ICS 35.040
L 80

中华人民共和国国家标准

GB/T 30270—2013/ISO/IEC 18045:2005

信息技术　安全技术
信息技术安全性评估方法

Information technology—Security technology—
Methodology for IT security evaluation

(ISO/IEC 18045:2005,IDT)

2013-12-31 发布　　2014-07-15 实施

中华人民共和国国家质量监督检验检疫总局
中国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。

本标准采用翻译法等同采用国际标准 ISO/IEC 18045:2005《信息技术　安全技术　信息技术安全性评估方法》。

与本标准中规范性引用的国际文件有一致性对应关系的我国文件如下：

——GB/T 18336—2008　信息技术　安全技术　信息技术安全性评估准则(ISO/IEC 15408:2005,IDT)。

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。

本标准主要起草单位：中国信息安全测评中心、吉林信息安全测评中心、华中信息安全测评中心。

本标准主要起草人：李守鹏、吴世忠、黄元飞、李斌、刘晖、刘春明、郭颖、付敏、谭运猛、徐长醒、宋小龙、简余良、郭涛、甘杰夫、张宝峰、石竑松、杨永生、毕海英、高金萍、王峰、李凤娟、唐喜庆、曾华春。

引　言

本标准提出的信息技术(IT)安全性评估方法仅限于对 ISO/IEC 15408 中定义的 EAL1～EAL4 评估,不提供 EAL5～EAL7 及其他保证包的评估指南。

本标准的读者对象主要是采用 ISO/IEC 15408 的评估者和确认评估者行为的认证者,以及评估发起者、开发者、PP/ST 作者和其他对 IT 安全感兴趣的团体。

本标准并不能解决所有有关 IT 安全评估的问题,有些问题还需要进一步的解释。这些解释将由各评估体制决定如何处理,即便它们要遵从多方互认协议。可以由各体制处理的评估方法相关活动列表见附录 A。

本标准提出了依据 ISO/IEC 15408《信息技术　安全技术　信息技术安全性评估准则》进行信息技术安全评估时的评估方法,是 ISO/IEC 15408 的配套标准。

信息技术　安全技术
信息技术安全性评估方法

1　范围

本标准描述了在采用 ISO/IEC 15408《信息技术　安全技术 信息技术安全性评估准则》所定义的准则和评估证据进行评估时，评估者应执行的最小行为集，是 ISO/IEC 15408 的配套标准。

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(包括所有的修改版)适用于本文件。

ISO/IEC 15408(所有部分)　信息技术　安全技术　信息技术安全性评估准则(Information technology—Security techniques—Evaluation criteria for IT security)

3　术语和定义

下列术语和定义适用于本文件。

3.1

行为　action

ISO/IEC 15408-3 的评估者行为元素。这些行为在 ISO/IEC 15408-3 保证组件中要么是直接声明为评估者行为，要么是间接从开发者行为(隐含的评估者行为)中导出。

3.2

活动　activity

ISO/IEC 15408-3 保证类的施用。

3.3

核查　check

通过简单比较形成一个**裁定**。评估者不一定必须具备专门技能。使用此动词的语句描述了需要核查的内容。

3.4

评估交付件　evaluation deliverable

评估者或监督者为执行一个或多个评估或评估监督活动所必需的，由发起者或开发者提交的所有资源。

3.5

评估证据　evaluation evidence

真实的**评估交付件**。

3.6

评估技术报告　evaluation technical report

由评估者编写并呈交给监督者、以文档形式记录总体裁定及其理由的报告。

3.7

检查 examine

评估者通过采用专业技能分析形成一个裁定。使用此动词的语句表明哪些是分析对象以及对象的哪些属性。

3.8

解释 interpretation

对 ISO/IEC 15408 中的要求、本标准中的要求或体制要求的一种澄清或详述。

3.9

方法 methodology

用于 IT 安全性评估的原则、程序和过程组成的体系。

3.10

观察报告 observation report

在评估过程中由评估者编写的用于澄清或标识一个问题的报告。

3.11

总体裁定 overall verdict

评估者发布的关于评估结果是“通过”还是“不通过”的决定。

3.12

监督裁定 oversight verdict

根据评估监督活动的结果,监督者发布的认可或否决总体裁定的决定。

3.13

记录 record

记录过程、事件、观察结果、所了解事项以及结果的书面描述。该描述需足够详细,以便评估过程中执行的工作能够重现。

3.14

报告 report

将评估结果和支持性材料纳入到评估技术报告或观察报告。

3.15

方案 scheme

评估管理机构制定的一套规则,这套规则定义了评估环境,包括 IT 安全评估所需的准则和方法。

3.16

子活动 sub-activity

ISO/IEC 15408-3 中一个保证组件的施用。本标准不处理保证族,因为评估子活动只用到保证族中的单个保证组件。

3.17

追溯 tracing

两个实体集合之间的简单定向关系,表明第一个集合中的哪些实体与第二集合中的哪些实体相对应。

3.18

裁定 verdict

评估者发布的关于 ISO/IEC 15408 中一个评估者行为元素、保证组件或类是“通过”“不通过”,还是“待定”的一项决定。

3.19

工作单元 work unit

评估工作的最小组成部分。每个评估方法行为由一个或多个工作单元组成，这些工作单元按照ISO/IEC 15408中“证据的内容和形式元素”或“开发者行为元素”组织到评估方法行为中。在本标准中，工作单元的呈现顺序与导出它们的ISO/IEC 15408元素的呈现顺序相同。工作单元用形如“4：ALC_TAT.1-2”的符号标识，其中第一个数字“4”表示EAL等级，字符串ALC_TAT.1表示ISO/IEC 15408组件(即本标准的子活动)，最后一个数字“2”代表这是子活动ALC_TAT.1的第二个工作单元。

4 缩略语

下列缩略语适用于本文件。

ETR：评估技术报告(Evaluation Technical Report)

OR：观察报告(Observation Report)

5 概述

5.1 本标准的组织

第6章定义了本标准中使用到的一些约定。

第7章描述了不需要做出裁定的通用评估任务，这些任务没有映射到ISO/IEC 15408评估者行为元素。

第8章定义了保护轮廓(PP)评估。

第9章定义了安全目标(ST)评估。

第10章～第13章定义了为完成EAL1～EAL4评估而需要的最小评估努力，并提供了完成评估的方法和手段指南。

第14章定义了缺陷纠正评估活动。

附录A提出了一些基本评估技术，用于为评估结果提供技术性证据。

6 文档约定

6.1 行文方式

ISO/IEC 15408中每个元素相对于族中所有组件都保持其标识符的最末一个数字不变，本标准则不同，当ISO/IEC 15408中的评估者行为元素从一个子活动变换到另一个子活动时，本标准可引入新的工作单元，因此，尽管工作单元没有改变，工作单元标识符的最末一个数字可以改变。例如，一个附加的工作单元，其标记为4：ADV_FSP.2-7被添加到EAL4，后续的FSP工作单元顺序号偏移了一位，此时工作单元3：ADV_FSP.1-8对应于工作单元4：ADV_FSP.2-9，这样表示虽然他们的编号不再直接对应但却是相同的要求。

任何不需要直接从ISO/IEC 15408要求中导出的特定方法论评估工作称为*任务*或*子任务*。

6.2 动词用法

在所有工作单元和子任务动词前都加以助动词“应”，并且动词和“应”都用***粗斜体***表示。只有当规定的条文是强制要求的时，才使用助动词“应”。为了得出裁定，评估者应执行工作单元和子任务中包含的强制活动。

工作单元和子任务附带的指导性条文给出了如何在一个评估中使用 ISO/IEC 15408 语句的进一步解释。描述方法是标准化的,也就是说助动词的用法与 GB/T 1.1 的约定是一致的,即:助动词"宜"表示强烈推荐该方法,"可"表示允许使用该方法但不是首选的(助动词"应"只用在工作单元或子任务中)。

动词"核查""检查""报告"和"记录"在本标准中有确定的意义,在使用时请参见第 3 章的定义。

6.3 通用评估指南

适用于多个子活动的指导性材料被集中到一个地方。适用性很广泛(跨越活动和 EAL)的一些指导性条文已统一放在附录 A 中。在各个活动的简介部分已提供了适合于该活动中多个子活动的指南。如果指南只适合某单一的子活动,则它在子活动中进行描述。

6.4 ISO/IEC 15408 和本标准结构间的关系

ISO/IEC 15408 结构(即类、族、组件和元素)与本标准的结构之间有直接的关系。图 1 说明了 ISO/IEC 15408 结构的类、组件和评估者行为元素对应本标准的活动、子活动和行为之间的关系。另外,有些评估方法工作单元可以从 ISO/IEC 15408 的"开发者行为元素"和"证据的内容和形式元素"中得出。如图 1。

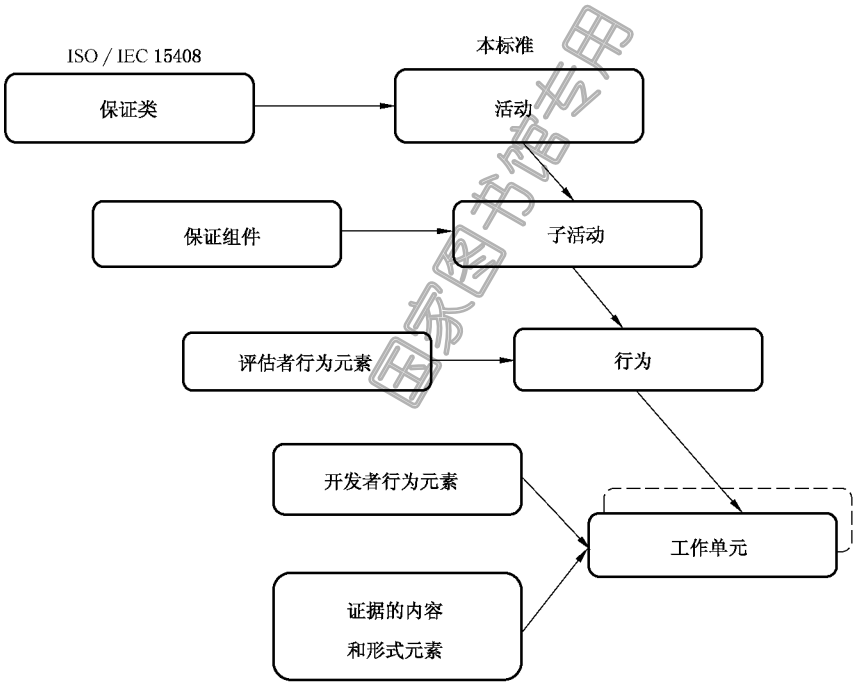

图 1 ISO/IEC 15408 与本标准结构间的映射

6.5 评估者裁定

评估者是对否满足 ISO/IEC 15408 的要求给予裁定而不是本标准的要求。要给予裁定的最小 ISO/IEC 15408 结构是评估者行为元素(明显的或隐含的)。作为执行相应评估方法行为及其组成工作单元的结果,每个 ISO/IEC 15408 评估者行为元素均被赋予一个裁定。最后给出 ISO/IEC 15408-1 的 6.3 所述的评估结果。

本标准认可三种互相排斥的裁定情形:

a) 通过:评估者完成了 ISO/IEC 15408"评估者行为元素",并确定接受评估的 PP、ST 或 TOE 的

要求得到满足。通过评估的条件在相关行为的组成工作单元中给定；

b) 待定：评估者未完成与 ISO/IEC 15408 评估者行为元素相关的一个或多个评估方法行为工作单元；

c) 不通过：评估者完成了 ISO/IEC 15408 评估者行为元素并确定接受评估的 PP、ST 或 TOE 未满足要求。

所有的裁定最初都是“待定”，直到被赋予“通过”或“不通过”裁定为止。

当且仅当所有组成部分的裁定都为“通过”，总体裁定才为“通过”。如图 2 所示，如果某个评估者行为元素的裁定为“不通过”，则相应保证组件、保证类的裁定和总体裁定都为“不通过”。

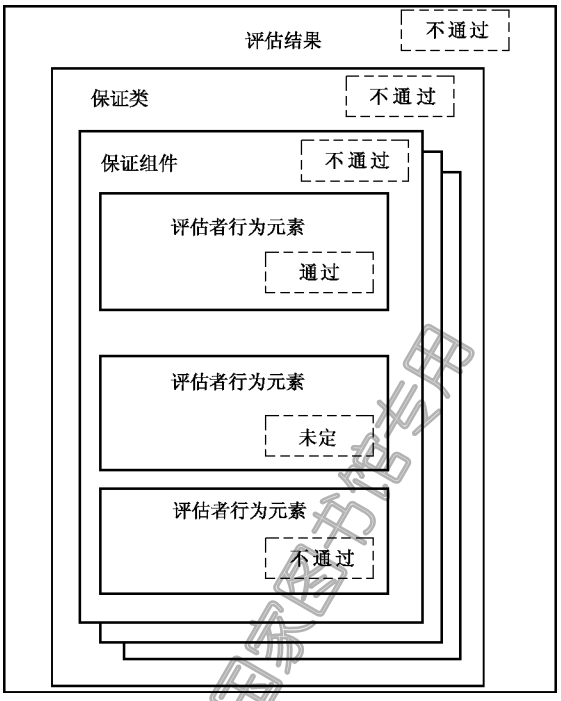

图 2 裁定规则示例

7 通用评估任务

7.1 简介

不管是 PP 或 TOE(包括 ST)评估，所有的评估都有两个通用评估者任务：输入任务和输出任务。这两个任务与评估证据的管理和报告的产生有关，本章对其进行了描述。每一个任务由一些适用于所有 ISO/IEC 15408 评估(PP 或 TOE 评估)的标准化的子任务组成。

尽管 ISO/IEC 15408 没有专门强制要求这些评估任务，但是本标准在其需要的地方进行了强制要求。不同于本标准中其他章节描述的活动，本章的这些任务没有与之关联的裁定，因此不能映射到 ISO/IEC 15408 评估者行为元素，执行它们就是为了遵守本标准。

7.2 评估输入任务

7.2.1 目的

本任务的目的是确保评估者能够获得正确版本的评估证据，且证据得到了充分保护。否则，就不能保证评估的技术精确性，也不能保证评估结果的可重复性和可再现性。

7.2.2 应用注释

提供所有必需的评估证据是评估发起者的责任。然而,大多数评估证据很可能是由开发者(代表评估发起者)产生和提供的。因为保证要求适用于整个 TOE,所以要使 TOE 组成部分的所有产品有关的评估证据对评估者都是可用的。这种评估证据的范围和所需内容不依赖开发者对每个产品(即 TOE 的组成部分)的控制水平。例如,如果要求高层设计,则 ADV_HLD"高层设计"要求将适用于所有子系统(即 TSF 的组成部分)。此外,需要采用核查程序的保证要求(例如 ALC_CAP"CM 能力"和 ALC_DEL"交付")将适用于整个 TOE(包括来自其他开发者的任何部分)。

建议评估者和评估发起者一起制定一个所需评估证据的索引。这个索引可以是一组文件参考资料的集合。这个索引应当包含足够的信息(例如每个文档的摘要或清晰的标题、对所关注条款的标记),以方便评估者更容易地查找所需证据。

需要的是评估证据中包含的信息,而不是任何特定的文档结构。一个子活动的评估证据可以通过一些不同的文档来提供,或者一个单独的文档可以满足一个子活动的若干输入要求。

评估者需要评估证据稳定的、正式发布的版本。当然,在评估期间也可以提供评估证据草稿。例如,草稿可用于帮助评估者进行前期的、非正式的评价,但不能用作裁定的依据。评估者查阅以下特定评估证据的草稿也是有帮助的,例如:

a) 测试文档,允许评估者对各种测试和测试程序作出早期评价;
b) 设计文档,为评估者提供理解 TOE 设计的背景材料;
c) 源代码或硬件图,允许评估者评价开发者对标准的应用情况。

在 TOE 评估和 TOE 开发同步进行时,评估证据可能遇到处于草稿阶段的评估证据。另外对已开发好的 TOE 进行评估期间也可能遇到草稿性评估证据,此时开发者应做一些额外工作来解决评估者提出的问题(例如纠正设计和实现中的差错)或者提供在现存文档中欠缺的那些安全性评估证据(例如,TOE 最初设计时没有满足 ISO/IEC 15408 要求的情况)。

7.2.3 评估证据子任务的管理

7.2.3.1 配置控制

评估者***应执行***评估证据的配置控制。

ISO/IEC 15408 默认评估者在收到每项评估证据后,能够对其进行标识和定位,并且能够确定评估者是否拥有文档的特定版本。

当评估者持有评估证据时,评估者***应保护***评估证据,以防证据改变或丢失。

7.2.3.2 处置

在评估结束时,评估方案需要控制评估证据的处置。应当用以下一种或几种方式处置评估证据:

a) 归还评估证据;
b) 存档评估证据;
c) 销毁评估证据。

7.2.3.3 保密性

在评估过程中,评估者可能接触到评估发起者和开发者的一些商业性敏感信息(例如 TOE 设计信息、专门工具),还可能接触到一些国家级敏感信息。评估发起者可能希望要求评估者维护评估证据的保密性。在保持与评估体制协调一致的前提下,评估发起者和评估者可以协商增加其他要求。

