ICS 35.040
L 80

中华人民共和国国家标准

GB/T 20283—2020
代替 GB/Z 20283—2006

信息安全技术
保护轮廓和安全目标的产生指南

Information security technology—Guide for the production of protection profiles and security targets

(ISO/IEC TR 15446:2017,Information technology—Security techniques—Guide for the production of protection profiles and security targets,NEQ)

2020-09-29 发布　　2021-04-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准代替 GB/Z 20283—2006《信息安全技术 保护轮廓和安全目标的产生指南》，与 GB/Z 20283—2006 相比，主要技术变化如下：

——修改了保护轮廓和安全目标概述(见第 5 章，2006 年版的第 4 章)；

——修改了安全目的(见第 9 章，2006 年版的第 7 章)；

——修改了安全要求(见第 11 章，2006 年版的第 8 章)；

——修改了 TOE 概要规范(见第 12 章，2006 年版的第 9 章)；

——删除了“PP 和 ST 的描述部分”“TOE 安全环境”“PP 声明”“PP 和 ST 基本原理”和“功能和保证包”(见 2006 年版的第 5 章、第 6 章、第 10 章、第 11 章和第 13 章)；

——增加了“缩略语”“保护轮廓/安全目标引言”“符合性声明”“安全问题定义”“扩展组件定义”“特殊情况”(见第 4 章、第 6 章、第 7 章、第 8 章、第 10 章和第 14 章)；

——删除了“指南核查”“防火墙 PP 与 ST 示例”和“数据库 PP 示例”三个附录(见 2006 年版的附录 A、附录 B 和附录 C)；

——增加了资料性附录“扩展组件定义示例”(见附录 A)。

本标准使用重新起草法参考 ISO/IEC TR 15446:2017《信息技术　安全技术　保护轮廓和安全目标产生指南》编制，与 ISO/IEC TR 15446:2017 的一致性程度为非等效。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位：中国信息安全测评中心、北京邮电大学、吉林信息安全测评中心、清华大学。

本标准主要起草人：杨永生、崔宝江、叶晓俊、高金萍、贾炜、王宇航、王峰、邓辉、唐喜庆、蒋显岚。

本标准所代替标准的历次版本发布情况为：

——GB/Z 20283—2006。

引　言

GB/T 18336—2015(所有部分)使用保护轮廓和安全目标构成灵活科学的安全测评框架，已成为表述安全的通用语言。本标准的目的是帮助开发者、使用者、测评者等更规范更详细地表述安全目标和安全要求。

信息安全技术
保护轮廓和安全目标的产生指南

1 范围

本标准给出了保护轮廓和安全目标文档各部分内容的描述，并提供了保护轮廓和安全目标概述、保护轮廓/安全目标引言、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、TOE 概要规范、组合及部件 TOE 的保护轮廓和安全目标、特殊情况等信息。

本标准适用于信息技术产品的测试、评估、采购，并为产品的使用者、开发者、测评者使用保护轮廓和安全目标提供指导。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 18336—2015(所有部分) 信息技术 安全技术 信息技术安全评估准则

GB/T 25069—2010 信息安全技术 术语

3 术语和定义

GB/T 25069—2010 和 GB/T 18336.1—2015 界定的术语和定义适用于本文件。

4 缩略语

下列缩略语适用于本文件。

COTS：商业现成品(Commercial Off the Shelf)

CRL：证书撤销列表(Certificate Revocation List)

DAC：自主访问控制(Discretionary Access Control)

DBMS：数据库管理系统(Database Management System)

EAL：评估保障级(Evaluation Assurance Level)

IT：信息技术(Information Technology)

LDAP：轻量目录访问协议(Lightweight Directory Access Protocol)

OSP：组织安全策略(Organizational Security Policy)

PIN：个人身份识别码(Personal Identification Number)

PKI：公钥基础设施(Public Key Infrastructure)

PP：保护轮廓(Protection Profile)

SAR：安全保障要求(Security Assurance Requirement)

SFR：安全功能要求(Security Functional Requirement)

SFP：安全功能策略(Security Function Policy)

SPD:安全问题定义(Security Problem Definition)
ST:安全目标(Security Target)
TOE:评估对象(Target of Evaluation)
TSF:TOE 安全功能(TOE Security Functionality)
TSFI:TOE 安全功能接口(TOE Security Functionality Interface)

5 保护轮廓和安全目标概述

5.1 简述

本章是对 PP 和 ST 的读者、目的、开发过程和使用等方面的概述,以说明在使用 GB/T 18336—2015(所有部分)进行信息安全评估时,PP 和 ST 在其中所起的作用。

5.2 读者

本标准适用于两类读者:

a) IT 专业人员:其具有一定安全知识,但并非信息安全评估方面的专家,且对 GB/T 18336—2015(所有部分)无过多了解;
b) 信息安全专家:其充分了解 GB/T 18336—2015(所有部分),并把开发 PP 和 ST 作为自己的工作内容。

对于 IT 专业人员,本章将为其提供理解 PP 和 ST 的目的与结构的信息,以及便于其阅读和理解 PP 和 ST 的背景信息。下文将详细解释 PP 和 ST 各部分的具体内容,并假定读者具备 GB/T 18336—2015(所有部分)的知识。

对于信息安全专家,其应已熟知本章的内容,可以使用随后章节提供的方法、技术和实用技巧,以有效且一致的方式来准备 PP 和 ST。

如果读者不是信息安全方面的专家,也可使用本标准来开发 PP 或 ST。但使用者仍需查询、阅读并理解与其要求相似的已发布的 PP 或 ST,同时也可考虑向有必备领域专业知识和经验的其他人寻求帮助。

5.3 保护轮廓和安全目标的使用

5.3.1 简述

GB/T 18336—2015(所有部分)的主要目的是用于评估 IT 产品的安全性。“IT 产品”一词并未在 GB/T 18336—2015(所有部分)中实际定义,但是它可用于理解为利用信息技术构建的任何实体,包括由一个机构使用的完整的 IT 系统,或者由某个产品制造商生产并销售给许多不同或不相关客户的 COTS。本标准在提及“IT 产品”或仅用“产品”等术语时,建议适用于上述提到实体,但当对某些产品存在局限时,将用系统、COTS 或其他特定的术语来表达。

IT 产品可以多种方式在多种环境中使用,安全的概念将随产品而变化。因此,由 GB/T 18336—2015(所有部分)产生的最终评估结果绝不是“此 IT 产品是安全的”,而是“此 IT 产品满足这个安全规范”。

GB/T 18336—2015(所有部分)对安全规范进行了标准化处理,以便于执行两项工作:

——在按照安全规范进行产品评估时强制要求分析特定内容;

——允许对不同产品的安全规范进行比较。

GB/T 18336—2015(所有部分)规定了两种不同类型的安全规范:保护轮廓和安全目标。两者之间

的区别在于其所起的作用不同，即当客户想要向开发者购买产品时，保护轮廓和安全目标在这个购买过程中发挥了不同作用。

客户、开发者和产品的概念是抽象的。客户是希望购买产品的人，其可以是个人、单一组织、集团组织、政府部门等。开发者是想出售产品的人，其可以是一个程序员、一个小公司、大型企业、集团企业等。产品可以是一个小到应用软件或智能卡，大到操作系统或包含数百个不同组件的复杂计算机系统。

当客户希望购买产品时，基本上存在两个过程：

——基于规范的采购过程：即客户向开发者提出需求，开发者研发出满足客户需求的产品。采用这种方式的花费昂贵，但客户得到了其所要的产品。

——基于选择的采购过程：即客户可从现有产品中选择某个产品。采用这种方式的花费相对低廉，但客户最终选择的产品可能满足其需求，也可能不完全满足其需求。

当IT安全需求非常重要时，对于一般客户，这两个采购过程也给其带来其他困难：

——很难确定其需要何种类型的IT安全；

——更难以确定一个声称有IT安全的给定产品是否是可用的，或有效地满足其需求；

——更加难以确定的是，如何判断产品所声称的安全属性是真实的。

为协助客户解决上述困难，可使用GB/T 18336—2015(所有部分)来评估产品，而保护轮廓与安全目标将在此过程中起到重要作用。以下两节将就评估在采购过程中的作用进行说明。

IT产品不是孤立工作的，其可被用户使用在一个已包含安全措施的运行环境中，并假设在运行环境中存在某些类型的安全特性，这些假设同样是PP或ST的组成部分。

5.3.2 基于规范的采购过程

5.3.2.1 概述

在基于规范的采购过程中，客户将书写的规范提交给开发者，开发者基于此规范开发产品。此过程包括如下步骤：

a) 客户应以非正式的方式来确定其安全要求；

b) 客户应将这些非正式的安全要求转换成适合于开发者使用的更正式的规范；

c) 开发者应基于此规范开发产品。

应严格把控每个步骤的质量，以便让客户明白此款产品是其所需要的。

5.3.2.2 非正式的安全要求

确定非正式的安全要求这一步骤，是要确定“安全问题是什么，应怎么解决这个问题”，这实际上已超出GB/T 18336—2015(所有部分)的范围，因此其不属于本标准的范围之内。

GB/T 18336—2015(所有部分)假定客户有能力确定其非正式的安全要求，否则，客户最终购买的产品可能无法符合真正的安全要求。

客户的要求一旦成文，常会有与之相关的安全问题接踵而至。非正式的客户要求通常有如下特点：

a) 不完整：未表明所有的要求，如缺少产品应对抗的重要威胁；

b) 非嵌入的：未充分协调产品运行的特定环境，或者对其环境的描述不够具体；

c) 隐含的：某些产品的要求有因果关系，但这些因果关系本身未包括在内。开发者可能未将这些隐含的要求考虑在内；

d) 不可测试：要求过于模糊，因此无法验证产品是否满足要求；

e) 过于详细：实际上已经写有实施举措，但并没有写为什么如此实施。在后期要求有所改动时，往往不能确定这些改动应如何实现；

f) 含糊其词：如“通信应是安全的”，却没有定义什么是“安全”；

g) 不一致：安全要求自相矛盾。

若将这类客户要求提交给开发者，可能使开发者产生误解而导致出现其他问题。而评估者对要求的解释也可能不同于客户和开发者，导致安全评估也可能出现其他问题。

在整个基于规范的采购过程中，重要的一步是要将客户要求正式化，即基于 GB/T 18336—2015（所有部分）的安全要求，利用 PP 文档予以正式化。PP 文档是以正式的、标准化的方式来定义客户的安全要求。

5.3.2.3 将 PP 作为规范使用

PP 包含多个部分，但作为一个安全规范，最重要的是“安全功能要求”。GB/T 18336—2015（所有部分）要求使用标准中明确定义的语言来描述这些要求。这种语言可确保 PP 具有如下特点：

a) 无歧义：该语言含有非常明确的术语，从而使开发者可以理解并正确解释要求；

b) 可测试：该语言限定了仅含有可测试的要求项目，故后期可以评估产品是否真正满足 PP；

c) 不拘于细节：该语言在某种程度上进行了抽象。这和客户要求紧密相关，客户想知道做了什么，但无需知道如何去做；

d) 更完整：该语言包含一些特定结构，以确保隐性需求也包括在内（例如：“如需要这个功能，那么也需要这个功能的其他功能”）。

5.3.2.4 通过 PP 构建产品

客户可通过一个 PP 给出其正式要求，并提交给相关开发者。开发者将此 PP 作为产品研发的起点，并撰写相应的 ST。

ST 与 PP 非常相似，PP 定义客户需求并由客户撰写，而 ST 是一个产品规范且由开发者撰写。

开发者不可以随意提交一个 ST 来响应客户的 PP，其 ST 应符合 PP，即开发者提供的产品应涵盖客户的所有要求。

ST 相较 PP 有如下特点：

——ST 比 PP 规定了更多内容：与客户要求相比，产品会提供更多的安全功能，但附加功能不允许与 PP 不兼容；

——ST 比 PP 包含了更多细节：PP 明确了“什么是安全的”，ST 解释了“该怎么做”，即开发者通过 ST 指出其如何实现了客户的要求。

PP 允许 ST 的撰写者可灵活地表述安全功能，更多详细信息见 5.5.6。

ST 为开发者定义了产品的安全功能，且 ST 也将作为后续开发过程的“安全要求规范”。

开发过程的最终成果应是一个可以提交给客户，同时客户也可以安装和使用的产品。当然，该产品应以 ST 描述的那样运行。

5.3.2.5 评估在基于规范的采购过程中的作用

在基于规范的采购过程中，开发者向客户阐明了如下信息：

a) 开发者的 ST 遵从客户的 PP；

b) 开发者的产品遵从开发者的 ST；

c) 开发者的产品符合客户的 PP 并且满足客户的要求。

客户如果接受这些陈述，采购过程即可结束。

客户如果要求对这些陈述进行独立验证，其可以借助第三方（如评估机构）依据 GB/T 18336—

2015(所有部分)的安全评估来检查这些符合性声明。在这个过程中,评估机构可通过 PP、ST、产品和 GB/T 18336—2015(所有部分)来评估以下两个声明:

a) ST 遵从 PP;

b) 产品遵从 ST。

评估之后,仍然留有两个值得注意的方面:

a) 客户非正式的安全要求到 PP 的转化过程。这个转化过程不属于 GB/T 18336—2015(所有部分)的范围,如果转化错误,PP 将不符合客户的要求,产品同样也有可能不符合客户要求。

b) 评估并不能"证明"合规性。GB/T 18336—2015(所有部分)评估不提供一个绝对的保证来说明产品满足 PP,它只能基于 PP 或 ST 所指定的深度和广度提供某种程度的保障。

5.3.3 基于选择的采购过程

5.3.3.1 概述

在客户无法承担定制产品成本的情况下,其应从现有产品中进行选择,基于选择的采购过程如下:

a) 开发者应开发产品及其相应规范,并将其提供给客户;

b) 客户应根据此规范确定该产品是否是最合适其想购买的产品。

应严格把控每个步骤的质量,以便让客户明白此款产品是其所需要的。

5.3.3.2 使用开发者提供的规范

在基于选择的采购过程中,客户应使用由开发者提供的规范。

该规范如果是非正式的,那么它同 5.3.2.2 中讨论的非正式的客户需求具有同样的不足。基于此,该规范同样需要正式化,应如 5.3.2.4 中所讨论的那样使用 ST。这里的 ST 与在 5.3.2.4 中讨论的 ST 相同,但是有一个明显的区别,由于 ST 不基于客户的 PP,此 ST 不能声称符合 PP。

开发者因为不知道客户的特定需求,将不得不先预估市场需要什么,然后撰写 ST,无法匹配任何客户的具体要求。

开发者根据 ST 研发产品,其过程与基于规范的采购过程相似。

5.3.3.3 比较安全目标

客户可以比较一定数量产品的 ST,并选择一个最符合其要求的(可能也会考虑非安全性的要求,如价格)。客户要想办法找出自己的非正式的安全要求(见 5.3.2.2),并与提供给自己的各个 ST 进行比较。如果能有一个或多个产品符合客户的要求,那样最好,否则客户将不得不选择"最贴近"的产品或找一些其他的解决方案(例如,改变客户的要求)。

正如 5.3.2 所述,生成非正式的客户安全要求的过程不在 GB/T 18336—2015(所有部分)和本标准的范围之内。要求与 ST 之间的比较也不在 GB/T 18336—2015(所有部分)的范围之内。

5.3.3.4 评估在基于选择的采购过程中的作用

与基于规范的采购过程相类似,开发者可以简单地宣称其产品满足 ST,如果客户对此予以接受,则采购过程即可结束。

开发者会提供证书来证明独立的第三方(评估机构)已验证了 ST,并依据 GB/T 18336—2015(所有部分)实施了安全性评估,确认该产品确实满足 ST。

评估之后,仍然留有两个值得注意的方面:

a) 证明客户非正式的安全要求与 ST 之间是等价的。这个过程不属于 GB/T 18336—2015

（所有部分）的范围，如果证明错误，ST 将不符合客户的要求，产品同样也有可能不符合客户要求。

b） 评估并不“证明”合规性。GB/T 18336—2015（所有部分）评估不提供一个绝对的保证来说明产品满足 ST，它只能基于 ST 所指定的深度和广度提供某种程度的保障。

5.3.4 PP 的其他用途

保护轮廓也还有其他的用途。例如，标准制定机构或供应商协会可能为特定类型的应用指定一个 PP 作为最佳实践的最低安全标准，政府和行业协会同意并授权使用。如果存在这种情况，客户和开发者可能都需要遵守这些 PP，也需提供附加的安全功能，以满足自身的特定需求。

组织机构指定或批准 PP，要确保此类 PP 是最低程度的（仅要求绝对必要的）和切合实际的（不能要求开发者完成无法实现的功能或保障）。

PP 也可表达对某种特定类型安全产品的需求，即使其在发布时还未存在这样的产品。这种情况下，产品开发者对待此类 PP 时要慎用。因为，当开发者开发完合适的产品时，需求可能已经过时，又或者是 PP 的发起者可能已经找到其他方式来满足他们的要求，而不想再购买这样的产品。

5.4 保护轮廓/安全目标开发过程

在 GB/T 18336.1—2015 的附录 A 和附录 B 以及前文所述的内容中，有关 PP 和 ST 要求的陈述，是建议 PP 和 ST 的开发应按逻辑顺序以“自上而下”的方式进行。例如，在 ST 中的顺序是：

a） 定义安全问题；

b） 确定与安全问题对应的安全目的；

c） 定义满足 TOE 安全目的安全要求；

d） 选取满足安全要求的安全功能。

不排除可能需要重复表述的情形。例如，定义安全要求时可能会突出表述所要满足的安全目的或安全问题；在验证威胁、组织安全策略、安全目的、安全要求和功能之间关系时可能有一定的重复；特别是在构建基本原理时，可能出现更多的重复。在基本原理中的所有问题都被消除后，才能假定 PP 或 ST 是完备的。

在 PP 或 ST 开发的过程中，可能出现安全问题之外的新信息，需要记录其所有改变，从而反映外部环境的变化情况，例如：

a） 识别出新的威胁；

b） 改变组织安全策略；

c） 由于费用和时间上的限制，希望由 TOE 担负或由 TOE 环境担负的责任划分发生变化；

d） 对于预期攻击潜力的改变将影响 TOE 的安全问题定义。

如果 TOE 是已开发好的产品，PP 或 ST 作者可能已经有 TOE 安全功能的明确思考，那么安全关注点和安全目的的定义将不可避免地受到 TOE 安全解决方案的影响，此时 PP 与 ST 的开发过程可能以“自下而上”的方式进行。

5.5 阅读和理解保护轮廓和安全目标

5.5.1 简述

本节内容可不提供给那些已拥有 GB/T 18336—2015（所有部分）知识的专家使用，其专门提供给那些对 PP 和 ST 知之甚少的读者，这些读者需要阅读 PP 或 ST 以了解相关产品的安全能力。本节的目的是强调那些在评估范围内可能被掩盖的潜在疏漏或不足。

详细了解 PP 和 ST 的内容，可阅读 GB/T 18336.1—2015 附录 A 和附录 B，其提供了有关安全目标和保护轮廓的详细信息。同时，也可以查阅已经公布且普遍使用的其他 PP 和 ST。

