问责"的具体含义)。

A. DIR_PROTTOE 所使用的目录服务器(如 LDAP)提供保护机制,防御针对存储在目录中的 TSF 数据的非授权访问,包括存储在目录中的 TSF 数据受访问控制机制保护,存储在目录中的 TSF 数据被管理人员合理地管理,并且目录服务器及其网络连接从物理和逻辑上都免于非授权人员的访问和干扰。

A. DIR_MGMT 企业授权用户应正确地管理存储在目录服务器中的企业用户信息(口令验证码、口令策略、角色和权限)。

A. COM_PROT 假定数据库服务器和应用终端之间、分布式数据库不同节点间的通信信道是安全可靠的(如满足私密性和完整性)。实现方式可通过共享密钥、公/私钥对,或者利用存储的其他密钥来产生会话密钥。

A. CLIENT_AP 客户端应用应依照 Oracle 应用开发文档正确地开发和部署,不使用未文档化的 TOE 客户端编程接口。

注意，在 CC 测试实验室的 TOE 评估期间，这些假设均被认为是真实的，即它们不会以任何方式被 TOE 评估者测试和验证。出于这些理由，我们只能对 TOE 的这些运行环境安全做假设。由于 TOE 评估的目的是检验 TOE 本身安全行为的正确性和防护措施的充分性，不是通过 TOE 假设断言是否真实来完成的，所以 PP/ST 编制者不应对 TOE 本身的安全行为做假设。

5.5.2 威胁

第 4 章第 4.5.2 节定义了 TOE 的潜在威胁，确定了它们发生的可能性和后果的严重程度。ST 编制者可以简单地重申 PP 中的这些信息。然而，最好是结合 TOE 实现技术与机制等对 TOE 潜在的威胁执行一些增量分析，特别是针对组合 TOE 的 ST，应该对组成 TOE 的每个 TOE 部分标识出潜在的安全威胁。

第 4 章表 4.12 详细列举了 PP 中一个组合 TOE 里分层的潜在威胁列表。该表可作为 ST 编制者进行安全威胁分析的输入，以决定哪些威胁是由 ST 里定义的 TOE 安全架构考虑。哪些由 ST 里定义的 TOE 安全问题考虑。

表 4.12 列出的 PP 里每个威胁都属于这两个分类里的一个。第一种威胁的合理性在 PP/ST 的安全要求原理中详细解释。除此之外，ST 编制者也可能识别 PP 中没有列出的新的潜在威胁。表 5.11 使用第 4 章的表 4.12 作为输入举例说明了这一过程。

表 5.11 TOE 和 TOE 环境面临的威胁（参考 Herrmann 2002）

编号	威　　胁	TOE	TOE 环境
T_1	**未检测出的资产威胁可能来自于以下事件**		
T_{1a}	授权用户执行了他未被授权的操作	X	
T_{1b}	攻击者（内部或外部人）伪装成一个授权用户尝试执行未被授权的操作	X	
T_{1c}	攻击者（内部或外部人）通过冒充授权用户访问未经授权的资源和信息	X	X
T_{1d}	授权或未经授权用户无意或故意阻止组织员工访问 TOE	X	X
T_{1e}	未经授权的用户获得了 TOE 控制权	X	X
T_{1f}	未经授权的用户将 TOE 设置为不可操作	X	X
T_{1g}	未经授权的用户试图绕过 TOE 的安全控制	X	
T_{1h}	未经授权的用户试图猜测身份标识及其验证数据	X	
T_{1i}	未经授权的用户通过欺骗等手段获得和使用有效的身份标识及其验证数据	X	
T_{1j}	未经授权的用户或外部 IT 实体查看、修改和删除传输到远程授权用户或管理员的安全相关信息	X	
T_2	**授权用户在未获得管理员许可情况下访问该信息或资源**	**X**	**X**
T_3	**攻击者可以窃听或用其他方式获取通过网络传播的数据**		
T_{3a}	未经授权的用户进行流量分析		X
T_{3b}	授权或未经授权的用户使用之前信息流的残余信息	X	
T_4	**授权或未授权用户通过消耗全局资源方式以阻止其他授权用户访问或使用这些资源**		
T_{4a}	借助网络/线路阻塞（声音或数据）		X
T_{4b}	借助服务拒绝（DoS）和分布式服务拒绝（DDoS）攻击（声音或数据）	X	X
T_{4c}	盗窃资源服务		X
T_5	**用户可能有意或无意地传输敏感信息给不允许看到它的用户**	**X**	

续表

编号	威　　胁	TOE	TOE 环境
T_6	**用户可能或者以发送者或者以接收者的身份参与到信息传输，随后否认这样的行为**	**X**	
T_7	**授权用户可能以软复制或者硬复制的方式导出信息，随后接受者以不符合指定安全敏感的方式处理这些信息**	**X**	**X**
T_8	**信息的完整性和可用性可能由于以下原因被削弱**		
T_{8a}	用户错误、固件错误、硬件错误或传播错误	X	X
T_{8b}	由攻击者的未经授权的修改或破坏的信息	X	X
T_{8c}	人为错误或软件、固件、硬件或电力供应故障造成突然中断操作，导致关键数据的损失或损坏	X	X
T_{8d}	存储介质老化或不当储存或不当处理存储介质		X
T_{8e}	一个授权用户无意中将病毒引入系统	X	X
T_{8f}	一个授权用户能将未经授权的软件引入到系统中		X
T_{8g}	授权或未经授权用户插入恶意代码或使用后门	X	X
T_{8h}	一个未经授权的人浏览、修改或破坏安全关键配置信息	X	
T_{8i}	未能执行足够的系统冗余或数据备份		X
T_{8j}	偶然或者蓄意删除	X	X
T_{8k}	插入伪造数据	X	X
T_{8l}	对数据进行未经授权的修改	X	X
T_9	**攻击者可能在某用户希望其对资源或服务的合法使用保密的情况下，观察该用户对资源或服务的使用情况**	**X**	**X**
T_{10}	**一个授权用户可能有意或无意地观察存储用户未授权的信息**		**X**
T_{11}	**安全关键组件可能受到物理攻击和(或)运行环境故障的影响，从而危及安全**		**X**
T_{12}	**已授权的内部用户或未经授权的局外用户可能会无意或故意导致安全相关的事件不被记录或可追溯**		
T_{12a}	丢失或覆盖合理的审计记录	X	
T_{12b}	审计记录不能与发生时间关联	X	
T_{12c}	审计记录不能与实际活动关联	X	
T_{12d}	人们可能因为审计记录不被审阅而不会为自己的行为负责	X	
T_{12e}	对用户或系统资源的危害可能在很长一段时间内未被发现	X	X
T_{13}	**体系架构、设计、实现、操作或维护中的脆弱性可能导致安全机制失效**	**X**	**X**
T_{14}	**已授权的内部用户或未经授权的局外用户可能会导致不当重启和(或)从失败的硬件、软件或固件的不当恢复，而导致安全危害**	**X**	**X**
T_{15}	**运行环境的变化可能会引入或暴露漏洞**		**X**
T_{16}	**一个知识渊博的攻击者可能绕过应对策略和缓解策略中意想不到的局限性或潜在缺陷**	**X**	**X**
T_{17}	**访问控制权和访问特权的定义、实现和强制访问可能以破坏安全性的方式完成**	**X**	
T_{18}	**自然灾害、战争行为或恐怖主义可能导致关键操作被中断或停止**		**X**
T_{19}	**资产的危害可能由管理员或其他特权用户的粗心，故意忽视或恶意执行导致**		
T_{19a}	硬件、软件和固件的操作不当	X	X

续表

编号	威　　胁	TOE	TOE 环境
T_{19b}	网络或语音电路故障		X
T_{19c}	过早关闭永久虚拟电路(PVC) 或虚拟专用网络(VPN)		X
T_{19d}	操作安全(OPSEC)程序规程不足		X
T_{19e}	操作安全(OPSEC)程序规程写得不严谨		X
T_{19f}	用户和管理员不熟悉安全操作(OPSEC)程序规程		X

第 4 章的表 4.12 已经为每个威胁分配了一个减轻风险的优先级。ST 编制者可以表 4.12 作为识别 ST 威胁的输入，分析 TOE 安全架构设计方案(技术、操作或规范)部署后的每个威胁潜在的安全风险。本质上，这种安全风险分析是对 TOE 开发者给出的安全架构鲁棒性、可恢复性等设计解决方案的评估。从 CEM 看，只有做出了这样的评估，ST 的概要规范原理解释部分才会基于这些评估说明其安全要求的合理性。表 5.12 使用第 4 章的表 4.12 作为输入举例说明了这一过程。表中有关风险程度说明参见第 4 章的 4.5.2 节内容。

表 5.12　ST 威胁残余风险评估(参考 Herrmann 2002)

编号	威　　胁	后果 严重性	发生 可能性	风险减低 优先级	残留 风险
T_1	**未检测出的资产威胁可能来自于以下事件**				
T_{1a}	授权用户执行了他未被授权的操作	一般～关键	偶尔	高	低
T_{1b}	攻击者(内部或外部人)伪装成一个授权用户尝试执行未被授权的操作	一般～关键	偶尔	高	低
T_{1c}	攻击者(内部或外部人)通过冒充授权用户访问未经授权的资源和信息	一般～关键	偶尔	高	低
T_{1d}	授权或未经授权用户无意或故意阻止组织员工访问 TOE	一般～关键	偶尔	高	低
T_{1e}	未经授权的用户获得了 TOE 控制权	一般～关键	很少	中至高	低
T_{1f}	未经授权的用户将 TOE 设置为不可操作	一般～关键	很少	中至高	低
T_{1g}	未经授权的用户试图绕过 TOE 的安全控制	一般～关键	频繁	中至高	低
T_{1h}	未经授权的用户试图猜测身份标识及其验证数据	一般～关键	频繁	中至高	中
T_{1i}	未经授权的用户通过欺骗等手段获得和使用有效的身份标识及其验证数据	一般～关键	很有可能	中至高	低
T_{1j}	未经授权的用户或外部 IT 实体查看、修改和删除传输到远程授权用户或管理员的安全相关信息	一般～关键	偶尔	中至高	低
T_2	**授权用户在未获得管理员许可情况下即访问该信息或资源**	一般～关键	很少	中	低
T_3	**攻击者可以窃听或用其他方式获取通过网络传播的数据**				
T_{3a}	未经授权的用户进行流量分析	一般	很少	低	低
T_{3b}	授权或未经授权的用户使用之前信息流的残余信息	一般	很少	低	低