保密性要求会在许多方面影响评估工作,包括对评估证据的接收、处理、存储和处置。

7.3 评估输出任务

7.3.1 目的

本条的目的是描述观察报告(OR)和评估技术报告(ETR)。评估体制可能还需要其他评估者报告(例如有关单个工作单元的报告),或者还要求在 OR 和 ETR 中包含其他信息。本标准并不排除在这些报告中加入其他信息,因为本标准只规定了最少的信息内容。

为满足评估结果的可重复性和可再现性原则,评估结果报告应保持一致性。一致性涵盖 ETR 和 OR 中所报告信息的类型和数量。不同评估间 ETR 和 OR 的一致性由监督者负责。

为使报告内容达到本标准的要求,评估者应执行以下两个子任务:

a) 编写 OR 子任务(如果评估需要的话);

b) 编写 ETR 子任务。

7.3.2 应用注释

在本标准中,没有明确要求提供有关支持再评估和再使用的评估者证据,也没有确定有关为协助再评估或再使用而由评估者工作产生的信息。评估发起者需要这些再评估或再使用信息时,应当向当前所处的评估体制咨询。

7.3.3 编写 OR 子任务

OR 为评估者提供一种要求解释(例如,需要监督者说明某个要求的使用)或确认评估中某个问题的机制。

在裁定为"不通过"的情况下,评估者***应提供***OR,以反映评估的结果。此外,评估者也可以使用 OR 作为表达需求的一种方式。

对每个 OR,评估者***应报告***以下信息:

a) 被评估 PP 或 TOE 的标识;

b) 该观察是在哪一个评估任务/子活动期间产生的;

c) 观察到的情况;

d) 严重程度评估(例如失败裁定、阻碍评估进展、需要在评估完成前给出解决办法);

e) 负责解决该问题的组织;

f) 解决问题的时限建议;

g) 问题解决失败时将对评估产生影响的估计。

OR 报告的目标读者及处理报告的流程取决于该报告的性质和评估体制。评估体制可根据所要求的信息和分发对象的不同(例如,OR 要给监督者或评估发起者)来区分 OR 的不同类型,或者定义附加类型。

7.3.4 编写 ETR 子任务

7.3.4.1 目的

评估者***应提供***一份 ETR,以给出裁定的技术依据。

ETR 可能包含开发者或评估发起者的专有信息。

本标准定义了 ETR 的最少内容要求,评估体制还可以指定其他内容和结构要求。例如,评估体制可以要求 ETR 中包含某些介绍性材料(例如免责声明和版权声明条款)。

ETR 的读者需要被假定为熟悉信息安全常规概念、ISO/IEC 15408、本标准、评估方法以及 IT。

ETR 支持监督者作出监督裁定,但是不能期望 ETR 提供监督需要的所有信息,并且该文档也无法提供必要证据供评估体制确认评估是否依据相关标准执行,这已超出本标准范围,应当用其他监督方式

来满足。

7.3.4.2 PP 评估的 ETR

本条描述 PP 评估的 ETR 所需要的最少内容。ETR 的内容如图 3 所示，在构建 ETR 文档的结构大纲时，可以此图作为指南。

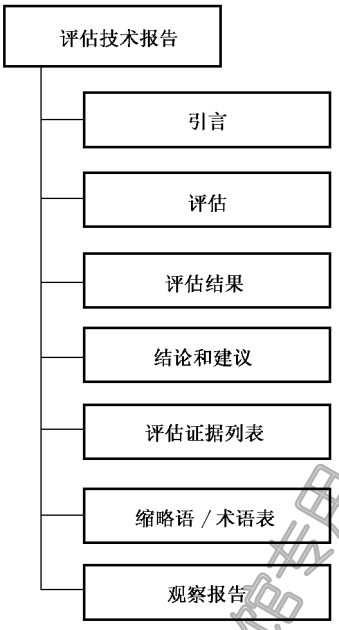

图 3 PP 评估的 ETR 信息内容

7.3.4.2.1 引言

评估者***应报告***评估体制的标识。

评估体制标识(例如标志)是明确地标识负责评估监督的评估体制信息。

评估者***应报告***ETR 配置控制标识。ETR 配置控制标识包含标识 ETR 的信息(例如，名称、日期、版本号)。

评估者***应报告***PP 配置控制标识。PP 配置控制标识(例如，名称、日期、版本号)用于标识出所评估的 PP，以便监督者核查评估者是否给出了正确的裁定。

评估者***应报告***开发者的身份。PP 开发者的身份用以标识出谁负责产生该 PP。

评估者***应报告***评估发起者的身份。评估发起者的身份用以标识出谁负责向评估者提供评估证据。

评估者***应报告***评估者的身份。评估者的身份用以标识出谁执行评估并且对评估裁定负责。

7.3.4.2.2 评估

评估者***应报告***所使用的评估方法、技术、工具和标准，注明在评估 PP 时所使用的评估准则、方法和解释。

评估者***应报告***所有对评估的限制、对评估结果处理的限制以及在评估期间所做的对评估结果有影响的假设。评估者可在报告中加入与法律法规、组织机构、保密性等相关的信息。

7.3.4.2.3 评估结果

评估者***应***针对组成 APE 活动的每个保证组件，***报告***其所作出的裁定及相应的基本原理，作为执行相应评估方法行为及其组成工作单元的结果。

基本原理应使用 ISO/IEC 15408、本标准、相关解释以及经过检查的评估证据来证明评估裁定是正

确的，并指出评估证据如何满足准则要求或者为何没有满足准则要求，包括对所做工作、所使用方法以及结果推导的描述。基本原理可以详细到本标准工作单元这种程度。

7.3.4.2.4 结论和建议

评估者***应报告***评估的结论，特别是如 ISO/IEC 15408-1 的 6.3 所规定的总体裁定，以及 6.5 所描述的裁定方式确定的总体裁定。

评估者提供的建议可能对监督者有用。这些建议可能包括评估期间发现的 PP 缺点，或者提及一些特别有用的特征。

7.3.4.2.5 评估证据列表

评估者***应报告***每项评估证据的以下信息：

——发布团体(例如，开发者、评估发起者)；

——标题；

——唯一索引(例如，发布日期、版本号)。

7.3.4.2.6 缩略语/术语表

评估者***应报告***ETR 中所使用的所有缩略语。

已由 ISO/IEC 15408 或本标准定义的术语在 ETR 中无须重复。

7.3.4.2.7 观察报告

评估者***应报告***一个能唯一标识在评估期间产生的 OR 及其状态的完整列表。

对于每个 OR，该列表应包含它的标识符、标题或其内容的摘要。

7.3.4.3 TOE 评估的 ETR

本条描述 TOE 评估的 ETR 所需要的最少内容。ETR 的内容如图 4 所示，在构建 ETR 文档的结构大纲时，可以此图作为指南。

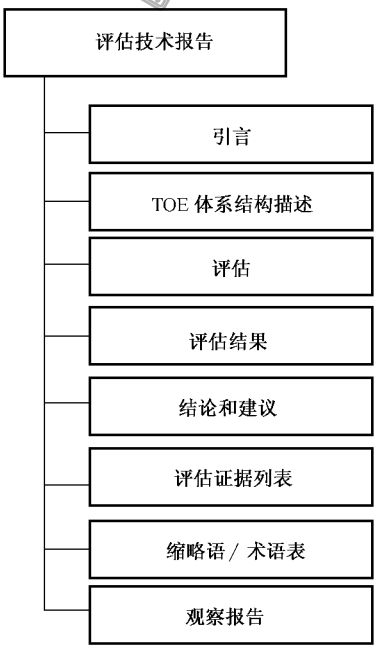

图 4 用于 TOE 评估的 ETR 内容

7.3.4.3.1 引言

评估者*应报告*评估体制的标识。评估体制标识(例如标志)是明确地标识负责评估监督的评估体制所需的信息。

评估者*应报告*ETR 配置控制标识。ETR 配置控制标识包含有标识 ETR 的信息(例如,名称、日期和版本号)。

评估者*应报告*ST 和 TOE 配置控制标识。ST 和 TOE 配置控制标识标识出正在被评估的内容,以便监督者核查评估者是否给出了正确的裁定。

如果 ST 声明 TOE 遵从一个或几个 PP 的要求,则 ETR 应报告相应 PP 的引用。

PP 引用中应含有能唯一地标识出 PP 的信息(例如,标题、日期、版本号)。

评估者*应报告*开发者的身份。需要 TOE 开发者的身份,以标识出谁负责产生该 TOE。

评估者*应报告*评估发起者的身份。需要评估发起者的身份,以标识出谁负责向评估者提供评估证据。

评估者*应报告*评估者的身份。需要评估者的身份,以标识出谁执行评估并且对评估裁定负责。

7.3.4.3.2 TOE 体系结构描述

评估者*应报告*TOE 的高级描述及其主要组件,该工作是基于 ISO/IEC 15408"高层设计"(ADV_HLD)保证族的评估证据描述。

本条的目的是表征各个主要组件间体系结构的分离程度。如果在 ST 中没有"高层设计"(ADV_HLD)要求,则本条要求不适用,并且被认为是满足的。

7.3.4.3.3 评估

评估者*应报告*所使用的评估方法、技术、工具和标准。

评估者可以注明在评估 TOE 时所使用的评估准则、方法和解释,注明在执行测试时所使用的设备。

评估者*应报告*所有对评估的限制、对评估结果分发的限制以及在评估期间所做的对评估结果有影响的假设。

评估者可在报告中加入与法律法规方面、组织机构、保密性等相关的信息。

7.3.4.3.4 评估结果

对于每个 TOE 评估活动,评估者*应报告*:

——恰当的活动名称;

——对组成该活动的每个保证组件所做的裁定和支持性基本原理,作为执行相应评估方法行为及其组成工作单元的结果。

基本原理应使用 ISO/IEC 15408、本标准、任何解释和已检查过的评估证据来证明评估裁定是正确的,并指出证据如何满足准则的每个方面或者为什么没有满足准则要求。基本原理包括对所做工作、所使用方法以及结果推导等的描述。基本原理可以详细到本标准工作单元这种程度。

评估者*应报告*工作单元明确需要的所有信息。

对于 AVA 和 ATE 活动,在 ETR 中报告标识信息的那些工作单元已经完成定义。

7.3.4.3.5 结论和建议

评估者*应报告*评估的结论,这些结论将涉及判定 TOE 是否已经满足其相关 ST,特别是如 ISO/IEC 15408-1 的 6.3 所规定的总体裁定,以及 6.5 所描述的裁定分配确定的总体裁定。

评估者提供一些对监督者可能有用的建议。这些建议可以包括在评估期间发现的IT产品的缺点,还可以提及一些特别有用的特征。

7.3.4.3.6 评估证据列表

评估者***应报告***每项评估证据的以下信息:

——发布团体(例如开发者、评估发起者);

——标题;

——唯一索引(例如发布日期、版本号)。

7.3.4.3.7 缩略语/术语表

评估者应报告ETR中所使用的所有缩略语或缩写词。

已由ISO/IEC 15408或本标准定义的术语在ETR中无须重复。

7.3.4.3.8 观察报告

评估者***应报告***一个能唯一标识在评估期间产生的OR及其状态的完整列表。

对于每个OR,该列表应当包含它的标识符、标题或其内容的摘要。

7.3.5 评估子活动

评估证据可以随着评估类型的不同而变化(PP评估只需PP,而TOE评估则需要特定的TOE证据)。评估输出结果可以是ETR或OR。在TOE评估中,评估子活动随着ISO/IEC 15408-3保证要求的不同而变化。

第8章～第13章内容是按照评估所要求的工作来组织的。第8章提出了得出PP评估结果必需的工作;第9章提出了ST评估必需的工作,尽管该工作没有独立的评估结果;第10章～第13章提出了得出EAL1到EAL4评估结果(结合ST)必需的工作。每章相对独立,可能有相互重复的内容。

图5描述了执行评估的工作概况。

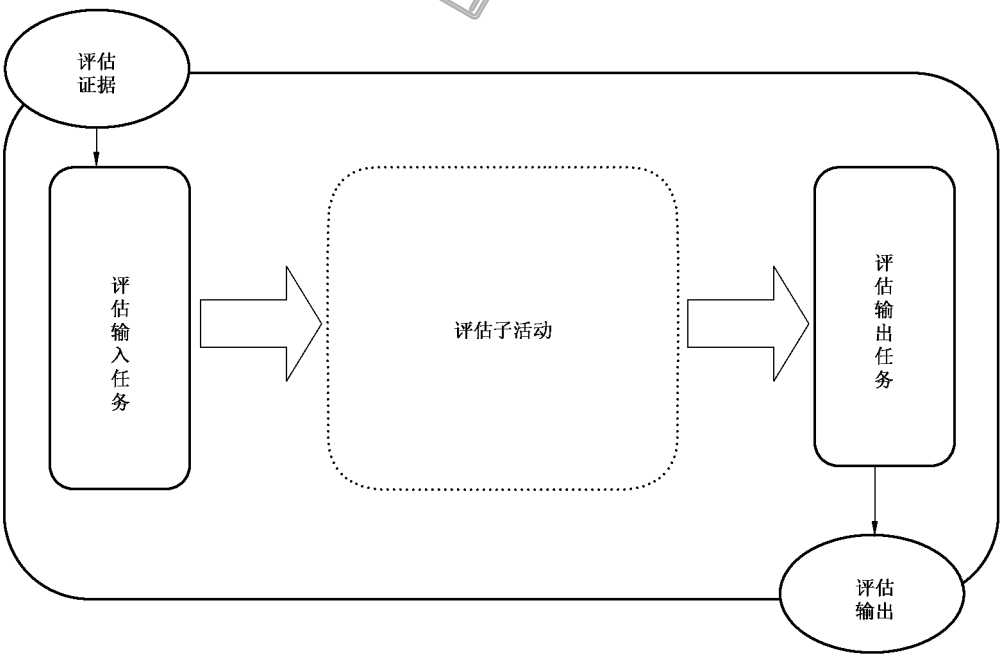

图5 一般评估模型

8 保护轮廓评估

8.1 简介

本章描述针对 PP 的评估。不管在 PP 中所声明的 EAL(或保证要求的其他集合)是什么,PP 评估的要求和方法对每个 PP 评估都是相同的。虽然本标准后继大量篇幅是以执行特定 EAL 评估为目标的,但本章适用于评估任何 PP。

本章所述的评估方法是建立在 ISO/IEC 15408-1 特别是附录 A,以及 ISO/IEC 15408-3 APE 类所规定的 PP 要求基础上的。

8.2 PP 评估相互关系

完备的 PP 评估包括以下活动:

a) 评估输入任务(第 7 章)。

b) PP 评估活动,包含以下子活动:

1) TOE 描述的评估(8.3.1);

2) 安全环境的评估(8.3.2);

3) PP 引言的评估(8.3.3);

4) 安全目的的评估(8.3.4);

5) IT 安全要求的评估 (8.3.5);

6) 明确陈述的 IT 安全要求的评估(8.3.6)。

c) 评估输出任务(第 7 章)。

第 7 章描述了评估输入任务和评估输出任务。PP 评估活动是由包含在 ISO/IEC 15408-3 中的 APE 保证要求导出的。

本章描述了 PP 评估包含的子活动。虽然子活动可能会或多或少同时进行,但是评估者应考虑子活动之间的依赖性。依赖性指南参见 A.4“依赖性”。

“明确陈述的 IT 安全要求”评估子活动仅适用于安全要求不是出自 ISO/IEC 15408-2 或 ISO/IEC 15408-3,但包含在 IT 安全要求陈述中的情况。

8.3 PP 评估活动

8.3.1 TOE 描述的评估 (APE_DES.1)

8.3.1.1 目的

本子活动的目的是确定 TOE 描述是否包含了有助于理解 TOE 用途及其功能的相关信息,以及确定该描述是否完备和一致。

8.3.1.2 输入

本子活动的评估证据是:

a) PP。

8.3.1.3 行为 APE_DES.1.1E

8.3.1.3.1 工作单元 APE_DES.1-1

ISO/IEC 15408-3 APE_DES.1.1C TOE 描述应描述 TOE 的产品类型和一般 IT 特征。

评估者***应检查***TOE 描述,以确定它描述了 TOE 的产品或系统类型。

评估者确定 TOE 描述能为读者提供足以全面理解产品或系统预期使用的信息,从而提供评估的背景。产品或系统类型的例子有:防火墙、智能卡、加密调制解调器、Web 服务器和内联网(intranet)。

某些情况下,产品或系统类型明确要求 TOE 具备一些功能,如果产品缺少这些功能,评估者应确定 TOE 描述是否对此进行了充分讨论。例如,防火墙类型的 TOE,在 TOE 描述中应对不能和网络相连的情况进行说明。