PP 或 ST 不能由一组简单的属性来概况，其描述了一系列复杂的安全属性。如果不仔细阅读 PP 或 ST，在购买或使用该产品时，可能导致意外情况的发生。如果对 GB/T 18336—2015(所有部分)没有深入了解，也几乎很难理解 PP 或 ST 里的某些部分。PP 或 ST 中较易理解的部分章节包含了关键信息，可用于理解 PP 要求的安全属性或 ST 所描述的产品。

相关且易读的章节包括：

a) TOE 概述；

b) TOE 描述；

c) 运行环境下的安全目的；

d) 符合性声明。

5.5.2 阅读 TOE 概述

在阅读 PP 或 ST 时，一般首先要阅读 TOE 概述，因为“TOE 概述的目的是帮助 TOE 的潜在消费者，他们通过查找已评估的 TOE 或产品列表找到可能满足他们安全需求，且是他们的硬件、软件和固件支持的 TOE”。(参见 GB/T 18336.1—2015 的 A.4.2)。

TOE 概述包括三个重要部分：

a) TOE 的用途及主要安全特性；

b) TOE 类型；

c) 需要的非 TOE 的硬件/软件/固件。

可在 GB/T 18336.1—2015 的 A.4.2 找到一些简单例子。TOE 用途及主要安全特性的描述是为了让公众对 TOE 在安全方面的能力以及在安全环境中的使用有一个大致的了解。

该部分内容比较精短，较易阅读与理解。因为针对的是消费者，内容不会太过技术性，且比较通用。

TOE 类型是描述 TOE 属于 IT 产品的哪个通用类别(如防火墙、智能卡、局域网等)。GB/T 18336—2015(所有部分)要求 TOE 概述应列出任何合理的预期，读者可从 TOE 类型中找到不被 TOE 支持的预期。具体如下：

a) 如果 TOE 类型使人认为 TOE 具有某种安全功能，但它实际并不具备此功能，则 TOE 概述中应列出这个缺失的功能；

b) 如果 TOE 类型使人认为 TOE 可以在某环境中使用，但实际并不能在这样的环境中使用，则 TOE 概述中应列出这一点。

这些警告信息仅在 PP 或 ST 的这个部分出现，PP 或 ST 的作者后续可用备注的方式在适当位置重复这个信息，但这并不是应要求的。

如果这些警告已被提出，并且它有可能影响预期用途，则应认真考虑是否仍然要在这些限制条件下使用此 TOE。

TOE(特别是软件类型的 TOE)有时不得不依靠硬件、固件和其他软件才能运行，因此 TOE 概述应要标识出非 TOE 的硬件/软件/固件。

PP 或 ST 并不要求应提供一个完整的、充分详细的有关所有硬件/软件/固件的标识信息，但标识信息应是完整的且充分详细的，以便能确定 TOE 需要使用的主要外部硬件/软件/固件。

应仔细评估是否有 TOE 所依赖的非标准组件，确认这些组件是否适合现有的基础设施、预算或公司政策等。

5.5.3 阅读 TOE 描述

某知名产品已被评估，但这并不意味着该产品所有的安全特性（甚至是大多数安全特性）都已被评估。可能只有某些安全功能特性被考虑，其余的都未作为被评估的安全功能的一部分。GB/T 18336.1—2015 中 A.4.1 描述禁止误导性的 TOE 标识，但开发者总是仅仅使用产品名称予以应付。需要检查被评估的功能是否满足需求。如果想要使用的安全功能被排除在外，则应对此加以留意。

TOE 描述最重要的作用之一就是让 ST 读者能发现这一点。为此 TOE 描述详细论述了 TOE 的物理和逻辑范围。

关于物理范围，是这样表述的，“TOE 描述应论述 TOE 的物理范围：构成 TOE 的所有硬件、固件、软件及指南部分的一个列表。该列表应在一定程度上进行详细描述，使读者对这些部分有一般性理解”（参见 GB/T 18336.1—2015 中 A.4.3）。

关于逻辑范围，是这样表述的，“TOE 描述也应论述 TOE 的逻辑范围：一定程度上描述 TOE 提供的安全特征，使读者获得对这些安全特征的一般性理解。该描述应比 TOE 概述中描述的重要安全特征更加详细”（参见 GB/T 18336.1—2015 中 A.4.3）。

物理范围介绍了 TOE 各个部分，而逻辑范围则说明 TOE 做什么。

应仔细检查 TOE 概述以确定需要的所有安全相关的功能是否都进行了评估，否则，不能从评估中获得操作该功能的任何保障。例如，如果客户希望产品具有远程管理功能，但在逻辑范围内并未提及远程管理，那么远程管理很可能未被评估，客户如想按评估配置使用该产品，最好不要打开远程管理功能。

5.5.4 运行环境下的安全目的

运行环境是指通常放置 TOE 的位置。为了使 TOE 正常工作，运行环境应满足一定的约束条件。例如，如果某 TOE 是一个高可用性的服务器，那么此 TOE 需要保护以防被篡改。这种保护可以由 TOE 提供，一般的运行环境应会强调并且指出需要上了锁的安全服务器机房。

这些类似的有关运行环境的要求会在 PP 或 ST 的运行环境安全目的一节中描述。这些目的的描述应由除 TOE 之外的事情来实现，以便 TOE 满足其安全要求。可在 GB/T 18336.1—2015 中 A.7.2.2 找到更多的运行环境安全目的的实例。

这些都不是仅供参考的指导，而是让 TOE 运转的必要条件。这些目的应充分满足，并由某个人或某个组织处理。如果这些目的中的任何一项没有被满足，TOE 都有可能无法安全地正常工作。因此，确认是否能够实现这些目的是至关重要的，如果其中有一项无法实现，那这个 TOE 可能就不适合客户使用。

5.5.5 阅读符合性声明

符合性声明通常在 PP 或 ST 的显著位置，一般是在开头部分。它通常包括如下形式的一句话。

保护轮廓/安全目标声明的符合性如下：

——GB/T 18336。声明所使用的 GB/T 18336 版本。

——第 2 部分扩展或第 2 部分。这一部分定义了安全功能要求的结构，从消费者的角度看，两种都是可以接受的。

——第 3 部分扩展或第 3 部分。这一部分定义了安全保障要求的结构。如果是“第 3 部扩展”，这意味着 PP 和 ST 的开发者设计了他们自己的质量保障测试，从消费者的角度看，应询问为什

么这是必要的。

——TOE 声明符合性的包列表。通常只有一个这样的包，它被命名为 EAL1，EAL2，....，EAL7。这些 EAL 内容将在 5.5.7 中进一步讨论。

——PP 或 ST 声明符合性的保护轮廓列表。

5.5.6 保护轮廓的符合性

ST 可能声明符合的 PP(但不强制)，PP 也可以声明符合其他的 PP。GB/T 18336—2015(所有部分)不允许任何形式的局部符合，如果有引用的 PP，则 PP 或 ST 应完全符合所引用的 PP。

PP 符合性意味着 PP 或 ST(如果 ST 是关于被评估的产品，那么该产品也一样)满足这一 PP 的所有要求。

阅读 PP 时，会发现这样一个声明，即 ST 和其他 PP 的符合性应是“严格符合性”或“可论证的符合性”。已发布的 PP 通常要求可论证符合性。这意味着 ST 声称符合 PP，那 ST 应为 PP 中所描述的通用安全问题提出解决方案，但可以是与 PP 描述等同或更严格的任何方式。“等同但更严格”在 GB/T 18336—2015(所有部分)中有所定义，但原则上它意味着，PP 和 ST 中可使用完全不同的陈述。

严格符合性只用在不允许 PP 和 ST 存在任何差异的情况下。ST 仍然可以引入额外的限制。如果 PP 要求严格符合性，而没有写出来，那它极不适合使用。

5.5.7 EAL 及保障问题

TOE 概述和 TOE 描述可表明 TOE 能够做什么(例如，由 TOE 提供的功能不能概括 IT 产品的所有功能)。一般功能相同的产品可通过不同的设置来使用。例如，同一个智能卡可被用于：

——存有少量数额的车票；

——信用额度为 1 万元的信用卡；

——绝密设施的访问控制措施。

第一种情况。如果黑客设法破解了公共汽车的车票，其也许能够免费乘搭公共汽车直到卡的参数变化。公共汽车公司的潜在收入损失并不显著(前提是其他卡没有被以同样的方式所攻击)。

第二种与第三种情况，则更需要信任卡片功能的正确执行，因为即使一张卡被攻击，其后果都非常严重。

这就涉及产品的保障问题。GB/T 18336—2015(所有部分)评估通过检查产品开发的诸多方面来衡量保障，如开发和生产的过程、设计、手册、产品开发者的测试等。

GB/T 18336—2015(所有部分)将保障分为 27 个类别(也称为保障族)。在每类中，规定了不同级别的符合性，满足越高，级别越好。

举个例子，产品可按开发者的测试范围打分：

——0：不知道开发者是否已对产品进行了测试；

——1：开发者针对产品的某些接口进行了一些测试；

——2：开发者针对产品的所有接口进行了一些测试；

——3：开发者针对产品的所有接口进行了大量测试。

从这个例子可以看出，付出的努力随级别逐步提高，不确定度在逐步减少。

GB/T 18336—2015(所有部分)设有 7 个预定义的级别，称为评估保障级(EAL)。从 EAL1 到 EAL7，EAL1 最低，EAL7 最高。

每个 EAL 可被看作是一个 27 个数字的集合，每一个对应一个子类别。例如，EAL1 分配等级 1 给

13 子类别，分配等级 0 给其他 14 个子类别。而 EAL2 分配等级 2 给 7 个子类别，分配等级 1 给 12 个子类别，分配等级 0 给其他 8 个子类别。

EAL 是严格的等级体系，所以如果 EAL n 分配了某一等级给某个子类别，那么 EAL $n+1$ 将分配相同或更高的等级给该子类别。严格来讲，EAL $n+1$ 整体来说比 EAL n 提供了更多的保障。

较高保障级也意味着成本的提高。在前面介绍的测试范围中，为 0 的等级将意味着没有成本，但对于每一个较高的等级，开发者应执行测试并对其进行描述，评估也将判断开发者是否已正确地执行了这些操作。更高的保障几乎总是意味着更多的成本。当然，更高的保障也降低了功能出现故障或含有可被利用漏洞的风险。

针对 EAL 及此 EAL 的保障特性，在每个 EAL 列表中都配有描述，可见 GB/T 18336.3—2015 中第 7 章的描述。

5.5.8 小结

本节主要是为了表述以下信息：

a) 可通过阅读 ST 中的一些章节合理地来理解 ST；

b) 但同时，这些章节也可能包含重要的警告信息，因此，了解评估的局限性至关重要。

曾有消费者表示需要一个 EAL4 级的防火墙，但即使通过 GB/T 18336—2015(所有部分)认证的 EAL4 防火墙，它可能因某种局限性而不适合消费者，也可能无法提供消费者所需的全部安全。

例如，假设消费者需要一个提供包路由和 HTTP/FTP 代理服务功能的防火墙。某通过 EAL4 评估的路由器的 TOE 类型包含了防火墙，而作为路由器，其仅提供了包路由控制功能，因而不适合作为防火墙使用。更有甚者，如果一个通过评估的防火墙可提供代理服务，但其逻辑范围又仅限于包路由，因此要谨慎处理此种情况。

5.5.9 延伸阅读

上述关于 PP 或 ST 的描述是 PP 和 ST 最基本的部分，其有助于非专业人员阅读。如果想了解更多有关产品的信息，可尝试阅读 TOE 概要规范，其更详细地介绍了 TOE 是如何实现的。TOE 概要规范不一定是易读的，其出现了各种缩写，如 FIA_UID.2.1。然而，开发者应以编写出既满足评估者要求，且可被用户理解的 TOE 概要规范为目标。

如果需要了解 PP 或 ST 的其他内容，可阅读随后章节。

6 保护轮廓/安全目标引言

本章针对 PP 或 ST 中的引言提供指导，这在 GB/T 18336.1—2015 中 A.4 和 B.4 中有所介绍，因此不需要给出额外的指导。

PP 引言包括以下要素：

——PP 标识；

——TOE 概述。

ST 引言包含以下要素：

——ST 和 TOE 标识；

——TOE 概述；

——TOE 描述。

非显而易见的部分是 TOE 概述中的“TOE 的使用和主要安全特性”。TOE 的使用是由 PP 或 ST

中的安全问题定义部分衍生来的，而 TOE 主要安全特性最好通过概括 TOE 的安全目的来描述，这可确保引言与 PP 或 ST 的更详细部分保持一致。

大多数情况下，引言可在 PP 或 ST 的其余部分都完成后再去撰写。

7 符合性声明

本章针对 PP 或 ST 中的符合性声明提供指导。ST 符合性声明的描述参见 GB/T 18336.1—2015 中 A.5，PP 符合性声明的描述参见 GB/T 18336.1—2015 中 B.5。

PP 或 ST 的符合性声明描述了 PP 或 ST 应如何符合于：

a) GB/T 18336。此处列出用于撰写 PP 或 ST 的 GB/T 18336 的确切版本。

b) 保护轮廓。此处列出 PP 或 ST 声称符合性的任何保护轮廓。一个简单列表足以，此处不需要额外的信息。

c) 包。此处列出由 PP 或 ST 中引用的任何包。声称与一个在 GB/T 18336.3—2015 中定义的保障包(EAL)具有符合性是很正常的，可能也带有增强要求。一个简单列表足以，此处不需要额外的信息。

这种符合性也适用于基于该 PP 或 ST 的任何 TOE。

如果已指定一个 PP，应定义其他 PP 和 ST 如何符合此 PP，这有如下两种选择：

a) 严格的符合性。从概念上讲，这意味着 PP/ST 应包含这个 PP 上的一切。

b) 可论证的符合性。从概念上讲，这意味着 PP/ST 应与这一 PP“等同”。

如果为正准备购买或开发的产品编写一个准确、完整规范的 PP，应要求严格的符合性。如果要指定一个 PP 用于任何其他目的，用可论证的符合性。

如果声称与某功能包或其他的 PP 符合，那么安全问题定义、安全目的和安全要求，应与包或 PP 兼容。

如果正在撰写一个 PP 或 ST，并为引用的 PP 增加额外的要求，那么应谨慎，以免造成不一致，使得未有 TOE 同时实现所有的要求。

8 安全问题定义

8.1 简述

本章针对 PP 或 ST 中的 SPD 提供指导。GB/T 18336.1—2015 中 A.6 和 B.6 分别描述了 PP 和 ST 的安全问题定义。

安全问题定义的目的是以一种正式的方式明确安全问题的本质和范围，如图 1 所示。

安全问题定义是 PP 或 ST 最重要的部分，但并非所有保护轮廓和安全目标都含有安全问题定义(详见第 14 章)。以下引自 GB/T 18336.1—2015：

“评估结果的有效性对 ST 依赖性很强，而且 ST 的有效性对安全问题定义的依赖性很强，因此花费有效资源并使用良好定义的过程分析推导安全问题定义常常是有价值的。”(参见 GB/T 18336.1—2015 A.6.1)。

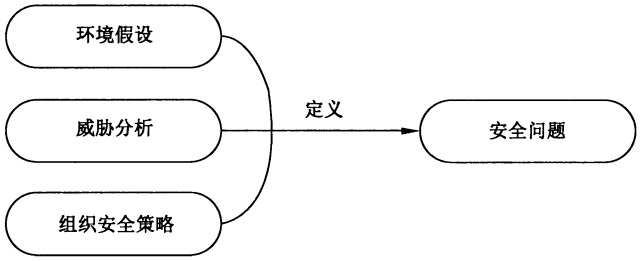

图 1　安全问题定义

如果定义的问题是错误的或含糊的，那么 PP 和 ST 的余下部分的内容也都将是错误的。更为糟糕的是，基于这样一个有效但不适用的评判规范，错误的产品就可能被选用或者购买。对开发者或是客户来说，被作为采购规范或采购选择参考标准的 PP 或者 ST，明确好其安全问题定义是极为重要的。

PP 和 ST 的后续章节将结合其运行环境阐述 TOE 是如何处理这些问题的，因此安全问题定义清晰简洁一致是很重要的。

GB/T 18336—2015(所有部分)未假设或授权安全问题定义的任何过程或方法。本章详细说明了一种在各类组织和环境中工作的简单方法，其包括如下步骤：

a) 识别和确认非正式的安全要求；

b) 通过威胁分析，识别和确定适用的威胁；

c) 描述适用的策略；

d) 描述适用的假设；

e) 完成和检查完整的 SPD。

不论采用何种方法，本标准假设安全问题定义代表了对现有的非正式安全要求的规范化描述。在实践中，有可能不是通过一个单一的文档就能直观地表述非正式的要求，甚至有些隐含的要求可能没有写到文档中。因此，第一步是要识别和确认非正式的要求，尽管其不会在 PP 或 ST 中呈现。非正式的要求可能是显而易见且明确的，但在某些情况下，开发 SPD 的很大一部分工作可能仅仅是识别非正式的要求，并从管理层和其他相关者确认这是一个正确和完整的表示。

有两方面并没有被 GB/T 18336—2015(所有部分)所要求，但在实践中发现其可以节省整体时间，避免 PP/ST 开发后期阶段的混乱和疑问，这包括：

a) 描述不用考虑的威胁；

b) 形成一个关于 SPD 与非正式安全要求之间的基本原理。

如果 SPD 不阐述基本原理，则会存在一定风险，导致部分非正式的要求可能会在制定 SPD 的过程中遗漏。因此，基本原理概述提供了一种重要的手段，用以检查 SPD 的一致性和完整性。

作为一般性原则，安全问题定义应避免在可能情况下对相应 TOE 产品形态的讨论，例如涉及 TOE 安全功能的详细信息。按照这个原则，本章将集中于安全问题方面。对于 TOE 如何满足安全目的的讨论将留给 PP 或 ST 的后续部分。若一个特定解决方案的任务是作为非正式安全要求的一部分，该解决方案将被表述为 SPD 中的一部分，以保障它被描述并且能够合理约束后续设计决策。

8.2　识别非正式的安全要求

8.2.1　简述

总有一些有关安全问题的相关事情和其预期的解决方案在安全问题定义开始之前就已知晓。这些要求和限制形成非正式的安全要求。因此，识别和描述非正式的安全要求是安全问题定义的第一步。

8.2.2 信息来源

8.2.2.1 概述

识别非正式的安全要求有多种方式。有可能存在本标准中描述的通用方法不能识别的情况，这就需要仔细全面地考虑安全要求。本节建议的潜在信息来源将辅助安全问题的识别。

8.2.2.2 所需的功能

如果安全功能是一个用户明确需求的一部分，那么应在 SPD 中指出要解决的问题。

8.2.2.3 风险评估

安全风险评估需覆盖整个系统，包括采购的 COTS 产品，以识别出需要靠 IT 安全控制来减少的风险，这些风险是安全问题的一部分。

有许多方法用于执行风险评估。这些方法普遍认为，描述存在的风险应包括三个要素：

——可被某种方式威胁或破坏的资产；

——可以破坏该资产的人或物，即威胁；

——可以损害该资产的漏洞和可以破坏资产的方式，即脆弱性。

如果缺少这三个要素的任何一个，则不会产生风险。这种形式的模型假定由 GB/T 18336—2015（所有部分）给出，如果实际的风险评估使用了相互矛盾的风险模型，在 SPD 中映射出的风险评估结果就会存在问题。