续表

编号	威　　胁	后果 严重性	发生 可能性	风险减低 优先级	残留 风险
T_4	**授权或未授权用户通过消耗全局资源方式以阻止其他授权用户访问或使用这些资源**				
T_{4a}	借助网络/线路阻塞（声音或数据）	一般～灾难	很少	高	低
T_{4b}	借助服务拒绝(DoS)和分布式服务拒绝(DDoS)攻击(声音或数据)	一般～灾难	很少	高	低
T_{4c}	盗窃资源服务	一般～灾难	很少	高	低
T_5	**用户可能有意或无意地传输敏感信息给不允许看到它的用户**	一般～关键	很少	中	低
T_6	**用户可能或者以发送者或者以接收者的身份参与信息传输，随后否认这样的行为**	一般	很少	低	低
T_7	**授权用户可能以软复制或硬复制的方式导出信息，随后接受者不符合指定安全方式处理这些信息**	一般～关键	偶尔	高	低
T_8	**信息的完整性和可用性可能由于以下原因被削弱**				
T_{8a}	用户错误、固件错误、硬件错误或传播错误	一般～灾难	偶尔	高	低
T_{8b}	由攻击者的未经授权的修改或破坏的信息	一般～灾难	很少	中	低
T_{8c}	人为错误或软件、固件、硬件或电力供应故障造成突然中断操作，导致关键数据的损失或损坏	一般～灾难	很少	中	低
T_{8d}	存储介质老化或不当储存或不当处理存储介质	一般～灾难	很少	中	低
T_{8e}	一个授权用户无意中将病毒引入系统	一般～灾难	频繁	高	中
T_{8f}	一个授权用户能将未经授权的软件引入到系统中	一般～灾难	频繁	高	中
T_{8g}	授权或未经授权用户插入恶意代码或使用后门	一般～灾难	偶尔	中	低
T_{8h}	一个未经授权的人浏览、修改或破坏安全关键配置信息	一般～灾难	偶尔	中至高	低
T_{8i}	未能执行足够的系统冗余或数据备份	一般	偶尔	中	低
T_{8j}	偶然或者蓄意删除	一般～关键	偶尔	中至高	低
T_{8k}	插入伪造数据	一般～关键	偶尔	中至高	低
T_{8l}	对数据进行未经授权的修改	一般～关键	偶尔	中至高	低
T_9	**攻击者可能在某用户希望其对资源或服务的合法使用保密的情况下，观察该用户对资源或服务的使用情况**	一般～关键	偶尔	高	低
T_{10}	**一个授权用户可能有意或无意地观察存储用户未授权的信息**	一般～关键	偶尔	中	低
T_{11}	**安全关键组件可能受到物理攻击和(或)运行环境故障的影响，从而危及安全**	不重要～灾难	几乎 不可能	低	低
T_{12}	**已授权的内部用户或未经授权的局外用户可能会无意或故意导致安全相关的事件不被记录或可追溯**	一般～灾难	很少	中	
T_{12a}	丢失或覆盖合理的审计记录	一般～灾难	很少	中	低

续表

编号	威　　胁	后果 严重性	发生 可能性	风险减低 优先级	残留 风险
T_{12b}	审计记录不能与发生时间关联	一般～灾难	很少	中	低
T_{12c}	审计记录不能与实际活动关联	一般～灾难	很少	中	低
T_{12d}	人们可能因为审计记录不被审阅而不会为自己的行为负责	一般～灾难	很少	中	低
T_{12e}	对用户或系统资源的危害可能在很长一段时间内未被发现	一般～灾难	很少	中	低
T_{13}	**体系架构、设计、实现、操作或维护中的脆弱性可能导致安全机制失效**	一般～关键	很少	中	低
T_{14}	**已授权的内部用户或未经授权的局外用户可能会导致不当重启和(或)从失败的硬件、软件或固件的不当恢复，而导致安全危害**	一般～关键	很少	中	低
T_{15}	**运行环境的变化可能会引入或暴露漏洞**	一般～关键	很少	低	低
T_{16}	**一个知识渊博的攻击者可能绕过应对策略和缓解策略中意想不到的局限性或潜在缺陷**	一般～关键	很少	中	低
T_{17}	**访问控制权和访问特权的定义、实现和强制访问可能以破坏安全性的方式完成**	一般～关键	很少	中	低
T_{18}	**自然灾害、战争行为或恐怖主义可能导致关键操作被中断或停止**	一般～灾难	几乎 不可能	低	低
T_{19}	**资产的危害可能由管理员或其他特权用户的粗心，故意忽视或恶意执行导致**				
T_{19a}	硬件、软件和固件的操作不当	一般～灾难	很少	中	中
T_{19b}	网络或语音电路故障	一般～灾难	很少	中	低
T_{19c}	过早关闭永久虚拟电路(PVC)或虚拟专用网络(VPN)	一般～灾难	很少	中	低
T_{19d}	操作安全(OPSEC)程序规程不足	一般～灾难	很少	中	低
T_{19e}	操作安全(OPSEC)程序规程写得不严谨	一般～灾难	很少	中	低
T_{19f}	用户和管理员不熟悉操作安全(OPSEC)程序规程	一般～灾难	很少	中	中

5.5.3 组织安全策略

本部分引用 4.5.3 节 PP 定义的组织安全策略(OSP)。OSP 包括 TOE 安全操作相关的规则、规范，以及一个机构为了保护其资产而推行的一系列 TOE 安全操作指南。依据行业、国家或是国际相关的法律法规都可推导出新的 OSP。为了遵循这样的法律法规的正确版本，给出 OSP 引用的出处对于 IT 产品消费者和评估者理解是很有用的。

OSP 对每个组织的使命和资产来说都是相当重要的。TOE 消费者是这些 OSP 的拥有者。因此，ST 编制者只能在 PP 规定的 OSP 基础上执行规定的操作。

(1) OSP 可能简单地只是逐字重申 PP 中相应的规则、规范或指南。

(2) 只要原始意图不变，ST 中的 OSP 可以为了贴近 TOE 的实现细节而进行定制。

引用 PP 中的 OSP 在 ST 中是不能够随意增加或是删除的。为了能够更加清晰，ST 中的 OSP 是可以被指定给 TOE 或是 TOE 环境。如果 ST 是描述一个组件 TOE，那么只有适用于这个 TOE 部件的 OSP 才是必须进行明确说明的。

5.6 安全目的

ISO/IEC TR 15446 技术报告并不建议 ST 编制者盲目地重复叙述 PP 中已经描述的安全目的，TOE 开发者应当结合其具体的 IT 产品体系架构、安全架构和安全功能实现技术与机制，充分地分析 PP 中的每个安全目的以做出以下决定。

(1) 确认 PP 描述的每个安全目的在 ST 第 4 部分是否仍有效。如果是，安全目的应当被一字不差地复制到 ST 中。如果不是，这一安全目的应当被删除、修改、重新分配或重新分类。

(2) 是否应当添加一个新的安全目的？

通常，PP 文档中 TOE 安全目的一般应在 ST 相应结构部分重复出现，但 ST 编制者需要结合 TOE 具体实现技术与机制对 PP 中的安全目的进行必要的修改，以保持与 ST 中 TOE 描述部分相关细化内容一致。但是，如果 PP 中定义的一些安全目的不再合适或与 TOE 开发者在 ST 中建议的安全方案不兼容，那么这些安全目的在 ST 中应被删除或需结合 ST 安全架构的具体细节进行重写。相对于 ST 所引用的 PP，如果在 ST 的第 3 部分有添加或裁剪的假设、威胁或组织安全策略，也可能需在 ST 中添加一些新的安全目的。另外，按照 TOE 安全目的是为了对抗潜在的威胁或满足 TOE 使用者的组织安全策略，ST 中的安全目的也细分为预防、检测或纠正等类型。因此，其他为适用于 TOE 或 TOE 环境而定义的安全目的，也应该依据需要细分为预防、检测或纠正安全目的。

ST 安全目的的作用有三方面。

(1) 为 TOE 安全问题提供高层的、以自然语言描述的安全方案：安全目的使用自然语言描述，这一抽象层次对于知识丰富的 TOE 潜在消费者而言将会是清晰和可理解的。

(2) 将安全方案分为两类，分别称为 TOE 安全目的和 TOE 运行环境安全目的，以反映出这个解决方案是由 TOE 本身实现、TOE 运行环境提供还是由 TOE 和 TOE 运行环境一起提供。

(3) ST 中的安全目的的原理说明证实上述两种安全方案构成了一个对 PP/ST 中 TOE 所有安全问题的完整解决方案。

5.6.1 TOE 安全目的

TOE 安全目的是解决 ST 文档中第 3 部分定义的 TOE 相关威胁和组织安全策略，由 TOE 本身应该实现的安全目标陈述组成。

TOE 安全目的示例如下。

(1) TOE 应保证在它和网络服务器或其他 IT 系统之间所传输数据或文件内容的保密性和完整性。

(2) 在允许 TOE 用户访问 TOE 提供的传输服务之前，TOE 应该标识和鉴别这个用户。

(3) TOE 应该根据 ST 附录 3 中描述的数据访问策略，通过它的数据访问引擎限制鉴别用户对相关数据资源的访问。

如果 TOE 在部署上是物理分布的，最好将 ST 中的 TOE 安全目的按照部署拓扑结构将 TOE 安全目的和部署划分对应起来，并以子章节方式对相关的安全目的进行描述。

5.6.2 运行环境安全目的

TOE运行环境应提供一些非TOE本身的IT技术和操作规程方面的措施，以帮助TOE正确提供(由TOE安全目的定义的)安全功能。该局部的安全目的解决方案被称为TOE的运行环境安全目的，是由一组TOE的运行环境IT技术应该达到的安全目标陈述组成。