8.3.1.3.2 工作单元 APE_DES.1-2

评估者***应检查***TOE 描述,以确定它是否概括性地描述了 IT 特征。

评估者确定 TOE 描述详细讨论了 TOE 提供的 IT 特征,特别是安全特征,其详细程度足以使读者对这些特征有一个全面理解。

8.3.1.4 行为 APE_DES.1.2E

8.3.1.4.1 工作单元 APE_DES.1-3

评估者***应检查***PP,以确定 TOE 描述是连贯的。

如果 TOE 描述的文本和结构都能被其目标读者(例如,开发者、评估者和客户)理解,则 TOE 描述是连贯的。

8.3.1.4.2 工作单元 APE_DES.1-4

评估者***应检查***PP,以确定 TOE 描述是内在一致的。

提醒评估者注意的是,PP 的这一节仅用于定义 TOE 的一般目的。

一致性分析的指南参见 A.3“一致性分析”。

8.3.1.5 行为 APE_DES.1.3E

8.3.1.5.1 工作单元 APE_DES.1-5

评估者***应检查***PP,以确定 TOE 描述与 PP 的其他部分是一致的。

评估者尤其应确定 TOE 描述没有描述那些在 PP 其他部分都未涉及的 TOE 威胁、安全特征或配置。

一致性分析的指南参见 A.3“一致性分析”。

8.3.2 安全环境的评估(APE_ENV.1)

8.3.2.1 目的

本子活动的目的是确定在 PP 中 TOE 安全环境的陈述是否为 TOE 及其应用环境所关注的安全问题提供了一个清晰、一致的定义。

8.3.2.2 输入

本子活动的评估证据是:

a) PP。

8.3.2.3 行为 APE_ENV.1.1E

8.3.2.3.1 工作单元 APE_ENV.1-1

ISO/IEC 15408-3 APE_ENV.1.1C TOE 安全环境陈述应标识并解释关于 TOE 预期使用和 TOE 使用环境的所有假设。

评估者***应检查***TOE 安全环境的陈述，以确定它标识并解释了所有假设。

这些假设可以分成 TOE 预期使用方面的假设和 TOE 使用环境方面的假设。

评估者确定 TOE 预期使用的假设关注了下述这些方面：TOE 预期应用、TOE 所保护资产的潜在价值以及使用 TOE 时可能存在的限制。

评估者确定 PP 中对 TOE 预期使用的所有假设都进行了足够详细的解释，以使客户能够确定其预期使用与这些假设相匹配。如果没有清楚理解这些假设，最终结果可能会导致客户在非预期的环境中使用 TOE。

评估者确定 TOE 使用环境的假设包括环境的物理、人员、连接性等方面：

a) 物理方面包括为了使 TOE 以安全方式行使其功能，而对 TOE 的物理场所或附加的外围设施所做的所有假设。例如：
   ——假设管理员控制台严格限制在管理员个人区域内；
   ——假设 TOE 所有文件的存储只能在 TOE 运行的工作站上进行。
b) 人员方面包括为了使 TOE 以安全方式行使其功能，而对 TOE 安全环境内的用户和管理员或其他人员(包括潜在的威胁主体)所作的所有假设。例如：
   ——假设用户具有独特技能或专门技术；
   ——假设用户具有确定的最小权限；
   ——假设管理员每月更新病毒防护数据库。
c) 连接性方面包括为了使 TOE 以安全方式行使其功能，而对 TOE 与 TOE 之外的 IT 系统或产品(硬件、软件、固件或它们的组合)之间连接所作的所有假设。例如：
   ——假设至少有 100MB 的外部磁盘空间可用于存储 TOE 产生的日志文件；
   ——假设在特定工作站上，TOE 是被运行的唯一的非操作系统应用程序；
   ——假定 TOE 的软驱是禁用的；
   ——假定 TOE 不会连接到任何不可信的网络。

评估者确定 TOE 使用环境的所有假设都得到足够详细的解释，使客户能够确定他们的预期环境与假设环境是否相匹配。如果没有清楚地理解这些假设，最终可能导致 TOE 在环境中不能安全行使其功能。

8.3.2.3.2 工作单元 APE_ENV.1-2

ISO/IEC 15408-3 APE_ENV.1.2C TOE 安全环境陈述应标识并解释针对 TOE 或其环境保护的资产的所有已知或假定威胁。

评估者***应检查***TOE 安全环境的陈述，以确定其标识并解释了所有的威胁。

如果 TOE 及其环境的安全目的仅源自组织安全策略和假设，那么 PP 中就可以不含威胁陈述。此时，本工作单元不适用，并视为已经满足。

评估者确定所有已标识的威胁都已按照威胁主体、攻击行为和作为被攻击主体的资产三方面进行了清楚解释。

评估者还确定威胁主体都是用专业技术、资源和动机等方面来描述的，攻击行为都是用攻击方法、可利用的脆弱性和时机等方面来描述的。

8.3.2.3.3 工作单元 APE_ENV.1-3

ISO/IEC 15408-3 APE_ENV.1.3C TOE 安全环境陈述应标识并解释 TOE 应遵守的所有组织安全策略。

评估者***应检查***TOE 安全环境陈述，以确定它标识并解释了所有组织安全策略。

如果 TOE 及其环境的安全目的仅源自假设和威胁，那么 PP 中就可以不包含组织安全策略。此时，本工作单元不适用，并认为已得到满足。

评估者确定组织安全策略陈述都是根据 TOE 或其环境应遵守的规则、惯例或方针而作出的，这些规则、惯例或方针是由控制 TOE 使用环境的组织制定的。例如，“要求密码生成和加密应符合国家标准”就是一条组织安全策略。

评估者确定 PP 中对所有组织安全策略都进行了解释或详细说明，以便于读者清晰地理解；应清晰地表述安全策略，以便将安全目的追溯到组织安全策略。

8.3.2.4 行为 APE_ENV.1.2E

8.3.2.4.1 工作单元 APE_ENV.1-4

评估者***应检查***TOE 安全环境的陈述，以确定它是连贯的。

如果 TOE 安全环境陈述的文本和结构都能被其目标读者（例如评估者和客户）理解，则 TOE 安全环境描述就是连贯的。

8.3.2.4.2 工作单元 APE_ENV.1-5

评估者***应检查***TOE 安全环境的陈述，以确定它是内在一致的。

TOE 安全环境内在不一致的示例有：

——TOE 安全环境的陈述包含某种威胁，其攻击方法不在威胁主体的能力范围内；

——TOE 安全环境的陈述包含“TOE 不应与因特网相连”这样的组织安全策略，但有一个威胁其威胁主体是来自因特网的入侵者。

一致性分析指南见 A.3“一致性分析”。

8.3.3 PP 引言的评估（APE_INT.1）

8.3.3.1 目的

本子活动的目的是确定 PP 引言是否完备、与 PP 的其他部分是否保持一致，以及是否正确标识了 PP。

8.3.3.2 输入

本子活动的评估证据是：

a) PP。

8.3.3.3 行为 APE_INT.1.1E

8.3.3.3.1 工作单元 APE_INT.1-1

ISO/IEC 15408-3 APE_INT.1.1C PP 引言应包含一个 PP 标识，提供识别、编目、注册和交叉引用这个 PP 所必需的标记性和描述性信息。

评估者***应核查***PP 引言是否提供了必要的 PP 标识信息以识别、编目、注册和交叉引用 PP。

评估者确定的 PP 标识信息包括：

a) 管理并唯一标识 PP 的必要信息(例如 PP 标题、版本号、出版日期、作者和申评机构)；

b) 用于开发 PP 的 ISO/IEC 15408 版本信息；

c) 注册信息，如果 PP 在评估前已注册；

d) 交叉引用，如果 PP 与其他 PP 相比照；

e) 评估体制要求的其他信息。

8.3.3.3.2 工作单元 APE_INT.1-2

ISO/IEC 15408-3 APE_INT.1.2C PP 引言应包含一个 PP 概述，以叙述的形式概括该 PP。

评估者***应核查***PP 引言，是否以叙述形式提供了 PP 概述。

PP 概述将为 PP 内容提供概要描述(更详细会在 TOE 描述中提供)，且详细到足以使 PP 的潜在用户能确认 PP 是否为他所需。

8.3.3.4 行为 APE_INT.1.2E

8.3.3.4.1 工作单元 APE _INT.1-3

评估者***应检查***PP 引言，以确定它是连贯的。

如果 PP 引言的文本和结构都能被其目标读者理解(例如，开发者、评估者和客户)，则 PP 引言就是连贯的。

8.3.3.4.2 工作单元 APE _INT.1-4

评估者***应检查***PP 引言，以确定它是内在一致的。

PP 概述为 PP 内容提供了概要描述，因此有关内在一致性分析自然就集中在 PP 概述上。

一致性分析指南见 A.3“一致性分析”。

8.3.3.5 行为 APE_INT.1.3E

8.3.3.5.1 工作单元 APE _INT.1-5

评估者***应检查***PP 引言，以确定 PP 引言与 PP 的其他部分是一致的。

评估者确定 PP 概述提供了 TOE 的一个准确概括。特别的，评估者应确定 PP 概述与 TOE 描述是一致的，且没有声明或隐含评估范围之外的安全特征。

评估者还确定 ISO/IEC 15408 一致性声明是否与 PP 的其他部分一致。

一致性分析指南见 A.3“一致性分析”。

8.3.4 安全目的的评估（APE_OBJ.1）

8.3.4.1 目的

本子活动的目的是，确定安全目的描述是否完备和一致，并确定安全目的是否能对抗已标识的威胁，达到已标识的组织安全策略并遵循规定的假设。

8.3.4.2 输入

本子活动的评估证据是：

a) PP。

8.3.4.3 行为 APE_OBJ.1.1E

8.3.4.3.1 工作单元 APE_OBJ.1-1

ISO/IEC 15408-3 APE_OBJ.1.1C 安全目的的陈述应为 TOE 及其环境定义安全目的。

评估者***应核查***安全目的的陈述，是否定义了 TOE 及其环境的安全目的。

评估者应确定每个安全目的是否明确地说明了适用于 TOE，还是环境，或者两者都适用。

8.3.4.3.2 工作单元 APE_OBJ.1-2

ISO/IEC 15408-3 APE_OBJ.1.2C TOE 的安全目的应可以追溯至由 TOE 对抗的多方面的确定威胁，和/或可以追溯至 TOE 所满足的组织安全策略。

评估者***应检查***安全目的的基本原理，以确定 TOE 的所有安全目的都能追溯到需要对抗的已标识的威胁，和/或 TOE 应遵循的组织安全策略。

评估者应确定 TOE 的每个安全目的都能追溯到至少一个威胁或组织安全策略。

不能追溯就意味着，或者安全目的的基本原理不完备，或者威胁及组织安全策略的陈述不完备，或者 TOE 的安全目的没有实际意义。

因此，一个威胁可以完全由一个或多个环境安全目的来处理。一种极端情况是没有 TOE 安全目的。尽管可以这样构建 PP/ST，但一个所有威胁和组织安全策略都由环境负责处理的 TOE 在实用上是有问题的，因为这样的 TOE 没有 TOE 安全功能要求。这种 TOE 的认证/认可是体制问题。

8.3.4.3.3 工作单元 APE_OBJ.1-3

ISO/IEC 15408-3 APE_OBJ.1.3C 环境的安全目的应可以追溯至不是完全由 TOE 对抗的多方面的确定威胁，和/或可以追溯至 TOE 未完全满足的组织安全策略或假设。

评估者***应检查***安全目的的基本原理，以确定环境安全目的能追溯到 TOE 环境所对抗的已标识的威胁，和/或追溯到 TOE 环境应遵循的组织安全策略，和/或 TOE 环境应满足的假设。

评估者应确定环境的每个安全目的都能追溯到至少一个假设、威胁或组织安全策略。

不能追溯就意味着，或者安全目的的基本原理不完备，或者威胁、假设及组织安全策略的陈述不完备，或者环境的安全目的没有实际意义。

8.3.4.3.4 工作单元 APE_OBJ.1-4

ISO/IEC 15408-3 APE_OBJ.1.4C 安全目的基本原理应证实所陈述的安全目的恰好对抗确定的安全威胁。

评估者***应检查***安全目的基本原理，以确定对于每个威胁，基本原理都包含了安全目的恰好对抗该威胁的适当论证。

如果威胁没有对应的安全目的，则本工作单元为“不通过”。

评估者应确定有关威胁的论证能够阐明：如果达到了所有能追溯到某威胁的安全目的，那么就消除了这个威胁，或者威胁被降低到可以接受的水平，或威胁的影响得到充分地缓解。

评估者还应确定当达到可以追溯到某威胁的所有安全目的时，实际上促成了该威胁的消除、降低或缓解。

消除威胁的例子：

——消除主体使用攻击方法的能力；

——通过威慑，消除威胁主体的动机；

——消除威胁主体（例如，移走经常导致网络崩溃的机器）。

降低威胁的例子：

——限制威胁主体使用攻击方法；

——限制威胁主体的攻击机会；

——减少成功发起攻击的可能性；

——要求威胁主体具有更高的专业知识或更多的资源。

缓解威胁影响的例子：

——经常备份资产；

——拥有 TOE 备份；

——经常改变通信会话使用的密钥，这样即使一个密钥被攻破，其影响也相对较小。

应当注意的是，安全目的基本原理中提供的从安全目的到威胁的回溯，可以是论证的一部分，但是其本身不是完整的论证过程。即使在安全目的仅仅反映试图防止特定威胁被实现的情形下，仍需进行论证，但在这种情况下可以是最低要求的论证。

8.3.4.3.5 工作单元 APE_OBJ.1-5

ISO/IEC 15408-3 APE_OBJ.1.5C 安全目的基本原理应证实所陈述的安全目的恰好覆盖所有确定的组织安全策略和假设。

评估者***应检查***安全目的基本原理，以确定对于每个组织安全策略而言，基本原理都包含安全目的恰好覆盖该组织安全策略的适当论证。

如果组织安全策略没有对应的安全目的，则本工作单元为“不通过”。

评估者应确定有关组织安全策略的论证能够阐明：如果达到了所有能追溯到该组织安全策略的安全目的，那么就实现了该组织安全策略。

评估者还应确定当达到可以追溯到组织安全策略的所有安全目的时，实际上促成了组织安全策略的执行。

应当注意的是，安全目的基本原理中提供的从安全目的到组织安全策略的回溯，可以是论证的一部分，但是其本身不是完整的论证过程。即使在安全目的仅仅反映试图实现特定组织安全策略的情形下，仍需进行论证，但是在这种情况下可以是最低要求的论证。

8.3.4.3.6 工作单元 APE_OBJ.1-6

评估者***应检查***安全目的基本原理，以确定对于每个假设而言，基本原理都包含环境安全目的恰好覆盖该假设的适当论证。

如果假设没有对应的环境安全目的，则本工作单元为“不通过”。

假设可以是有关 TOE 预期使用的假设，也可以是有关 TOE 预期使用环境的假设。

评估者应确定有关 TOE 预期使用假设的论证能够阐明：如果实现了追溯到假设的所有环境安全目的，那么就支持预期的使用。

评估者还应确定当达到可追溯到 TOE 预期使用假设的所有环境安全目的时，实际上促成了预期使用的支持。

评估者应确定有关 TOE 使用环境假设的论证能够阐明：如果实现了追溯到假设的所有环境安全目的，那么环境就与假设是一致的。

评估者还确定当达到可追溯到 TOE 使用环境假设的所有环境安全目的时，实际上促成了环境与假设一致。

应当注意的是，安全目的基本原理中提供的从环境安全目的到假设的回溯，可以是论证的一部分，但是其本身不是完整的论证过程。即使在环境安全目的仅仅是对假设重述的情形下，仍需进行论证，但是在这种情况下可以是最低要求的论证。

8.3.4.4 行为 APE_OBJ.1.2E

8.3.4.4.1 工作单元 APE_OBJ.1-7

评估者*应检查*安全目的的陈述，以确定它是有条理的。

如果安全目的的文本和结构能被其目标读者（如评估者和客户）所理解，那么安全目的的表述就是有条理的。

8.3.4.4.2 工作单元 APE_OBJ.1-8

评估者*应检查*安全目的的陈述，以确定它是完备的。

如果安全目的足以对抗所有已标识的威胁，并能覆盖所有已标识的组织安全策略和假设，那么安全目的是完备的。本工作单元可以同工作单元 APE_OBJ.1-4、APE_OBJ.1-5 和 APE_OBJ.1-6 一道执行。

8.3.4.4.3 工作单元 APE_OBJ.1-9

评估者*应检查*安全目的陈述，以确定它是内在一致的。

如果安全目的之间不相互冲突，安全目的的陈述就是内在一致的。安全目的相互冲突的例子有：两个安全目的，一个是“用户身份从来都不应被公开”，另一个则是“用户身份可被其他用户利用”。