8.2.2.4 威胁评估

威胁评估是风险评估的弱化形式，假定如果一个威胁存在，资产可能会被损坏，因此风险存在。在这种情况下，所识别的威胁代表了安全问题的一部分。

在试图确定明确安全问题的人并非资产所有者的情况下，威胁评估就十分重要，因而进行风险评估或确定资产的价值时不能只从一个角度出发。

8.2.2.5 管理策略

安全要求的提出可能源于一个管理决策，例如，在一个特定的机构中，所有的系统将执行某些标准化的 IT 安全控制。这个过程有时被称为“最低标准”或“规避风险”。策略也可能是不确定的，比如，遵循某些相似机构的业务特点或相关逻辑要求。

即使一个策略以法律或合同为逻辑基础，其规定的安全控制措施可能并不适用于特定的系统或组织，或者可能只适用于一部分。

8.2.2.6 表象性策略

安全要求可能源于一种期望，它试图证明某组织或者 COTS 产品可以实行的一些 IT 安全控制。该策略可能源于市场需求，也可能源自一种遵循业界最佳实践的愿景。

这类安全问题非常适合 GB/T 18336—2015（所有部分）评估，因为，评估机构在评估完成后会颁发官方证书，并针对安全控制提供独立的验证。已发布的 PP 可用于标识适合的安全控制。

8.2.2.7 评估策略

组织可以实施这样的策略，即 IT 产品应通过 GB/T 18336—2015（所有部分）评估。

8.2.3 描述非正式的要求

安全风险评估的结果是有关安全问题定义的最佳信息来源。识别可接受的和不可接受的风险可以使安全问题在设计阶段得到修正。如果以消除特定风险所需要的安全控制是难以实现或难以评估的，仍然可以通过用多种方法，使用多种安全控制，来应对不同的潜在风险，最终达到可接受的总体风险水平。

当然，第三方为其自身目的而进行风险评估时可能采用不同的方法判断风险。在这种情况下，应谨慎使用其结果。

相关信息可能不仅与待开发的IT产品相关，而且与其运行环境相关。该运行环境决定了对人员，程序和物理控制的可依赖水平。公共空间与密闭服务器机房有非常不同的安全需求。人员、程序和物理控制也应被研究，这是安全问题定义的一个重要组成部分。

对于有关风险和控制的信息，设计决策可能已经决定了某些安全功能应如何实现。例如，使用生物识别身份验证而不是口令，或者使用某些安全可靠通信协议定义安全特性。

安全问题定义的某些部分可能无法通过技术手段解决，它们只能由人员、程序和物理控制来解决，但它们仍然要在安全环境中加以描述。事实上，确定安全问题定义的任何方面都应描述为非正式安全要求的一部分。

当所有可用的信息已被确定、核对和检查后，相应信息被归类为三个方面：

a) 该产品应应对潜在攻击；

b) 该产品应具备的安全属性或功能；

c) 该产品不需要具备的安全属性或功能。

这类区分是很重要的，因为它们在PP编制的后续步骤处理中要使用不同的方法。潜在的攻击应被视为对TOE的威胁并予以应对。产品应具备应对该威胁的安全属性和功能，包括规定的安全解决方案，符合组织安全策略。对于该产品不需要具备的属性和功能，则被处理成假设。

从不同来源获得的非正式要求的不同部分可能会重复，甚至可能是矛盾的。这些有矛盾的信息需要在安全问题定义之前被挑出来，达到不重、不漏地表述非正式要求各方面的目标。

8.3 识别和确定威胁

8.3.1 简述

一旦非正式的安全要求已被描述，并且攻击和属性已被定义，下一步就是进行威胁分析以识别应对潜在威胁。GB/T 18336—2015(所有部分)并没有指定任何用来识别威胁的特别方法。

威胁分析和识别比定义组织安全策略和假设更加复杂和困难。但是如果非正式的要求主要来自组织安全策略或强制性要求(见8.2)，则可能更优先定义安全问题中的策略和假设(见8.4和8.5)，然后再如本节所述方法进行威胁分析，最后重新审视并完成策略和假设的定义。如果策略和假设可以很容易地确定，那么他们可以立即被使用来排查威胁，从而简化威胁分析。

为了执行威胁分析，有必要执行如下三个活动：

a) 决定要使用的分析方法；

b) 识别该方法所需的参与者；

c) 应用方法。

8.3.2 决定威胁分析方法

识别威胁的最佳方法，取决于非正式的安全要求是如何得到的。如果要求是根据风险评价的结果

规定的，那么一系列的威胁可能已被作为风险评估的结果。如果不是这样，仍然可从其他现有的信息来识别相关威胁。

有多种可用来进行威胁分析的方法，可使用如下技术：

a) 威胁树分析；

b) 威胁数据库搜索；

c) 特别识别。

威胁树分析是一个针对问题分解的分析技术，广泛应用于风险管理与可靠性工程领域。将经过深思熟虑的第一个抽象定义作为树的根，随后在下一级细化创建出一组新的、更详细的，连接到根的节点。这里每个节点将成为下一个新子树的根。最终，叶子节点的描述将足够具体而不需要进一步细化，其将作为 PP 或 ST 中规定的实际威胁。威胁树还提供了一个威胁选择原理，并保障没有相关威胁被忽略。

数据库搜索是基于一个或多个预定义的通用威胁数据库，查看哪些条目与识别出的产品攻击相匹配。数据库搜索的优点是可以考虑到各种各样的威胁，这些威胁以一致的方式进行表述和规定。数据库搜索的缺点是未覆盖针对特殊产品的专业威胁，因此无法识别出这些威胁。同时，数据库中的威胁在产品适应性上的描述过于笼统，也不易识别出相应的威胁。

特别识别是要从考虑产品问题开始，以非结构化的方式来标识威胁。

8.3.3 识别参与者

8.3.3.1 简述

GB/T 18336—2015(所有部分)要求每个威胁描述应包括威胁主体-资产和攻击动作，“资产”应理解为有多种类型的抽象资产，因为在 COTS 产品的案例中，要保护的实际资产对 PP 或 ST 编制者来说是未知的。

8.3.3.2 威胁主体

GB/T 18336—2015(所有部分)的威胁主体定义为“可对资产产生负面作用的实体”。当描述 PP 和 ST 中的威胁时，定义威胁主体最好尽可能的简单。威胁主体列表可涉及五种类型：

a) 攻击者；

b) 授权用户；

c) 特权用户；

d) 管理员；

e) 系统的所有者和开发者。

攻击者是指未经授权的，想要访问受 IT 产品所保护的资产的人。这其中也包括经过授权却故意隐瞒自己身份的用户。对 IT 系统所有者来说，攻击者是不可知的，除非其攻击行为被检测到，且能链接到一个确定身份的人。

授权用户是指已授权的，可以根据安全策略使用产品的人，并且能得到资产所有者的许可来访问受产品所保护的资产。授权用户对系统所有者来说是已知的，其不敢破坏资产，否则会被追究责任。

特权用户是指已授权的，可用与安全策略相反的方式来使用 IT 产品的人，并且可以在资产所有者没有明确许可的条件下访问资产。大多数系统管理员应是特权用户。当然，还有其他类型的特权用户，如维修硬件和软件的工程师。虽然 IT 产品无法对特权用户的行为所造成的损害进行防护，但特权用户要对自己的行为负责。

管理员是指当 IT 产品安装在运行环境上之后，那些负责其正确操作的人。管理员负责建立控制来防止损坏资产，以及当资产损坏时负责检测和恢复。管理员所能做的动作应被限制，这是因为如果管

理员未正确执行操作，产品可能无法充分保护资产。

系统的所有者和开发者是指那些负责规范、设计、实施一个系统或 COTS 产品的人。这些人虽然不会直接损害资产，但如果其决定不正确，产品可能无法充分保护资产。

通过使用这些定义，在不同的时间内，一个人也可能成为这些角色当中的多个角色。

8.3.3.3 资产类型

资产对威胁分析来说非常重要，需要得到正确地识别。大多数威胁分析方法可以处理不精确或重叠的敌对行为，但需可辨识并清楚地描述资产。本节提供一个详细方法来确定需要由一个特定的 IT 产品保护的资产或资产类型。

针对一个系统，作为系统组成部分的受保护资产往往会被准确地识别。针对一个 COTS 产品，产品的实际作用往往不是已知的，因此只可能确定产品计划保护的资产类型。

与 IT 系统相关的资产通常分为三类：

a) 信息资产；

b) 过程资产；

c) 物理资产。

信息资产表现为对组织有价值的数据。信息资产类型示例如下：

——一般数据；

——系统数据；

——专业数据库；

——客户数据。

专业数据库表现为对一些用户有价值的信息。例如人事数据库(只对人力资源部门有价值)或客户数据库(只对部门的订单处理、销售的人有价值)。客户数据可以指那些不归系统所有者占有的数据或一个特殊的合法数据。

对于一个系统来说，通常有可以识别实际数据库名称与特点，或其他受保护的资产信息。

在最简单的情况下，所有的数据都可以被视为拥有相等的价值和被攻击的风险，并由一个单一的信息资产表现出来。

将系统数据与其他数据区分开来是必要的。如果系统数据被修改或删除，TSF 可能失效或不能正确操作，会放行攻击。而其他数据如果被修改，TSF 将继续发挥作用，保护相关资产。因此，在通常情况下资产可分为两类，一个表现为 TSF 数据，另一个表现为受产品保护的所有其他数据，称为用户数据。

注意，不同类型的 TSF 数据如果泄露，可能会受到不同的攻击，或有不同的后果。因此需要对系统数据加以区别。TSF 数据类型示例如下：

——TSF 配置数据；

——鉴别信息数据库；

——审计记录。

有时受限和特定形式的数据很容易受到专门攻击，例如密钥，应加以区分。

业务过程资产表现为各种应用程序，在这些过程中数据被转换或被分析，其与信息资产的区别是相关数据在未被应用程序处理的情况下几乎毫无价值。过程资产类型示例如下：

——财务；

——通信；

——后勤；

——制造；

——办公自动化。

财务应用可能包括工资、投资管理或账户管理。通信系统包括电子邮件或网络信息处理。后勤系统可能包括订单处理、仓库控制和资源调度。制造应用可能包括实时过程控制。办公自动化可能覆盖结构化文本处理。

对于一个应用系统来说，识别需要受保护的实际过程的名称和特点通常是可能的。

一般来说，过程资产会受到修改或拒绝服务攻击。例如，相关应用软件的功能可能发生改变，或删除了授权检查，或改变财务处理功能。

物理资产表现为实际的信息处理设备，用于支持信息和过程资产。物理资产类型示例如下：

——关键网络基础设施；

——便携式电脑；

——数据中心。

物理保护或被排除在外，或由运行环境来提供，并且通过假设来处理。物理资产一般不会出现在PP或ST中。然而，也有适用的技术，如断电自动关闭技术可以对物理资产提供保护，在此情况下，物理资产可能要在PP或ST中体现。

不是要识别出大量的资产或资产类型，如果两种资产或资产类型有相同攻击和攻击后果的潜在可能性，应将其组合成一个复合资产类型。大多数TOE只会保护两种类型的资产，即TSF数据和用户数据。

8.3.3.4 敌对行为

GB/T 18336—2015(所有部分)没有提供任何关于如何描述敌对行为方面的指导。至于威胁主体，最好的建议是列举出尽可能简单的一系列行为。一个简单且广泛的敌对行为集如下：

——不适当的访问；

——访问权的不当传递；

——拒绝合法访问；

——未尽责任。

此行为集涵盖了实践中可能出现的威胁，尽管有时特别的敌对行为可能会产生不同的后果，但需分别进行阐述。可能有其他的、专业的敌对行为类型不属于上述行为集，从非正式的安全要求来看，需分别处理。

8.3.4 威胁分析方法

一旦选定威胁分析方法，且运用该方法的必要信息已准备好，下一步就是要生成一个威胁列表。

在实践中，许多可能的威胁不用考虑，这可通过两个技术来识别，一是识别出已排除的或可容忍的威胁，二是识别出已被策略覆盖的威胁。

作为非正式安全要求的一部分，许多类型的威胁可能不用考虑，这或是因为其已被排除在IT产品范围之外，或是因为其相关风险影响很小而被容忍，或是因为其已被转移给了第三方(如保险公司)。

在COTS产品中，应用上面的威胁排除方法是很普通的事情。例如，假设买方希望购买一个专业防病毒产品，或者在不受感染的环境下使用产品，那么操作系统供应商可能决定不在其产品中集成防病毒功能。

容忍威胁通常是在系统环境中发现的。这要求对资产价值进行评估，而COTS产品制造商不会去做这些事情。

在许多IT产品中，事先就已决定了要包括安全功能，而不是通过实际威胁的独立分析导出这些安全功能。这在COTS产品中是很常见的，例如，即使产品被设计成单用户使用，操作系统供应商通常也还会使产品包括用户标识与鉴别功能。

如果强制功能去对抗一个特定类型的威胁，那么无需再进一步调查这个威胁。

威胁的相关信息通常在IT产品应具备的属性列表中显而易见。如果不是，它需要被证实，然后添加到该列表中，它也应以策略声明的形式记录下来。

应识别和考虑所有威胁，并产生完整的威胁列表，从主体、资产和敌对行为等方面来描述每个威胁。

8.3.5 实用建议

威胁表明了IT产品可能被攻击的可能途径。因此，针对威胁描述的措辞最好方法是使用动词，如“可能”，例如如下威胁描述：

T.UNAUTH 一个未经授权的人可能会尝试访问和使用 TOE 资源。

注：针对PP或ST中的有关威胁、策略、假设、安全目的、安全要求的陈述示例用斜体字表示，以区别于本标准的正文内容，此约定适用于后续章节。

用一个威胁名来开始威胁的描述，按照惯例，大多数的PP和ST作者以“T”作为威胁名称的开头，说明应尽量简短，突出重点。

威胁分析方法，无论在本章节中描述的或是自己选择的，切不可盲目使用。它们应是合适的和可解释的，以满足特定的安全问题的要求。

如果威胁的主体、资产和敌对行为是相似的，那么威胁可以进行组合。这将减少威胁列表的大小，并在之后节省时间，因为相同的控制往往会被用来对抗相关威胁。

资料表明，未被考虑的威胁往往是间接表述的。例如如下陈述：

管理员可以被假定为无恶意的，值得信赖的和有能力的。

这主要表现在威胁主体方面，大多数类型的威胁通常与该类型的主体相关联。有些专门针对管理员的威胁类型可能因此而无需考虑。其他类型的威胁仍然适用，但是可能仅限定于其适用的威胁主体，例如普通用户。同时，应把这些可缩小威胁范围的假设添加到假设列表中。

在某些情况下，仅因其相关风险是不可接受的，而可能无法识别威胁主体或敌对行为。例如，一个基本的抽象机未能执行其相关的安全模型。在这种情况下，创建基于猜测或想象的描述是没有意义的，这种威胁是不被安全问题定义所接受的，并应加以识别。

一旦威胁的最终列表被制定出来，应始终检查其完整性和一致性。

威胁分析有可能没有识别出任何适用于TOE的威胁，这在GB/T 18336—2015(所有部分)评估中完全可以接受的，描述威胁的章节可保留为空，以表明没有特别被识别的威胁。

8.4 识别和确定策略

安全问题定义也应包含一系列TOE应遵守的OSP。对比威胁，策略一般更容易识别和描述。

组织安全策略是IT产品应做的事情的声明，这与所面临的威胁或其他情况无关，一个清晰且适当的策略可参考如下陈述：

P.IDAUTH 管理员在访问任何 TOE 功能或数据之前要验证自己的身份。

像威胁描述一样，用一个策略名来开始策略的描述。策略的描述应尽量短，重点突出。按照惯例，大多数的PP和ST的作者将策略以“P”开头命名。

在GB/T 18336—2015(所有部分)，策略通常被称为OSP。本标准通常采用简单的术语“策略”来表述。

多数适用的策略应在非正式安全要求的识别过程或在威胁分析过程中已被确定。然而，最终应做

一个检查用来识别任何与安全问题相关的策略。

策略用于规定如下内容：

——要在 TOE 中纳入强制性的安全功能；

——将用于实现特定安全功能(这隐含 TOE 应提供的功能)强制性的技术/方法。

策略也可以被用来代替威胁，如下列情况：

——无法确定某个特定的威胁是否已存在，但策略已决定进行保护以应对这种威胁；

——策略已决定如何应对特定的威胁。例如，规定某种控制措施来防止攻击，或规定在发生攻击时该如何处理；

——策略已决定采用特殊方法来应对一些相关威胁。

在最后的检查过程中识别出的策略可能需要对前期的安全问题定义活动进行修正，例如，删除已被新策略覆盖的威胁。

策略陈述有时也会出现误用情况，其所陈述的要求实际上不能由 TOE 来完成，而是应由 TOE 的运行环境来执行。如果一个要求不能被 TOE 所实现，正确做法是将其作为涉及运行环境的假设。如果策略既不能由 TOE 来执行，也不能由运行环境来执行，那这样的策略就是毫无意义的。

在识别安全问题、解决问题的过程中，所提出的 TOE 边界可能需要更改，以实现 TOE 功能和运行环境之间的转换。这可能会导致策略成为假设，或假设成为策略，或者为顾及新的 TOE 边界而重新规定策略或假设。同样，在能被分解成若干处理不同安全问题部件的组合 TOE 中，一个部件的假设通常被另一个部件作为策略来要求。在这种情况下，细致的策略陈述将有助于策略在其他 SPD 中作为假设来使用，以确保兼容性和检查的一致性。

可能存在这样的情况，即在准备安全问题定义时，还不清楚策略是由 TOE 还是 TOE 运行环境来实现。当安全功能的要求较为明确时，这个问题可以在安全目的的定义过程中予以解决。TOE 安全目的和环境安全目的都可以反向链接到策略，一个策略甚至可部分由 TOE 实现，部分由环境实现。

并非所有的安全问题都需要策略，这在 GB/T 18336—2015(所有部分)评估中是完全可以接受的，描述策略的章节可保留为空，以表明无可适用的策略。

8.5 识别和确定假设

安全问题定义的第三个方面是应包含一系列适当的假设，用以限制或排除 TOE 内部的安全特性。

假设是针对事项的声明，用以表明这些事项无需 IT 产品来实现，也不需考虑威胁或其他事项，假设只是在陈述事实。一个明确且表述良好的假设可参考如下陈述：

A.PHYSICAL TOE 将放置在一个物理安全的地方。

假设有两个用途：

——要表明一个特定控制或控制类型将由运行环境提供，并不是由 TOE 提供；

——要表明特定威胁或威胁类型不用考虑，因为在假定的运行环境中，它们将不存在或者并不重要。

应加以区分环境控制方面的假设与未被考虑的威胁方面的假设，因为前者是由 GB/T 18336—2015(所有部分)要求的，而后者是本标准的建议，以简化显示安全目的涵盖只适用于威胁和策略。

假设描述应尽量短，突出重点，并为每个假设设定一个简短的名称。按照惯例，假设名称一般以“A”开头命名。

关于运行环境的假设可分为三类：

——物理保护；

——人员和程序；

——TOE 的外部技术功能。

GB/T 18336—2015(所有部分)涉及“运行环境的物理、人员和连通性方面”(参见 GB/T 18336.1—2015 中 A.6.4)。然而这是不够的,例如,有关外部技术控制的假设:

A.INTERNET TOE 要与互联网隔离。

关于技术控制的其他假设往往也是必要的,例如:

A.NO_DEV_TOOLS 在 TOE 的运行环境中,不允许再出现开发者对系统进行功能性修改的工具。

在许多情况下,策略和威胁将会由 TOE 和部分环境协同处理。例如,TOE 内的技术控制措施可能需要支持的程序或物理措施,以便有效地工作。这样的环境配套措施应识别并标识为假设。

在评估过程中,假设是不会被测试的,其被视为始终真实有效,这有助于说明安全问题的一致性和完整性。

很多假设都可能在确定非正式的安全要求或威胁分析过程中被识别出来。在安全问题定义过程中,可执行一个全面检查来识别任何相关的假设。

假设通常可以用来抵御多种相关的威胁,如果采用威胁树方法,多个被环境抵御的威胁将共享威胁树远端的分层节点。例如,如果不考虑由管理员的敌对行为而造成的威胁,这可以表述成一个单一的假设,如下所示:

A.NO_POOR_ADMINISTRATION 管理人员有必需的技能、培训、时间和资源来执行所有的已分配的管理功能,并能够成功执行。

在阐述假设时,如果假设的陈述是不真实的,TOE 有可能会被攻击成功。

通过类型来分隔假设将有助于识别和确定安全目的。首先,应分隔出关于人员、程序和物理安全的假设。其次,是与 IT 运行环境所提安全功能相关的假设。最后,是关于威胁不被考虑的假设。这些假设都不能推导出安全目的,其应被分隔。

有些安全问题可能不需要任何假设,这在 GB/T 18336—2015(所有部分)评估过程中是完全可以接受的,描述假设的章节可保留为空,以表明没有必需的假设。

8.6 完成安全问题定义

最后的阶段是完成 SPD。这涉及两个任务:

——准备一个完整的威胁、策略和假设列表;

——执行一致性和完整性检查来确认 SPD 可准确地描述安全问题。

威胁、策略和假设的陈述对评估目的来说是非常明确的,因此在 GB/T 18336—2015(所有部分)中并未要求提供一个 SPD 基本原理。但在实践中,还是建议生成一个 SPD 基本原理,其可将每个 SPD 元素映射到非正式的安全要求,并表明这个覆盖是完整的。如果要求发生改变,基本原理可使 SPD 更容易重新定义,并减少引入错误的风险。

一致性和完整性检查应检查所有在安全问题范围内的约束和要求是否已反映在策略或假设中,应检查所有识别出的威胁是否可通过某种方式予以抵抗或不予考虑。SPD 的所有策略、威胁和假设应可反向链接到原始的非正式的安全要求,可通过创建一个交叉引用表来显示这种一致性和完整性。

假设和策略有时可能出现冲突,例如,策略是“要去做这件事”,而假设是“不需要做这件事”,这时策略和假设之间产生了矛盾。在描述实际要求时,需要使用良好的解释和精确的用语。

9 安全目的

9.1 简述

本章针对 GB/T 18336.1—2015 中 A.7 和中 B.7 的要求，就 ST 或 PP 中的安全目的提供指导。至于安全目的，GB/T 18336.1—2015 中 B.7 指向了 GB/T 18336.1—2015 中 A.7，暗示两者的预期内容是相同的，且 GB/T 18336.3—2015 中，对这两者的验证要求也是相同的。

安全目的是安全问题预期反应的简明陈述(见 GB/T 18336.3—2015 的 9.4.1 和 10.4.1)。如果安全目的被表示为所需安全功能的概述和结构，并且提供了一个 SFR 细节与 SPD 抽象问题定义之间的链接，那这个安全目的才算符合要求。

GB/T 18336—2015(所有部分)定义了两种类型的安全目的：

a) TOE 安全目的，通过实施 TOE 的 IT 措施来满足；

b) 环境安全目的，由 IT 环境，或由非 IT 措施来满足。

如图 2 所示。

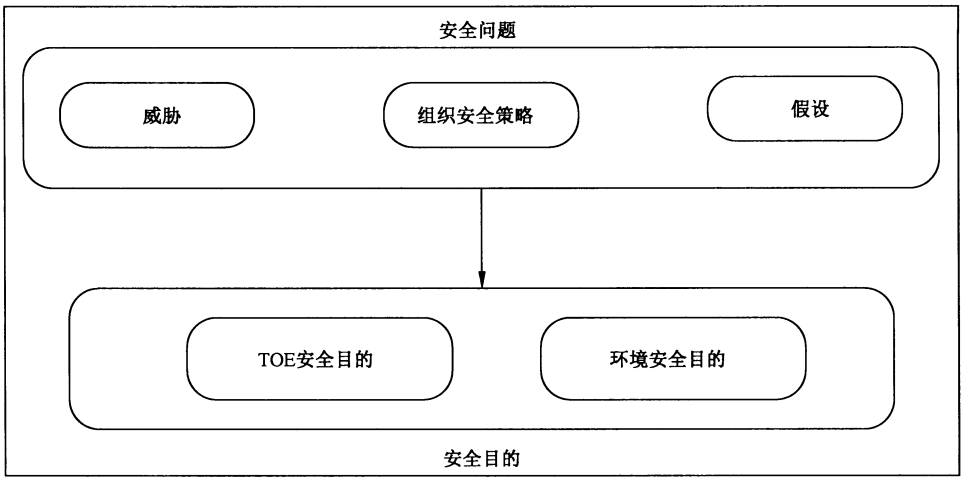

图 2 安全目的类型

所有的 PP 和 ST 都应确定环境安全目的，低保障级的 PP 和 ST(见第 14 章)不必指定 TOE 安全目的。

本节的其余部分假定这两种类型的目的都是必要的，并能追溯到安全问题定义。

GB/T 18336—2015(所有部分)未设定编制安全目的的特定过程或方法论，用户可以使用任意方法。本章介绍了一种在实践中尝试和测试过并且在许多组织和环境中十分有用的简单方法，此方法包括如下步骤：

a) 构建所有安全目的涵盖的威胁，策略和假设列表；

b) 确定非 IT 运行环境目的；

c) 确定 IT 运行环境目的；

d) 确定 TOE 目的；

e) 确定安全目可反向链接回已被识别的威胁、策略和假设。

GB/T 18336—2015(所有部分)指出安全目的应简明扼要，在实践中，需要在以下两方面之间取得平衡：

a) 安全目的应有助于读者理解在安全问题定义中标识的那些安全问题是由 TOE 来处理。理想情况下，TOE 安全目的应与实现是无关的。关注的重点是安全目的是什么，而不是如何去实现安全目的。

b) 应确保安全目的的定义不是在重复安全问题定义中的威胁、OSP 等信息，应以一种不同的方式去说明如何应对安全问题。

当构建安全目的和安全要求基本原理时，应检查安全目的的细节描述是否正确。如果其中一个原理内容过于简单，而另一个却过于复杂且难以理解，这有可能是安全目的的描述过于详细或过于抽象而造成的。

明确的 TOE 安全目的定义有助于确保选择的安全功能要求满足安全目的，也有助于最大限度地减少 TOE 评估的成本和时间。

9.2 构建威胁、策略和假设

首要任务是构建一个涵盖所有威胁、策略和假设的列表。

某些看似可能与 TOE 相关的威胁，在经过风险分析和环境因素的考虑之后，应判断其可不被考虑或可被忽略。如果遵循本标准推荐的方法，将在 SPD 阶段将这些威胁识别为假设。这类威胁不会产生安全目的，应确保这类威胁已从 SPD 中排除。

其余的威胁、策略和假设应被分为如下类型：

——与非 IT 运行环境相关的；

——与 IT 运行环境相关的；

——与 TOE 功能相关的。

这种区分表明：需要物理控制的策略只适用于非 IT 环境，针对 TOE 潜在的攻击威胁面对的是 TOE 安全功能，假设适用于运行环境。

如果一项策略或需求同上面几个类型存在交叉，应要加以细分。例如，威胁 T.EAVESDROP 可能被分成两个：

——T.EAVESDROP(通信)，分配给 IT 运行环境；

——T.EAVESDROP(内部)，分配给 TOE 功能。

如存在疑问，可把有关政策或威胁拆分成多个条目，进而删除不必要的条目。另一方面，有用而缺失的条目也会造成安全目的的缺失，这将在 PP/ST 验证过程中带来繁重的检测成本。

9.3 识别非 IT 运行环境安全目的

与 TOE 相比，定义其运行环境的安全目的更加容易，并且非 IT 运行环境安全目的比 IT 运行环境安全目的更容易定义，因此应先关注非 IT 运行环境安全目的。

为确定这些安全目的，第一步是应把所有分配给非 IT 运行环境的假设改写为和它们一一对应的安全目的。在 PP 和 ST 中以及 TOE 评估过程中不再对环境安全目的做进一步分析。

其他非 IT 运行环境安全目的可能包括：

a) 建立和实施以确保 TOE 安全使用的程序(特别是根据环境的假设)；

b) 在安全实践中用于教育、培训管理员与用户的目的。

在此阶段确定这些目的可能很难，因为其与 TOE 安全目的相关。如果这些目的比较明显就添加进来，否则就在随后的环境目的检查阶段再添加这些目的。

环境安全目的的识别命名通常以“OE”开头，这有助于与通常以“O”开头的 TOE 安全目的进行区分。应清楚的描述以指出实现环境目的的方法是程序上的，还是物理上的，如有必要，可将非 IT 环境

也包含在目的描述中。

从假设得出环境安全目的的措辞与假设的措辞相比最好不要发生变化，即作为事实陈述，例如：

OE.RESIDUAL 磁介质在最终处置之前要先被消磁或被碎掉。

从威胁和策略中衍生的环境安全目的应被描述成要求，例如：

OE.AUD_REVIEW 操作人员应定期审查审计跟踪异常的行为。

大多数非 IT 运行环境目的来自于假设。单独从威胁中导出的环境安全目的可能弥补在安全问题定义中未被识别出的假设，应检查 SPD，并对其做必要的修改。

单个目的定义可以覆盖几个相关的假设，或一个假设和相关威胁，或策略及相关的威胁。如果整体结果是清晰的，那么可把这些元素结合在一起，否则不应这样操作。

9.4 识别 IT 运行环境安全目的

IT 运行环境目的识别技术与非 IT 操作环境的识别技术是相同的，将其与非 IT 目的分开是非常重要的，如果 TOE 边界发生变化，那么 IT 环境安全目的可能会成为 TOE 安全目的。

按照惯例，IT 运行环境目的以“OE”开头的命名方法进行识别。针对它们的描述中应包括“IT 环境”，或以其他方式明确表示它们会由 TOE 之外的技术手段来实现。

早期版本允许为 IT 环境目的指定安全要求，以便定义和解释它们是如何被实现的，这在 GB/T 18336—2015(所有部分)中是不允许的。

在组合产品中，一个域的 IT 环境安全目的将成为其他安全域的 TOE 目的。

9.5 识别 TOE 安全目的

TOE 安全目的是最重要且最难表述。与环境安全目的不同的是它们将被用来作为推导出 TOE 安全功能要求的依据。安全目的陈述应能清楚地表达且明确它们的意图，并在安全要求和安全问题之间提供详细且良好的可追溯性。

本节建议基于安全功能的类型来对 TOE 目的进行组织，并与 GB/T 18336.2—2015 的安全功能类和族的结构相关联。依照广度和深度区分主从目的，并分开描述它们。

识别 TOE 目的的第一步应将前面分配给 TOE 的威胁和策略列表重新排序，以便把相关威胁和策略放在一起。应注意的是没有关于 TOE 功能的假设，因为假设只涉及运行环境。

对于具体 PP 或 ST 的威胁和策略分组形式将取决于相关 TOE 的特性。如果分组与 GB/T 18336.2—2015 的安全功能要求结构有关，那么这有助于生成 SFR。

本节提出了一种覆盖所有威胁和策略的简单分组方法，如下所示：

a) 访问控制(客体、属性、操作、访问规则)；

b) 用户管理(用户类型、标识、鉴别)；

c) TOE 自保护(故障检测、可信恢复等)；

d) 安全通信(通信链路连接、链路属性、规则)；

e) 审计(事件记录、响应、事件管理、分析)；

f) 安全架构要求(所需的属性和约束)；

g) 其他功能(不包括在这些范围下的，如可信时间源、随机数发生器)。

这个分组与第 11 章提及的安全要求结构之间存在者密切联系，以便识别和确定安全功能要求。

下一步是为选定的安全服务和安全防护要求类型给出简单的定义。此过程不是试图分析和总结安全问题定义，而是应从 SPD 反向链接到非正式安全要求。通过非正式安全要求可以很容易得出每种类别的主要安全功能。如果某些区域未被提及，或被识别为明确不相关，则可在此阶段忽略这些类别。

将安全服务列表与威胁和策略列表相比较。对于每个安全服务，判断与哪个策略和威胁是相关。将未匹配的策略和威胁归为其他安全服务。

下一步，将与每个服务相关的威胁和政策分成通用和具体的相关要求。通用要求应适用于服务定义的所有方面，特殊的要求适用特殊方面。

最后，将服务定义为一个能解决通用要求的陈述，这个成为此服务的主要目的。将每个具体要求定义为与这个服务相关的，但独立的从属安全目的。

TOE 安全目的用来对抗威胁，这通过移除或阻止构成威胁的必要要素来实现。例如移除威胁主体执行敌对行为的能力，或移动、改变资产，从而使敌对行为不再适用，或消除威胁主体（例如，通过引入物理访问控制的环境目的）。威胁也可被间接处理，例如通过实施问责审计行为，熟练的实践阻止偶然的用户错误，经常备份以便丢失或受损的资产可以很容易地恢复。

并不是所有的威胁都可被防止。有时最好的行动就是检测相关事件，并产生报警或审计日志条目。

在规范过程中，有必要重新分配威胁和策略。当安全服务被逐步细化并被定义时，特定的威胁或策略可能更适合于从属目的而不是主要目的，反之亦然，或者它们甚至可能更适合作为另一个安全服务的一部分。这个过程通常用于确定遗漏的运行环境相关安全目的。例如，如果告警被选择作为特定威胁的一个响应，那么需要一个管理员来响应告警。在某些情况下，设计决策甚至可能把对特定威胁或策略的保护从 TOE 目的完全移动到运行环境，反之亦然。这些变化都是预期的。其应重复几次，直到得到一个明确的覆盖所有类别的安全目的列表。

同描述通用保护要求（直接关联到一个主要目的）一样，特殊的策略有时被用来约束相关的技术解决方案。这种类型的约束应被表示为一个与通用要求关联的从属目的。

有时威胁也可直接对应到一个从属安全目的，此时可将次要的安全目的直接映射到问题源。这样能方便后面的可追溯性，一方面便于在安全原理部分关联到安全问题，另一方面也易于读者的理解。

另一个定义从属目的是所需的控制类型。控制可以是预防性的（阻止事件发生）、检测性的（预测一个事件发生）或纠正性的（修复事件的后果）。

下面是一个预防性的安全目的的例子，其要求 TOE 对用户进行标识和鉴别：

在用户被授权访问 TOE 设施之前，TOE 要确保每个用户是唯一标识的，且已被鉴别。

访问控制和信息流控制的安全目的也归入预防类。授权访问一般要求 TOE 应执行多个访问控制和信息流控制策略，建议识别每个策略的安全目的，这有助于简化安全要求基本原理的编制。

下面是一个检测性的安全目的的例子，其要求 TOE 可提供原发抗抵赖性的能力：

TOE 将提供一种方法，信息获取者可通过这种方法产生用于证明信息原发的证据。

下面是一个纠正性的安全目的的例子，其要求 TOE 对检测到的入侵做出响应：

TOE 对即将发生的违反安全的事件进行检测，以中断 TOE 用户服务的时间最短为目标，采取适当措施遏制攻击，

不要期望安全目的和威胁或策略之间的一一对应，处理一个策略的主要安全目的也对抗某些威胁。同时，威胁和策略可能需要用不同的方法处理不同类型的资产，并且每种类型的资产也需要不同的从属目的。

TOE 安全目的一般是以“O”而不是以“OE”开头命名的，以便区分环境目的，其应明确表明实施目的的方法应是 TOE 执行的一部分。

9.6 产生安全目的基本原理

确定安全目的的最后一步是产生基本原理，将安全目的映射到 SPD 的威胁、策略和假设，以表明识别的安全目的是必要的，并显示所有 SPD 中的威胁、策略和假设都被安全目的所覆盖，或者考虑其是否

需要进一步排除。除了低保障要求的评估，基本原理在 GB/T 18336—2015(所有部分)中是必要的，并在 PP/ST 中进行验证。

产生基本原理的方法是准备一个 SPD 与目的之间的关系表，并检查是否有任何不一致。

假设每个安全目的可以对应到至少一个威胁、策略或假设，关系表可显示那个安全目的是必要的。这并不能保证是否有多余的安全目的，因为其他的安全目的也可以对应到相同的威胁、策略和假设，并提供足够的覆盖范围，这可以通过充分性来进行检查。如果一个 PP 或 ST 声称符合其他 PP，基本原理应表明 TOE 安全目的与被引用 PP 的安全目的陈述是一致的。

10 扩展组件定义

当 PP 或 ST 作者有可能无法准确确定安全功能要求和保障要求时，将不得不改进 GB/T 18336.2—2015 或 GB/T 18336.3—2015 的现有组件。在这种情况下允许定义扩展组件，本章旨在为扩展组件提供指导。

应说明的是应尽可能避免使用扩展组件定义。使用扩展组件将使得很难去比较不同产品在安全功能和保障要求之间的不同。相反，应尽可能地使用 GB/T 18336—2015(所有部分)现有组件，只有在现有组件不能满足条件的时候才使用扩展组件。

GB/T 18336.1—2015 要求以类似 GB/T 18336—2015(所有部分)现有组件的方式定义扩展要求。最好采用与 GB/T 18336—2015(所有部分)相同的结构来描述扩展组件。关于扩展组件的命名，应确认如果这个组件符合其中一个已经在 GB/T 18336—2015(所有部分)中定义的类或者族，就应以这个类名或者族名加上一个指示符进行命名。ST 或 PP 作者可更容易获取扩展组件以及按照其要求进行初始化。

使用 GB/T 18336.2—2015 功能组件作为模型扩展 SFR 组件将涉及：

a) 定义的 SFR 扩展组件要与 GB/T 18336.2—2015 组件在一个相似的抽象水平上；

b) 使用与 GB/T 18336.2—2015 组件相似的风格和语法；

c) 使用与 GB/T 18336.2—2015 组件相同的拓扑结构和命名方法。

GB/T 18336.2—2015 功能组件的表现形式的具体特点包括：

a) 大多数功能要求以 TSF 应或者 TSF 应能再加上“允许”“检测”“强制”“确保”“限制”“监控”“许可”“预防”“保护”“提供”和“限定”等词语开始；

b) 使用标准术语，例如安全属性或者授权用户；

c) 每个元素往往都是独立的，可以不参考之前元素进行理解；

d) 每个安全要求都可以被评估，例如：应确定其是否满足 TOE 的要求。

在构建一个扩展组件的时候，应考虑 SFR 的如下情况：

a) 应包含的任何赋值或者选择操作应由 ST 或者 PP 作者完成；

b) 指出应在 PP 或者 ST 之中的对其他 SFR 的依赖关系；

c) 描述可审计的任何事件，并且应记录相应的事件信息；

d) 针对安全管理的影响，例如依赖需要管理的安全属性。

为未包括在 GB/T 18336.2—2015 中的扩展 SFR 命名，应使用 GB/T 18336.2—2015 的拓扑结构和命名约定形式。扩展安全功能组件应使用“F”作为功能，其次是相应的类，族名后跟组件编号。基于现有的类扩展组件可以被插入到适当的位置。当扩展组件和现有类是无关命名时，为了明确其新的扩展安全要求，可以构建“EX”类或者在组件名后加上“EX”。如何定义扩展组件应在 PP 或者 ST 的应用说明中予以解释。应注意的是，扩展组件命名规范不应与 GB/T 18336.2—2015 冲突。