运行环境安全目的的示例如下。

(1) TOE运行环境应提供安装了版本为13.01b的某操作系统的工作站来运行TOE。

(2) 在允许操作TOE之前，TOE运行环境应确保所有TOE用户接受适当培训。

(3) TOE运行环境应限制管理人员和由管理人员陪同的维护人员对TOE的物理访问。

(4) 在将TOE审计日志发送给中央审计服务器之前，TOE运行环境应保证这些TOE运行日志文件内容的保密性。

如果TOE的运行环境由多个场所组成，每个场所可能都有不同的安全特性，ST编制者最好将运行环境安全目的的ST章节划分为几个子章节来反映这种场所分布情况。

5.6.3 安全目的原理

安全目的原理是为了证实ST第4部分里声明的TOE安全目的和运行环境安全目的已经响应了ST第3部分里描述的TOE安全问题。换句话说，ST第4部分应说明安全目的与安全问题定义之间的依赖关系，它分为两部分。

(1) 追溯部分：用于描述每个安全目的分别处理哪些威胁、组织安全策略和假设。

(2) 证明部分：用于论述所有的威胁、组织安全策略和假设都可以被相应的TOE安全目的或运行环境安全目的有效处理。

追溯部分说明了安全目的如何映射到安全问题定义中描述的威胁、组织安全策略和假设，包括但不限于以下几个方面。

(1) 没有无效的安全目的：每个安全目的至少追溯到一个威胁、组织安全策略和假设。

(2) 完全覆盖了安全问题定义：每个威胁、组织安全策略和假设至少可由一个安全目的覆盖到(即全部安全问题都有了解决方案)。

(3) 正确追溯：由于假设总是围绕着TOE运行环境中的TOE，所以TOE安全目的不能追溯到假设。CC允许的追溯关系如图5.7中所描述。

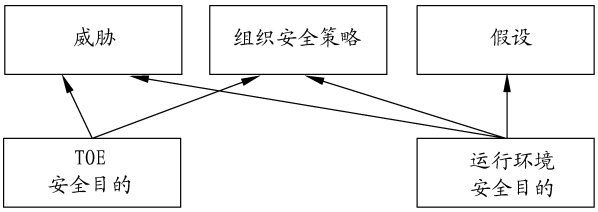

图5.7 安全目的和安全问题定义间的追溯

多个安全目的可以追溯到相同的威胁，表明这些安全目的共同对抗该威胁。对组织安全策略和假设也是如此。

安全目的基本原理也应证实追溯是有效的：如果所有安全目的对特定的威胁、组织安全策略和假设的追溯都已完成，那么所有给定的威胁、组织安全策略和假设均被处理(如，分

别被对抗、被实施、被支持)。

该证实分析实现对抗威胁、实施组织安全策略和支持假设的相关安全目的的效果,并且得出确实如此的结论。

在某些情况下,部分安全问题定义与某些安全目的很相似,此时证实可以很简单,如:威胁"T17:威胁主体读取了 A 和 B 之间的机密信息",TOE 的一个安全目的"OT12:TOE 应确保 A 和 B 之间所有传输信息保持保密性",证实"T17 直接由 OT12 与之对抗"。

表 5.13 给出了安全目的追溯原理。

表 5.13　安全目的追溯原理

例 1:TOE 安全目的原理

- O1 这一安全目的对抗威胁 T1(重演)。O1 需要 TOE 来防止验证数据的重用——即使取得了有效的验证数据,也不能用来发动攻击。
- O2 这一安全目的对抗威胁 T2 和 T3(欺骗和残留信息)。O2 需要:(a)所有的 TOE 信息流被先行协调;(b)没有残留信息被 TOE 内部或外部发送。
- O3 这一安全目的对抗威胁 T4(TSF 攻击)。O3 需要 TOE 来保护自己不受绕开、停用或 TOE 安全攻击篡改的尝试。

例 2:安全目的到威胁的追溯

安全目的	威胁			
	T1	T2	T3	T4
O1	X			
O2		X	X	
O3				X

例 3:运行环境安全目的原理

- O4 这一非 IT 安全目的对抗威胁 T5(使用)。O4 需要 TOE 在一个安全的方式下被交付、安装、管理。
- O5 这一非 IT 安全目的对抗威胁 T5(使用)。O5 需要认证管理员和用户定期接受合适的训练:(a)TOE 的安全使用;(b)任一残留风险。

残余的安全目的是一个 TOE 安全环境假设的重申。

例 4:环境安全目的到假设的映射

安全目的	威胁	假设		
	T5	A17	A18	A21
O4	X			
O5	X			
O6		X		
O7			X	
O8				X

例 5:假设的合理性论据

- TOE 3 个安全假设(A15、A19、A20)在这一 ST 里被修改。由于特殊的 TOE 硬件和软件平台,所以更详细的假设是必须的。然而,修改后的假设应维持 PP 中原始意图。
- PP 里的安全目的 O23 和威胁 T17 不再适用于这一 ST,因为只有 TOE 的个人用户才能是认证系统管理员。不存在终端用户。

表5.13中，例1给出了每个TOE安全目的为什么能对抗相关威胁的充分和必要说明。一个安全目的可能映射到一个或多个威胁；同样地，可能不止一个安全目的会映射到相同的威胁。这一讨论反映到例2的安全目的到威胁的追溯汇总表，从该表描述的安全目的和安全问题映射可以确保所有的假设、威胁和组织安全策略都被考虑到了。例3讨论了为什么每个运行环境安全目的能充分地对抗相关威胁。在这一示例中，两个安全目的映射到同样的威胁，几个假设被用来证明提出的安全目的是合理的。这一讨论反映到例4的运行环境安全目的到威胁和假设的追溯汇总表。

安全目的原理论据也必须解释和证明为什么PP里包含的某些假设、威胁、组织安全策略和安全目的，要么被裁剪，要么不包含在ST里。ST编制者必须提供关于修改或排除PP中安全问题或安全目的的有效技术或操作原因。当然ST中所有新的假设、威胁或安全目的的合理性也必须被证明。例5举例说明了两个可能的应用场景。

根据安全目的和安全目的基本原理，可以得出下列结论：如果所有安全目的都可实现，那么就解决了在ASE_SPD(安全问题定义)中定义的所有安全问题，因为所有的威胁都被应对了，所有的组织安全策略都将得到TOE组织的实施，而所有的假设也都得到了TOE运行环境安全目的的支持。

5.7 扩展组件定义

一般情况下ST中的安全要求都可用源自于CC第2部分和第3部分的标准安全功能和安全保障组件来描述，并按照CC允许的组件元素操作，依照TOE实现相关的技术和机制，对选择的安全组件进行定制，从而给出满足TOE安全目的的解决方案。然而，在某些情况下，ST中的某些安全要求可能不能通过对CC第2部分和第3部分的组件元素进行操作而得到。因此，PP/ST编制者可通过新组件(扩展组件)定义来描述TOE特定的安全要求。ISO/IEC TR 15446技术报告建议这些特定的安全要求应该在PP/ST的第5部分“扩展组件”一节集中进行定义，这样在PP/ST第6节的“安全要求”中引用这些扩展组件就可描述TOE特定的安全要求。有关扩展组件定义可参见第4章PP中扩展组件定义的相关说明，扩展组件定义结构要求与CC预定义的安全组件结构相同。

是否要在CC安全功能组件、安全保障要求或预定义评估保障级别中对IT产品安全进行增强或扩展也由TOE消费者决定，TOE开发者提供的TSF增强与扩展只能为采用CC/CEM评估的消费者提供IT产品选择或合同采购的依据。但TOE开发者和TOE评估者在增强与扩展安全功能和保障组件的元素操作上应遵循CC组件元素定制相关操作要求。

5.8 安 全 要 求

CC第1部分的附录A规定在ST第6部分描述TOE安全要求，并对TOE安全要求进行原理性解释。TOE安全功能应针对安全功能要求和安全保障要求分开描述。

5.8.1　安全功能要求

TOE 安全功能要求是由 ST 第 4 部分的 TOE 安全目的导出的一个详细但抽象的安全功能行为描述，并且以 CC 安全功能组件形式表述 TOE 用户对 TSF 行为的期待。CC 要求 ST 编制者在这部分概述满足所有 TOE 安全目的的安全功能要求（TOE 安全目的必须被 TOE 安全功能组件完全对应）。因此，安全功能组件的选择应参照 ST 定义的 TOE 安全目的，参照 CC 第 2 部分安全功能族设想的安全目的，通过与 TOE 安全目的对应关系确定 TOE 应具备的安全功能组件。对于一个组合 TOE，ST 编制者需指明适用于 TOE 安全目的的相关 TOE 部件的安全功能组件。CC 要求 PP/ST 编制者使用组件这个术语，且由 TOE 安全目的导出 TOE 安全要求有两个理由。

（1）提供比较准确的规范化评估内容描述：因为 TOE 的安全目的一般用自然语言描述，转化为规范化的 CC 安全功能组件使得 TOE 安全功能行为描述更加准确。

（2）允许用户比较不同的 ST 安全方案：不同的 PP/ST 作者可能使用不同的术语描述他们的安全目的，但他们都得使用 CC 标准化的安全组件术语和概念来表达他们 TOE 的安全功能要求。这使得我们容易比较不同 TOE 开发者提供的 IT 产品安全功能。

ST 编制者需要响应符合性声明中描述的引用 PP 的安全要求，ST 编制者可能需要做到以下几点。

（1）简单地逐字重申 PP 中的 SFR（如果 ST 是针对一个 TOE 部件的，选择适用的 SFR）。

（2）完成 PP 中安全功能组件未执行的元素操作。

（3）解决 PP 中未解决的组件依赖关系。

（4）细化或反复功能组件操作来反映 ST 所建议的安全方案。

（5）明确 PP 中未提供的审计要求。

（6）添加由于 ST 的实现依赖特性而必须添加的新 SFR。

（7）忽略非必要的、冗余的或冲突的 SFR。

上述的后 6 项给 ST 编制者提供进一步分解 PP 安全功能要求的机会，包括添加 TOE 实现细节相关的新的安全模型、安全技术、安全机制等 TOE 特殊安全功能要求的机会。

5.8.2　安全保障要求

TOE 消费者通过 PP 确定了合适的评估保障级别和相应的安全保障要求组件后，ST 编制者可简单地重申 PP 中的安全保障要求，即按照 CC 第 3 部分安全保障组件格式陈述 TOE 开发者的行为要求、证据内容与格式要求以及评估者行为要求，以表示他们理解 TOE 需要执行的安全保障要求的特性和范围。（如果由于某些原因，TOE 开发者得出结论认为 PP 指定的 EAL 是难以达到的、过分的或过弱的，这将在 ST 的第 2 节的符合性声明原理部分讨论。）