一致性分析指南见 A.3“一致性分析”。

8.3.5 IT 安全要求的评估（APE_REQ.1）

8.3.5.1 目的

本子活动的目的是确定 TOE 安全要求（包括 TOE 安全功能要求和 TOE 安全保证要求）和 IT 环境安全要求是否完备和一致，并为 TOE 的开发提供充分的基础，以达到其安全目的。

8.3.5.2 输入

本子活动的评估证据是：

a） PP。

8.3.5.3 行为 APE_REQ.1.1E

8.3.5.3.1 工作单元 APE_REQ.1-1

ISO/IEC 15408-3 APE_REQ.1.1C TOE 安全功能要求的陈述应标识从 ISO/IEC 15408-2 功能要求组件中选取的 TOE 安全功能要求。

评估者*应核查*TOE 安全功能要求的陈述是否标识了从 ISO/IEC 15408-2 功能要求组件中选取的那些 TOE 安全功能要求。

评估者应确定从 ISO/IEC 15408-2 中选取的所有安全功能要求组件都已标识，这种标识或者通过引用 ISO/IEC 15408-2 的单个组件，或者通过在 PP 中复制来实现。

8.3.5.3.2 工作单元 APE_REQ.1-2

评估者*应核查*对每个 TOE 安全功能要求组件的引用的正确性。

评估者应确定 ISO/IEC 15408-2 是否包含所引用的每一个 ISO/IEC 15408-2 TOE 安全功能要求组件。

8.3.5.3.3 工作单元 APE_REQ.1-3

评估者***应核查***从 ISO/IEC 15408-2 中选取出的在 PP 中重现的 TOE 安全功能要求组件都得以正确重现。

评估者应确定在没有对允许操作进行检查的情况下，TOE 安全功能要求陈述正确地重现了这些要求。对组件操作正确性的检查在工作单元 APE_REQ.1-11 中进行。

8.3.5.3.4 工作单元 APE_REQ.1-4

ISO/IEC 15408-3 APE_REQ.1.2C TOE 安全保证要求的陈述应标识从 ISO/IEC 15408-3 保证要求组件中选取的 TOE 安全保证要求。

评估者***应核查***TOE 安全保证要求陈述是否标识了从 ISO/IEC 15408-3 保证要求组件中选取的 TOE 安全保证要求。

评估者应确定从 ISO/IEC 15408-3 选取的所有 TOE 安全保证要求组件都已标识，这种标识或者通过引用 EAL，或者通过引用 ISO/IEC 15408-3 的单个组件，或者通过在 PP 中复制来实现。

8.3.5.3.5 工作单元 APE_REQ.1-5

评估者***应核查***对每个 TOE 安全保证要求组件的引用的正确性。

评估者应确定 ISO/IEC 15408-3 是否包含所引用的每一个 ISO/IEC 15408-3 TOE 安全保证要求组件。

8.3.5.3.6 工作单元 APE_REQ.1-6

评估者***应核查***从 ISO/IEC 15408-3 中选取出的在 PP 中重现的 TOE 安全保证要求组件都得以正确重现。

评估者应确定在没有对允许操作进行检查的情况下，TOE 安全保证要求陈述正确地重现了这些要求。对组件操作正确性的检查在工作单元 APE_REQ.1-11 中进行。

8.3.5.3.7 工作单元 APE_REQ.1-7

ISO/IEC 15408-3 APE_REQ.1.3C TOE 安全保证要求的陈述应包括一个在 ISO/IEC 15408-3 中定义的评估保证级(EAL)。

评估者***应核查***TOE 安全保证要求陈述，以确定它包含了 ISO/IEC 15408-3 所定义的 EAL，或恰当地证明了它不包含 EAL。

如果不包含 EAL，评估者应确定相关的证明说明了 TOE 保证要求陈述不包含 EAL 的理由。该证明可以说明为什么不可能、不需要或不适合包含一个 EAL，或说明为什么不可能、不需要或不适合包含构成 EAL1(ACM_CAP、ADO_IGS、ADV_FSP、ADV_RCR、AGD_ADM、AGD_USR 和 ATE_IND)族的特定组件。

8.3.5.3.8 工作单元 APE_REQ.1-8

ISO/IEC 15408-3 APE_REQ.1.4C 证据应证明 TOE 安全保证要求的陈述是恰当的。

评估者***应检查***安全要求基本原理，以确定基本原理充分证明了 TOE 安全保证要求的陈述是恰当的。

如果保证要求包含一个 EAL，则证明将 EAL 作为一个整体来选择，而不是选择 EAL 的所有单个组件。如果保证要求包含 EAL 增强组件，则评估者应该确定每个增加的组件都是单独被证明过的。如果保证要求包含明确陈述的保证要求，评估者应该确定每个明确陈述的保证要求都是单独被证明

过的。

评估者应确定安全要求基本原理足以证明:保证要求相对于给定的安全环境和安全目的陈述是足够的。例如,如果需要防范拥有专业知识的攻击者,就不适合规定 AVA_VLA.1“开发者脆弱性分析”,因为该组件不要求探测明显的脆弱性之外的漏洞。

论证可能包含如下理由:

a) 评估体制、政府或其他组织实施的特定要求;

b) 与 TOE 安全功能要求相关的保证要求;

c) 与 TOE 一起使用的系统或产品的保证要求;

d) 客户的要求。

ISO/IEC 15408-3 的 10.2 提供了每个 EAL 的目的和目标概述。

应该提醒评估者的是:确定保证要求是否适当可能是主观性的,因此在对证明的充分性进行分析时不应过于苛刻。

如果保证要求不包含一个 EAL,本工作单元可以与工作单元 APE_REQ.1-7 一起执行。

8.3.5.3.9 工作单元 APE_REQ.1-9

ISO/IEC 15408-3 APE_REQ.1.5C 如果适当的话,PP 应标识 IT 环境的所有安全要求。

适当时,评估者***应核查***IT 环境的安全要求是否被标识。

如果 PP 中不包含 IT 环境的安全要求,则本工作单元不适用,并视为已经满足。

评估者应确定 TOE 与其环境中的其他 IT 之间的任何依赖关系,在 PP 中都清晰标识为 IT 环境安全要求,这些依赖关系为 TOE 实现其安全目的提供了安全功能。

IT 环境安全要求的例子有:一个防火墙,它依赖于底层操作系统提供管理员的身份鉴别和审计数据的永久储存。这样,IT 环境安全要求应包含 FAU“安全审计”类和 FIA“标识和鉴别”类的功能组件。

应该注意的是,IT 环境安全要求既包含功能要求,也包含保证要求。

IT 环境依赖性的例子如:一个软件密码模块周期性地检查它自己的代码,在代码被篡改时自我禁用。为了恢复,要求使用 FPT_RCV.2“自动恢复”。因为这个加密模块自我禁用后不能自己恢复,这就需要对 IT 环境提出要求。FPT_RCV.2“自动恢复”的一个依赖关系是 AGD_ADM.1“管理员指南”,所以这个保证要求也就变成 IT 环境的保证要求。

应该提醒评估者的是:凡涉及 TSF 的 IT 环境安全要求,皆认为属于环境的安全功能,而不是 TOE 的安全功能。

8.3.5.3.10 工作单元 APE_REQ.1-10

ISO/IEC 15408-3 APE_REQ.1.6C 应标识 PP 中 IT 安全要求的所有已完成操作。

评估者***应核查***IT 安全要求的所有操作都被标识。

允许 PP 包含未完成操作的元素。即 PP 可以包含这样的安全要求陈述,该陈述包括一些未完成的赋值或选择操作。这些操作会在实例化 PP 的 ST 中完成。这就使 ST 作者在开发 TOE 和相应的声称遵从特定 PP 的 ST 时,有更多的灵活性。

ISO/IEC 15408-2 和 ISO/IEC 15408-3 中组件允许的操作有赋值、反复、选择和细化。赋值和选择操作只允许用于组件中特别指定的地方。反复和细化允许用于所有组件。

评估者应确定所有操作都在使用该操作的组件中被标识。完成的操作和未完成的操作需要通过能区分操作并清楚操作是否完成的方式来标识。标识可以通过排版不同,或者通过周围的文字明确标记,或者通过其他与众不同的方式来实现。

8.3.5.3.11 工作单元 APE_REQ.1-11

评估者***应检查***IT 安全要求的陈述,以确定是否正确实施了操作。

应该提醒评估者的是:对安全要求的操作不必在 PP 中进行和完成。

评估者应比较每条陈述和导出陈述的元素,以确定:

a) 对于赋值操作,所选的参数或变量的值符合赋值要求的指定类型。

b) 对于选择操作,选择项是在元素选择部分中指定的一项或多项。评估者也应确定符合要求的所选项的数目。某些要求只需要选取一个选项(例如 FAU_GEN.1.1.b),有些情况允许有多个选项(如 FDP_ITT.1.1 第二个操作)。

c) 对于细化操作,组件以这样的方式细化:如果 TOE 满足细化要求,也应该满足非细化要求。如果细化后的要求超过该限制,则认为是一个扩展要求。

例如,ADV_SPM.1.2.C TSP 模型应描述所有能被模型化的 TSP 策略的规则和特征。细化:TSP 模型只需要覆盖访问控制。如果访问控制策略是唯一的 TSP 策略,那么这就是有效的细化。如果 TSP 中还有标识和鉴别策略,而且细化声明只有访问控制需要被模型化,那么这就不是一个有效的细化。

细化的一种特殊情形是编辑上的细化,即在要求上做一个小的变化,也就是因遵守正确语法对句子进行改写。这种变化不允许以任何方式改变要求的含义。

编辑细化的一个例子是带有单一行为的 FAU_ARP.1,PP 作者可以将文字"当检测到潜在的安全侵害时,TSF 应向操作员发出通知",改写成"当检测到潜在的安全侵害时,TSF 应通知操作员"。

应提醒评估者的是编辑上的细化应清楚地标识(见工作单元 APE_REQ.1-10)。

d) 对于反复操作,一个组件的每个反复操作都不同于该组件的另一次反复(至少组件的某个元素不同于另一个组件的对应元素),或这个组件将应用于 TOE 的不同部分。

8.3.5.3.12 工作单元 APE_REQ.1-12

ISO/IEC 15408-3 APE_REQ.1.7C 应标识 PP 中 IT 安全要求的任何未完成操作。

评估者***应检查***IT 安全要求的陈述,以确定是否标识了所有未完成操作。

评估者应确定所有操作都在使用该操作的组件中被标识。完成的操作和未完成的操作需要通过能区分操作并清楚操作是否完成的方式来标识。标识可以通过排版不同,或者通过周围的文字明确标记,或者通过其他与众不同的方式来实现。

8.3.5.3.13 工作单元 APE_REQ.1-13

ISO/IEC 15408-3 APE_REQ.1.8C 应满足 PP 中 IT 安全要求之间的依赖关系。

评估者***应检查***IT 安全要求的陈述,以确定 IT 安全要求陈述中使用的组件所要求的依赖关系都得到了满足。

依赖关系可以通过将相关组件(或从属于相关组件的组件)包含到 TOE 安全要求陈述中来满足,或作为一个要求,声称由 TOE 的 IT 环境来满足。

尽管 ISO/IEC 15408 通过依赖关系包含列表为依赖关系分析提供支持,但不能证明没有其他的依赖关系存在。其他依赖关系的例子有:涉及"所有客体"或"所有主体"的元素与列出这些客体或主体的另一个元素或元素集的细化之间就存在依赖关系。

IT 环境中必要的安全要求依赖关系应在 PP 中陈述并得到满足。

应该提醒评估者的是:ISO/IEC 15408 并不要求所有依赖关系都得到满足,见下一个工作单元。

8.3.5.3.14 工作单元 APE_REQ.1-14

ISO/IEC 15408-3 APE_REQ.1.9C 证据应证明为何一个未满足的依赖关系却是适当的。

评估者***应检查***安全要求基本原理,以确定对每一种没有满足安全要求依赖关系的情况都作了适当的证明。

给定已标识的安全目的,评估者应确定该证明解释了不必包括依赖关系的原因。

评估者应确认未满足的依赖关系并没有妨碍安全功能要求充分体现安全目的。该分析见 APE_REQ.1.13C。

适当证明的例子如，当一个软件 TOE 有一个安全目的“鉴别失败时，应将用户的身份、时间和日期记录下来”且采用 FAU_GEN.1“审计数据产生”作为功能要求来满足这个安全目的。FAU_GEN.1 包含了与 FPT_STM.1“可靠时间戳”的依赖关系。由于 TOE 不包含时钟机制，FPT_STM.1 则被 PP 作者定义为 IT 环境要求。PP 作者用这样一个理由说明这个要求没有得到满足：“在特定环境下，可能会存在时间戳机制攻击行为，因此环境就不能传送可靠的时间戳。然而，一些威胁主体没有执行攻击时间戳机制的能力，而且由这样的威胁主体实施的攻击可以通过记录攻击的时间和日期来分析”。

8.3.5.3.15 工作单元 APE_REQ.1-15

ISO/IEC 15408-3 APE_REQ.1.10C PP 应包含一个关于 TOE 安全功能要求的最低功能强度级别的陈述，可适当选取基本级功能强度、中级功能强度或高级功能强度中的一个。

评估者***应核查***PP 是否包括一个 TOE 安全功能要求的最低功能强度级别陈述，这个级别可以是基本级功能强度（基本级 SOF）、中级功能强度（中级 SOF）或高级功能强度（高级 SOF）中的任一个。

如果 TOE 安全保证要求不包括 AVA_SOF.1“TOE 安全功能强度评估”，则本工作单元不适用，并视为已经满足。

密码算法的强度超出了 ISO/IEC 15408 的范围。功能强度只适用于非加密的概率或置换机制。因此，当 PP 包含一个最低 SOF 的声明时，该声明不适用于任何与 ISO/IEC 15408 评估有关的密码机制。当 TOE 包含密码机制时，评估者应该确定 PP 是否包含一个清晰的陈述，说明对算法强度的评估不属于该评估的范围。

TOE 可能包括多个不同的域，PP 作者认为每个域有一个最低的功能强度级别，比 TOE 作为一个整体有一个最低的功能强度级别更加实用。在这种情况下，允许将 TOE 安全功能要求划分成不同的组，每个组有不同的最低功能强度级别。

例如分布式终端系统，该系统的用户终端在公共区，管理员终端在物理安全区。用户终端的鉴别要求的安全功能强度是中级 SOF，管理员终端的鉴别要求的安全功能强度是基本级 SOF。并没有说 TOE 的最低功能强度是基本级 SOF，否则，可能会使 TOE 潜在的客户相信利用用户终端攻击鉴别机制是一件相对容易的事情，因此 PP 作者把 TOE 划分为用户域和管理域，将 TOE 安全功能要求划分成两组分属这两个域，分配给属于管理域的一组要求的最低功能强度为基本级 SOF，分配给属于用户域的一组要求的最低功能强度为中级 SOF。

8.3.5.3.16 工作单元 APE_REQ.1-16

ISO/IEC 15408-3 APE_REQ.1.11C 安全要求的陈述应标识所有需要一个明确的功能强度声明的安全功能要求，连同每一个这种安全功能要求的明确的功能强度声明。

评估者***应核查***PP 是否标识了所有特定的 TOE 安全功能要求，对这些要求给出明确的功能强度声明是适当的，相应的特定功能强度或度量也是合适的。

如果 TOE 安全保证要求不包括 AVA_SOF.1“TOE 安全功能强度评估”，则本工作单元不适用，并视为已经满足。

明确的功能强度声明既可是基本级功能强度、中级功能强度或高级功能强度，也可是一个既定的特定尺度。如使用的是特定尺度，评估者应确定对特定的功能要求类型，该强度声明是合适的，并且指定的尺度是可评估的。本工作单元涉及 PP 作者需要调整特定 SOF 要求（即比 PP 的总体 SOF 声明更高）或使用一个度量的情形。TOE 安全功能要求的明确 SOF 声明可以由 PP 作者规定。如果没有任何明确的声明，PP 的总体声明适用于 PP 所规定的所有 TOE 安全功能要求。评估者应确认明确的 SOF 声明是与 PP 的其他部分是一致的。

一个 PP 可能拥有多个 SOF 声明规范。对 PP 可能有一个总体 SOF 声明，PP 中的 TOE 安全功能要求可能有一个 SOF 声明。

评估体制可能会提供有关功能强度度量的适合性和适宜性的进一步指导。

8.3.5.3.17 工作单元 APE_REQ.1-17

ISO/IEC 15408-3 APE_REQ.1.12C 安全要求基本原理应证实 PP 的最低功能强度级别连同任何明确的功能强度声明，与 TOE 的安全目的是一致的。

评估者***应检查***安全要求基本原理，以确定它证实了最低功能强度级别及任何明确的功能强度声明与 TOE 安全目的是一致的。

如果 TOE 安全保证要求不包括 AVA_SOF.1“TOE 安全功能强度评估”，则本工作单元不适用，并视为已经满足。

评估者应确定基本原理考虑了诸如在 TOE 安全环境陈述中描述的攻击者可能具有的专门知识、资源和动机等细节。例如，如果要求 TOE 提供防范以对抗具有高攻击潜力的攻击者，则基本级 SOF 声明就是不适当的。