附录 A 提供了一个关于扩展组件的例子，并且指明它和 GB/T 18336.2—2015 中定义的组件类似。

附录 A 中的例子，描述扩展的安全功能组件的方法也能描述扩展保障组件。当该保障活动不包含在 GB/T 18336.3—2015 的现有组件中时，为安全目标或保护轮廓中所描述的产品定义一个特别保障活动是可以的。除了以类似于描述在 GB/T 18336.3—2015 中的保障组件方法，扩展保障组件还需要定义一个评估方法，用来阐述评估者确认产品符合扩展保障组件。

扩展保障组件的定义中应提供下列要素：

a) 开发者活动；

b) 开发者应提供内容和形式元素的要求；

c) 评估者活动。

GB/T 18336.3—2015 指出与保障组件关联的要素特征如下：

a) 开发者活动要素用来表示开发者应执行的活动，通常提供评估证据；

b) 开发者应提供内容和形式元素；

c) 评估者行为元素有两种形式：

——评估者活动形式通常为：评估者应确认所提供的信息满足证据的内容和形式的所有要求；

——评估者行为元素一般采取评估独立工作陈述和评估者的决定。

对于证据的内容和形式要求不仅应清楚、明确地表达，也要尽可能避免评估者的主观判断。

当定义扩展保障组件时，还需要定义在评估中符合扩展保障组件的评估者工作单元。工作单元应针对扩展保障组件的所有方面，给出评估者在评估中的明确建议。

11 安全要求

11.1 简述

本章针对 PP 或 ST 中的 IT 安全要求提供指导。PP 或 ST 指定 IT 安全要求分为两类：

a) TOE 安全功能要求(SFR)：指出 TOE 的安全功能应满足以实现其安全目的的要求；

b) TOE 安全保障要求(SAR)：指出实现 SFR 所需要的保障级别。

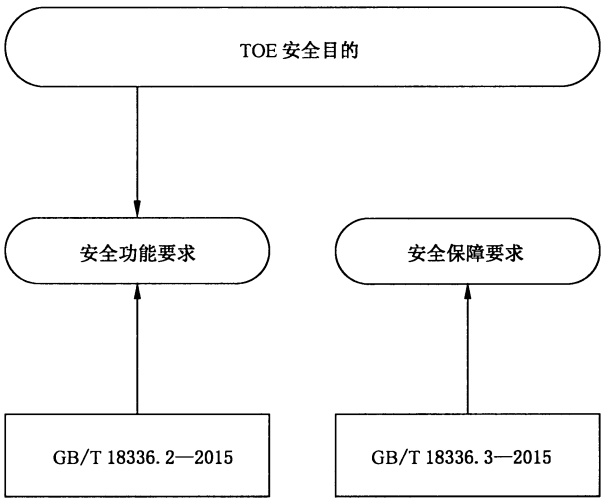

图 3 IT 安全要求来源

如图 3 所示，IT 安全要求的一个显著特征就是应尽可能地使用 GB/T 18336.2—2015 中定义的安全组件和 GB/T 18336.3—2015 中定义的保障组件来构建。使用 GB/T 18336—2015(所有部分)是为

了在IT安全要求呈现的方式上保证一定程度的标准化，使用GB/T 18336—2015(所有部分)来表示IT安全要求是为了更加方便地比较PP与ST。

可能存在这样的情况：在GB/T 18336.2—2015或GB/T 18336.3—2015中没有适当的功能组件或保障组件。在这种情况下，IT安全要求可能不能从GB/T 18336—2015(所有部分)选取。但是，自定义的IT安全要求应是无歧义的、可评估的，并且其表达方式与GB/T 18336—2015(所有部分)中的组件结构相似。

GB/T 18336—2015(所有部分)通过允许使用一组操作，即赋值、反复、选择和细化，用以适当地裁剪安全要求，使得在SFR和SAR的表述上有一定程度的灵活性。

GB/T 18336.2—2015和GB/T 18336.3—2015中的每个安全组件都有其在GB/T 18336—2015(所有部分)中的唯一参考：

a) 例如，在GB/T 18336.2—2015中，组件FAU_GEN.1.2的含义如下：
   ——“F”表明其为功能要求；
   ——“AU”表明其属于SFR中的安全审计类；
   ——“GEN”表明其属于安全审计类中的安全审计数据产生族；
   ——“1”表明其为安全审计数据产生族中的审计数据产生组件；
   ——“2”表明其为审计数据产生组件中的第二个元素。
b) GB/T 18336.3—2015中的组件也使用类似的方法，只是通过追加一个字母来指明其属于哪一类别，这些字母如下：
   ——字母“D”表明其属于开发者行为元素，是开发者实施的行为；
   ——字母“C”表明其属于内容和形式元素，是为了传达证据的信息；
   ——字母“E”表明其属于评估者行为元素，是评估者实施的行为。
c) 例如，在GB/T 18336.3—2015中，组件ADV_TDS.1.2C的含义如下：
   ——“A”表明其为保障要求；
   ——“DV”表明其属于SAR中的开发类；
   ——“TDS”表明其属于开发类中的TOE设计族；
   ——“1”表明其为TOE设计族中的基本设计组件；
   ——“2”表明其为基本设计组件的第二个元素；
   ——“C”表明其为这个组件的内容和形式元素。

SFR和SAR是从组件级别上进行选择的：如果一个组件包含在PP或ST中，那么该组件中所有定义的元素也应包含在PP或ST中。需要注意的是，组件之间存在两种关系能够作用于选择IT安全要求的过程：

a) 一个族中的组件可能存在层次关系，这表明该族中的一个组件包括同族另一个组件中指定的所有要求。比如，FAU_STG.4与FAU_STG.3存在层次关系，因为后者定义的所有功能元素都包含在前者中。然而，FAU_STG.4与FAU_STG.1之间没有层次关系，故在相同的PP或ST中有可能包含这两个组件。
b) 组件可能依赖其他族中的组件，这表明当一个组件不能够满足要求时，需要依靠另一个组件功能或与另一个组件的交互，才能正常发挥其自身功能。比如，FIA_UAU.1(对用户身份的鉴别)依赖于FIA_UID.1(需标识用户)。这些组件也应包含在一个PP或ST中，否则这些依赖被认为与威胁和安全目的无关。

11.2 安全范型

11.2.1 安全范型的解释和用法

为了更好地理解 GB/T 18336.2—2015 中为安全功能要求所定义的类、族和组件的结构，本标准对 GB/T 18336.2—2015 中第 5 章描述的安全功能范型进行说明。

GB/T 18336—2015(所有部分)提供安全范型的目的是为构建 TOE 安全功能模型提供一个基础，以表明 TOE 安全目的都被该安全功能模型所覆盖。前面章节中提到的范型，在这里可以用来构建一个安全功能的抽象模型，之后再使用 GB/T 18336.2—2015 中定义的 SFR 来表述。以下章节为如何构建这样的模型以及如何使用 SFR 进行描述提供了指导。

11.2.2 资源与客体的访问控制

11.2.2.1 解释

在 GB/T 18336.2—2015 的范型中，安全功能控制和管理资源的使用，这些资源由 TOE 所保护，它可能在 TOE 内部(如内存、CPU 时间、磁盘空间、服务等)，也可能在 TOE 的外部，但这些资源只有通过 TOE 功能(如其他系统的网络服务)的控制才能访问(至少对一些实体来说是这样的)。

为了满足安全目的，可能需要控制的资源举例如下：

——存储(包括内存和磁盘空间)；

——CPU 时间；

——外设或网络连接；

——功能。

GB/T 18336.1—2015 中的用户是这样定义的：TOE 以外的，并与 TOE 交互(或可能交互)的任何实体(人或 IT)。GB/T 18336.1—2015 中的主体是这样定义的：TOE 内部的，对客体执行操作的主动实体。用户和主体是向 TOE 请求服务从而处理客体和资源的主动实体。

为了实现安全目的，TOE 在对资源进行使用时应遵循一些需要强制执行的规则。这些规则可以控制资源的使用，同时也记录了资源的使用情况。

作为这些规则所有参数的列表举例如下：

——发起请求的实体的类型和身份；

——发起请求的实体的其他属性；

——请求指定的资源的类型和身份；

——请求指定的资源的其他属性；

——请求的类型；

——日期和时间；

——TOE 的内部状态。

为了执行基于以上参数的规则，TOE 需要维护并管理以下参数：

——对于外部实体(也称为“用户”)，TOE 需要识别并可能需要鉴别外部实体。如果规则仅属于特定外部实体集合或组的外部实体，对于 TOE 来说识别(或可能需要鉴别)这个集合或组就已足够。

——TOE 维护一个允许使用处于 TSF(TOE 安全功能)控制下的外部实体列表(或可能同时维护它们的安全属性)。在这种情况下需要有管理这个外部实体列表以及它们的安全属性的功能(假设列表是非静态的)。

外部实体和主体在请求服务并使用受控的资源时都需要使用 TSF 接口(TSFI)。

在某些情况下,主体可能代表外部实体进行操作。这些情况下外部实体"绑定"在主体上。作为绑定过程的一部分,主体的安全属性将经常被修改来反映绑定的情况。例如,TOE 的主体继承了外部实体的安全属性,但或许存在更多复杂的规则,用于定义主体的安全属性在绑定过程中是如何派生的。

对不同类型客体的访问和使用控制规则通常是有区别的。为了避免混淆,GB/T 18336—2015(所有部分)允许对不同的客体、主体和操作的规则集合进行分组,组成相应的"安全功能策略"(SFP),并通过在独立的 SFR 中引用 SFP 来表明 SFR 所属的安全功能策略。一个安全功能策略总是需要一个定义范围,其中定义了策略应用的主体、用户、客体、资源和操作的集合,这个定义应是无歧义的,以保证 SFP 的域是完整的。之后,针对主体或用户在使用客体或资源时的操作所执行的规则被定义为 SFP 的一部分。这些规则通常会基于主体、用户、客体或资源的特定属性。影响 SFP 规则的属性称为"安全属性"。在 SFP 中起重要作用的安全属性的管理要求同时也是 SFP 的一部分,其中包括定义 SFP 中实体的安全属性在其创建、导入、注册(针对用户)时是如何初始化的。总之,一个 SFP 描述了一组为特定集合的活动实体(用户或主体)使用特定集合的操作访问和利用特定集合的客体或资源而制定的规则,以及管理在这些规则中所用到的安全属性的功能。

一个典型的例子就是操作系统中针对文件系统的访问控制策略。进程是主动实体,其中一些进程代表用户进行操作,因此具有从用户绑定时的安全属性所派生出来的安全属性。对文件系统的操作如打开、读取文件,写、更新文件,查看或修改文件属性,创建、删除文件等,是 SFP 的操作。访问控制策略中还存在管理进程或文件系统的安全属性的操作。

在 SFP 中,安全属性的典型例子如下:

——客体安全属性:访问控制列表,文件类型;

——用户安全属性:用户身份,用户角色;

——进程安全属性:进程身份,进程受信任级别。

其他的 SFP 可能规定外部实体直接而非通过中间主体执行的操作。例如防火墙,它控制外部系统如何使用网络服务和功能。有主动的实体(发起请求的外部系统)、客体(外部系统请求的目标)和操作(网络服务)。这个 SFP 中的规则可能基于操作中的外部系统身份、操作种类(如使用的端口)、操作上下文(比如一个指定端口的连接是否事先被建立)和网络包内容。

为同一个用户、主体、客体和操作集合定义超过一个 SFP 并不罕见。例如:一个任意的访问控制策略作为其中一个 SFP,一个强制访问控制策略作为一个附加的 SFP。尽管受 SFP 约束的用户、主体、客体和操作集合是同一个,但 SFP 的规则和这些规则中使用的安全属性的集合是不同的。

11.2.2.2 用法

访问控制策略是从资源和客体以及 TOE 允许的主动实体(在 TOE 内部或外部)在这些资源和客体上进行的操作的角度来对 TOE 安全功能进行建模的。因此导出 TOE 安全功能模型的访问控制的第一步就是标识出 TOE 提供的资源、客体、操作以及触发操作的主体和用户。这个模型一开始只应包含从 TOE 安全目的和从 PP 或 ST 最初描述的 TOE 通用功能获得的那些资源、客体、操作、主体和用户。为一个已知产品或系统开发 ST 的时候,TOE 的安全模型中应存在这些定义的实体。当然在定义 TOE 安全功能要求时,可能需要在最初的集合上添加新的资源、客体、操作、主体和用户,以保证访问控制策略的一致性和完整性。

定义 TOE 安全功能模型中不存在的实体将会在评估过程中导致不少问题,这是因为在 GB/T 18336—2015 中假设 SFR 和 SFR 提到的实体是 TOE 中存在的抽象实体,且这些实体在 TOE 的设计与实现阶段,能够通过细化映射到具体的资源、客体、操作、主体和用户。

在定义了访问控制策略涉及的资源、客体、操作、主体和用户后，下一步就可定义用来管理在模型中定义主体和用户对资源和客体进行访问和使用操作的规则，以满足 TOE 安全目的。为一个已知 TOE 定义 ST 的规则应尝试从模型定义实体的真实行为中抽象而来，以保证 TOE 实现的规则是模型中规则的严格细化。

对规则中用到的参数进行标识是规则定义的一部分，很可能需要定义资源、用户、主体和客体的“安全属性”。这些安全属性需要收集并列出清单，因为规则的初始化和管理可能需要用到这些安全属性。

定义这些规则的时候，需要经常认识到不同集合的资源、客体、用户、主体和操作所需的规则之间的差别。为了简化模型的描述，需要将资源、客体、用户、主体和操作的集合（即所谓“类型”）使用相同（或基本相同）的规则分组到安全功能策略中。为每个安全功能策略命名，以便能够唯一标识该策略。

为创建和删除主体和客体定义规则。这些规则可能因主体、客体的种类不同而不同，同时需要定义这些主体和客体的安全属性如何初始化。

为主体和客体的非静态安全属性的管理定义规则。这些规则可能包括外部实体通过 TSFI 所触发的操作，有些规则描述安全属性应如何被修改，而这些修改动作是 TSF 执行的一部分操作。

需要为注册（也即“创建”）和注销（也即“删除”）用户定义规则。用户注册规则中也包括为用户安全属性初始化的规则。有些情况下用户不需要注册，用户能够请求服务并且使用他们所具有的证书进行标识和鉴别。这些证书可能也包括用户的安全属性。在这些情况下，需要定义如何接受和校对证书的规则。

为用户的标识和鉴别（如果需要）定义规则。这些规则定义了用户应出示的证书（证书类型，证书的一些可能的限制如最小和最大长度，最小和最大生命期等等）以及当接收到不正确的证书时，TSF 应做出的反映。

为用户安全属性的管理定义规则，其方式与定义主体和客体安全属性的规则类似。

如果 TOE 支持用户与主体绑定的功能，那么包括这些绑定的规则需要被定义。这些规则可能包括：

——需要满足允许绑定的条件；

——绑定后，主体安全属性的设置。

当这些规则制定后，应检查是否需要额外的管理规则。比如允许创建一个新的安全属性的规则，可能还有要定义如何管理这些安全属性的规则。

11.2.3 用户管理

11.2.3.1 解释

在 GB/T 18336—2015（所有部分）的范型中，用户是使用 TOE 接口请求服务的 TOE 外部实体。用户在能够使用 TOE 服务之前可能需要注册，或者 TOE 允许未经注册的用户也可以请求服务。在多数情况下，TOE 通过用户的某些安全属性来决定是否对其提供服务。用户安全属性可由用户附带着请求一起提交，也可从 TOE 存储的用户或用户组的数据中提取出来。

第一种情况下，TOE 需要保证用户提交的安全属性是可信的。这意味着在用户合理使用安全属性方面，TOE 应实现如何评估安全属性并建立信任的规则。

第二种情况下，TOE 需要知道用户或用户组的身份。同时，在这种情况下，TOE 需要实现如何验证用户或用户组中成员所声明的身份正确性的规则。这个过程叫作鉴别，即用户向 TOE 提交用来对所声明的身份或组成员的正确性的信任凭证。这需要定义规则，以规定鉴别过程如何执行，鉴别过程中的参数如何管理。

当用户注册时，需要对用户如何注册、用户的安全属性如何管理等定义规则。

某些情况下 TOE 会使用自身的一个主体来代表用户执行动作。在这样的情况下，主体与用户通过 TSF 绑定，当主体绑定到用户时，TSF 会有相应的规则来定义主体的安全属性是如何产生的。很多情况下，主体继承了用户的部分安全属性，允许执行以用户安全属性为基础的访问控制策略。

11.2.3.2 用法

为了定义用户管理功能，需要执行下面的步骤：

——标识并定义可以访问 TOE 的用户种类(以及每类用户可能具有的安全属性集)；

——标识每种在使用 TOE 功能前需要注册的用户；

——对需要注册的用户，对用户注册以及在注册时需要为用户设定的安全属性定义规则；

——标识出所有需要用户标识的用户种类，如果存在这样的用户，为如何标识用户定义规则；

——标识所有需要鉴别的用户种类，如果存在这样的用户，为如何鉴别用户定义规则，并定义用户鉴别时需要的条件；

——定义如何管理鉴别过程的规则(包括对鉴别中所用证书的管理)；

——为每类用户定义如何管理用户安全属性的规则；

——当用户与主体间可能需要绑定时，为如何绑定定义规则，尤其在绑定过程中，需要定义主体的安全属性如何设置的规则。

11.2.4 TOE 自保护

11.2.4.1 解释

当满足下列条件之一时，需要保护安全功能自身：

——在 TOE 预期环境中可能存在攻击安全功能的威胁，而导致无法实现安全目的；

——由于 TOE 环境因素的故障而导致无法实现安全目的；

——由于 TSF 中元素的故障而导致无法实现安全目的。

以上情况需要定义自保护功能作为 TSF 的一部分，能够对上述条件进行检测并作出响应，以便在上述条件发生时仍然能使安全目的得到满足。

在功能模型中定义 TOE 自保护的要求如下：

——标识出对可能违背安全目的的攻击场景和故障；

——标识出能够防止攻击或故障的功能，比如为 TOE 增加物理防护来防止特定的物理攻击；

——在无法预防(多数情况下)时，标识出能够检测出攻击或故障并适当做出响应的功能。

检测 TOE 使用环境中的外部攻击或系统故障需要监控 TSFI 的使用并检查引起攻击的条件，监控在通信链路中引起攻击的条件或监控 TOE 专门用于检测攻击的传感器。