ST 编制者有两种方法增强 TOE 的安全保障要求。

（1）通过组件元素操作：该机制允许 ST 作者定义个性化的安全保障要求。CC 第 1 部分文档中定义了 4 种组件元素操作，赋值、选择、反复、细化，其中在 SAR 中可运用反复和细化两种操作对安全保障组件元素进行增强。

(2) 通过组件间依赖关系：该机制支持 ST 编制者对 SAR 进行更全面的分析和挖掘，找出潜在的安全保障组件。在 CC 第 3 部分中，某个 SAR 可以有对其他 SAR 的依赖关系，这表示如果 ST 使用了该 SAR，那么，它一般也需要使用另外一些依赖的 SAR。对于 ST 作者来说需要更大的努力以便在 TOE 中包含 PP 中未能明确的必要的 SAR，从而提高 ST 安全保障要求的全面性。

另外，选择 CC 第 3 部分的预定义评估保障级别应注意以下两点。首先，预定义评估保障级别仅适用于 CC 推荐的评估配置；用户可在 PP/ST 中通过扩展组件增加 TOE 可选安全功能或增强保障级别以满足自己的特殊安全要求。其次，TOE 开发者是依照 ST 设计和开发 IT 产品的，而不是依据 TOE 消费者编制的 PP 构建，所以 CC 测试实验室对 TOE 安全评估的依据是 ST，而不是 ST 参考的 PP。

5.8.3 安全要求原理

ST 编制者在安全要求原理部分证明 TOE 安全要求响应并满足了 ST 第 4 节的所有 TOE 安全目的。特别是，以下安全要求基本原理必须被证实。

(1) 安全要求组合是必要的、充分的和互相支持的。

(2) TOE 安全功能和安全保障组件集合满足 ST 里声明的所有 TOE 安全目的。

(3) TOE 特定的 SFR 和 SAR 的选择原理必须证明是合理的，特别地：①扩展组件(TOE 特定安全要求)的使用；②预定义评估保障级别增强和扩展；③TOE 中未满足组件依赖关系的解释。

安全要求原理就是通过必要性、充分性和相互支持性 3 个方面对 5.8.1 节安全功能要求和 5.8.2 节安全保障要求进行说明。换句话说，安全原理部分必须证明 ST 中的所有安全要求是必要的、充分的和相互支持的。ST 编制者一定要关注 TOE 安全目的或安全要求之间的不匹配应当在这部分的安全要求原理中描述，例如相对于 PP 定义新的安全目的或安全要求或对其进行裁剪操作，都需要从必要性、充分性和相互支持性这 3 个方面进行讨论。

1. 必要性说明

为了证明 TOE 安全要求是必要的，TOE 开发者必须证实 ST 中每个安全要求(SFR 和 SAR)是必需的，并且不包含冗余的和额外的安全要求，即所有的 TOE 安全要求都必须与 TOE 安全目的相一致。一个简单的安全要求必要性证实方法是通过一个 TOE 安全目的到安全要求需求的交叉引用表来检查 TOE 安全目的和安全要求之间的映射关系。

2. 充分性说明

充分性说明是指通过构建形式化论据来解释为什么安全要求能充分满足 TOE 安全目的。所有的安全要求都应被检查：标准的 SFR 和 SAR、扩展的 SFR 和 SAR。ST 编制者要特别关注 ST 中对安全组件元素的相关操作：如何以及为什么要对安全组件执行这些元素操作。充分性分析也可以通过验证特定级别的审计事件是否已经达到(查看表 5.14 和表 5.15)来完成。

表 5.14　安全要求原理必要性原理论据

4.6.1　安全要求原理

4.6.1.1　SFR 必要性

下面的文本叙述和表格描述了 ST 满足 PP 里指明的 SFR。

FDP_IFC.1＋1.子集信息流控制

这一组件定义了信息流控制 TSP 中非身份验证机制涉及的实体，使用除了 HTPP、SMTP、FPT 和远程登录之外的所有网络服务。这一组件可追溯到安全目的 O_{21}，并辅助安全目的 O_{21} 的实现。

FDP_IFC.1＋2.信息流控制子集

这一组件定义了信息流控制 TSP 中身份验证机制涉及的实体。这一组件可追溯到安全目的 O_{21}，并辅助安全目的 O_{21} 的实现。

FDP_IFF.1＋1.简单安全属性

这一组件定义在非用户身份认证 TSP 中发送和接收信息的用户属性，包括信息自身的属性。该策略规定了 FDP_IFC.1＋1 组件功能必须执行的一些规则，并描述该功能如何得到安全属性。这一组件可追溯到安全目的 O_{22}，并辅助安全目的 O_{22} 的实现。

FDP_IFF.1＋2.简单安全属性

这一组件定义在认证 TSP 中发送和接收信息的用户的属性，还有信息自身的属性。通过允许或限制信息流来实施这一策略。这一组件可追溯到安全目的 O_{22}，并辅助安全目的 O_{22} 的实现。

下表总结了 SFR 和安全目的之间的映射。

SFR 映射到安全目的

SFR	安全目的 O_{21}	安全目的 O_{22}
FDP_IFC.1＋1	X	
FDP_IFC.1＋2	X	
FDP_IFF.1＋1		X
FDP＋IFF.1＋2		X

表 5.15　安全要求：审计事件原理说明

4.6.1.x　*审计事件原理*

ABC 提供的审计事件被按照审计事件最低或基础审计级别功能需求检查。ABC 在所有领域的应用功能提供可审计事件，只去除了导出、导入、保密性和完整性。这是因为对 ABC 来说上述四类审计活动是不合适的，因为在两个 ABCs 之间发送的所有用户数据消息：(a)使用了一个完整性检验；(b)被加密以确保保密性；(c)只从两个 ABCs 导入或导出。对于 ABC 这些是日常活动，因为涉及大量数据，没有必要对其审计。因此，“未指定”被审计级别选择并且所有审计事件被列举。

SAR 的充分性评估是以确定 CC 预定义评估保障级是否是适合以及任一增强和扩展是否进行了恰当的说明。某个具体 EAL 的充分性论据证明包括：①EAL 既不过强也不过弱；②考虑到 TOE 实现细节和技术的当前状态在技术上是可行的。表 5.16 举例说明了 EAL 2 的一个安全保障必要性和充分性论据。

表 5.16　安全要求：SAR 必要性与充分性

4.6.2　保障要求原理

该安全目标满足保护轮廓中定义的 SAR。该文档的 4.6.2 节给出了满足 EAL 2 的系统开发过程、指南文档、生命周期支持、测试和脆弱性评定保障措施要求。

选择 EAL 2 是为了提供一个低到中等级别的安全性保障。这个保障级别与下列假设的安全威胁模型一致：恶意攻击是中等的，且产品经过了一个详细的缺陷搜索。

3. 相互支持性说明

安全原理第3部分也需要证实安全要求之间是相互支持的，目的是证实IT安全要求的完整性和一致性。这种相互支持性一般通过以下3步骤完成。

(1) 分析组件的依赖关系是满足的。

(2) 分析安全要求内容是内部一致性。

(3) 分析SFR对攻击的积极抵抗能力。

组件依赖分析检验所有3个可能的依赖组合：SFR与SFR、SFR与SAR和SAR与SAR之间的依赖是否满足。组件依赖关系的描述可通过参考CC第2部分和第3部分的组件定义来确定。为了保证TOE安全要求的完整性，当基于具有依赖关系的组件的要求被合并到PP/ST中时，它们之间的依赖关系应该被满足。构造组件包时，包编辑者也应该对这些组件依赖关系进行分析。

ST编制者必须依照CC对各个SFR/SAR的每个依赖关系进行分析研究，证明哪些组件依赖关系被考虑，并指出哪些组件依赖关系未满足。对所有未满足的依赖关系必须提供一个理由，解释了在PP/ST中为什么没必要包含这些依赖组件支持的需求。潜在的原因可能是ST中包含的实现细节使得需求不必要，或者支持的需求功能被TOE运行环境需求满足(如数据库产品的时间戳安全功能组件一般由支撑其运行的操作系统支持)。组件依赖分析的结果可通过一个表格总结来补充说明，如表5.17所示。

内部一致性分析证实ST中没有重叠的、冲突的或有歧义的安全需求。组件结构中的审计需求、管理需求、组件反复和元素操作等因素都在内部一致性分析的范围内。如果ST是某个组合TOE的一个TOE部件，那么与这些ST相关的TOE部件对象也应当被作为内部一致性分析的一部分进行评估。这些内部一致性分析的结果应通过相关表格总结以补充相关的文本信息。

SFR对攻击的积极抵抗能力分析可关注下列关键因数。

(1) 不可旁路性(如内存管理机制)。

(2) 抗篡改(实施自我保护)。

(3) 安全攻击检测能力。

(4) 安全攻击可探测性等。

首先针对前两个因数，在CC/CEM v2.X中定义了不可旁路性(FPT_RVM.1)和安全功能域的隔离(FPT_SEP.1)两个安全功能组件，包括TSF物理保护(FTP_PHP)和安全属性的管理(FMT_MSA.1)组件来一起积极地抵抗各种安全攻击。但由于它们仅描述了TSF最低安全保障相关的一些属性，所以这两个因数在CC v3.1中由ADV(开发)类的ADV_ARC(安全架构)保障要求族负责处理。ADV_ARC族要求充分描述TSF的安全架构，并且充分说明TSF是如何保证不被旁路和如何保护它本身的。CC将这两个功能要求修改成保障要求的原因是由于在过去的TOE安全评估中缺乏一种可以理解的方法去阐述不可旁路性(FPT_RVM.1)和安全功能域的隔离(FPT_SEP.1)评估原则。因而在CC v3.1中，ADV_ARC族要求TOE开发者必须提供TOE安全架构描述信息，必须提供相应的TOE设计和功能规范等评估证据以供TOE评估者进行安全性分析(注：表5.17未标注SFR与SAR之间的依赖关系)。