评估者还应确定基本原理考虑了安全目的中所有特定的强度相关特性。评估者可采用将要求追溯到目的的方式，来确定如果合适的话，能够追溯到安全目的的带有特定的强度相关特性的那些要求是否具有适当的功能强度声明。

8.3.5.3.18 工作单元 APE_REQ.1-18

ISO/IEC 15408-3 APE_REQ.1.13C 安全要求基本原理应证实 IT 安全要求正好满足安全目的。

评估者***应检查***安全要求基本原理，以确定 TOE 安全要求能够追溯到 TOE 的安全目的。

评估者确定每个 TOE 安全功能要求至少能追溯到 TOE 的一个安全目的。

如果不能追溯，则表明安全要求基本原理是不完备的，或安全目的是不完备的，或 TOE 安全功能要求没有实际意义。

TOE 的某些或所有安全保证要求不一定追溯到 TOE 的安全目的。

TOE 的安全保证要求映射到 TOE 安全目的的例子如，PP 中包含“用户通过用一台误认为是 TOE 的设备，而无意泄露信息”这样一个威胁，且 TOE 的安全目的“TOE 应该清楚标出版本号”能对抗此种威胁。TOE 的安全目的可以通过满足 ACM_CAP.1“版本号”来实现，因此 PP 作者就将 ACM_CAP.1 追溯到该 TOE 安全目的。

8.3.5.3.19 工作单元 APE_REQ.1-19

评估者***应检查***安全要求基本原理，以确定 IT 环境安全要求能够追溯到环境安全目的。

评估者确定每个 IT 环境安全功能要求至少能追溯到一个环境安全目的。

如果不能追溯，则表明安全要求基本原理是不完备的，或环境安全目的是不完备的，或 IT 环境安全功能要求没有实际意义。

IT 环境的某些或所有安全保证要求不一定追溯到环境安全目的。

8.3.5.3.20 工作单元 APE_REQ.1-20

评估者***应检查***安全要求基本原理，以确定对于每个 TOE 安全目的，该原理都包含一个证明 TOE 安全要求适于满足该安全目的的适当理由。

如果 TOE 安全要求都不能追溯到 TOE 的安全目的，则本工作单元为“不通过”。

评估者应确定有关 TOE 安全目的的论证阐明了：如果追溯到安全目的的所有 TOE 安全要求都得到满足，那么就实现了对应的 TOE 安全目的。

评估者还应确定每个可追溯到 TOE 安全目的的 TOE 安全要求得到满足时，实际上促成了该 TOE 安全目的的达到。

应当注意的是，在安全要求基本原理中将 TOE 安全要求追溯到 TOE 安全目的，可以作为论证的一部分，但其本身不是完整的论证过程。

8.3.5.3.21 工作单元 APE_REQ.1-21

评估者***应检查***安全要求基本原理，以确定对于每个 IT 环境安全目的，该原理都包含一个证明 IT 环境安全要求恰好满足 IT 环境安全目的的适当论证。

如果 IT 环境安全要求都不能追溯到 IT 环境的安全目的，则本工作单元为“不通过”。

评估者应确定有关 IT 环境安全目的的论证阐明了：如果追溯到安全目的的所有 IT 环境安全要求都得到满足，那么就实现了对应的 IT 环境安全目的。

评估者还应确定每个可追溯到 IT 环境安全目的的 IT 环境安全要求得到满足时，实际上促成了该 IT 环境安全目的的达到。

应当注意的是，在安全要求基本原理中将 IT 环境安全要求追溯到 IT 环境安全目的，可以作为论证的一部分，但其本身不是完整的论证过程。

8.3.5.3.22 工作单元 APE_REQ.1-22

ISO/IEC 15408-3 APE_REQ.1.14C 安全要求基本原理应证实这组 IT 安全要求组成了一个相互支持并内在一致的整体。

评估者***应检查***安全要求基本原理，以确定它证实了该组 IT 安全要求是内在一致的。

评估者应确定所有将不同 IT 安全要求应用到同一类型的事件、操作、数据和实施的测试等的情形，这些要求可能会互相冲突，此时应该提供适当的证明来说明事实并非如此。

例如，如果 PP 包含关于单个用户责任可追查性和用户匿名两方面的要求，则需要阐明这些要求不会冲突。这可通过说明单个用户责任可追查性的可审计事件与需要用户匿名的操作无关来证明。

一致性分析指南见 A.3“一致性分析”。

8.3.5.3.23 工作单元 APE_REQ.1-23

评估者***应检查***安全要求基本原理，以确定它证实了该组 IT 安全要求形成一个互相支持的整体。

本工作单元建立在工作单元 APE_REQ.1-18、APE_REQ.1-19、APE_REQ.1-20 和 APE_REQ.1-21 所作决定的基础上，其中 APE_REQ.1-18 和 APE_REQ.1-19 检查 IT 安全要求能否追溯到安全目的，APE_REQ.1-20 和 APE_REQ.1-21 检查 IT 安全要求是否恰好满足安全目的。本工作单元要求评估者考虑这种可能性：因缺乏其他 IT 安全要求的支持，安全目的实际上不能实现。

由于存在这样的情况：功能要求 A 依赖于功能要求 B，而 B 通过定义支持 A，所以本工作单元也建立在前述工作单元依赖关系分析的基础上。

评估者确定安全要求基本原理能够证实功能要求在必要的时候互相支持，即使没有迹象表明这些要求之间存在依赖关系。该证实应提出如下安全功能要求：

a) 防止其他安全功能要求的旁路，如 FDP_ RVM.1“TSP 的不可旁路性”；

b) 防止其他安全功能要求的篡改，如 FPT_SEP“域分离”；

c) 防止其他安全功能要求的失效，如 FPT_MOF.1“安全功能行为的管理”；

d) 激活对试图挫败其他安全功能要求的攻击行为的探测，如 FAU“安全审计”类的组件。

在分析时，评估者应考虑已执行的操作是否影响要求间的相互支持。

8.3.5.4 行为 APE_REQ.1.2E

8.3.5.4.1 工作单元 APE_REQ.1-24

评估者***应检查***IT 安全要求陈述，以确定其是有条理的。

如果 IT 安全要求描述的文本和结构能被其目标读者(即评估者和客户)理解，则，IT 安全要求陈述就是有条理的。

8.3.5.4.2 工作单元 APE_REQ.1-25

评估者***应检查***IT 安全要求陈述，以确定它们是完备的。

本工作单元利用来自 APE_REQ.1.1E 和 APE_SRE.1.1E 所要求工作单元的结果，特别是评估者对安全要求基本原理的检查结果。

如果评估者判定安全要求足以确保所有的 TOE 安全目的都得到满足，则安全要求陈述就是完备的。

8.3.5.4.3 工作单元 APE_REQ.1-26

评估者***应检查***IT 安全要求陈述，以确定它们是内在一致的。

本工作单元利用来自 APE_REQ.1.1E 和 APE_SRE.1.1E 所要求工作单元的结果，特别是评估者对安全要求基本原理的检查结果。

如果评估者确定安全要求都互不冲突(因为冲突的话安全目的就不能完全满足)，那么安全要求陈述就是内在一致的。

一致性分析指南见 A.3“一致性分析”。

8.3.6 明确陈述的 IT 安全要求的评估 (APE_SRE.1)

8.3.6.1 目的

本子活动的目的是确定未引用 ISO/IEC 15408 进行表述的安全功能要求或安全保证要求是否适当和充分。

8.3.6.2 输入

本子活动的评估证据是：

a) PP。

8.3.6.3 应用注释

本条只适于 PP 中包含未引用 ISO/IEC 15408-2 或 ISO/IEC 15408-3 进行明确陈述的 IT 安全要求的情形。否则，本条的所有工作单元都不适用，并视为已经满足。

APE_SRE“明确陈述的 IT 安全要求”是对 APE_REQ“IT 安全要求”的补充，而不是替代。也就是说，未引用 ISO/IEC 15408-2 或 ISO/IEC 15408-3 进行明确陈述的 IT 安全要求应按照 APE_SRE“明确陈述的 IT 安全要求”标准和包括 APE_REQ“IT 安全要求”在内的其他安全要求标准组合进行评估。

8.3.6.4 行为 APE_SRE.1.1E

8.3.6.4.1 工作单元 APE_SRE.1-1

ISO/IEC 15408-3 APE_SRE.1.1C 应标识所有未引用 ISO/IEC 15408 而明确陈述的 TOE 安全要

求。

评估者***应核查***IT 安全要求陈述，是否标识了所有未引用 ISO/IEC 15408 而明确陈述的 TOE 安全要求。

任何不使用 ISO/IEC 15408-2 功能组件的 TOE 安全功能要求，应该被清晰地标识。同样，任何不使用 ISO/IEC 15408-3 保证组件的 TOE 安全保证要求，也应被清晰地标识。

8.3.6.4.2 工作单元 APE_SRE.1-2

ISO/IEC 15408-3 APE_SRE.1.2C 应标识所有未引用 ISO/IEC 15408 而明确陈述的 IT 环境安全要求。

评估者***应核查***IT 安全要求陈述，是否标识了所有未引用 ISO/IEC 15408 而明确陈述的 IT 环境安全要求。

任何不使用 ISO/IEC 15408-2 功能组件的 IT 环境安全功能要求，应该被清晰地标识。同样，任何不使用 ISO/IEC 15408-3 保证组件的 IT 环境安全保证要求，也应该被清晰地标识。

8.3.6.4.3 工作单元 APE_SRE.1-3

ISO/IEC 15408-3 APE_SRE.1.3C 应有证据证明为何这些安全要求应被明确陈述。

评估者***应检查***安全要求基本原理，以确定它恰当地证明了为何每个明确陈述的 IT 安全要求应被明确陈述。

评估者确定对于每个明确陈述的 IT 安全要求，证明应解释为什么已有的功能或保证组件（分别选自 ISO/IEC 15408-2 和 ISO/IEC 15408-3）不能用于表达所讨论的明确陈述安全要求。在做出决定时，评估者应该考虑对已有的功能或保证组件实施诸如赋值、反复或细化等操作的可能性。

8.3.6.4.4 工作单元 APE_SRE.1-4

ISO/IEC 15408-3 APE_SRE.1.4C 明确陈述的 IT 安全要求应以 ISO/IEC 15408 的要求组件、族和类作为表述的模板。

评估者***应检查***每个明确陈述的 IT 安全要求，以确定该要求是用 ISO/IEC 15408 的组件、族和类作为表述的模板。

评估者确定明确陈述的 IT 安全要求与 ISO/IEC 15408-2 或 ISO/IEC 15408-3 组件的表述形式相同且达到相当的详细程度。评估者还确定功能要求被分解成单个功能元素，保证要求指定了开发者行为元素、证据的内容和形式元素以及评估者行为元素。

8.3.6.4.5 工作单元 APE_SRE.1-5

ISO/IEC 15408-3 APE_SRE.1.5C 明确陈述的 IT 安全要求应是可度量的，并陈述了客观的评估要求，这样就可以判断和系统地证实一个 TOE 是否遵从这些要求。

评估者***应检查***每个明确陈述的 IT 安全要求，以确定它是可度量的并陈述了客观的评估要求，这样就能判断并系统地证实一个 TOE 是否遵从这些要求。

评估者确定功能要求以某方式陈述，即它们是可测试的，并且是可通过适当的 TSF 表述进行追溯的。评估者还确定保证要求避免了要求评估者做出主观判定。

已有的 ISO/IEC 15408 功能和保证要求都可以用作遵从本要求的模板。

8.3.6.4.6 工作单元 APE_SRE.1-6

ISO/IEC 15408-3 APE_SRE.1.6C 明确陈述的 IT 安全要求应被清楚且无歧义地表述。

评估者***应检查***每个明确陈述的 IT 安全要求，以确定其表述是清楚且无歧义的。

已有的 ISO/IEC 15408 功能和保证要求都可以用作遵从本要求的模板。

8.3.6.4.7 工作单元 APE_SRE.1-7

ISO/IEC 15408-3 APE_SRE.1.7C 安全要求基本原理应证明保证要求是适用的，并且适合于支持任何明确陈述的 TOE 安全功能要求。

评估者***应检查***安全要求基本原理，以确定它证明了保证要求是适用的，并适于支持任何明确陈述的 TOE 安全功能要求。

评估者确定特定保证要求的应用是否会得到关于每个明确陈述的安全功能要求的有意义的评估结果，或者是否应指定其他保证要求。比如，一个明确陈述的功能要求可能隐含要求特殊的文档证据（诸如一个 TSP 模型）、测试深度或分析（诸如 TOE 安全功能强度分析或隐通道分析）。

8.3.6.5 行为 APE_SRE.1.2E

8.3.6.5.1 工作单元 APE_SRE.1-8

评估者***应检查***IT 安全要求陈述，以确定任何明确陈述的 IT 安全要求的所有依赖关系都已被标识。

评估者确认 PP 作者未忽略任何可用的依赖关系。

例如以下情况可能存在依赖关系：如果明确陈述的功能要求提到审计，则可能与 FAU“安全审计”类的组件有依赖关系；如果明确陈述的保证要求提到源代码或 TOE 实现表述，则可能与 ADV_IMP“实现表示”有依赖关系。

9 ASE 类：安全目标评估

9.1 简介

本章描述 ST 的评估。由于 ST 为 TOE 评估子活动提供依据和评估背景，所以 ST 评估应在所有 TOE 评估子活动之前启动。鉴于 TOE 评估过程中子活动的有关发现可能会导致 ST 的改变，因此直到 TOE 评估完成后，才可能形成对 ST 的最终裁定。

不管 ST 中宣称的 EAL（或另外一套保证标准）是多少，对于每个 ST 评估，其要求和方法是完全相同的。尽管本标准中后继更多的章节是针对特定的评估保证级别而言，但是本章适用于所有级别的 ST 评估。

本章所述的评估方法是建立在 ISO/IEC 15408-1 中特别在附录 B，以及 ISO/IEC 15408-3 ASE 类中规定的 ST 要求的基础上的。

9.2 ST 评估相互关系

完备的 ST 评估应包括以下活动：

a) 评估输入任务（第 7 章）。

b) ST 评估活动，包含以下子活动：

   1) TOE 描述的评估（9.3.1）；

   2) 安全环境的评估（9.3.2）；

   3) ST 引言的评估（9.3.3）；

   4) 安全目的的评估（9.3.4）；

   5) PP 声明的评估（9.3.5）；

   6) IT 安全要求的评估（9.3.6）；

7) 明确陈述的 IT 安全要求的评估(9.3.7);

8) TOE 概要规范的评估(9.3.8)。

c) 评估输出任务(第 7 章)。

第 7 章描述了评估输入任务和评估输出任务。评估活动是由 ISO/IEC 15408-3 的 ASE 保证要求中导出的。

本章描述了 ST 评估包含的子活动。尽管通常所述的子活动有可能同时进行,但是评估者应该考虑子活动之间的依赖性。依赖性指南参见 A.4“依赖性”。

不是所有的 ST 评估都要进行 PP 声明评估和明确陈述的 IT 安全要求评估:只有在做了 PP 声明的情况下,才需要进行 PP 声明的评估;只有当安全要求不是从 ISO/IEC 15408-2 和 ISO/IEC 15408-3 抽出的,但包含在 IT 安全要求的陈述中,才需要对应的明确陈述 IT 安全要求进行评估。

ST 需要的一些信息可以通过引用而被包含进来。例如,如果在 ST 中有 PP 一致性声明,那么 PP 中包含的诸如环境和威胁的信息应视为 ST 的一部分,且 ST 应该遵循这些准则。

如果 ST 声称与一个已评估过的 PP 保持一致,且很大程度依赖 PP 的内容,那么在实施上面列出的一些评估子活动时,可以重用 PP 的评估结果。特别在评估安全环境、安全目的和 IT 安全要求的陈述时可以重复使用 PP 评估结果。允许一个 ST 声称遵从多个 PP。

9.3 ST 评估活动

9.3.1 TOE 描述的评估(ASE_DES.1)

9.3.1.1 目的

本子活动的目的是确定 TOE 描述是否包含了有助于理解 TOE 用途及其功能的相关信息,以及确定该描述是否完备和一致。

9.3.1.2 输入

本子活动的评估证据是:

a) ST。

9.3.1.3 应用注释

TOE 与客户购买的产品之间可能会有差别,有关这个问题的讨论见附录 A.6“TOE 边界”。

9.3.1.4 行为 ASE_DES.1.1E

9.3.1.4.1 工作单元 ASE_DES.1-1

ISO/IEC 15408-3 ASE_DES.1.1C TOE 描述应描述产品或系统的类型,并从物理和逻辑两方面概括性地描述 TOE 的范围和边界。

评估者***应检查***TOE 描述,以确定它是否描述了 TOE 的产品或系统类型。

评估者确定 TOE 描述能为读者提供了足以全面理解产品或系统预期使用的信息,从而提供评估的背景。产品或系统类型的例子有:防火墙、智能卡、加密调制解调器、Web 服务器和内联网。