11.2.4.2 用法

TOE 自保护功能的选择与否需要通过安全问题定义来确定，这类功能是必要的，应选择是采用预防外部攻击(如某些增强的物理防护)的措施，还是采用能够对攻击或故障进行检测并做出响应的措施。

应首先列出在 TOE 预期环境中可能发生的攻击或故障，这些攻击或故障如果不经处理就可能违背安全目的。对其中的每一条，需要定义这些可能的攻击或故障应如何处理，即通过 TOE 实现的安全功能来抵御它们，或是 TOE 的安全功能能够检测出攻击或故障，并做出相应的响应。

在 TOE 使用安全功能抵御攻击的情况下，功能需要使用某些合理理由来描述，这些理由表明它们应预防哪些种类的攻击。

在检测、响应攻击或故障的情况下，需要定义检测(抽象层面的)和响应的标准和规则(作为声明这

种情况下 TOE 应做什么的抽象的规则)。

TSF 的故障检测可通过监控内部状态变量、内部功能自测或通过功能或数据的冗余以及一致性检查来执行。

响应产生的纠正措施列表如下:

——消除攻击或故障所带来影响的纠正措施,比如基于数据或功能冗余的检测及自动纠错功能;

——消除部分攻击或故障所带来影响的纠正措施,但导致了 TOE 功能的衰减(衰减需与安全目的一致),比如从失败或攻击中恢复功能,恢复可能需要一定的时间并且可能不会完全恢复,在这种情况下,需要保证由于不完全恢复而导致的功能延迟或数据丢失不违背任何安全目的;

——为 TOE 准备的手动纠正措施,比如将 TOE 受到攻击或故障影响的部分停止工作,或整个 TOE,停止的部分或整个 TOE 需要从安全模式重新启动;

——停止 TOE 失败的部分或整个 TOE,且 TSF 不提供安全启动的方法。比如 TOE 在检测到攻击或故障时销毁重要功能或数据,以保证不违背其安全目的。

上述纠正措施的列表是依据其对 TOE 整体功能影响逐渐增大而进行的排序。

11.2.5 安全通信

11.2.5.1 解释

在 TOE 与外部实体之间或分布式 TOE 不同部分之间使用不可靠、不可信的通信信道进行通信的情况下,需对那些保护数据的功能进行附加建模。为了对通信进行建模,需要定义通信信道的安全属性。这些属性可能包括如下内容:

——对通信伙伴的鉴别;

——对信道传输数据的完整性保护;

——对信道传输数据的机密性保护;

——保护数据以免丢失;

——提供信息的发送接收的不可否认性。

为了对通信信道进行建模,需要定义通信双方以及信道的安全属性,这些定义适用于在线或离线的通信信道。

11.2.5.2 用法

标识出安全通信所需的功能需要以下步骤:

——标识通信链路;

——定义每条通信链路所需的安全属性,比如:

- 对通信实体的鉴别;
- 完整性保护(如防重放、消息序列保护等);
- 机密性保护(对通信数据的分析保护);
- 不可否认性的规定;
- 避免通信数据丢失的规定。

对每一条通信链路,其所需的安全属性都需要定义。在 ST 中,这些机制也被用来实现这些安全属性的定义(尤其是与密码相关的机制)。在 PP 中,这些机制仅需要定义到所要求的细节。需要注意的是,当任何符合该 PP 的 TOE 也要求满足互操作要求时,这个级别可能相当高。在这些情况下,PP 可能指定这些机制下降到所需的特定协议以及协议选项(比如密码算法)的级别,以保证互操作性。

当标识通信链路列表时,不应只识别物理通信链路,同时也应标识出需要特定保护的逻辑链路(如

在应用协议层的链路)。这样的通信链路可能存在于不同的协议层,而独立的协议层提供不同类型的保护。比如 IPsec 会提供对等实体的鉴权以及完整性和机密性保护,而一个 IPsec 之上的应用协议(或其他的不同逻辑通信链路)会提供额外的鉴别(如用户或应用)以及不可否认性功能。这种情况下 IPsec 和应用协议应被列为不同的通信链路,以及它们各自特定的安全属性也是不同的。

需要注意的是,大多数安全通信链路功能通过检测完整性和数据丢失等条件强制使用完整性保护和数据丢失保护。与在 TOE 自保护章节中描述的检测功能类似,TOE 检测到这些条件时的响应可能需要定义。同时,对失败的鉴别尝试以及非法的不可否认性的响应措施也可能需要定义。

请注意,当通信实体未知时,输出 TOE 控制下的 TSF 或用户数据,以及向 TOE 输入 TSF 或用户数据可被认为是通信的特殊情况。在这种输出和输入的情况下,如下的属性可能需要考虑:

——完整性保护(如防重放,新鲜性检查等);

——机密性保护;

——不可否认性的规定(输出、输入,或二者兼有)。

11.2.6 安全审计

11.2.6.1 解释

监控哪些被定义的安全关键事件以及维护这些事件的记录以便未来进行分析或为了评估对此类事件的自动响应,是 TOE 为满足安全目的的另一个安全功能。安全关键事件可以是主动实体直接使用 TOE 服务请求有关的事件,也可以是安全关键状态监测或是不直接关系到请求的事件。

下面是一些安全关键事件的例子:

——成功和(或)被拒绝使用 TSF 提供服务;

——意外到达失败状态;

——一个远程可信 IT 产品意外或错误的行为;

——自检功能的检测失败;

——超过定义的安全关键阈值;

——对 TSF 关键数据的改变;

——累积的事件,因为每个独立的事件都不被认为是足够关键而值得审计。

11.2.6.2 用法

为了对安全审计进行建模,需要做如下事情:

——列出需要审计的事件;

——定义规则,以控制何时审计事件(比如仅当请求被拒绝时进行审计);

——定义每个事件需要收集的数据;

——定义所收集到的审计数据该如何处理和分析的规则。

如果存在与安全功能相关的且需要审计的事件时,可对每个独立的安全功能做分析。此外,当到达产生审计记录的关键内部状态时,需要分析安全功能模型。

11.2.7 体系结构要求

11.2.7.1 解释

除了以上列出的要求,或许还需要指定 TOE 体系结构的要求,这样的要求是为了确保分析 TOE 的体系结构,并支持读者对 TOE 架构的理解。这些要求通常与 TOE 应强制遵循的特定属性有关,这

种属性如下：

——容错性；

——信息流控制；

——私密性；

——实时性。

体系结构要求常常受前面章节所述要求的支持。比如，信息流控制和私密性通常伴随着管理客体访问控制的特定规则，容错性经常伴随用于检测故障的安全审计要求。这些访问控制规则，尤其是安全审计规则是必要的，但通常不足以强制要求。

体系结构要求比其他的安全功能要求更难以标识和规定，然而它们或许可以完全满足某些安全目的，它们因此才被定义为 PP 或 ST 安全功能要求的一部分。

11.2.7.2 用法

为了对体系结构要求进行标识和建模，使用如下步骤：

——标识出在前面的步骤中未被处理或完全已被处理的安全目的；

——标识出为了满足这些安全目的所需的体系架构支持；

——定义有助于体系架构支持的规则。

在 ST 中，这些要求最有可能被预定义在 ST 的 TOE 结构中。比如，如果 TOE 已知是分布式的，那么 TOE 各分布式之间的保持数据一致性的要求，或在各部分之间传输时保护数据不被未授权访问的要求。

11.3 确定安全功能要求

11.3.1 选择安全功能要求

在定义了作为安全问题定义一部分的 TOE 安全目的之后，需要详细说明应如何满足这些安全目的，这通过选择上面提到的组件级别、合适的 SFR 集合来完成。当然，如果已经有可用的满足 TOE 安全目的的预定义功能包，选择 SFR 的过程明显更加容易。

SFR 的选择基于 TOE 的总体功能模型，这个功能模型定义了资源、用户、主体、客体和操作，SFR 定义安全功能以便在 TOE 功能模型中满足安全目的。同任何模型一样，这些功能是 TOE 真实功能的抽象，但其抽象级别应足以理解 TOE 的功能原理。不需要为了满足安全目的而去控制资源、用户、主体、客体和操作，它们在定义 SFR 的过程中可以忽略。例如，如果 TOE 安全目的仅是控制对数据的访问，那么在定义 SFR 时，可以不需要考虑“CPU 时间”这个资源。

为 PP 或 ST 选择 SFR 的过程分为若干个阶段。在考虑选择过程时，区分以下两种 SFR 是有帮助的：

a) 主要 SFR，也即直接满足识别出的 TOE 安全目的；

b) 支持 SFR，也即不直接满足 TOE 安全目的，但为主要 SFR 提供支持，并因故间接地帮助满足相关 TOE 安全目的。

虽然 GB/T 18336—2015(所有部分)没有显式地区分这两种 SFR，在考虑功能组件之间的依赖以及 SFR 间的相互支持时，这种区分是隐式的。因此，虽然没有必要在 PP 或 ST 中显式的将 SFR 分类为主要和支持，认识到有这两种 SFR 会在撰写 PP 或 ST 基本原理说明时可带来明显便利。

SFR 选择过程的第一步，就是为功能模型识别出直接满足 TOE 的每个安全目的的主要 SFR。一旦建立了完整的主要 SFR 集合，接下来就可以通过迭代过程来识别完整的支持 SFR 集合。如上所述，所有 SFR(主要的和支持的)在可能的情况下都该使用 GB/T 18336.2—2015 中适合的功能组件表达。

11.3.2 为识别通用安全功能要求应使用哪些功能组件提供指南。从 GB/T 18336.2—2015 中选择功能组件时，应参考 GB/T 18336.2—2015 附录中的指南以确定组件是否适当，以及组件应如何被解释。

这两种 SFR 的关系如图 4 所示。需要注意的是，这种关系与 PP 或 ST 的基本原理相关，需要描述 SFR 的相互支持。

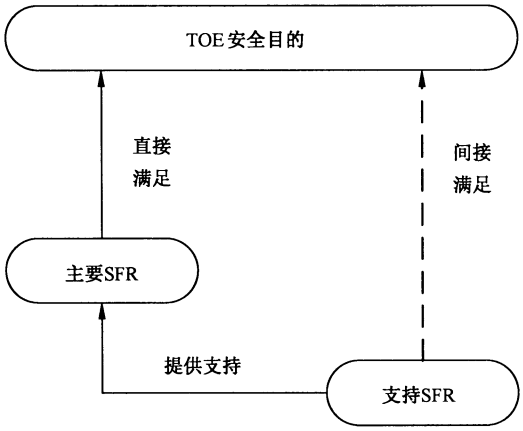

图 4　主要 SFR 和支持 SFR 的作用

识别完整的支持 SFR 集合包含以下三步：

a) 识别需要满足所有主要 SFR 依赖(如 GB/T 18336.2—2015 中定义相关的功能组件)的额外 SFR；

b) 识别任何保证 TOE 安全目的实现的、必要的额外 SFR，这包括保护主要 SFR 免受组合攻击所需的 SFR，这些攻击先会攻陷某个功能，再安装该功能所抵抗的威胁；

c) 对前两个阶段所标识出的支持 SFR 继续依赖性标识，发现更多的额外 SFR。

对满足 GB/T 18336.2—2015 中确定依赖的支持 SFR 的识别可能是一个迭代过程，比如：

a) 假设 PP 或 ST 包含一个安全目的，该安全目的需要 TOE 对监测到指示一次即将发生的安全违例的事件提供特定响应，这导致基于组件 FAU_ARP.1 的主要 SFR 包括在其中；

b) 根据 GB/T 18336.2—2015，FAU_ARP.1 依赖于 FAU_SAA.1，那么该组件也应作为支持 SFR；

c) FAU_SAA.1 依赖于 FAU_GEN.1；

d) FAU_GEN.1 依赖于 FPT_STM.1；

e) FPT_STM.1 没有额外的功能组件的要求。

需要注意的是，GB/T 18336—2015(所有部分)允许保留一些“未满足”的依赖，前提是需要解释为什么相关的 SFR 不需要用来满足安全目的(并指出安全问题)。

应整体采取一致的方法来应用依赖关系。例如，在 FAU_ARP.1 中，一致性由安全要求的本质特征来决定(FAU_ARP.1 所依赖的潜在安全违背事件是由 FAU_SAA.1.2 定义的)。

对其他组件来说，一致性可能更成问题。比如，在 FDP_ACC.1 中，PP 或 ST 会识别出与之相关的特定访问控制 SFP。为满足 FDP_ACC.1 到 FDP_ACF.1 的依赖，应保证 FDP_ACF.1 应用与 FDP_ACC.1 相同的访问控制 SFP。如果迭代操作应用在 FDP_ACC.1 并使用了不同的访问控制 SFP，FDP_ACF.1 的依赖就需要满足每一个这样的 SFP。

对额外的支持 SFR(在 GB/T 18336.2—2015 中不被认定为从属的)的识别包括识别必要的、用来支持 TOE 安全目的实现的其他任何 SFR，这些 SFR 通常会通过减少攻击者可用的选择或机会，或提高攻击者成功实施攻击所需要的专业知识或资源的级别来提供支持。以下内容应被考虑：

a) 基于 GB/T 18336.2—2015 同一类的相关组件的 SFR。例如，如果 FAU_GEN.1(审计数据产

生)被包括,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(需要一个及以上的FAU_STG族安全组件)并需要用来检查生成的审计数据的工具(需要一个及以上的FAU_SAR族安全组件)。另外,生成的数据可能被导出到其他系统来检查。

b) 基于FPT类相关组件的SFR。这些SFR通常会保护其他SFR依赖的TSF或TSF数据的完整性和(或)可用性,尽管它们也可以保护其保密性。例如FPT_TEE.1(外部实体测试)以及FPT_PHP(物理防护)族的组件,这些组件可能需要用来在某些情况下支持安全目的,以保护TSF免受诸如TSF失效、崩溃、恶意修改等影响;

c) 基于FMT类相关组件的SFR。这些FMT组件会用于指定任何必要的支持安全管理的SFR。例如,FMT_REV.1用于处理安全属性的撤销,应考虑其与处理安全属性的SFR间的关联。

应根据安全目的和功能模型来选择这些支持SFR。应避免包括不需要用来实现安全目的的支持SFR,这将限制PP或ST的可接受性,比如:

a) 某些TOE或许不能够满足这样的SFR;

b) SFR数量的增加会增加评估过程中的开销和无用要求的维护。

如果PP或ST使用一个相关的PP作为基础来构建,SFR选择的过程可被极大简化。正被构建的PP或ST应包括不同的SFR,如果合适,也要考虑TOE安全问题定义与安全目的之间的任何差异。

11.3.2 从GB/T 18336.2—2015中选择SFR

表1~表6提供了GB/T 18336.2—2015解释的范型和其定义的SFR组件的映射。一些组件覆盖了不止一方面的范型,因此在表中出现不止一次。

表1 访问控制

要求	可用组件
定义主体、客体、操作	FDP_ACC.1,FDP_ACC.2,FDP_IFC.1, FDP_IFC.2, FMT_SMF.1
定义安全属性	FDP_DAU.1,FDP_DAU.2,FDP_IFF.1,FDP_IFF.2, FRU_PRS.1 FRU_PRS.2, FRU_RSA.1, FRU_RSA.2
创建主体,客体	FDP_ITC.1, FDP_ITC.2, FMT_SMF.1
输出客体	FDP_ETC.1, FDP_ETC.2
管理安全属性	FDP_ITC.2,FIA_USB.1,FMT_MSA.1,FMT_MSA.2, FMT_MSA.3, FMT_MTD.1 FMT_MTD.2,FMT_MTD.3,FMT_REV.1, FMT_REV.2, FMT_SAE.1, FTA_LSA.1
定义访问规则	FDP_ACF.1, FDP_IFF.1, FDP_IFF.2, FDP_ROL.1, FDP_ROL.2 FRU_PRS.1, FRU_PRS.2, FRU_RSA.1, FRU_RSA.2
管理访问控制规则	FMT_MOF.1, FMT_SMF.1

表2 用户管理

要求	可用组件
定义用户类型	FMT_SMF.1
定义安全属性	FIA_ATD.1

表2(续)

要求	可用组件
用户标识规则	FIA_UID.1，FIA_UID.2
用户鉴别规则	FIA_AFL.1，FIA_SOS.1，FIA_SOS.2，FIA_UAU.1，FIA_UAU.2 FIA_UAU.3，FIA_UAU.4，FIA_UAU.5，FIA_UAU.6，FIA_UAU.7
用户凭证和安全属性的管理	FMT_MSA.1，FMT_MSA.2，FMT_MSA.3，FMT_MSA.4，FMT_MTD.1 FMT_MTD.2，FMT_MTD.3，FMT_REV.1，FMT_REV.2，FMT_SAE.1 FMT_SMR.1，FMT_SMR.2，FMT_SMR.3，FTA_LSA.1，FTA_MCS.1，FTA_MCS.2
管理标识和鉴别规则	FMT_MOF.1，FMT_MTD.1，FMT_MTD.2，FMT_MTD.3，FMT_SMF.1
用户-主体绑定的管理	FIA_USB.1

表 3　TOE 自我防护

要求	可用组件
故障检测	FPT_TEE.1，FPT_ITI.2，FPT_ITT.3，FPT_PHP.1，FPT_PHP.2 FPT_PHP.3，FPT_RPL.1，FPT_TST.1，FRU_FLT.1，FRU_FLT.2
故障响应	FPT_ITT.3，FPT_PHP.2，FPT_PHP.3，FPT_RCV.1，FPT_RCV.2 FPT_RCV.3，FPT_RCV.4，FPT_RPL.1，FRU_FLT.1，FRU_FLT.2
管理检测和响应规则	FMT_MOF.1，FMT_MTD.1，FMT_MTD.2，FMT_MTD.3，FMT_SMF.1

表 4　安全通信

要求	可用组件
建立通信链路	FMT_SMF.1，FTP_ITC.1，FTP_TRP.1
定义通信链路属性	FCO_NRO.1，FCO_NRO.2，FCO_NRR.1，FCO_NRR.2，FDP_UTC.1 FDP_UIT.1，FDP_UIT.2，FDP_UIT.3，FPT_ITC.1，FPT_ITI.1 FPT_ITI.2，FPT_RPL.1，FTP_ITC.1，FTP_TRP.1
管理通信链路属性	FMT_MSA.1，FMT_MSA.2，FMT_MSA.3，FMT_MTD.1，FMT-MTD.2 FMT_MTD.3，FMT_REV.1，FMT_REV.2，FMT_SAE.1
管理链路建立规则	FMT_MOF.1，FMT_MTD.1，FMT_MTD.2，FMT_MTD.3，FMT_SMF.1 FTA_SSL.1 FTA_SSL.2，FTA_SSL.3，FTA_SSL.4，FTA_TAB.1，FTA_TAH.1，FTA_TSE.1

表 5　审计

要求	可用组件
定义审计的事件	FAU_GEN.1，FAU_GEN.2，FAU_SEL.1
定义事件的响应	FAU_ARP.1，FAU_SAA.1，FAU_SAA.2，FAU_SAA.3，FAU_SAA.4
定义事件的管理	FAU_SAR.1，FAU_SAR.2，FAU_SAR.3
定义审计迹的管理	FAU_STG.1
管理审计规则	FMT_MOF.1，FMT_MTD.1，FMT_MTD.2，FMT_MTD.3