表 5.17　安全要求原理：组件依赖分析

8.2.3　组件依赖性分析

为完整起见，表 8.1 列出了 ST 中所有 SFR 组件，而不管他们是否具有相关性。从表中看出，除了 FMT_MSA.3 外，所有组件依赖关系都满足通用评估准则，这是由于静态属性初始化功能是由 IT 环境安全需求提供的：用户属性设置(ITENV.1)和 TSF 数据修改(ITENV.2)。表中有两种依赖是由组件层次关系导出的：FDP_IFF.2 对 FDP_IFF.1 有依赖和 FIA_UID.2 对 FIA_UID.1 有依赖。这两个基于组件层次的安全要求在表中依赖关系以 H 表示。

表 8.1　SFR 和 SFR 组件依赖关系分析

序号	组件标识	组件名称	依赖关系	解决方案
1	FAU_GEN.1	审计数据产生	FPT_STM.1	19
2	FAU_SEL.1	选择性审计	FAU_GEN.1 FMT_MTD.1	1 14
3	FDP_ACC.1	子集访问控制	FDP_ACF.1	4
4	FDP_ACF.1	基于安全属性的访问控制	FDP_ACC.1 FMT_MSA.3	3 ITENV.1 ITENV.2
5	FDP_ETC.1	不带安全属性的用户数据输出	FDP_ACC.1 或 FDP_IFC.1	3 —
6	FDP_IFC.1	子集信息流控制	FDP_IFF.1	7H
7	FDP_IFF.2	分级安全属性	FDP_IFC.1 FMT_MSA.3	— ITENV.1 ITENV.2
8	FDP_ITC.1	不带安全属性的用户数据输入	FDP_ACC.1 或 FDP_IFC.1 FMT_MSA.3	— 6 ITENV.1 ITENV.2
9	FDP_UCT.1	基本的数据交换机密性	FTP_ITC.1 或 FTP_TRP.1 FDP_ACC.1 或 FDP_IFC.1	21 — 3 —
10	FDP_UIT.1	数据交换的完整性	FDP_ACC.1 或 FDP_IFC.1 FTP_ITC.1	3 — 21
11	FIA_ATD.1	用户属性定义	无	—
12	FIA_UAU.2	任何动作前的用户鉴别	无	—
13	FIA_UID.2	任何动作前的用户标识	无	—
14	FMT_MTD.1	TSF 数据的管理	FMT_SMR.1	17
15	FMT_REV.1	撤销	FMT_SMR.1	17
16	FMT_SAE.1	时限授权	FMT_SMR.1 FPT_ STM.1	17 19
17	FMT_SMR.1	安全角色	FIA_UID.1	13H
18	FPT_ITI.1	TSF 间修改的检测	无	—
19	FPT_STM.1	可靠的时间戳	无	—
20	FPT_TDC.1	TSF 间基本的 TSF 数据一致性	无	—
21	FTP_ITC.1	TSF 间可信信道	无	—

5.9 TOE 概要规范

TOE 概要规范(TSS)是 TOE 开发者用来描述为满足 ST 里声明的安全要求所采用的设计方法及其实现技术与机制。TSS 描述的详细程度应该使潜在 TOE 消费者能够充分理解 TOE 安全功能行为及其实现技术与机制。

例如，如果 TOE 是一个互联网服务，其 SFR 包含的 FIA_UAU.1 指出用户身份鉴别需求，那么 TSS 就应该说明这个鉴别如何实现，如采用口令、令牌或人脸识别等不同的用户身份标识和鉴别方式。相对于 ST 第 1 部分的 TOE 安全描述，TSS 会给出 TOE 更多开发和实现方法与技术机制有关信息，如 TOE 用于满足 SFR 的可适用标准，或者也可以提供更多安全功能要求实现的技术细节描述。

TOE 概要规范一般通过跟踪矩阵来保证 PP/ST 安全要求实现的完整性和一致性。

(1) 满足 ST 第 6 部分中每个 SFR 的具体 IT 安全功能。

(2) 用于实现上述每个安全功能的准确的安全机制或技术。

(3) 满足 ST 第 6 部分里定义的 SAR 的准确的安全保障措施。

通过跟踪矩阵执行这一映射是为了确保以下两点。

(1) 所有的安全要求(SFR 和 SAR)都被 TSS 设计方法考虑到。

(2) ST 没有引入新的非规范化安全功能说明。

ST 第 6 部分的每个 SFR 都必须映射到 TOE 至少一个 IT 安全功能(TSF)；同样地，每个 IT 安全功能都必须映射到至少一个 SFR(参见图 5.8)。

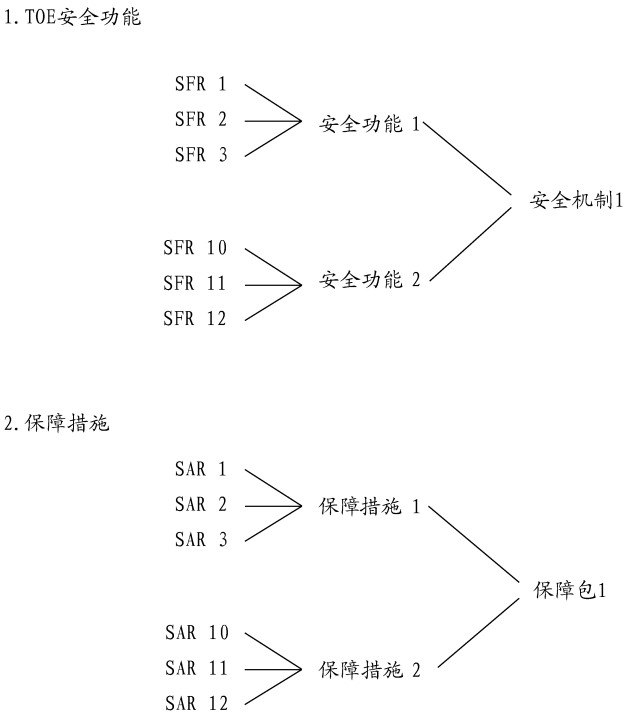

图 5.8 TOE 概要规范映射

依据 ST 文档结构，TSS 的一个安全功能可能对应于 PP/ST 中的一组安全功能组件。之后安全功能被映射到 TOE 具体的安全技术或实现机制，安全保障措施被映射到具体的 CC 安全保障组件或组件集合(如预定义的 EAL)。

ST 的 TOE 概要规范描述一般包含 3 部分内容：TOE 安全功能、TOE 安全保障措施和 TOE 概要规范原理。

5.9.1　TOE 安全功能

TOE 安全功能详细描述实现时 IT 厂商采用的具体安全技术与机制，以及由 TOE 执行的安全功能行为表现。在对 TOE 安全功能描述时，CC 建议按照评估对象功能接口(TFI)类型情况来区分 *SFR-执行*、*SFR-支撑*或 *SFR-无关*子系统或模块，然后再按照这些子系统或模块所完成的安全功能行为进行测试和评估。评估对象的 3 种功能接口类型的定义如下。

(1) ***SFR-执行***：一个可以直接追溯到安全功能要求(SFR)的接口。如果通过一个接口可获得的安全服务能够被追溯到 TSF 的一个安全功能要求，则该接口被称为 *SFR-执行*。注意该接口可能有多种服务和反馈结果，其中一些可能用于 *SFR-执行*，另一些可能用于调用其他模块或服务，例如自主访问控制、用户身份鉴别等子系统或模块。

(2) ***SFR-支撑***：一个支持 TOE 安全策略调用的接口。如果是 *SFR-执行*功能所依赖的，且只需正确运行以保持 TOE 安全策略的那些服务接口(或通过接口相关的服务)，则称其为 *SFR-支撑*，例如操作系统中的设备驱动、内存管理等子系统或模块。

(3) ***SFR-无关***：一个没有 *SFR*-执行功能依赖的接口。即 *SFR-执行*功能不依赖的服务接口称为 *SFR-无关*。

应注意 *SFR-支撑*和 *SFR-无关*必须不依赖 *SFR-执行*服务或者 *SFR-执行*的结果。相反，*SFR-执行*可能需要有 *SFR-支撑*服务(例如，设置系统时钟的能力可能是一个接口的 *SFR-执行*服务，但是如果同一个接口用作显示系统日期，那么该服务可能只是 *SFR-支撑*)。纯 *SFR-支撑*接口的例子是既被用户使用又为了用户利益而运行的一部分 TSF 使用的系统调用接口。例如在 Linux 操作系统中，通常仅部分内核实现安全执行机制(如自主访问控制、安全审计等)，而在内核域的设备驱动程序虽然不直接实现安全功能，但它们可能会导致产品的安全功能失效。因而，贡献于安全执行的设备驱动程序为 *SFR-支撑*，内核中也存在没有实现 SFR 的其他功能(例如，具备优化调度策略的负载管理器)，也没有安全功能依赖于它，因而这些机制是 *SFR 无关*的。针对应用程序也是相同的，Linux 操作系统的 passwd 命令实现了更新用户口令的安全执行机制，这个应用包含了解析文件“/etc/passwd”的逻辑接口，它应属于 *SFR-支撑*，当这种解析逻辑任务失败时，更新用户口令的安全执行功能也会失败。

在 ST 中以类、族和组件的标准化形式组织这些 TOE 安全功能实现技术与机制，提高了 TOE 概要规范的可读性和可理解性。TOE 和 TSF 之间有清晰的区别，需要与 ST 第 1 部分中定义的逻辑和物理边界一致。然而，如果 TOE 是一个只能执行安全功能的产品，TOE 和 TSF 可能是完全相同的。另外，TSF 控制范围(TSC)和 TOE 安全功能接口(TSFI)应被清楚地描绘。TSC 是那些伴随或在 TOE 里发生的，受 TOE 安全策略定义的规则约束的各种交互接口(TSFI)集合。用户通过这些 TSFI 接口既可访问到受 TOE 保护

的资源，又可从 TSFI 获取到 TSF 相关信息。因此，在 TSS 中需要详细阐述所有 TSFI 的目的与方法，描述每个 TSFI 的调用参数，并且要对每个 TSFI 依据其所完成的功能来划分为 *SFR-执行* TSFI、*SFR-支撑* TSFI 或 *SFR-无关* TSFI。例如在操作系统中，相关的 TSFI 可以是以下几种。

(1) ***SFR-执行* TSFI**：系统调用(open、msgctl)，应用的命令行(passwd、login)，配置文件(/etc/passwd，/etc/shadow)。