某些情况下,产品或系统类型明确要求 TOE 具备一些功能,如果产品缺少这些功能,评估者应确定 TOE 描述是否对此进行了充分讨论。例如,防火墙类型的 TOE,在 TOE 描述中应对不能和网络相连的情况进行说明。

9.3.1.4.2 工作单元 ASE_DES.1-2

评估者*应检查*TOE 描述，以确定它是否概括性地描述了 TOE 物理范围和边界。

评估者确定 TOE 描述详细讨论了构成 TOE 的硬件、软件和固件组件或模块，且详细到使读者对组件或模块能够全面理解的程度。

如果 TOE 与产品不是完全相同的，评估者应确定 TOE 描述是否充分描述了 TOE 与产品之间的物理关系。

9.3.1.4.3 工作单元 ASE_DES.1-3

评估者*应检查*TOE 描述，以确定它是否概括性地描述了 TOE 逻辑范围和边界。

评估者确定 TOE 描述详细讨论了 TOE 提供的 IT 特征，特别是安全特征，且详细到能够使读者对这些特征有一个全面理解的程度。

如果 TOE 与产品不是完全相同的，评估者应确定 TOE 描述是否充分描述了 TOE 与产品之间的逻辑关系。

9.3.1.5 行为 ASE_DES.1.2E

9.3.1.5.1 工作单元 ASE_DES.1-4

评估者*应检查*ST，以确定 TOE 描述是有连贯的。

如果 TOE 描述的文本和结构都能被其目标读者（例如，评估者和客户）理解的话，TOE 描述就是有连贯的。

9.3.1.5.2 工作单元 ASE_DES.1-5

评估者*应检查*ST，以确定 TOE 的描述是内在一致的。

应该提醒评估者的是，ST 的这一节仅用于定义 TOE 的一般目的。

一致性分析指南见 A.3“一致性分析”。

9.3.1.6 行为 ASE_DES.1.3E

9.3.1.6.1 工作单元 ASE_DES.1-6

评估者*应检查*ST，以确定 TOE 描述与 ST 的其他部分是一致的。

评估者尤其应确定 TOE 描述没有描述那些在 ST 其他部分都未涉及的 TOE 威胁、安全特征或配置。

一致性分析指南见 A.3“一致性分析”。

9.3.2 安全环境的评估（ASE_ENV.1）

9.3.2.1 目的

本子活动的目的是确定 ST 中 TOE 安全环境的陈述是否为有关 TOE 及其预期应用环境的安全问题提供了一个清晰、一致的定义。

9.3.2.2 输入

本子活动的评估证据是：

a） ST。

9.3.2.3 行为 ASE_ENV.1.1E

9.3.2.3.1 工作单元 ASE_ENV.1-1

ISO/IEC 15408-3 ASE_ENV.1.1C TOE 安全环境陈述应标识并解释关于 TOE 的预期使用和 TOE 使用环境的所有假设。

评估者***应检查***TOE 安全环境的陈述，以确定它标识并解释了所有假设。

这些假设可以分成 TOE 预期使用方面的假设和 TOE 使用环境方面的假设。

评估者确定 TOE 预期使用的假设阐明了 TOE 预期使用的下述方面：TOE 预期应用、TOE 所保护资产的潜在价值以及使用 TOE 时可能存在的使用限制。

评估者确定 ST 中对 TOE 预期使用的所有假设都进行了足够详细的解释，以使得客户能确定其预期使用与这些假设是否相匹配。如果没有清楚理解这些假设，最终可能导致客户在非希望的环境中使用 TOE。

评估者确定 TOE 使用环境的假设包括环境的物理、人员、连接性等方面：

a) 物理方面包括为了使 TOE 以安全方式行使其功能，而对 TOE 的物理场所或附加的外围设施所做的所有假设。例如：
   ——假设管理员控制台严格限制在管理员个人范围内；
   ——假设 TOE 所有文件的存储只能在 TOE 运行的工作站上进行。
b) 人员方面包括为了使 TOE 以安全方式行使其功能，而对在 TOE 安全环境内的用户和管理员或其他个人(包括具有潜在威胁的主体)所做的所有假设。例如：
   ——假设用户具有独特技能或专门技术；
   ——用户具有确定的最小权限；
   ——管理员每月更新防病毒数据库。
c) 连接性方面包括为了使 TOE 以安全方式行使其功能，而对 TOE 与 TOE 之外的 IT 系统或产品(硬件、软件、固件或它们的组合)之间连接所做的所有假设。例如：
   ——假设存储 TOE 产生的日志文件至少需要 100MB 的外部磁盘空间；
   ——假设 TOE 只是在特定工作站上运行的非操作系统应用程序；
   ——假定 TOE 的软驱是禁用的；
   ——假定 TOE 不会连接到任何不可信的网络。

评估者确定 TOE 使用环境的所有假设都得到足够详细的解释，使客户能够确定他们的预期环境与假设环境是否相匹配。如果没有清楚地理解这些假设，最终可能导致 TOE 在环境中不能安全行使其功能。

9.3.2.3.2 工作单元 ASE_ENV.1-2

ISO/IEC 15408-3 ASE_ENV.1.2C TOE 安全环境陈述应标识并解释针对 TOE 或其环境保护的资产的所有已知或假定威胁。

评估者***应检查***TOE 安全环境的陈述，以确定其标识并解释了所有的威胁。

如果 TOE 及其环境安全目的仅源于组织安全策略和假设，那么 ST 中就可以不含威胁陈述。此时，本工作单元不适用，并视为已经满足。

评估者确定所有已标识的威胁都已按照威胁主体、攻击行为和受攻击资产三个方面进行了清楚解释。

评估者还确定威胁主体都是用专业技术、资源和动机等方面来刻画的，攻击行为都是用攻击方法、可利用的任何脆弱性和时机等方面来描述的。

9.3.2.3.3 工作单元 ASE_ENV.1-3

ISO/IEC 15408-3 ASE_ENV.1.3C TOE 安全环境陈述应标识并解释 TOE 应遵守的所有组织安全策略。

评估者***应检查***TOE 安全环境陈述，以确定它标识并解释了所有组织安全策略。

如果 TOE 及其环境的安全目的仅源于假设和威胁，那么 ST 中就可以不包含组织安全策略陈述。此时，本工作单元不适用，并视为已经满足。

评估者确定组织安全策略陈述都是根据 TOE 或其环境应遵守的规则、惯例或方针而作出的，这些规则、惯例或方针是由控制 TOE 使用环境的组织制定的。例如，要求密码生成和加密应符合国家标准就是一条组织安全策略。

评估者确定 ST 中对每个组织安全策略都进行了详细解释，以便于读者清晰地理解；应对组织安全策略陈述进行清楚地表述，以便使安全目的能够追溯到组织安全策略。

9.3.2.4 行为 ASE_ENV.1.2E

9.3.2.4.1 工作单元 ASE_ENV.1-4

评估者***应检查***TOE 安全环境的陈述，以确定它是连贯的。

如果 TOE 安全环境陈述的文本和结构都能被其目标读者(例如评估者和客户)理解的话，TOE 安全环境描述就是连贯的。

9.3.2.4.2 工作单元 ASE_ENV.1-5

评估者***应检查***TOE 安全环境的陈述，以确定它是内在一致的。

TOE 安全环境内在不一致性的示例有：

——TOE 安全环境的陈述包含某种威胁，其攻击方法不在威胁主体的能力范围内。

——TOE 安全环境的陈述包含“TOE 不应与因特网相连”这样的组织安全策略，但有一个威胁其威胁主体是来自因特网的入侵者。

一致性分析指南见 A.3“一致性分析”。

9.3.3 ST 引言的评估（ASE_INT.1）

9.3.3.1 目的

本子活动的目的是确定 ST 引言是否完备、与 ST 的其他部分是否保持一致，以及是否正确标识了 ST。

9.3.3.2 输入

本子活动的评估证据是：

a) ST。

9.3.3.3 行为 ASE_INT.1.1E

9.3.3.3.1 工作单元 ASE_INT.1-1

ISO/IEC 15408-3 ASE_INT.1.1C ST 引言应包含一个 ST 标识，提供控制和标识 ST 及其对应的 TOE 所必需的标记性和描述性信息。

评估者***应核查***ST 引言是否提供了必要的 ST 标识信息以控制和标识 ST 以及它所参照的 TOE。

评估者确定 ST 标识信息包括：

a) 管理和唯一标识 ST 的必要信息(例如 ST 标题、版本号、出版日期和作者)；

b) 控制和唯一标识 ST 所参照 TOE 的必要信息(例如 TOE 的身份、TOE 的版本号)；

c) 用于开发 ST 的 ISO/IEC 15408 版本信息；

d) 评估体制要求的其他信息。

9.3.3.3.2 工作单元 ASE_INT.1-2

ISO/IEC 15408-3 ASE_INT.1.2C ST 引言应当包含一个 ST 概述，以叙述形式概括该 ST。

评估者***应核查***ST 引言，以叙述形式提供 ST 概述。

ST 概述将为 ST 内容提供概要描述(更详细的描述在 TOE 描述中提供)，且详细到足以使潜在的用户能确认 TOE(因此是 ST 的支撑基础)是否是他所需要的。

9.3.3.3.3 工作单元 ASE_INT.1-3

ISO/IEC 15408-3 ASE_INT.1.3C ST 引言应当包含一个 ISO/IEC 15408 一致性声明，该声明陈述该 TOE 与 ISO/IEC 15408 一致性的所有可评估声明。

评估者***应核查***ST 引言是否包含一个 ISO/IEC 15408 一致性声明，该声明陈述了 TOE 与 ISO/IEC 15408 的一致性。

评估者确定 ISO/IEC 15408 一致性声明与 ISO/IEC 15408-1 的 6.4 是一致的。

评估者确定 ISO/IEC 15408 一致性声明包含 ISO/IEC 15408-2 一致性或 ISO/IEC 15408-2 的扩展。

评估者确定 ISO/IEC 15408 一致性声明包含 ISO/IEC 15408-3 一致性或 ISO/IEC 15408-3 的扩展。

如果声明 ISO/IEC 15408-3 扩展且保证包包含 ISO/IEC 15408-3 中的保证要求，评估者就应确定 ISO/IEC 15408 一致性声明是否陈述了哪些保证要求是 ISO/IEC 15408-3 的。

如果声称包选定一致，评估者就应确定 ISO/IEC 15408 一致性声明是否陈述了所声称的那个包。

如果声称包选定增强，评估者就应确定 ISO/IEC 15408 一致性声明是否陈述了所声称的那个包以及如何对包进行增强。

如果声称 PP 一致，评估者就应确定 ISO/IEC 15408 一致性声明是否陈述了与哪个或哪些 PP 保持一致。

需提醒评估者的是：如果声称 PP 一致，那么可以采用 ASE_PPC.1“PP 声明评估”标准进行评估；如果声称 ISO/IEC 15408-2 扩展或 ISO/IEC 15408-3 扩展，那么可以采用 ASE_SRE.1“明确陈述的 IT 安全要求评估”标准进行评估。

9.3.3.4 行为 ASE_INT.1.2E

9.3.3.4.1 工作单元 ASE _INT.1-4

评估者***应检查***ST 引言，以确定它是有条理的。

如果 ST 引言的文本和结构都能被其目标读者理解(例如评估者和客户)，那么 ST 引言就是有条理的。

9.3.3.4.2 工作单元 ASE _INT.1-5

评估者***应检查***ST 引言，以确定它是内在一致的。

ST 概述为 ST 内容提供概要描述，因此有关内在一致性分析会自然就集中在 ST 概述上。

一致性分析指南见 A.3“一致性分析”。

9.3.3.5 行为 ASE_INT.1.3E

9.3.3.5.1 工作单元 ASE _INT.1-6

评估者***应检查***ST 引言,以确定 ST 引言与 ST 其他部分是一致的。

评估者确定 ST 概述提供了 TOE 的一个准确概括。评估者特别应确定 ST 概述与 TOE 描述是一致的,且没有规定或暗示存在评估范围之外的安全特征。

评估者还应确定 ISO/IEC 15408 一致性声明是否与 ST 的其他部分一致。

一致性分析指南见 A.3“一致性分析”。

9.3.4 安全目的的评估(ASE_OBJ.1)

9.3.4.1 目的

本子活动的目的是确定安全目的描述是否完备和一致,并确定安全目的是否能对抗已标识的威胁,实现已标识的组织安全策略并遵循规定的假设。

9.3.4.2 输入

本子活动的评估证据是:

a) ST。

9.3.4.3 行为 ASE_OBJ.1.1E

9.3.4.3.1 工作单元 ASE_OBJ.1-1

ISO/IEC 15408-3 ASE_OBJ.1.1C 安全目的的陈述应为 TOE 及其环境定义安全目的。

评估者***应核查***安全目的的陈述,是否定义了 TOE 及其环境的安全目的。

评估者应确定每个安全目的是否明确地说明了适用于 TOE,还是环境,或者两者都适用。

9.3.4.3.2 工作单元 ASE_OBJ.1-2

ISO/IEC 15408-3 ASE_OBJ.1.2C TOE 的安全目的应可以追溯至由 TOE 对抗的多方面的确定威胁,和/或可以追溯至 TOE 所满足的组织安全策略。

评估者***应检查***安全目的的基本原理,以确定 TOE 的所有安全目的都能追溯到 TOE 能够对抗的确定威胁和/或 TOE 应遵循的组织安全策略。

评估者应确定 TOE 的每个安全目的能追溯到至少一个威胁或组织安全策略。

不能追溯就意味着安全目的的基本原理是不完备的,威胁或组织安全策略的陈述是不完备的,或 TOE 的安全目的没有实际意义。

9.3.4.3.3 工作单元 ASE_OBJ.1-3

ISO/IEC 15408-3 ASE_OBJ.1.3C 环境的安全目的应可以追溯至不是完全由 TOE 对抗的多方面的确定威胁,和/或可以追溯至 TOE 未完全满足的组织安全策略或假设。

评估者***应检查***安全目的的基本原理,以确定环境安全目的能追溯到 TOE 环境能够对抗的确定威胁,和/或追溯到 TOE 环境应遵循的组织安全策略,和/或 TOE 环境应满足的假设。

评估者应确定环境的每个安全目的都能追溯到至少一个假设、威胁或组织安全策略。

不能追溯就意味着安全目的的基本原理是不完备的,威胁、假设或组织安全策略的陈述是不完备

的,或环境的安全目的没有实际意义。

9.3.4.3.4 工作单元 ASE_OBJ.1-4

ISO/IEC 15408-3 ASE_OBJ.1.4C 安全目的基本原理应证实所陈述的安全目的恰好对抗确定的安全威胁。

评估者***应检查***安全目的基本原理,以确定对于每个威胁,基本原理都包含了安全目的恰好对抗该威胁的适当论证。

如果没有安全目的能追溯到对应的威胁,则本单元为不通过。

评估者应确定有关威胁的论证能够阐明:如果所有能追溯到威胁的安全目的都达到,那么就消除了这个威胁,或者说威胁被降低到可以接受的水平,或威胁的效果得以充分地缓解。

评估者还应确定当达到可以追溯到威胁的所有安全目的时,实际上促成了该威胁的消除、降低或缓解。

消除威胁的例子如下:

——消除主体使用攻击方法的能力;

——通过威慑,消除威胁主体的动机;

——消除威胁主体(例如:移走经常使网络崩溃的机器)。

降低威胁的例子如下:

——限制威胁主体使用攻击方法;

——限制威胁主体的攻击机会;

——减少成功发起攻击的可能性;

——要求威胁主体具有更高的专业知识或更多的资源。

缓解威胁效果的例子如下:

——经常备份资产;

——拥有 TOE 备份;

——经常改变通信会话使用的密钥,这样即使一个密钥被攻破,其影响也相对较小。

应当注意的是,安全目的基本原理中提供的从安全目的到威胁的映射,可能是论证的一部分,但是其本身不是完整的论证过程。即使在安全目的仅仅反映试图防止特定威胁被实现的情形下,仍需进行论证,但是在这种情况下可以是最低要求的论证。

9.3.4.3.5 工作单元 ASE_OBJ.1-5

ISO/IEC 15408-3 ASE_OBJ.1.5C 安全目的基本原理应证实所陈述的安全目的恰好覆盖所有确定的组织安全策略和假设。

评估者***应检查***安全目的基本原理,以确定对于每个组织安全策略而言,基本原理都包含安全目的恰好覆盖该组织安全策略的适当论证。

如果没有安全目的追溯到这个组织安全策略,则本工作单元为“不通过”。

评估者应确定有关组织安全策略的论证能够阐明:如果达到了所有能追溯到组织安全策略的安全目的,那么就实现了组织安全策略。

评估者还应确定当达到可以追溯到组织安全策略的所有安全目的时,实际上促成了组织安全策略的执行。

应当注意的是,安全目的基本原理中提供的从安全目的到组织安全策略的映射,可能是论证的一部分,但是其本身不是完整的论证过程。甚至在安全目的仅仅反映试图实现特定组织安全策略的情形下,仍需进行论证,但是在这种情况下可以是最低要求的论证。