表 6　体系结构要求

要求	可用组件
审计迹保护	FAU_STG.2，FAU_STG.3，FAU_STG.4
密码功能	FCS_CKM.1，FCS_CKM.2，FCS_CKM.3，FCS_CKM.4，FCS_COP.1
信息流控制	FDP_IFF.3，FDP_IFF.4，FDP_IFF.5，FDP_IFF.6
TOE 内部传出	FDP_ITT.1，FDP_ITT.2，FDP_ITT.3，FDP_ITT.4
预留信息保护	FDP_RIP.1，FDP_RIP.2
存储数据完整性	FDP_SDI.1，FDP_SDI.2
管理	FMT_MTD.1
隐私保护	FPR_ANO.1，FPR_ANO.2，FPR_PSE.1，FPR_PSE.2，FPR_PSE.3， FPR_UNL.1，FPR_UNO.1，FPR_UNO.2，FPR_UNO.3，FPR_UNO.4
失败安全	FPT_FLS.1
可用性	FPT_ITA.1，FPT_ITT.1，FPT_ITT.2
状态同步	FPT_SSP.1，FPT_SSP.2
安全时间戳	FPT_STM.1
数据一致性	FPT_TDC.1，FPT_TRC.1

表 1～表 6 意图帮助识别合适的 SFR 组件，一旦安全功能模型根据 11.2 和 11.3.1 定义，选择什么样的组件以及如何使用这些组件和允许的操作来表达安全功能模型，这些方面的问题留给 PP 或 ST 的作者。

11.3.3 操作安全功能要求

11.3.3.1 允许的操作

某些功能组件包含了允许的操作。这些操作包括：

a) 赋值，允许规定已标识的参数；

b) 反复，允许多次使用同一个功能组件来表达不同要求；

c) 选择，允许从列表中选取一个或多个元素；

d) 细化，允许在安全要求上附加细节。

11.3.3.2 反复

反复操作经常被用于表达使用 FMT 类组件的 SFR，这些组件常被作为 GB/T 18336.2—2015 中许多不同功能组件的依赖而被使用。为满足这种依赖，通常可用同一个组件完成不同的赋值和选择操作。例如，FMT_MSA.1 可能被反复操作多次，以定义与不同安全属性管理有关的 SFR。类似的，FDP_ACC 和 FDP_ACF 族的组件在 TOE 执行不同的访问控制策略的情况下也会被多次使用，如自主访问控制(DAC)和基于角色的访问控制(RBAC)。

为了增强 PP 或 ST 的明晰度，可以鼓励使用反复操作，如将一个复杂的 SFR 拆分为清晰的、可管理的功能要求。使用反复操作可能在 PP 或 ST 中表述 SFR 时带来其他潜在问题。

11.3.3.3 赋值和选择

在赋值操作中，参数的值可能为空，而使用选择操作至少要选出一个已标识参数的值。

一般情况下，ST 作者来完成赋值或选择操作。在 PP 中完成相关操作或产生过多的细节可能会限

制能声明与 PP 一致性的 TOE。平衡这些相关操作要基于 PP 需求：

a) 作者要求的完整集合；

b) 与实现无关的；

c) 充分详细地证明安全目的被满足。

为满足安全目的所需的程度，完成赋值和选择操作是必要的。用以证明 IT 安全要求适用性的参数不应依赖 SFR 中没有指定的细节。比如，在基于 FDP_ACF.1 的访问控制 SFR 中，如果访问规则已在 OSP 中定义，可将访问控制规则的描述留给 ST 作者来完成。这种情况下，PP 作者完成只需满足通用安全目的的赋值和选择操作，而将定义 TOE 实现的访问控制规则留给 ST 作者来完成。

为了解决以上问题，用到一种方法，即完成部分操作。使用这种方法，可以给予 ST 作者最大的灵活性，虽然这同时也排除了与 TOE 安全目的不一致的赋值和选择操作。

比如，在下面这个 SFR 中(基于 FAU_STG.4.1)，通过排除“忽略可审计事件”选项，选择操作已被部分完成，这相当于 PP 作者已判断出与 TOE 安全目的不一致性，SFR 会提供给 ST 作者从二者中选择一个可接受的选项：

如果审计迹已满，TSF 应[选择：“阻止可审计事件，具有特权的授权用户产生的事件除外”，“覆盖所存储的最早的审计记录”]以及[赋值：审计存储失效时所采取的其他动作]。

通过赋值，PP 作者希望限制 ST 作者从可接受的选项集合中进行选择。这种情况下，PP 作者或许希望通过将赋值操作转变为包含合法选项的选择操作来完成赋值操作，这样，这些操作就留给 ST 作者来完成。

作为一般原则，如果选项集是原始功能组件所允许的选项集的子集，那么部分完成的选择操作是有效的。类似地，如果完成赋值所允许的值在最初的功能组件中也是合法的，那么部分完成的赋值操作也是合法的。如果任何条件都无法满足，那么需要使用不同的赋值或选择操作来构建一个扩展的功能组件。

完成赋值或选择操作相当简单。对于赋值，只需要保证参数是无歧义的。对于选择，仅需要基于 TOE 安全目的的考虑，选择合适的条目。如果有任何疑问，应参考 GB/T 18336.2—2015 的附录中的指南。

当 PP 中的赋值或选择操作已被执行，那么可将被指定的文本突出显示。通常是采用用斜体字的方式，但也可以使用加粗或不同字体。

例如，FMT_SAE.1.1 可以被表述如下：

*TSF 应仅限于**授权管理员能够为用户口令**指定有效期*。

上面的例子使用加粗来突出文本，同时作为一个例子，文本已经是斜体。

如果一个操作处于未完成的状态，那么对 ST 的作者来说，完成这个操作是强制的。

任何未完成(或部分完成)的操作都应为 ST 作者做解释(如果合适)，其内容为如何完成该操作。例如，FDP_RIP.1.1 在 PP 中可以这样指定：

TSF 应确保一个资源的任何先前信息内容，在分配资源到下列客体[赋值：ST 作者指定的客体列表]时不再可用。

对于 PP 中包含的每个 SFR，需要判断否完成赋值或选择操作，而在 ST 中，所有的赋值和选择操作都需是已经完成的。

11.3.3.4 细化

对每个包括在 PP 或 ST 中的 SFR 来说，需要判断是否对 SFR 做细化。

细化操作可能作用于任何功能组件元素，并且涉及指定的额外技术细节，这些细节不在已经指定的

文本中增加任何新的要求，但会限制可接受的实现集。如果满足细化的要求也满足未细化的要求，那么细化操作是可接受的。细化的使用在下列情况下是合适的：

a) 编辑 PP 的组织有附加技术细节，比如组织策略信息，而 GB/T 18336.2—2015 中未含有适当的组件；

b) 当所选择的功能组件使得实现方法不明确，或者不适于所针对的 TOE 类型时，需要通过细化操作来消除这些问题（例如出于互用性的原因）；

c) 提高 SFR 的可读性。

与赋值和选择操作一样，建议将被细化的文本突出显示。

细化操作的用法举例如下（基于 FMT_MTD.3.1）：

*TSF 应确保 TSF 数据只接受安全的值。**细化：TSF 应确保 TOE 规定的最小口令长度被设置为至少 6 个字符**。*

11.3.4 确定审计要求

如果 PP 或 ST 包括审计要求（例如，基于 FAU_GEN.1），则 GB/T 18336—2015（所有部分）要求通过考虑 PP 或 ST 中包含的所有其他功能要求以指定最低限度的可审计事件及记录信息。

这取决于多种因素，包括：

a) 定义在 OSP 中的有关安全审计的安全策略要求；

b) 审计在实现安全目的中的重要性；

c) 与安全目的相关的潜在事件及其特征；

d) 开销或效益分析。

例如，如果 TOE 意图抵御恶意用户或黑客，那么在 PP 或 ST 中应包括这样的 SFR，即其可对登录、违反访问控制等事件进行审计。然而，与管理功能使用相关的事件可能无需审计，这取决于管理员的可信程度，作为假设，管理员的可信性需要事先声明。

开销或效益分析可能包括以下问题：

a) 收集信息的好处是否值得牺牲对性能的影响；

b) 如果信息被收集，管理员是否具有足够的资源（如支持工具）来有效地分析这些数据；

c) 对收集到的数据进行管理和归档的可能开销是哪些。

GB/T 18336—2015（所有部分）确定了三种预定义的审计级别，分别称作最小级、基本级或详细级。对其中的每种级别，GB/T 18336.2—2015 都介绍了何种事件应被审计，以及需要记录的最低限度的信息。这三个级别的特征大致如下：

a) 最小级通常只要求某些定义过的、与给定的可审计功能组件相关的操作或事件的子集。这个子集一般被定义为最明显的一类事件；

b) 基本级通常要求给定的可审计功能组件相关的所有操作或事件，比如成功和不成功的登录尝试；

c) 详细级不同于基本级，其需要记录额外的感兴趣的信息。这个级别只在生成的审计数据数量预计很少时或者数据会被复杂的审计分析工具或入侵检测设备分析时才是更适合。

如果上面的级别没有一个是适合的，那么需要选择未规定级别，并显式列出 FAU_GEN.1.1 中所有需要审计的事件。例如，可能使用最小级别作为指导，但在某些指定情况下选择违背最小级别的要求，这是由于另一个不同的操作或事件子集与安全目的更加相关，比如，若在 PP 或 ST 中包括 FDP_ACF.1，或许不成功的访问尝试相比成功的访问尝试更应被审计（这是 GB/T 18336.2—2015 中对最小级的要求）。

需要通过遍历每个用到的功能组件来编写一个可审计事件清单，对于预定义的最小级、基本级、详细级，其在每个组件族的审计部分已被明显标识。可使用表格形式，在上面标识事件以及可能记录的附加信息，这些信息可适当从 FAU_GEN.1.1 和 FAU_GEN.1.2 中引用。

11.3.5 确定管理要求

GB/T 18336.2—2015 在每个组件族包含的管理部分列出为组件考虑的管理活动，这可能需要包括 FMT(安全管理)类型中特定的组件。

当功能组件提及了或隐含了存在需要管控的可配置的 TSF 数据，那么可能的管理活动都被要标明。例如，如果 TOE 管理员的修改数据能力未被限制，TOE 安全目的可能被削弱。因此，为了定义支持 SFR，常常要包括 FMT 组件，以便确保满足 TOE 安全目的，且 SFR 作为一个整体是互相支持的。

管理活动可以从 TOE 功能模型派生。典型的需要考虑的管理活动如下：

——用户的注册或注销；

——客体的创建；

——用户、客体、会话等的安全属性的修改；

——安全功能行为的改变(包括启动或停止 TOE 所有或部分功能)；

——审计参数的修改；

——安全相关的 TSF 内部状态变量的变化(例如转变到维护模式)。

在从 FMT 类型中选择组件的时候，应参考 GB/T 18336.2—2015 的附录 H 给出的关于该类型的指导。

11.3.6 确定 PP 中的 SFR

当 ST 声明与一个或多个 PP 一致时，SFR 可能全部或大部分是由 PP 指定的。这种情况下，ST 作者应要决定是否全文引用 PP 功能要求，或是否仅仅引用 PP 并指出与 PP 中 SFR 的不同点。

后者会简化 ST，但需要读者同时阅读 PP 和 ST 来了解全部内容。相对于 SFR，ST 的读者可能更感兴趣的是 IT 安全功能，这其中也包括 TOE 评估者(评估证据，例如设计、测试文档和指南文档，比 SFR 更容易与 TOE 概要规范中的 IT 安全功能关联起来)。在 ST 中指定 SFR 的主要目的是能够论证其与相关 PP，以及与在 GB/T 18336.2—2015 中定义的 SFR 的可追溯性。

PP 中某些 SFR 可能存在留给 ST 作者完善的操作(例如赋值或选择)。这种情况下，建议对 SFR 详细说明，并使用合适的字体(如斜体)强调已完成的操作。任何必要的解释都需要使用相同的字体来添加。这种方式会使 ST 读者(特别是 ST 评估者)更容易看到这些操作是以何种方式完成的，这也为 ST 基本原理的构建提供了便利。

11.3.7 确定未在 PP 中的 SFR

在某些情况下，需要说明 ST 中的 SFR 有哪些与 PP 不一致，例如如下情况：

a) 没有合适的可让 TOE 声明一致性的 PP；

b) 由 PP 指定的功能或保证要求所产生的功效可能导致出现额外的成本。

在这种情况下，规范 SFR 的方法与前文中所描述的相同。凡是除了那些由 PP 额外指定的 SFR 之外，ST 的作者应确保不与 PP 中的 SFR 冲突(ST 的基本原理需要证明这种冲突不会发生)。

11.3.8 确定未在 GB/T 18336.2—2015 中的 SFR

如果 PP 或 ST 作者希望包括一个功能要求，而在 GB/T 18336.2—2015 中又未有合适的功能组件，

可使用 GB/T 18336.2—2015 中的组件作为表示模型来指定 SFR。

确定在 GB/T 18336.2—2015 中是否有合适的功能组件可供使用，需要高度熟悉相关内容。建议参见 11.3.2 关于在 GB/T 18336.2—2015 确定适合的功能组件表达安全功能要求的内容。通常情况下，所需的安全功能要求可以通过适当应用细化操作，或者通过允许的赋值或选择操作来获得。但是，建议不要试图为功能组件硬塞一个安全功能要求，这会导致读者不容易理解 SFR 的含义或意图，或(通过使用不适当的组件)引入了不恰当的依赖性。

11.3.9 表述 SFR

制定一组明确符合 GB/T 18336—2015(所有部分)要求的 SFR 不是 PP 或 ST 作者的唯一目的，还应考虑如何最好地呈现和表达 SFR，使一般读者能够理解什么是安全要求，可在不影响 GB/T 18336—2015(所有部分)一致性的前提下采取一些提高可读性的步骤。

首先，对 SFR 进行分组。

其次，建议采用在 GB/T 18336.2—2015 中使用的功能元素标记方式来标记 PP 或 ST 中的 SFR。采用自己的标记系统也是可以的，但需要提供 SFR 与 GB/T 18336.2—2015 相关功能组件间的映射。在 PP 或 ST 包含被多次调用的功能组件也是可取的。

第三，通过用与 TOE 类型或安全功能描述相关的具体术语取代通用术语(如安全属性)，规范地使用细化操作可以提高 SFR 的可读性。例如，下面基于 FMT_MSA.3.1 的 SFR：

TSF 应执行 DAC 策略为客体权限提供受限的默认值。

在这个例子中，执行细化后，用“客体权限”代替了 FMT_MSA.3.1 中的“以便为用于执行 SFP 的安全属性”。

任何这样的细化操作的使用应清楚地在 PP 和 ST 基本原理中强调和解释(以便用于支持 PP 或 ST 评估)。

11.3.10 安全功能要求基本原理

除非安全目标或保护轮廓是低保障级别的，那么就需要基本原理来表示安全目的是如何由安全功能要求所满足的。该基本原理需要追溯所有的安全目的和对应安全目的的安全功能要求。追溯需要展示每一项安全要求能够对应至少一个安全目的，同时每个安全目的至少有一个安全功能要求与之对应。

多数情况下，一个单独的安全目的会对应多个安全功能要求，而一个单独的安全功能要求会支持多个安全目的，在多数安全目标和保护轮廓中，安全功能要求的数量会比安全目的的数量多，这是因为与安全功能要求相比，安全目的更通用。例如如下安全目的：

TOE 会确保每个用户被单独标识，并且在用户获取 TOE 设备访问权之前，对其身份进行鉴别。

这会映射出多个安全功能要求：

——用户如何被标识；

——用户如何被鉴别；

——鉴别失败后会怎么样；

——如何创建和管理用户及其鉴别数据；

——如何将用户与主体绑定。

相比证明安全客体具有安全要求，证明安全客体满足这些安全要求更重要。由上面举出的例子可知，理由很容易推导出来，但不适用于所有的安全目的。尤其是 TOE 模型中的用户特权，即使客体符合要求也可能不满足标准。例如如下安全目的：

TOE 需要确保未有信息从一个安全标签高的主体操作流向安全标签低或不相容的主体操作。

很难证明基于强制访问控制策略的安全功能要求完全满足安全目的。可能需要添加额外的安全功能要求，例如为信息流控制提供很好支持的架构也不可能显示所有满足安全目的安全功能要求。即使上述例子中所有安全功能要求都被正确执行，仍可能存在隐通道允许数据以违反安全目的的方式流动。完备性证明作为安全要求原理的一部分应承认这一点，并表明 TOE 模型内提供的安全功能要求与安全目的是完全对应的，例如，提供证据显示没有安全功能要求与安全目的相冲突。

一般来说，当安全目的以功能而不是属性来描述时，安全目的与安全功能要求间的追溯以及完备性证明变得更容易。因此安全目标应当尽可能的精确。当编写安全目标或保护轮廓时，重新考虑安全目的并尝试更准确地制定它们，在这种情况下，要对安全目的到安全功能进行追溯，或证明安全功能要求完全满足安全目的的。

11.4 确定安全保障要求

11.4.1 选择安全保障要求

保障要求的选取需要考虑多个方面的平衡，包括：

a) 被保护资产的价值和其他损害资产的已知风险；

b) 技术可行性；

c) 可能的生产和评估成本；

d) 开发及评估 TOE 所需的时间进度；

e) 已知的市场需求(以产品为例)；

f) 功能组件与保障组件之间的相互依赖的关系。

被保护资产的价值越高，这些资产面临的风险就越大，用于保护这些资产的安全功能所需要的保障级别就越高。这应在安全目的的描述中得以体现。组织可以定义自己的政策和规则来确定保障的级别，以确保这些保障可以将其资产的风险降低到可接受的水平。

其他诸如成本和时间因素，往往在实际中会限制保障级。如果指定的保障组件所需的证据不切实际，那技术可行性也是考虑的因素之一。这可能与遗留系统(无法获得大量详细设计文档)有关，或者需要一个更高保障级，而在可接受的时间内形成所需的半形式化或形式化证据在技术上也是不可行的。当对所需达到的保障有约束时，其所达到最高保障会低于理想情况。这种接受风险的举措，应当在安全目的中陈述。

安全目的陈述也可能需要具体表明 SAR 中的保障需求，例如：

a) TOE 安全目的可以声明 TOE 应能够抵御高攻击潜能的攻击者。在 AVA_VAN.5 中明确要求需要对这种抵抗进行证明。

b) 安全目的应表明要关注自保护、域分离、不可旁路性，纳入 ADV_ARC.1 组件是有必要的。尽管 ADV_ARC 只含有一个组件，但所需的架构描述的级别依赖于从 ADV_TDS 类中所选择的组件。

c) 安全目的也应注意 TOE 的安全性也依赖于安全的开发环境。这表明 SAR 应包括 ALC_DVS 族中的组件，以确保可检测开发环境的安全性。

SAR 的选择相对简单，只需要简单地选择一个合适的保障包即可。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。当一个保障包能够提供所需的大部分保障级，但对应安全目的某些特定方面仍有不足，这种情况下适合引入增强的保障要求来确保安全目的得以满足。

当要求增强的保障要求时，PP 或 ST 的作者应确保附加的需求也要满足保障组件的依赖关系。举个例子，如果 PP 或 ST 用 AVA_VAN.3 组件对 EAL3 增强，那么同样也应在 ADV_TDS.3 和 ADV_IMP.1 进行增强，尽管他们并不包含在 EAL3 里，同时，因为 ADV_TDS.3 依赖于 ADV_FSP.4，还需将