(2) ***SFR-支撑* TSFI**：非 *SFR-执行* TSFI 的系统调用。

(3) ***SFR-无关* TSFI**：应用的命令行(ls、rm)，配置文件(vimrc)。

在 TSS 中阐明 TOE 安全功能可遵循以下 5 个步骤，每一步都应提供更详细的 TOE 安全技术或实现机制细节。所有这样的信息都必须满足 ST 保障评估(ASE)的完整性、一致性、连贯性、准确性和确定性要求。相应的文本描述都应当尽可能以图表形式来补充。

(1) TOE 安全功能到 CC 的 SFR 的映射。

(2) 定义 TOE 安全功能之间的关系。

(3) 定义 TOE 安全功能的具体实现技术与机制。

(4) 说明 TOE 安全功能的安全审计需求的获取方法。

(5) 描述 TOE 安全功能的管理需求的实现方法。

表 5.18 举例说明了第一步。从安全技术层面，TOE 包含 6 大类安全功能，按照它们的标识和名称被列入表格的前两个列。来自 PP/ST 的标准化 SFR 被映射到 TOE 相关的安全功能。ST 第 6 部分的 TOE 所有 SFR 都必须映射到这部分的 TOE 安全功能：来自 PP 的，由 ST 添加或修改的，针对 TOE 的 SFR。如前所述，每个 SFR 都必须映射到至少一个 TOE 安全功能，同样地，每个 TOE 安全功能都必须映射到至少一个 SFR。在该例中我们发现有 3 个 SFR(表最后 3 个组件)没有与 TOE 安全功能对应起来，其他的 SFR 都映射到了一个且仅有一个 TOE 安全功能。因此，为了使某个 IT 产品的 ST 被 TOE 开发者认可，ST 编制者必须完成以下 3 件工作。

(1) 在 ST 第 7 部分，即 TOE 概要规范，必须做一个声明来解释为什么这 3 个 SFR 中的安全组件没有被整合到 TOE 设计的安全功能中。

(2) 在 ST 第 2 部分，即 PP 声明，声明被引用的 PP 只能提供部分一致性。

(3) 在 ST 第 7 部分后面，即 TOE 概要规范最后解释排除这 3 个 SFR 的理由。

表 5.18 TOE 安全功能说明第 1 步：TSF 映射举例

标 识	名 称	来自 PP/ST 的 SFR	组 件 名 称
GRD_ADM	安全管理	FMT_SMR.1	安全角色管理
		FMT_MOF.1	安全功能行为的管理
		FIA_ATD.1	用户属性定义
GRD_INA	鉴别与认证	FIA_UID.2	任何动作前的用户标识
		FIA_UAU.1	鉴别的时机
GRD_FLO	信息流控制	FDP_IFC.1	子集信息流控制策略
		FDP_IFF.1	子集信息流控制
		FDP_RIP.2	完全残余信息保护

续表

标　识	名　称	来自 PP/ST 的 SFR	组 件 名 称
GRD_DFL	默认配置	FMT_MSA.3	静态属性初始化
		ADV_ARC.1	安全架构
		FPT_STM.1	可靠的时间戳
GRD_AUD	安全审计	FAU_GEN.1	安全审计数据生成
		FAU_SAR.1	审计查阅
		FAU_SAR.3	可选审计查阅
		FAU_STG.1	受保护的审计迹存储
		FAU_STG.4	防止审计数据丢失
无	无	FIA_AFL.1	鉴别失败处理
		FIA_UAU.4	一次性鉴别机制
		FCS_COP.1	密码运算

表 5.19 举例说明了 TOE 安全功能说明的第 2 步，它描述了 TOE 安全功能之间的层次关系，且列出了每个 TOE 安全功能的主要行为描述内容。在该例中，TSF 包含 5 个功能组件：安全管理、鉴别和认证、信息流控制、默认配置和安全审计。所有这 5 个 TSF 包都在同一层次，它们执行的功能独立。安全管理类包含 7 个功能，而信息流控制类只包含 2 个功能。

表 5.19　TOE 安全功能说明第 2 步：TSF 结构示例

1. TSF
1.1　安全管理
　　1.1.1　启动、关闭
　　1.1.2　创建、写、编辑、删除、读信息流控制规则
　　1.1.3　创建、写、编辑、删除、读用户属性
　　1.1.4　设置日期和时间
　　1.1.5　创建、删除、读、归档审计跟踪数据
　　1.1.6　创建系统备份
　　1.1.7　启动系统恢复
1.2　鉴别与认证
　　1.2.1　操作系统层次
　　1.2.2　应用系统层次
　　1.2.3　人员
　　1.2.4　内部 IT 实体和过程
　　1.2.5　外部 IT 实体
1.3　信息流控制
　　1.3.1　外部资源访问控制
　　1.3.2　内部资源访问控制
1.4　默认配置
　　1.4.1　安全、生成和启动过程中流量阻塞
　　1.4.2　安全、生成和启动过程中事务阻塞
　　1.4.3　维护独立逻辑域的每个会话
1.5　安全审计
　　1.5.1　生成审计数据
　　1.5.2　可选择审计数据检查
　　1.5.3　保护审计存储
　　1.5.4　预防审计数据丢失

表 5.20 举例说明了 TOE 安全功能说明的第 3 步，描述了实现每个安全功能的安全技术与机制，以及默认设置、约束、操作参数和算法细节。在该例中，实现 TSF 安全审计的安全技术与机制被指明。（注意在一个 ST 中，每个 1.6.×.×条项可以包含几段到几页的具体实现技术与机制细节。）

表 5.20 TOE 安全功能说明第 3 步：映射安全技术与机制到 TSF

1.6 安全审计

1.6.1 生成审计数据

1.6.1.1 模块 A 生成监控信息，例如审计跟踪、安全事件日志和警告 SNMP 陷阱。

1.6.1.2 模块 B 送模块 A 生成的审计跟踪、安全事件日志和警告给后台组件以进一步处理。

1.6.1.3 为以下事件生成审计记录：

- TOE 和 TSF 的启动和关闭；
- 对认证管理员角色的部分的群组用户的修改；
- 所有用户认证机制的使用，包含提供的用户身份；
- 所有认证机制的使用；
- 所有信息流请求的决定；
- 对允许或拒绝信息流的信息流安全策略规则的创建、写、删除、编辑和读；
- 创建、写、删除、编辑和读取用户属性；
- 设置和修改系统时间和日期；
- 归档、创建、删除、读和清理审计跟踪；
- 事务备份和恢复。

1.6.2 可选择的审计数据检查

1.6.2.1 XYZ 工具有一个 GUI，该 GUI 允许认证的系统管理员读取、检索和基于事件类型、日期与时间、IP 地址范围排序审计记录。

1.6.3 保护审计存储

1.6.3.1 审计文件被安全文件系统（NTFS）保护。

1.6.3.2 只有认证用户可以访问审计文件。

1.6.3.3 NTFS 检测对审计文件的尝试修改。

1.6.3.4 NTFS 记录成功和不成功的创建、读、写、编辑、删除、修改权限和（或）获得审计文件所有权的尝试。

1.6.4 预防审计数据丢失

1.6.4.1 如果系统不能够获取或记录审计数据，TOE 和 TSF 操作停止。

1.6.4.2 直到以上情形被纠正，只有认证系统管理员可能执行功能。

表 5.21 举例说明了 TOE 安全功能说明第 4 步，指明了安全审计需求层次和对每个适用的 SFR 可被审计和获取的审计事件细节。

表 5.21 TOE 安全功能说明第 4 步：审计需求示例

安全功能组件	审 计 层 次	审 计 事 件
FMT_SMR.1	最小	• 对认证管理员角色的部分群组用户的修改 • 执行以上修改的认证管理员的身份 • 与认证管理员角色相关的用户身份
FIA_UID.2	基本	• 所有对用户机制的使用 • 提供给 TOE 安全功能（TEF）的用户身份
FIA_UAU.1	基本	• 所有对认证机制的使用 • 提供给 TOE 安全功能（TSF）的用户证书

续表

安全功能组件	审 计 层 次	审 计 事 件
FIA_AFL.1	最小	• 未成功认证尝试阈值 • 认证管理员的用户认证能力的随后恢复 • 违规用户身份 • 执行恢复的认证系统管理员的身份
FDP_IFF.1	基本	• 信息流请求的决定 • 源和目的体的推测地址
FPT_STM.1	最小	• 系统时间的修改 • 修改系统时间的认证系统管理员的身份

TOE 安全功能说明第 5 步是描述管理需求的实现方法。在 CC 第 2 部分中，安全管理类(FMT)组件定义了管理要求，TOE 开发者可以从这个类中选择合适的那些管理要求，也可以开发新的管理需求。例如，针对 FMT_REV.1 包括以下管理行为：

管理：FMT_REV.1

FMT 中的管理功能可考虑下列行为：

(1) 管理能够调用安全属性撤销这一功能的角色组；

(2) 管理可能发生撤销的用户、主体、客体和其他资源列表；

(3) 管理撤销规则。

换句话说，CC 第 2 部分建议管理①谁可以执行撤销功能；②哪些实体是能作为撤销的主体；③如何决定执行撤销的阈值。这 3 项与 FMT_REV.1 组件元素定义直接相关：

FMT_REV.1.1TSF 应仅限于[**赋值**：*已标识的授权角色*]能够撤销在 TSF 控制下的与[选择：*用户、主体、客体、[赋值：其他额外资源]*]相关联的安全属性[赋值：*安全属性列表*]。

FMT_REV.1.2TSF 应执行规则[**赋值**：*撤销规则的详细说明*]。

选择操作与管理行为条项(2)管理需求相关，而赋值操作与管理行为条项(1)和条项(3)管理需求相关。

如果考虑到撤销时间范围的管理需求，则 ST 编制者可能想要添加第 4 条管理行为：

(4) 管理执行日常基础撤销的频率和执行一次应急基础撤销的时间。

为了这样做，就要在 ST 第 5 部分增加一个扩展组件，显式的定义下列元素要求：

FMT_REV.1.3 TSF 应当在 5 秒内执行需求撤销和完成事务。

TSS 描述了 TOE 管理功能如何被实现。对于这里的例子，提供了以下关于固件/软件模块如何做到的细节。

(1) 撤销安全属性和什么属性会被撤销。

(2) 限制授权用户执行这一操作的能力。

(3) 在指定时间范围内执行撤销功能。

在 CC 第 2 部分的 FMT 类管理功能之间的交互也要被描述，尤其是所有的依赖关系。不选择管理需求的原理应该在 ST 的 5.8.3 部分里进行解释。

需要指出的是，管理需求可能在一个 PP 里被指明，尤其是如果客户有特殊的操作需

求；然而，考虑到管理要求与 ST 的实现依赖关系，最好是将管理需求的指定延迟到 ST 编制阶段。

5.9.2 TOE 安全保障措施

TSS 描述用来满足 ST 里指明的每个 SAR 的具体安全保障措施，包括所有 EAL 增强和扩展相关的保障措施都需要在这一部分被重述。然后，组成 EAL 的每个保障类和族相关的安全保障措施应详细讨论。为了增强可理解性，图表相关的文本材料应尽可能都提供。特别地，应当提供一个矩阵来映射 SAR 到具体的安全保障措施。此外，每个 SAR 都必须映射到至少一个安全保障措施，而每个安全保障措施都必须映射到至少一个 SAR。