9.3.4.3.6 工作单元 ASE_OBJ.1-6

评估者*应检查*安全目的基本原理，以确定对每个假设而言，基本原理都包含环境安全目的恰好覆盖该假设的适当论证。

如果没有环境安全目的追溯到这个假设，则本工作单元为“不通过”。

假设可以是有关 TOE 预期使用的假设，也可以是有关 TOE 预期使用环境的假设。

评估者应确定有关 TOE 预期使用假设的论证能够阐明：如果实现了追溯到假设的所有环境安全目的，那么就支持预期的使用。

评估者还应确定达到可追溯到假设的所有环境安全目的时，实际上促成了预期使用的支持。

评估者应确定有关 TOE 使用环境假设的论证能够阐明：如果实现了追溯到假设的所有环境安全目的，那么环境就与假设是一致的。

评估者还应确定当达到可追溯到 TOE 使用环境假设的所有环境安全目的时，实际上促成了环境与假设一致。

应当注意的是，安全目的基本原理中提供的从环境安全目的到假设的映射，可能是论证的一部分，但是其本身不是完整的论证过程。即使在环境安全目的仅仅是对假设重述的情形下，仍需进行论证，但是在这种情况下可以是最低要求的论证。

9.3.4.4 行为 ASE_OBJ.1.2E

9.3.4.4.1 工作单元 ASE_OBJ.1-7

评估者*应检查*安全目的陈述，以确定它是有条理的。

如果安全目的的文本和结构能被其目标读者（如评估者和客户）所理解，那么安全目的的表述就是有条理的。

9.3.4.4.2 工作单元 ASE_OBJ.1-8

评估者*应检查*安全目的陈述，以确定它是完备的。

如果安全目的足以对抗所有已标识的威胁，并能覆盖所有已标识的组织安全策略和假设，那么安全目的是完备的。本工作单元可以同工作单元 ASE_OBJ.1-4、ASE_OBJ.1-5 和 ASE_OBJ.1-6 一道被执行。

9.3.4.4.3 工作单元 ASE_OBJ.1-9

评估者*应检查*安全目的陈述，以确定它是内在一致的。

如果安全目的之间不相互冲突，安全目的的陈述就是内在一致的。安全目的相互冲突的例子有：两个安全目的，一个是“用户身份从来都不应被公开”，另一个则是“用户身份可以被其他用户利用”。

一致性分析指南见 A.3“一致性分析”。

9.3.5 PP 声明的评估（ASE_PPC.1）

9.3.5.1 目的

本子活动的目的是确定 ST 是不是 PP 的一个正确实例，该 PP 是 ST 所声明遵从的。

9.3.5.2 输入

本子活动的评估证据是：

a） ST；

b) ST 声称遵从的 PP。

9.3.5.3 应用注释

本条只适用于 ST 中声明遵从一个或多个 PP 的情形。否则,本条中的所有工作单元都不适用,并视为已经满足 。

9.3.5.4 行为 ASE_PPC.1.1E

9.3.5.4.1 工作单元 ASE_PPC.1-1

ISO/IEC 15408-3 ASE_PPC.1.1C 每一个 PP 声明应标识所声明遵从的 PP,包括该声明所需要的一些限制。

评估者***应核查***每个 PP 声明是否标识了所声明遵从的 PP。

评估者确定任何参考的 PP 都已被清晰标识(例如通过名称和版本号或通过包含在 PP 引言中的标识)。应该提醒评估者的是:ISO/IEC 15408 不允许声明部分遵从一个 PP。

9.3.5.4.2 工作单元 ASE_PPC.1-2

ISO/IEC 15408-3 ASE_ PPC.1.2C 每一个 PP 声明应标识那些满足 PP 许可操作或者进一步限制 PP 要求的 IT 安全要求陈述。

评估者***应核查***每个 PP 声明是否标识了那些满足 PP 许可操作或进一步限制 PP 要求的 IT 安全要求。

ST 不需重述那些没有任何更改的 PP 中的安全要求陈述。但如果 PP 的安全功能要求包括未完成的操作,或 ST 作者已对 PP 的安全要求实施了细化操作,那么这些要求应在 ST 中明确标识。

9.3.5.4.3 工作单元 ASE_PPC.1-3

ISO/IEC 15408-3 ASE_PPC.1.3C 每一个 PP 声明应标识那些包含在 ST 中但不包含在 PP 中的安全目的和 IT 安全要求陈述。

评估者***应核查***每个 PP 声明是否标识了补充 PP 所包含安全目的和 IT 安全要求的那些安全目的和 IT 安全要求。

评估者应确定包含在 ST 中,而不含在 PP 中的所有安全目的和安全要求都已明确标识。

9.3.5.5 行为 ASE_PPC.1.2E

9.3.5.5.1 工作单元 ASE_PPC.1-4

对每个 PP 声明,评估者***应检查***ST,以确定所有对 PP 中 IT 安全要求实施的操作都是在 PP 设定的范围之内的。

本工作单元不仅包括 PP 中未完成的赋值或选择操作,还包括对 PP 中安全要求的细化操作。

9.3.6 IT 安全要求的评估(ASE_REQ.1)

9.3.6.1 目的

本子活动的目的是确定 TOE 安全要求(包括 TOE 安全功能要求和 TOE 安全保证要求)和 IT 环境安全要求是否完备和一致,并为 TOE 的开发提供充分的基础,以达到其安全目的。

9.3.6.2 输入

本子活动的评估证据是:

a) ST。

9.3.6.3 行为 ASE_REQ.1.1E

9.3.6.3.1 工作单元 ASE_REQ.1-1

ISO/IEC 15408-3 ASE_REQ.1.1C TOE 安全功能要求的陈述应标识从 ISO/IEC 15408-2 功能要求组件中选取的 TOE 安全功能要求。

评估者***应核查***TOE 安全功能要求的陈述是否标识了从 ISO/IEC 15408-2 功能要求组件中选取的那些 TOE 安全功能要求。

评估者应确定从 ISO/IEC 15408-2 中选取的所有安全功能组件要求都已标识,这种标识或者通过引用 ISO/IEC 15408-2 的单个组件,或者引用 ST 所声明遵从 PP 中的单个组件,或者通过在 ST 中复制来实现。

9.3.6.3.2 工作单元 ASE_REQ.1-2

评估者***应核查***对每个 TOE 安全功能要求组件的引用的正确性。

评估者应确定 ISO/IEC 15408-2 是否包含所引用的每一个 ISO/IEC 15408-2 TOE 安全功能要求组件。

评估者应确定 PP 中是否包含所引用的每一个 PP 中的 TOE 安全功能要求组件。

9.3.6.3.3 工作单元 ASE_REQ.1-3

评估者***应核查***从 ISO/IEC 15408-2 中选取出的在 ST 中重现的 TOE 安全功能要求组件都得以正确重现。

评估者应确定在没有对允许操作进行检查的情况下,TOE 安全功能要求陈述正确地重现了这些要求。对组件操作正确性的检查在工作单元 ASE_REQ.1-11 和 ASE_REQ.1-12 中进行。

9.3.6.3.4 工作单元 ASE_REQ.1-4

ISO/IEC 15408-3 ASE_REQ.1.2C TOE 安全保证要求的陈述应标识从 ISO/IEC 15408-3 保证要求组件中选取的 TOE 安全保证要求。

评估者***应核查***TOE 安全保证要求陈述是否标识了从 ISO/IEC 15408-3 保证要求组件中选取的 TOE 安全保证要求。

评估者应确定从 ISO/IEC 15408-3 选取的所有 TOE 安全保证要求组件都已标识,这种标识或者通过引用 EAL,或者通过引用 ISO/IEC 15408-3 的单个组件,或者通过引用 ST 所声明遵从的 PP,或者通过在 ST 中复制来实现。

9.3.6.3.5 工作单元 ASE_REQ.1-5

评估者***应核查***对每个 TOE 安全保证要求组件的引用的正确性。

评估者应确定 ISO/IEC 15408-3 是否包含所引用的每一个 ISO/IEC 15408-3TOE 安全保证要求组件。

评估者应确定 PP 中是否包含所引用的每一个 PP 中的 TOE 安全保证要求组件。

9.3.6.3.6 工作单元 ASE_REQ.1-6

评估者***应核查***从 ISO/IEC 15408-3 中选取出的在 ST 中重现的 TOE 安全保证要求组件都得以正确重现。

评估者应确定在没有对允许操作进行检查的情况下，TOE 安全保证要求陈述正确地重现了这些要求。对组件操作正确性的检查在工作单元 ASE_REQ.1-11 和 ASE_REQ.1-12 中进行。

9.3.6.3.7 工作单元 ASE_REQ.1-7

ISO/IEC 15408-3 ASE_REQ.1.3C TOE 安全保证要求的陈述应包含一个在 ISO/IEC 15408-3 中定义的评估保证级(EAL)。

评估者***应核查***TOE 安全保证要求陈述，以确定它包含了 ISO/IEC 15408-3 所定义的 EAL，或恰当地证明了它不包含 EAL。

如果不包含 EAL，评估者应确定相关的证明说明了 TOE 保证要求陈述不包含 EAL 的理由。该证明可以说明为什么不可能、不需要或不适合包含一个 EAL，或说明为什么不可能、不需要或不适合包含构成 EAL1(ACM_CAP、ADO_IGS、ADV_FSP、ADV_RCR、AGD_ADM、AGD_USR 和 ATE_IND)族的特定组件。

9.3.6.3.8 工作单元 ASE_REQ.1-8

ISO/IEC 15408-3 ASE_REQ.1.4C 证据应证明 TOE 安全保证要求的陈述是恰当的。

评估者***应检查***安全要求基本原理，以确定基本原理充分证明了 TOE 安全保证要求的陈述是恰当的。

如果保证要求包含一个 EAL，则证明将 EAL 作为一个整体来选择，而不是选择 EAL 的所有单个组件。如果保证要求包含 EAL 增强组件，则评估者应该确定每个增加的组件都是单独被证明过的。如果保证要求包含明确陈述的保证要求，评估者应该确定每个明确陈述的保证要求都是单独被证明过的。

评估者应确定安全要求基本原理足以证明：保证要求相对于给定的安全环境和安全目的陈述是足够的。例如，如果需要防范拥有专业知识的攻击者，就不适合规定 AVA_VLA.1“开发者脆弱性分析”，因为该组件不要求探测明显的脆弱性之外的漏洞。

论证可能包含的如下理由：

a) 在 ST 声称遵从的 PP 中出现的保证要求；

b) 评估体制、政府或其他组织实施的特定要求；

c) 与 TOE 安全功能要求相关的保证要求；

d) 与 TOE 一起使用的系统/产品的保证要求；

e) 客户的要求。

ISO/IEC 15408-3 的 10.2 提供了每个 EAL 的目的和目标概述。

应该提醒评估者的是：确定保证要求是否适当可能是主观性的，因此在对证明的充分性进行分析时不应过于苛刻。

如果保证要求中不包含一个 EAL，本工作单元可以与工作单元 ASE_REQ.1-7 一起执行。

9.3.6.3.9 工作单元 ASE_REQ.1-9

ISO/IEC 15408-3 ASE_REQ.1.5C 如果适当的话，ST 应标识 IT 环境的所有安全要求。

适当时，评估者***应核查***IT 环境的安全要求是否被标识。

如果 ST 中不包含 IT 环境的安全要求，则本工作单元不适用，并视为已经满足。

评估者应确定 TOE 与其环境中的其他 IT 之间的任何依赖关系，在 ST 中都清晰标识为 IT 环境安全要求，这些依赖关系为 TOE 实现其安全目的提供了安全功能。

IT 环境安全要求的例子有：一个防火墙，它依赖于底层操作系统提供管理员的身份鉴别和审计数据的永久储存。这样，IT 环境安全要求应包含 FAU“安全审计”类和 FIA“标识和鉴别”类的功能组件。

应该注意的是,IT 环境安全要求既包含功能要求,也包含保证要求。

IT 环境依赖性的例子如:一个软件密码模块周期性地检查它自己的代码,在代码被篡改时自我禁用。为了恢复,要求使用 FPT_RCV.2“自动恢复”。因为这个加密模块自我禁用后不能自己恢复,这就需要对 IT 环境提出要求。FPT_RCV.2“自动恢复”的一个依赖关系是 AGD_ADM.1“管理员指南”,所以这个保证要求也就变成 IT 环境的保证要求。

应该提醒评估者的是:凡涉及 TSF 的 IT 环境安全要求,皆认为属于环境的安全功能,而不是 TOE 的安全功能。

9.3.6.3.10 工作单元 ASE_REQ.1-10

ISO/IEC 15408-3 ASE_REQ.1.6C 应标识并完成所有包含在 ST 中的 IT 安全要求的操作。

评估者***应核查***IT 安全要求的所有操作都被标识。

ISO/IEC 15408-2 和 ISO/IEC 15408-3 中组件允许的操作有赋值、反复、选择和细化。赋值和选择操作只允许用于组件中特别指定的地方。反复和细化允许用于所有组件。

评估者应确定所有操作都在使用该操作的组件中被标识。标识可以通过排版不同,或者通过周围的文本明确标记,或者通过其他与众不同的方式来实现。

9.3.6.3.11 工作单元 ASE_REQ.1-11

评估者***应检查***IT 安全要求的陈述,以确定实施了所有的赋值和选择操作。

评估者应确定所有组件中的所有赋值和选择操作都已被完全实施(在组件中没有留下任何选择需要做),或者没有完全实施但有适当的理由。

例如,在 FTA_MCS.1“多重并发会话的基本限制”中,当对属于同一用户的并发会话数实施赋值操作时,指定数值的范围就是一个没有完全实施的操作。对此做出适当解释的理由就是这个数值将由管理员在 TOE 安装时从数值范围中选出。

9.3.6.3.12 工作单元 ASE_REQ.1-12

评估者***应检查***ST,以确定所有操作都已正确执行。

评估者应比较每条陈述和导出陈述的元素,以确定:

a) 对于赋值操作,所选的参数或变量的值符合赋值要求的指定类型。

b) 对于选择操作,选择项是在元素选择部分中指定的一项或多项。评估者也应确定符合要求的所选项的数目。某些要求只需要选取一个选项(例如 FAU_GEN.1.1.b),有些情况允许有多个选项(如 FDP_ITT.1.1 第二个操作)。

c) 对于细化操作,组件以这样的方式细化:满足细化要求的 TOE 也满足非细化要求。如果细化后的要求超过该限制,则认为是一个扩展要求。

例如,ADV_SPM.1.2.C TSP 模型应描述所有能被模型化的 TSP 策略的规则和特征。细化:TSP 模型只需要覆盖访问控制。如果访问控制策略是唯一的 TSP 策略,那么这就是有效的细化。如果 TSP 中还有标识和鉴别策略,而且细化声明只有访问控制需要被模型化,那么这就不是一个有效的细化。

细化的一种特殊情形是编辑上的细化,即在要求上做一个小的变化,也就是因遵守正确语法对句子进行改写。这种变化不允许以任何方式改变要求的含义。

编辑细化的一个例子是带有单一行为的 FAU_ARP.1,ST 作者可以将文字“当检测到潜在的安全侵害时,TSF 应向操作员发出通知”,改写成“当检测到潜在的安全侵害时,TSF 应通知操作员”。

应提醒评估者的是编辑上的细化应清楚地标识(见工作单元 ASE_REQ.1-10)。

d) 对于反复操作,一个组件的每个反复操作都不同于该组件的另一次反复(至少组件的某个元素不同于另一个组件的对应元素),或这个组件将应用于 TOE 的不同部分。

9.3.6.3.13 工作单元 ASE_REQ.1-13

ISO/IEC 15408-3 ASE_REQ.1.7C 应满足 ST 中 IT 安全要求之间的依赖关系。

评估者应检查 IT 安全要求的陈述,以确定 IT 安全要求陈述中使用的组件所要求的依赖关系都得到了满足。

依赖关系可以通过将相关组件(或从属于相关组件的组件)包含到 TOE 安全要求陈述中来满足,或作为一个要求,声称由 TOE 的 IT 环境来满足。

尽管 ISO/IEC 15408 通过依赖关系包含列表为依赖关系分析提供支持,但不能证明没有其他依赖关系存在。其他依赖关系的例子有:涉及"所有客体"或"所有主体"的元素与列出这些客体或主体的另一个元素或元素集的细化之间就存在依赖关系。