ADV_FSP.4 也包含进来。

11.4.2 操作安全保障要求

以下的操作是可行的：

a) 反复，允许相同的保障组件多次使用；

b) 细化，允许在不引进任何依赖其他 SAR 的情况下，给保障要求添加细节；

c) 赋值，允许给带赋值参数的 SAR 元素进行赋值；

当对应用于 TOE 不同部分的同一保障组件进行不同细化时，或在 PP 或 ST 对组合 TOE 的不同部分指定不同的保障要求时，才会使用到反复操作。

SAR 上的细化操作可能被用于以下情况：

a) 约束开发者的行为，可通过使用特定开发工具、方法论、生命周期模型、分析技术、符号、遵守特定标准等要求来对其约束；

b) 约束评估者的行为，比如：

——在 ADV_IMP.1 的例子中，指定 TOE 的哪一部分实现表示应包括在被检查的子集中；

——在 AVA_VAN.1 的例子中，标识出一组来源于公共域下的脆弱性。

11.4.3 确定未包括在 GB/T 18336.3—2015 中的 SAR

如果 PP 或 ST 的作者想要包含一个扩展的 SAR，该 SAR 在 GB/T 18336.3—2015 中没有合适的保障组件来定义，那么这个扩展的 SAR 应使用一个 GB/T 18336.3—2015 组件作为原始模型来定义。

11.4.4 安全保障要求基本原理

保护轮廓和安全目标的结构同样要求给出为什么选择某个安全保障要求集合的基本原理。如图 3 所示的安全保障要求不需要来自定义安全问题或安全目的，因此可能来自其他来源。GB/T 18336.1—2015 允许不提供推导安全保障要求的原因，或仅需指出这些安全保障要求由何种规章制度决定。

在多数情况下，安全保障要求是根据威胁得出的，并且威胁主体能够通过安全保障要求的选择倾向来识别安全问题，因此 TOE 被期望能够抵抗包括在安全问题定义里面的通过威胁主体发动的攻击。如果是这种情况，就应在安全保障要求选择的基本原理中对此进行表述。

12 TOE 概要规范

TOE 概要规范是安全目标要求的，但不适用于保障轮廓。因此本章内容仅适用于安全目标。

TOE 概要规范的目的是为消费者提供一个说明 SFR 是如何被满足的 TOE 安全功能描述。TOE 概要规范根据 TOE 整体的功能和体系架构描述安全功能，为得到 TOE 整体的抽象视图以及 TOE 是如何实现 SFR 而提供充分的详述。

TOE 概要规范提出了一个以整体 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。

一个构建 TOE 概要规范的方法是从整体概述开始，对包括 TSF 边界的 TOE 架构进行抽象表述。即使不需要满足 ASE_TSS.2 的要求，对于描述 TSF 如何保护它自身以防被篡改或者被旁路也是有好处的。然后再基于用来推导出 SFR 的功能模型来描述安全功能。撰写 TOE 概要规范与描述 SFR 同

步进行是一个很好的实践，能够确保每一个 SFR 的得出是和功能模型一致的，因此能够构造出在 TOE 概要规范中描述的安全功能到 SFR 的映射。TOE 概要规范基本上应包括功能模型，而这个模型应适用于 TOE 的功能和架构。这也给读者一个整体的理解：为什么要选择这些特定安全功能或其细节，同时解释这些功能和细节如何支持 TOE 的总体功能性。此外，由于 TSS 和 SFR 来源于同一模型，所以可以自动获得 TSS 到 SFR 的映射。

对于组合 TOE 的情况，TOE 概要规范需要描述每一部件以及它们之间是如何相互作用来满足 SFR 的。描述应使读者理解组合 TOE 的 SFR 与部件 SFR 的映射关系以及这些 SFR 是如何相互作用。

13 组合及部件 TOE 的保护轮廓和安全目标

13.1 组合 TOE

绝大多数 TOE 在其运行环境中都会与其他 IT 产品或系统进行交互。在很多情况下，TOE 需要这样的 IT 产品或系统的支持以满足安全功能要求。举例说明，一个数据库系统 TOE 依赖于底层操作系统提供的文件保护、地址空间分离和用户鉴别功能。另一个例子是操作系统依赖于用于存储鉴别用途的数字证书和证书撤销列表的外部 LDAP 服务器；这个操作系统也依赖于一个用来产生证书、证书撤销列表，并且通过 LDAP 服务器及时发布这些证书和证书撤销列表的外部 PKI。将这两个例子合并，数据库管理系统（虽然依赖于操作系统实现用户鉴别）也依赖于实现用户鉴别的 LDAP 服务器和 PKI 系统。当使用智能卡用于用户鉴别时，这个案例也可以很容易地被扩展。在这种情况下，依赖性不仅针对智能卡本身，也依赖于智能卡个人化系统。

从这些例子中可以看出，一个看上去很简单的安全功能要求（用户鉴别）可能需要很多不同 IT 产品之间正确、安全的协同合作才能实现，而这些 IT 产品本身已单独通过评估。本节主要讨论的问题是 TOE 特定的安全功能要求与 TOE 环境安全目的的结合，旨在解决 IT 产品组合后对安全功能要求满足的相关问题。对于以上陈述的案例，可以总结出以下依赖性：

——数据库管理系统依赖于操作系统实现用户鉴别、文件保护和地址空间分离；

——操作系统依赖于底层硬件实现地址空间分离，防止未授权程序直接访问附加的 I/O 设备和专用的处理器配置寄存器；

——操作系统依赖于 LDAP 服务器实现防止非授权访问的用户鉴别相关信息的保护，也依赖 LDAP 服务器适时的提供信息请求，同时对 LDAP 服务器与操作系统传递信息时提供保护，避免信息被篡改；

——操作系统依赖于 PKI 系统，实现用户鉴别相关的数字证书的生成和对证书正确性的管理（包括及时在 LDAP 服务器上发布证书和 CRL）；

——操作系统还依赖智能卡去保护用户的私钥，只有在接收到正确的鉴别信息时才能使用私钥（如 PIN 码的使用）；

——智能卡依赖于特定主机的操作系统，实现从用户输入 PIN 码开始，到 PIN 码传输到智能卡，直到 PIN 码从主机操作系统的内存中安全删除为止全程保护用户 PIN 码。同时也依赖主机操作系统，避免对用户 PIN 码的误用，如在没有被用户授权的情况下 PIN 码不能提交给智能卡。

这仅仅是一个用来演示 PP 或者 ST 中如何处理依赖性的列表。

当在分析依赖关系的时候，可以很容易地识别：

——数据库依赖操作系统提供的安全功能；

——操作系统对硬件有依赖；

——操作系统对 LDAP 服务器有依赖；

——操作系统对 PKI 有依赖；

——操作系统对智能卡有依赖；

——智能卡对主机操作系统有依赖。

当一个部件依赖于另外一个部件的时，GB/T 18336—2015(所有部分)中将他们称为“依赖”和“基础”部件。在所举的例子中，数据库和操作系统的组合中，数据库是依赖部件，操作系统是基础部件。与此类似，在操作系统和硬件的组合中，操作系统是依赖部件，硬件是基础部件。在智能卡和操作系统的例子中，两者同时依赖于对方，因此两者互为依赖部件，同时互为基础部件。

当在为一个依赖部件制定安全目标或者保护轮廓时，对基础部件的依赖关系应通过假设和从这些假设推导出的运行环境安全目的进行陈述。以 DBMS 为例，定义的假设可以这样陈述：

——*假设 1：运行环境能够保护 DBMS 软件免受其他与 DBMS 软件运行在同一系统上的其他应用软件的干扰或篡改；*

——*假设 2：运行环境能够保护 DBMS 用来存储用户和 TSF 数据的文件不被未经授权访问；*

——*假设 3：运行环境能够标识和鉴别个人用户，为 DBMS 提供获得向 DBMS 发起请求的用户身份的方法。*

这些假设可以被进一步用来定义作为运行环境一部分的操作系统相关的安全目的。这些目的描述的详细程度很大程度上取决于 DBMS 的具体要求。例如，如果审计功能是 DBMS 的一个安全功能要求，它就有必要从操作系统获得相应的审计等级，以检测那些试图绕过或篡改 DBMS 依赖的操作系统安全功能的行为。以下是一个从以上假设得到的安全目的举例：

——*该操作系统需要提供安全机制以允许 DBMS 在其自己的执行域中执行，并且这个执行域受到保护以防止被另外运行于操作系统控制之下的其他应用程序的干扰和篡改；*

——*该操作系统需要保护 DBMS 的可执行程序不被未授权访问；*

——*该操作系统需要提供一个 DBMS 软件完整性检测机制，当检测到不可修复的完整性错误时将禁止 DBMS 的启动；*

——*该操作系统需要提供文件访问控制机制，至少以读、写/更新访问权限进行区分，并且允许单独地定义细化到单个用户(包括“无权访问”)的访问级别；*

——*该操作系统应可以允许限制单个用户或用户组对文件访问权限的管理；*

——*该操作系统应当在个人用户调用 DBMS 功能前标识并鉴别这些用户；*

——*该操作系统需要使用一个鉴别保护机制使得发生用户鉴别错误概率小于 1/1,000,000；*

——*该操作系统应当有审计功能，对鉴别成功和不成功的鉴别尝试进行审计，并且审计记录中包括用户身份和鉴别尝试发生的时间和日期；*

——*该操作系统应当提供一个接口供 DBMS 使用以正确获取调用数据库功能的用户身份标识。*

上述大多数安全目的都能够比较容易的与 GB/T 18336.2—2015 定义的安全功能要求进行对应。只有第一个安全目的不同，因为它说明了域分离的架构特性。安全架构文档需要描述操作系统是如何实现这种属性的。安全架构文档对于 EAL2 及以上级别是强制要求的。

存在一种情况，DBMS 作为依赖部件而操作系统作为基础部件，为操作系统定义的安全目的内容细化级别较高已非常接近安全功能要求的细节程度。在任何时候提供这种等级的细节描述都是可能的。

还有另外一些情况，假设和来自这些假设而定义的运行环境安全目的内容是很通用的。举一个操作系统作为依赖部件 LDAP 服务器作为基础部件的例子，定义假设为：

运行环境应保护操作系统用于用户鉴别而使用的数字证书和 CRL，避免其被未经授权的修改和

添加。

ST 或 PP 可预留保护措施的细节允许赋值不同的方法来满足假设。从此假设获得的运行环境安全目的为：

——*在改变或添加证书、CRL 之前，LDAP 服务器应先通过操作系统标识和鉴别用户身份*；

——*运行环境应保护 LDAP 服务器和操作系统之间的通信避免传输的数据被修改(包括添加和重放)*。

在这个例子中，可能不想对如何满足运行环境安全目的的方法定义的过于具体，允许不同的方法去满足这些要求。在上述例子中，故意预留开放性使得安全目的既可以通过使用加密保护通信协议获得也可以通过物理手段进行互联网保护的方式获得满足。

当为依赖部件撰写安全目标或保护轮廓时，撰写者应区分以下两种情况的不同，一种是基础部件已经通过评估，当评估依赖部件时，基础部件的评估结果可用，另一种情况是基础部件没有被评估，或是基础部件的评估结果不可用。

GB/T 18336.3—2015 中包含的 ACO 保障类为评估过的部件组合定义了评估标准。为组合 TOE 制定安全目标或保护轮廓的作者应从 ACO 类中选择适合于保障级别的组件。为完成这一目标，GB/T 18336.3—2015 还为组合 TOE 定义了三个“组件保障包”可用于安全目标或保护轮廓中。如果决定从 ACO 类中选择组件且不同于已经定义的包，那应确保依赖关系已经满足。

13.2 部件 TOE

尽管有一些 TOE 是自给自足的，对其环境中的其他 IT 部件没有明确的依赖关系，但是有一些 TOE 不是这样，这些 TOE 被定义为“部件 TOE”，典型的例子如下：

——一个软件包提供了定义的安全功能，但是要整合到其他的不同产品之中。软件包依赖于要整合到的那些产品才能对 TSF 和 TSF 数据进行保护和实现对 TSF 数据的管理；

——一个应用实现对自身客体进行的访问控制，但需依赖环境提供的用户标识和鉴别功能；

——一个应用或者操作系统依赖密码协处理器提供的加解密和对密钥对的管理功能。

在上述所有情况下，多少会有一部分安全目的是 TOE 自身无法满足而需要映射到环境安全要求的，因此，该 TOE 的评估需要基于这样的假设，即环境正确地实现安全功能要求，从而满足了这部分安全目的。

一个部件的安全目标或保护轮廓与一个能够自给自足的产品没有太大的区别，唯一的区别是 IT 环境安全目的需要精确地对应满足目的的环境中的 IT 产品类型(如果可能的话)。在 13.1 的例子中可以看到，针对操作系统的安全目标中明确定义的安全目的，可以由底层硬件、LDAP 服务器，PKI 系统和智能卡来满足。那些安全目的应被定义的足够准确，以使得较容易的能与安全目标中定义的安全功能要求组件相对应。这使得对于组合 TOE 评估部件数目的时候可以很容易地进行对应和梳理。

14 特殊情况

14.1 低保障级的保护轮廓和安全目标

当保障级别不高于 EAL1 级的情况下，GB/T 18336—2015(所有部分)允许对 PP 或 ST 进行简化，ST 或 PP 可忽略如下内容：

——安全问题定义；

——安全目的；

——安全目的基本原理；

——安全要求基本原理，但对于安全要求组件之间未解决的依赖关系而做的解释是不能忽略的。

以上允许对安全目标和保护轮廓的简化针对的是低保障级别产品。但其他的部分需要和之前描述一致。

一个低保障级别的安全目标或保护轮廓可以声称仅与一个低保障级别的保护轮廓相一致，但一个非低保障级别的保护轮廓或安全目标也可能声称与一个低保障级别的保护轮廓相一致。这种情况下，非低保障级别的保护轮廓或安全目标需要包括低保障级别保护轮廓或安全目标中所有强制要求的部分。因此，在声称一致的低保障级别保护轮廓中简化的部分内容也应包含在非低保障级别的保护轮廓或安全目标中。

14.2 功能和保障包

除保护轮廓外，GB/T 18336—2015(所有部分)还允许定义功能和保障包。一个功能包中包含了一套安全功能要求，一个保障包中包含了一套安全保障要求，而包含安全功能要求和安全保障要求的混合包是不允许的。

这样的包应有一个标识自身的包名，而且它应包含一系列有用且有效的要求。例如，一个功能包可能包含定义某一特定安全特性的安全功能要求。一个典型的例子是，一个只定义审计功能相关的功能包(可对最小事件集进行审计、保护审计迹、审计回溯、审计管理)。这样的功能包面对不同类型的安全产品(如操作系统、数据库管理系统、防火墙)时可被重用。当定义一个这样的功能或保障包时，应直接在包内说明依赖关系，或提供针对未解决的依赖关系该如何处理的建议。

附 录 A
（资料性附录）
扩展组件定义示例

以下部分提供了一个为解决 TSF 数据恢复而定义扩展安全功能组件的例子，此例子展示了在 ST 或 PP 中应以何种方式来定义扩展组件的结构以及组件的基本原理。

TSF 数据恢复(FPT_REC_EXT)

族行为

TSF 数据恢复允许为 TSF 数据设置检查点，以便符合检查点的时机时对 TSF 数据进行恢复。在其检测到 TSF 数据被修改(如管理员的错误操作或硬件或软件故障而引起的错误)后，可允许恢复这些 TSF 数据。

组件分级

FPT_REC_EXT.1 基本 TSF 数据恢复要求设置检查点，并可在管理员明确的行为下从检查点进行数据恢复。

FPT_REC_EXT.2 高级 TSF 数据恢复要求设置检查点，并可自动的或在管理员明确的行为下从检查点进行数据恢复。

管理：FPT_REC_EXT.1，FPT_REC_EXT.2

FMT 中的管理功能可考虑下列行为：

——对定义检查点和/或启动恢复权限的管理。

——对作为检查点而存储的 TSF 数据的管理。

审计：FPT_REC_EXT.1，FPT_REC_EXT.2

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”，下列行为应是可审计的：

——最小级：所有成功的恢复操作；

——基本级：所有试图执行的恢复操作；

——详细级：所有试图执行的恢复操作，所有检查点操作。

FPT_REC_EXT.1 基本 TSF 数据恢复

从属于：无其他组件。

依赖关系：FMT_SMR.1 安全角色，FMT_MOF.1 安全功能行为的管理

FPT_REC_EXT.1.1 TSF 应当允许具有[赋值：角色的列表]的用户为[赋值：TSF 数据列表]定义检查点，并存储这些 TSF 数据

FPT_REC_EXT.1.2 TSF 应当允许具有[赋值：角色的列表]的用户从检查点恢复 TSF 数据。

FPT_REC_EXT.1.3 TSF 应执行以下操作[赋值：一致性和完整性检查的行动列表]，以确保 TSF 数据恢复后的一致性和完整性。

FPT_REC_EXT.1.4 当检测到的 TSF 数据不一致或恢复过程中完整性被破坏时，TSF 应执行以下操作[赋值：操作列表]。

FPT_REC_EXT.2 TSF 数据自动恢复

从属于：FPT_REC_EXT.1

依赖关系：FMT_SMR.1 安全角色，FMT_MOF.1 安全功能行为的管理

FPT_REC_EXT.2.1 TSF 应为[赋值：TSF 数据列表]在下列条件[选择：在管理员定义的时间间隔，当下列条件满足时[赋值：条件列表]，[赋值：其他条件]]下定义检查点，并存储这些 TSF 数据。

FPT_REC_EXT.2.2 TSF 应在下列条件[赋值：条件列表]下从检查点恢复 TSF 数据。

FPT_REC_EXT.2.3 TSF 应执行以下操作[赋值:一致性和完整性检查的行动列表],以确保 TSF 数据恢复后的一致性和完整性的。

FPT_REC_EXT.2.4 当检测到 TSF 数据不一致或恢复过程中完整性被破坏时,TSF 应执行以下操作[赋值:操作列表]。

FPT_REC_EXT.2.5 TSF 应仅在确保 TSF 数据一致性和完整性时才能使用恢复的 TSF 数据。

扩展组件定义的基本原理

GB/T 18336.2—2015 未定义在检查点执行 TSF 数据恢复的 SFR,而这种恢复对于确保 TOE 安全运行又很重要。功能要求规定了作为检查点而定义的那部分 TSF 数据的存储条件,以及之后进行恢复的条件。可能会产生恢复的 TSF 数据与 TSF 状态不一致的情况,因此应确保存储 TSF 数据的完整性。有必要执行检查以确保数据恢复后 TSF 的整体状态是一致的、安全的,且恢复的 TSF 数据未被修改。在数据恢复之后和 TOE 继续正常运行之前,SFR 要执行一致性和完整性检查。

如果这些一致性检查失败,TOE 可决定采取自动纠正措施,进入可通过管理员手动修正的维护模式,也可执行其他操作以防止 TOE 进入不安全状态。FPT_REC_EXT.2 不允许使用恢复的 TSF 数据,除非其一致性和完整性已得到保证。

此安全功能要求组件是 GB/T 18336.2—2015 中定义的 FPT 类安全功能组件的扩展组件。

GB/T 20283—2020