TOE 开发者负责解释安全保障组件的开发者行为元素和内容与形式元素是如何满足每个 SAR。TOE 开发者没有责任考虑评估者行为元素的安全保障措施。然而，TOE 开发者必须确保定义在评估者行为元素里的所有要求都应被满足，这是 CC 测试实验室用来确定 ST 是否通过评估验证的前提。对于 EAL 2 和以下保障级别的 ST，安全保障措施可以引用现有的项目文档，例如配置管理过程，而不是重复 CC 里的信息。需要指出的是：①必须在 ST 被提交正式评估前编制好这些项目文档；②项目成员确实知道并且遵守评估相关文档的归档过程。

表 5.22 举例说明了在 EAL 2 和 EAL 3 两种场景下如何针对 ADV_FSP.1 保障组件来编写安全保障措施的文本描述。在第一个例子里，引用了现有的项目文档来满足需求；在第二个例子里，开发者行为元素和内容与形式元素被反映。“应当”被替换为“将要”，也有其他一些必要的小的编辑修改，以告知 TOE 开发者需提供的安全保障方法。

表 5.22 示例 TSS 安全保障措施

例 1：EAL 2（参照项目现有文档）

7.2.3 AVD_FSP.1 基本功能规范

下面列出的 ABC 功能规范，实现了 AVD_FSP.1 的安全保障要求：

- ABC 功能规范，版本 3.0，2015 年 3 月 31 日。

例 2：EAL 3

7.2.3 ADV_FSP.1 基本功能规范

下面列出的 ABC 功能规范，实现了 AVD_FSP.1 的安全保障要求：

- ADV_FSP.1.1D 开发者将要提供一个功能规范。
- ADV_FSP.1.2D 开发者将要提供功能规范到安全功能要求的追溯关系。
- ADV_FSP.1.1C 功能规范应描述每个 *SFR-执行* 和 *SFR-支撑* 的 TSFI 的目的和使用方法。
- ADV_FSP.1.2C 功能规范应识别每个 *SFR-执行* 和 *SFR-支撑* 的 TSFI 相关的所有参数。
- ADV_FSP.1.3C 功能规范应提供暗含的 *SFR-无关* 的接口分类的基本原理。
- ADV_FSP.1.4C 功能规范应证实安全功能要求到 TSFI 的追溯。

表 5.23 介绍了一个 SAR 到安全保障措施的示例映射矩阵。因为这一示例是针对 EAL 2 的，所以引用了现有的项目文件提供的功能和接口规范、指导性文档和 TOE 安全架构的基本描述，通过分析一个完整的 ST 中的安全功能要求来提供保障，以理解 TOE 安全行为。这种分析由对 TSF 的独立测试、TOE 开发者基于功能规范自测试、对 TOE 开发者

测试结果的选择性确认、证实可抵御具有基本攻击潜力攻击者攻击的脆弱性分析(基于功能规范、TOE 设计、安全架构描述和提供的指南类证据)等证据来支持。

表 5.23　TSS 安全保障要求与保障措施映射表

安全保障要求	安全保障措施
ADV_ARC.1	• 提供 TSF 安全架构的描述文档
ADV_FSP.2	• 提供一个功能规范文档 • 提供功能规范到安全功能要求的追溯关系
ADV_TDS.1	• 提供 TOE 的设计文档 • 提供从功能规范的 TSFI 到 TOE 设计中最底层分解的映射
AGD_OPE.1	• 提供操作用户指南
AGD_PRE.1	• 提供 TOE,包括它的准备程序文档
ALC_CMC.2	• 提供 TOE 及其标识 • 提供 CM 文档
ALC_CMS.2	• 提供 TOE 配置项列表：TOE 本身、安全保障要求的评估证据和 TOE 的组成部分 • 提供对于每个 TSF 相关的配置项,配置项列表应简要说明该配置项的开发者
ALC_DEL.1	• 提供把 TOE 或其部分交付给消费者的程序文档化 • 提供应使用交付程序
ATE_COV.1	• 提供如何与功能规范中的 TSF 接口对应的测试文档 • 提供测试覆盖分析报告
ATE_FUN.1	• 提供应测试 TSF,并文档化测试结果和测试规范 • 提供测试文档
ATE IND.2	• 提供用于有效地重现开发者的测试的必须材料,包括机器可读的测试文档、测试程序等 • 提供一组与开发者 TSF 功能测试中同等的一系列资源
AVA_VAN.2	• 提供公共领域的调查以标识 TOE 的潜在脆弱性 • 提供分析过程中使用的指导性文档、功能规范、TOE 设计和安全架构描述

5.9.3　TOE 概要规范原理

TOE 概要规范原理部分是说明 TOE 安全功能及其实现技术与机制和安全保障措施适合于满足 TOE 安全要求。特别地,必须证明以下 3 项要求。

(1) 给出的安全要求解决方案满足 ST 中的所有 SFR。

(2) TOE 开发者对 TOE 脆弱性分析声明是有效的。

(3) 给出的安全保障措施满足 ST 里的所有 SAR。

TSS 原理说明应覆盖 ST 前面所有的 SFR,既包括从 PP 继承来的那些 SFR,也涵盖由 ST 增加或裁剪的那些 SFR,但不包括由 ST 删除的那些 PP 中的 SFR。同样地,所有的 SAR 也都在 TSS 原理论证范围内,包含增强和扩展的 SAR。相互支持性应采用同样的准则,以便用来生成必要的、充分的和互相支持的 TSS 论据。

5.6.3 部分论证了 TOE 安全目的和假设、威胁和组织安全策略之间的一致性、准确性、完整性和相关性；5.8.3 部分论证了 TOE 安全目的和安全要求之间、安全要求之间的一致性、准确性、完整性和相关性。本节主要通过提供缺失的安全问题、安全目的、安全要求和安

全技术与机制这个链接完成图 5.9 所示的映射关系证明：①安全技术与机制和安全要求之间的；②安全技术与机制之间的一致性、完备性、完整性和相关性。

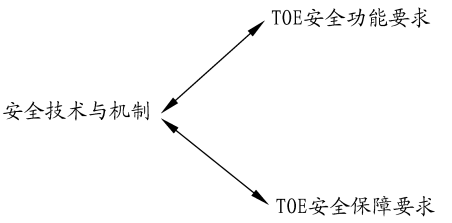

图 5.9 TOE 概要规范原理论证

安全要求与安全技术与机制，以及安全技术与机制之间的相关性证明可使用 CC/CEM 推荐使用的用于证明安全目的和安全要求之间的相关性的相同过程来证明(参见 5.6.3 和 5.8.3 节内容)。ST 第 6 部分的每个 SFR 都被映射到 TSS 部分 TOE 实现特定功能的具体安全技术与机制。所有的 SFR 必须映射到至少一个安全技术与机制，而每个安全技术与机制都必须映射到至少一个 SFR。不应该存在任何没被映射的 SFR 或安全技术与机制。通过构建这样的映射关系(如图表方式)来确保以下几点。

(1) 没有 SFR 未对应的安全技术与机制，以避免造成潜在的安全脆弱性/缺陷。

(2) TOE 实现安全技术与机制中没有遗漏 ST 中的 SFR。

(3) 不会因为 TOE 实现细节需要而导致安全要求分解时引入可能的脆弱性/缺陷。

(4) 给出的 TOE 安全要求设计与实现解决方案充分、稳定且有一定灵活性。

TSS 必要性准则也是采用安全目的和安全要求那样的方式，通过表格映射形式来证实。充分性和相互支持性准则一般通过文本方式描述。相关表达方法可参照安全目的和安全要求原理部分编制：通过表格形式描述映射关系，以论证必要性，通过自然语言陈述来论证充分性和相互支持性。

总之，本节的目标是 ST 编制者通过组合 TOE 的各种安全技术与实现机制，来论证前面给出 TOE 安全目的导出的相关安全要求可以得到满足，以便在 ST 中给出 TOE 安全功能实现解决方案和相关的安全保障控制措施是有效的结论。

5.10 本章小结

TOE 开发者主导编制的 ST 文档是响应 IT 产品消费者安全需求(PP)，与实现相关的某个具体 IT 产品的安全方案，它也是某个 IT 产品厂商针对具体 IT 产品安全规范的描述文档。因此，TOE 评估发起者在启动该 IT 产品的 CC 认证前，会按照 ISO/IEC TR 15446 技术报告编制 IT 产品相应的 ST。

ST 包括引言、符合性声明、安全问题定义、安全目的、扩展组件定义、功能和保障要求和 TOE 概要规范这些内容。ST 是被 IT 产品开发者用作 TOE 开发和评估的基础。换句话说，PP 从 TOE 消费者角度指明了 IT 产品安全功能和保障要求，而 ST 从 TOE 开发者角度提供了 IT 产品安全功能具体实现技术与机制，包括安全保障措施的详细解决方案，以给 TOE 消费者提供可能的 IT 产品选择方案。因此，ST 可以回答以下问题(或更多)。

(1) 如何能够在多个已评估的 ST/TOE 中找出 IT 产品用户所需的 ST/TOE？该问题由 ST 引言部分的 TOE 功能概述和 TOE 安全描述两部分内容组成，其中 ST 编制人员给出了目标 IT 产品的通用功能和安全功能的简要描述。

(2) TOE 是否适合 IT 产品用户现有的 IT 运行基础设施环境？该问题由 ST 引言部分的 TOE 功能概述阐述，其中标识出了运行 TOE 所需要的硬件/固件/软件元素。

(3) TOE 是否适合 IT 产品用户现有的运行环境？这个问题由 ST 第 3 部分的运行环境安全目的进行阐述，其中标识了 TOE 为发挥安全功能作用所需的运行环境相关约束条件。

(4) TOE 能做什么？该问题由 ST 安全目的部分阐述，其中 ST 编制人员给出了 TOE 安全目的和运行环境安全目的，ST 编制人员以简明抽象的方式对 TOE 安全问题定义中所定义的威胁、组织安全策略和假设的预期解决方案进行了陈述。

(5) TOE 能提供什么(潜在 TOE 消费者)？该问题由 ST 第 6 部分的安全要求处理，其中给出了 TOE 的安全功能和安全保障要求。

(6) TOE 具体做了什么(采用的技术和机制)？该问题由 ST 第 7 部分的 TOE 概要规范阐述，其中提供了 TOE 安全功能实现技术与机制的深层次的描述。

(7) TOE 将会做什么(专家)？该问题由 ST 第 6 部分描述的 SFR 以及由提供了附加细节的 TOE 概要规范阐述。

(8) TOE 处理政府/组织定义的问题了吗？如果政府/组织等 TOE 消费者已经定义了 PP，答案可以在 ST 的符合性声明中找到，ST 编制人员从中列出了 ST 符合的所有 PP。

(9) TOE 处理 IT 产品用户的安全问题了吗？什么是 TOE 对抗的威胁？它实施的组织安全策略是什么？做了哪些有关运行环境的假设？这些问题由 ST 的安全问题定义阐述。

(10) CC 用户可以信任 TOE 到什么程度？这能够在 ST 第 6 部分的安全要求的 SAR 中找到，ST 编制人员在其中提供了评估 TOE 的评估保障级别，因而提供了对 TOE 正确性的信任程度。

TOE 利益相关人可能参与 ST 编制：TOE 开发者编写的 ST 文档由潜在的 IT 产品用户阅读，由评估者按照 CEM 中定义的 ASE 对 ST 进行检查和评估。通过评估后的 ST 被 TOE 开发者用作构建一个 TOE 的基础。当然 ST 并不是固定不变的，而是随着用户需求、信息技术、应用环境等的发展而不断修订的一份 IT 产品安全规范文档。基于 CC/CEM 的 TOE 生命周期活动及其相关文件都可映射到 IT 产品的软件生命周期和采购流程的某个阶段。在软件工程生命周期中，一个 ST 相当于设计阶段文档——由 TOE 开发者响应客户在一个 PP 里声明的安全要求而生成的一个设计文档，且这一设计的质量需要通过 ASE 类安全保障活动来验证。在 IT 产品采购流程中，一个 ST 相当于合同认可前采购活动需要 TOE 开发者提交的一部分技术文档；换句话说 ST 应包含在潜在应标人提交的合同提案文档中，并且由合同招标源选择团队对其可行性进行评估。

CC 强制 TOE 开发者使用 ST 文档结构描述 IT 产品安全方案，是为了规范 IT 产品安全需求及其规范说明的编制，确保 ST 是 IT 产品所有不同用户能准确地一致地进行解读的规范化文档。ST 各部分内容是一个联系紧密的有机整体，ST 文档中的各部分内容之间的依赖及其一致性需遵循 ISO/IEC TR 15446 技术报告要求。

ST 第 1 部分通过定义 ST 范围和状态、TOE 类型、安全架构、逻辑和物理边界等来概述一个 ST。TOE 类型是试图通过定义 TOE 实现技术与机制来分类 TOE。TOE 安全描述部分的一个主要目标是区分 TOE 和 TOE 安全架构。TOE 安全架构定义了 TOE 安全功能(TSF)必须的语境。TSF 包含正确执行 TOE 安全策略所需的所有 TOE 硬件、软件和

固件。TOE 安全架构定义了由 TOE 架构约束下的 TSF 实现的相关内容。如果 ST 是为了描述一个特定安全的商业化产品套件，TOE 和安全架构可能相同。相对地，如果 ST 是为了描述一个 IT 系统中的 TOE 部件，TOE 和安全架构之间可能存在区别。物理安全边界表示了 TOE 安全功能对什么边界有效。这一边界里的 IT 实体在 TSF 控制范围里(TSC)，并且以指定的方式在一定程度上被保护。在这一边界外的 IT 实体则不在 TSC 中，不一定被信任。TSC 表示可能出现于 TOE 以及可能受 TOE 安全策略约束的 IT 实体集合。物理安全边界是通过明确声明哪些硬件、固件、软件平台、组件和模块包含与 TSF 实现独立的实例来定义的。

ST 第 2 部分描述 ST 是否声明与某些 PP 或包符合，具体与哪些 PP 或包符合。阐明 ST 是用来响应哪一个 PP，并解释该 ST 和被引用的 PP 之间的符合度。ST 符合性声明可以是 PP 符合性声明的无、完全、裁剪、增加和部分符合。该部分是一个 ST 和被引用的 PP 和包之间的符合度说明和解释。所有的 PP 和包符合性声明必须通过充分解释，其理由和凭据应被证实。

ST 第 3 部分声明了 TOE 运行安全相关的假设，分析了 TOE 面临的威胁，并且列出了适用于 TSF 的组织安全策略。ST 安全问题定义部分反映了 PP 适用的安全环境。PP 和 ST 这部分之间的差异性来自于这样的事实，PP 是实现独立的，而 ST 是实现依赖的。

ST 第 4 部分描述了 TOE 安全目的和运行环境安全目的。这些安全目的来自对第 3 部分假设、威胁和安全策略的分析。TOE 开发者应响应 PP 里合适的安全目的，决定：①PP 里的安全目的是否是有效的；②是否必须增加新的安全目的。

ST 第 5 部分是 TOE 扩展组件定义，通过 CC 组件格式描述 IT 产品特定的安全功能或安全保障要求。

ST 第 6 部分通过选择和定义 TOE 安全功能要求(SFR)和安全保障要求来实现第 4 部分中描述的 TOE 安全目的。这些 SFR 和 SAR 来自对第 2 部分对安全架构和边界的讨论，以及第 3 部分中描述的安全风险分析。TOE 开发者响应 PP 中的需求，PP 中的安全需求在 ST 中可能被简单地重申，ST 编制者也可能添加如下与 TOE 实现相关细节。

(1) 完成 PP 中安全组件未执行的元素操作。

(2) 解决 PP 中未解决的组件依赖。

(3) 通过细化或反复操作功能组件来反映 ST 编制者的 TOE 安全方案。

(4) 指定 PP 中未提供的审计需求。

(5) 增加由于 ST 的实现依赖特性而必须增加的 SFR。

(6) 为 IT 环境重分配 SFR。

(7) 忽略非必要的、冗余的或冲突的 SFR。

ST 第 7 部分，TOE 概要规范(TSS)，定义了以下内容。

(1) 满足 ST 第 6 部分中定义的每个 SFR 的具体的 IT 安全功能(TSF)。

(2) 用于实现每个安全功能的准确的安全机制或技术。

(3) 用于满足第 6 部分定义的 SAR 的准确的安全保障措施。

如果 ST 基本原理比较多，可以添加第 8 部分，以证明以下几点。

(1) 第 4 部分安全目的响应了第 3 部分 TOE 安全问题定义。

(2) 第 6 部分安全要求实现了第 4 部分的所有安全目的。

(3) 第 7 部分的 TOE 概要规范实现了第 6 部分的所有安全要求。

(4) PP 合规性和安全功能强度声明是有效的。

上述 4 种安全原理说明论据证明了 ST 是完整的、正确的、一致和连贯的。ST 编制者证明了安全目的、安全要求和安全概要规范是必要的、充分的和相互支持的。

5.11 问题讨论

1. 简述 ST 在 IT 产品生命周期和安全评估中的角色和作用，包括 ST 在 IT 产品生命周期中不应承担的角色。

2. 比较 PP 和 ST 文档结构，分析二者之间的差异，以及各部分之间的联系和依赖关系。

3. 简述安全目标引言内容，描述 TOE 功能概述和 TOE 安全描述的主要内容。

4. 简述组合 TOE 与引用 ST 和 PP 之间的关系。

5. 阐述组合 TOE 安全目的和单体、组件和组合 TOE 之间的关系。

6. 在 PP 中只要讨论 TOE 边界，但在 ST 中需要区分 TOE 物理边界和逻辑边界。简述为何在 ST 里要区分这两种边界类型，并概述 ST 中逻辑和物理安全边界作用。

7. 简述 TOE 消费者和评估者在未来 IT 产品使用或评估中如何使用 ST 中安全问题定义的一个假设声明。

8. 如何分类 ST 安全问题定义部分声明的威胁？这与它引用的 PP 中的威胁分类有什么不同？

9. 与软件工程其他详细的安全设计规范相比，解释使用 ST 文档结构描述 TOE 概要规范的优缺点。

10. 阐述 TOE、TSF、TSC 和针对(a)TOE 部件、(b)组合 TOE、(c)商用现货产品(COTS)和(d)系统的 TSFI 之间的关系。

11. 讨论延迟解决 PP 中组件依赖关系到一个 ST 编制期间的正反两方面的优缺点。

12. 描述 TOE 体系架构和安全架构之间的相似性和不同。

13. TOE 概要规范中描述安全审计和管理需求的目的是什么？

14. 使用什么准则来证明安全要求是：(a)必要的、(b)充分的、(c)互相支持的？

15. 简述 TOE 概要规范主要内容，简述如何通过跟踪矩阵来保证 PP/ST 安全要求完整性和一致性。

16. 简述 *SFR-执行*(SFR-enforcing)、*SFR-支撑*(SFR-supporting)与 *SFR-无关*(SFR-non-interfering)3 种模块及其接口异同及其在 TOE 安全评估中的作用。

17. 简述 TOE 概要规范原理部分内容，通过讨论 TSS 和 TSS 原理之间的关系，解释为何说 ST 是实现相关的 IT 产品安全规范说明。

18. 组件依赖分析证明了什么？在组件依赖分析范围里有什么组件？

19. (a)SFR 和 SFR、(b)SFR 和安全技术与机制、(c)SFR 和安全保障措施、(d)SAR 和 EAL 之间的关系是什么？

20. 面向 TOE 消费者和评估者，ST 可以回答他们即将采购或评估 IT 产品的哪些问题？