IT 环境中必要的安全要求依赖关系应在 ST 中陈述并得到体现和满足。

应该提醒评估者的是:ISO/IEC 15408 并不要求所有依赖关系都得到满足,见下一个工作单元。

9.3.6.3.14 工作单元 ASE_REQ.1-14

ISO/IEC 15408-3 ASE_REQ.1.8C 证据应证明为何一个未满足的依赖关系却是适当的。

评估者***应检查***安全要求基本原理,以确定对每一种没有满足安全要求依赖关系的情况都作了适当的证明。

给定已标识的安全目的,评估者应确定该证明解释了不必包括依赖关系的原因。

评估者应确认任何未满足的依赖关系并没有妨碍安全功能要求充分体现安全目的。该分析见 ASE _REQ.1.12C。

适当证明的例子如:当一个软件 TOE 有一个安全目的"鉴别失败时,应将用户的身份、时间和日期记录下来"且采用 FAU_GEN.1"审计数据产生"作为功能要求来满足这个安全目的。FAU_GEN.1 包含了与 FPT_STM.1"可靠时间戳"的依赖关系。由于 TOE 不包含时钟机制,FPT_STM.1 则被 ST 作者定义为 IT 环境要求。ST 作者用这样一个理由说明这个要求没有得到满足:"在特定环境下,可能会存在时间戳机制攻击行为,因此环境就不能传送可靠的时间戳。然而,一些威胁主体没有执行攻击时间戳机制的能力,而且由这样的威胁主体实施的攻击可以通过记录攻击的时间和日期来分析"。

9.3.6.3.15 工作单元 ASE_REQ.1-15

ISO/IEC 15408-3 ASE_REQ.1.9C ST 应包含一个关于 TOE 安全功能要求的最低功能强度级别的陈述,可适当选取基本级功能强度、中级功能强度或高级功能强度中的一个。

评估者***应核查***ST 是否包括一个 TOE 安全功能要求的最低功能强度级别陈述,这个级别可以是基本级功能强度(基本级 SOF)、中级功能强度(中级 SOF)或高级功能强度(高级 SOF)。

如果 TOE 安全保证要求不包括 AVA_SOF.1"TOE 安全功能强度评估",则本工作单元不适用,并视为已经满足。

密码算法的强度超出了 ISO/IEC 15408 的范围。功能强度只适用于非加密的概率或置换机制。因此,当 ST 包含一个最低 SOF 的声明时,且该声明不适用于任何与 ISO/IEC 15408 评估有关的密码机制。当 TOE 包含密码机制时,评估者应该确定 ST 是否包含一个清晰的陈述,说明算法强度的评估不属于该评估的范围。

TOE 可能包括多个不同的域,ST 作者认为每个域有一个最低的功能强度级别,比 TOE 作为一个整体有一个最低的功能强度级别更加实用。在这种情况下,允许将 TOE 安全功能要求划分成不同的组,每个组有不同的最低功能强度级别。

例如分布式终端系统,该系统的用户终端在公共区,管理员终端在物理安全区。用户终端的鉴别要求的安全功能强度是中级 SOF,管理员终端的鉴别要求的安全功能强度是基本级 SOF。并没有说

TOE 的最低功能强度是基本级 SOF，否则，可能会使 TOE 潜在的客户相信利用用户终端攻击鉴别机制是一件相对容易的事情，因此 ST 作者把 TOE 划分为用户域和管理域，将 TOE 安全功能要求划分成两组分属这两个域，分配给属于管理域的一组要求的最低功能强度为基本级 SOF，分配给属于用户域的一组要求的最低功能强度为中级 SOF。

9.3.6.3.16 工作单元 ASE_REQ.1-16

ISO/IEC 15408-3 ASE_REQ.1.10C 安全要求的陈述应标识所有需要一个明确的功能强度声明的安全功能要求，连同每一个这种安全功能要求的明确的功能强度声明。

评估者***应核查***ST 是否标识了所有特定的 TOE 安全功能要求，对这些要求给出明确的功能强度声明是适当的，相应的特定功能强度或度量也是合适的。

如果 TOE 安全保证要求不包括 AVA_SOF.1“TOE 安全功能强度评估”，则本工作单元不适用，并视为已经满足。

明确的功能强度声明既可是基本级功能强度、中级功能强度或高级功能强度，也可是一个既定的特定尺度。如使用的是特定尺度，评估者应确定对特定的功能要求类型，该强度声明是合适的，并且指定的尺度是可评估的。本工作单元涉及 ST 作者需要调整特定 SOF 要求（即比 ST 的总体 SOF 声明更高）或使用一个度量的情形。TOE 安全功能要求的明确 SOF 声明可以由 ST 作者规定。如果没有任何明确的声明，ST 的总体声明适用于 ST 所规定的所有 TOE 安全功能要求。评估者应确认明确的 SOF 声明是与 ST 的其他部分是一致的。

一个 ST 可能拥有多个 SOF 声明规范。对 ST 可能有一个总体 SOF 声明，ST 中的 TOE 安全功能要求可能有一个 SOF 声明。

评估体制可能会提供有关功能强度度量的适合性和适宜性的进一步指导。

9.3.6.3.17 工作单元 ASE_REQ.1-17

ISO/IEC 15408-3 ASE_REQ.1.11C 安全要求基本原理应证实 ST 的最低功能强度级别连同任何明确的功能强度声明，与 TOE 的安全目的是一致的。

评估者***应检查***安全要求基本原理，以确定它证实了最低功能强度级别及任何明确的功能强度声明与 TOE 安全目的是一致的。

如果 TOE 安全保证要求不包括 AVA_SOF.1“TOE 安全功能强度评估”，则本工作单元不适用，并视为已经满足。

评估者应确定基本原理考虑了诸如在 TOE 安全环境陈述中描述的攻击者可能具有的专门知识、资源和动机等细节。例如，如果要求 TOE 提供防范以对抗具有高攻击潜力的攻击者，则基本级 SOF 声明就是不适当的。

评估者还应确定基本原理考虑了安全目的中所有特定的强度相关特性。评估者可采用将要求追溯到目的的方式，来确定如果合适的话，能够追溯到安全目的的带有特定的强度相关特性的那些要求是否具有适当的功能强度声明。

9.3.6.3.18 工作单元 ASE_REQ.1-18

ISO/IEC 15408-3 ASE_REQ.1.12C 安全要求基本原理应证实 IT 安全要求正好满足安全目的。

评估者***应检查***安全要求基本原理，以确定 TOE 安全要求能够追溯到 TOE 的安全目的。

评估者确定每个 TOE 安全功能要求至少能追溯到 TOE 的一个安全目的。

如果不能追溯，则表明安全要求基本原理是不完备的，或安全目的是不完备的，或 TOE 安全功能要求没有实际意义。

TOE 的某些或所有安全保证要求不一定追溯到 TOE 的安全目的。

TOE 的安全保证要求回溯到 TOE 的安全目的的例子如:ST 中包含“用户通过用一台误认为是 TOE 的设备,而无意泄露信息”这样一个威胁,且 TOE 的安全目的“TOE 应该清楚标出版本号”能对抗此种威胁。TOE 的安全目的可以通过满足 ACM_CAP.1“版本号”来实现,因此 ST 作者就将 ACM_CAP.1 追溯到该 TOE 安全目的。

9.3.6.3.19 工作单元 ASE_REQ.1-19

评估者***应检查***安全要求基本原理,以确定 IT 环境安全要求能够追溯到环境的安全目的。

评估者确定每个 IT 环境安全功能要求至少能追溯到一个环境安全目的。

如果不能追溯,则表明安全要求基本原理是不完备的,或环境安全目的是不完备的,或 IT 环境安全功能要求没有实际意义。

IT 环境的某些或所有安全保证要求不一定追溯到环境安全目的。

9.3.6.3.20 工作单元 ASE_REQ.1-20

评估者***应检查***安全要求基本原理,以确定对于每个 TOE 安全目的,该原理都包含一个证明 TOE 安全要求恰好满足安全目的的适当论证。

如果 TOE 安全要求都不能追溯到 TOE 的安全目的,则本工作单元为“不通过”。

评估者应确定有关 TOE 安全目的的论证阐明了:如果追溯到安全目的的所有 TOE 安全要求都得到满足,那么就实现了对应的 TOE 安全目的。

评估者还应确定每个可追溯到 TOE 安全目的的 TOE 安全要求得到满足时,实际上促成了该 TOE 安全目的的达到。

应当注意的是,在安全要求基本原理中将 TOE 安全要求追溯到 TOE 安全目的,可以作为论证的一部分,但其本身不是完整的论证过程。

9.3.6.3.21 工作单元 ASE_REQ.1-21

评估者***应检查***安全要求基本原理,以确定对于每个 IT 环境安全目的,该原理都包含一个证明 IT 环境安全要求恰好满足 IT 环境安全目的的适当论证。

如果 IT 环境安全要求都不能追溯到 IT 环境的安全目的,则本工作单元为“不通过”。

评估者应确定有关 IT 环境安全目的的论证阐明了:如果追溯到安全目的的所有 IT 环境安全要求都得到满足,那么就实现了对应的 IT 环境安全目的。

评估者还应确定每个可追溯到 IT 环境安全目的的 IT 环境安全要求得到满足时,实际上促成了 IT 环境安全目的的达到。

应当注意的是,在安全要求基本原理中将 IT 环境安全要求追溯到 IT 环境安全目的,可以作为论证的一部分,但其本身不是完整的论证过程。

9.3.6.3.22 工作单元 ASE_REQ.1-22

ISO/IEC 15408-3 ASE_REQ.1.13C 安全要求基本原理应证实这组 IT 的安全要求组成了一个相互支持并内在一致的整体。

评估者***应检查***安全要求基本原理,以确定它证实了该组 IT 安全要求是内在一致的。

评估者应确定所有将不同 IT 安全要求应用到同一类型的事件、操作、数据和实施的测试等的情形,这些要求可能会互相冲突,此时应该提供适当的证明来说明事实并非如此。

例如,如果 ST 关于单个用户责任可追查性和用户匿名两方面的要求,则需要阐明这些要求不会冲突。这可通过说明单个用户责任可追查性的可审计事件与需要用户匿名的操作无关来证明。

一致性分析指南见 A.3“一致性分析”。

9.3.6.3.23 工作单元 ASE_REQ.1-23

评估者**应检查**安全要求基本原理，以确定它证实了该组 IT 安全要求形成一个互相支持的整体。

本工作单元建立在工作单元 ASE_REQ.1-18、ASE_REQ.1-19、ASE_REQ.1-20 和 ASE_REQ.1-21 所作决定的基础上，其中 ASE_REQ.1-18 和 ASE_REQ.1-19 检查 IT 安全要求能否追溯到安全目的，ASE_REQ.1-20 和 ASE_REQ.1-21 检查 IT 安全要求是否恰好满足安全目的。本工作单元要求评估者考虑这种可能性：因缺乏其他 IT 安全要求的支持，安全目的实际上不能实现。

由于存在这样的情况：功能要求 A 依赖于功能要求 B，而 B 通过定义支持 A，所以本工作单元也建立在前述工作单元依赖关系分析的基础上。

评估者确定安全要求基本原理能够证实功能要求在必要的时候互相支持，即使没有迹象表明这些要求之间存在依赖关系。该证实应提出安全功能要求能：

a) 防止其他安全功能要求的旁路，如 FDP_ RVM.1“TSP 的不可旁路性”；

b) 防止其他安全功能要求的篡改，如 FPT_SEP“域分离”；

c) 防止其他安全功能要求的失效，如 FPT_MOF.1“安全功能行为的管理”；

d) 激活对试图挫败其他安全功能要求的攻击行为的探测，如 FAU“安全审计”类的组件。

在分析时，评估者应考虑已执行的操作是否影响要求间的相互支持。

9.3.6.4 行为 ASE_REQ.1.2E

9.3.6.4.1 工作单元 ASE_REQ.1-24

评估者**应检查**IT 安全要求陈述，以确定其是有条理的。

如果 IT 安全要求描述的文本和结构能被其目标读者(即评估者和客户)理解的话，IT 安全要求陈述就是有条理的。

9.3.6.4.2 工作单元 ASE_REQ.1-25

评估者**应检查**IT 安全要求陈述，以确定它们是完备的。

本工作单元利用来自 ASE_REQ.1.1E 和 ASE_SRE.1.1E 所要求工作单元的结果，特别是评估者对安全要求基本原理的检查结果。

如果所有要求的操作都已完成，且评估者判定安全要求足以保证所有 TOE 安全目的都已满足，则安全要求陈述就是完备的。

9.3.6.4.3 工作单元 ASE_REQ.1-26

评估者**应检查**IT 安全要求陈述，以确定它们是内在一致的。

本工作单元利用来自 ASE_REQ.1.1E 和 ASE_SRE.1.1E 所要求工作单元的结果，特别是评估者对安全要求基本原理的检查结果。

如果评估者确定没有安全要求与任何其他的安全要求相冲突，因为冲突的话安全目的就不能被完全满足，那么安全要求陈述就是内在一致的。

一致性分析指南见 A.3“一致性分析”。

9.3.7 明确陈述的 IT 安全要求的评估（ASE_SRE.1）

9.3.7.1 目的

本子活动的目的是确定未引用 ISO/IEC 15408 进行表述的安全功能要求或安全保证要求是否适当和充分。

9.3.7.2 输入

本子活动的评估证据是：

a) ST。

9.3.7.3 应用注释

本条只适于ST中包含未引用ISO/IEC 15408-2或ISO/IEC 15408-3进行明确陈述的IT安全要求的情形。否则，本条的所有工作单元都不适用，并视为已经满足。

ASE_SRE“明确陈述的IT安全要求”是对ASE_REQ“IT安全要求”的补充，而不是替代。也就是说，未引用ISO/IEC 15408-2或ISO/IEC 15408-3进行明确陈述的IT安全要求应按照ASE_SRE“明确陈述的IT安全要求”标准和包括ASE_REQ“IT安全要求”在内的其他安全要求标准的组合进行评估。

9.3.7.4 行为 ASE_SRE.1.1E

9.3.7.4.1 工作单元 ASE_SRE.1-1

ISO/IEC 15408-3 ASE_SRE.1.1C 应标识所有未引用 ISO/IEC 15408 而明确陈述的 TOE 安全要求。

评估者***应核查***IT安全要求陈述，是否标识了所有未引用ISO/IEC 15408而明确陈述的TOE安全要求。

任何不使用ISO/IEC 15408-2功能组件的TOE安全功能要求，应该被清晰地标识。同样，任何不使用ISO/IEC 15408-3保证组件的TOE安全保证要求，也应该被清晰地标识。

9.3.7.4.2 工作单元 ASE_SRE.1-2

ISO/IEC 15408-3 ASE_SRE.1.2C 应标识所有不引用 ISO/IEC 15408 而明确陈述的 IT 环境安全要求。

评估者***应核查***IT安全要求陈述，是否标识了没有引用ISO/IEC 15408而明确陈述的所有IT环境安全要求。

任何不使用ISO/IEC 15408-2功能组件的IT环境安全功能要求，应该被清晰地标识。同样，任何不使用ISO/IEC 15408-3保证组件的IT环境安全保证要求，也应该被清晰地标识。

9.3.7.4.3 工作单元 ASE_SRE.1-3

ISO/IEC 15408-3 ASE_SRE.1.3C 应由证据证明为何这些安全要求应被明确陈述。

评估者***应检查***安全要求基本原理，以确定它恰当地证明了为何每个明确陈述的IT安全要求应要被明确陈述。

评估者确定对于每个明确陈述的IT安全要求，证明应解释为什么已有的功能或保证组件(分别选自ISO/IEC 15408-2和ISO/IEC 15408-3)不能用于表达所讨论的明确陈述IT安全要求。在做出决定时，评估者应该考虑对已有的功能或保证组件实施诸如赋值、反复或细化等操作的可能性。

9.3.7.4.4 工作单元 ASE_SRE.1-4

ISO/IEC 15408-3 ASE_SRE.1.4C 明确陈述的 IT 安全要求应以 ISO/IEC 15408 的要求组件、族和类作为表述的模板。

评估者***应检查***每个明确陈述的IT安全要求，以确定该要求用ISO/IEC 15408要求的组件、族和类作为表述的模板。

评估者确定明确陈述的IT安全要求与ISO/IEC 15408-2或ISO/IEC 15408-3组件的表述形式相同且达到相当的详细程度。评估者还确定功能要求被分解成单个功能元素，并且保证要求详细说明了开发者行为元素、证据的内容和形式元素以及评估者行为元素。

9.3.7.4.5 工作单元 ASE_SRE.1-5

ISO/IEC 15408-3 ASE_SRE.1.5C 明确陈述的IT安全要求应是可度量的，并陈述了客观的评估要求，这样就可以决定和系统地证实一个TOE是否遵从这些要求。

评估者***应检查***每个明确陈述的IT安全要求，以确定它是可度量的并陈述了客观的评估要求，这样就能决定并系统地证实一个TOE是否遵从这些要求。

评估者确定功能要求以某种方式表述，使得它们是可测试的，并且是可通过适当的TSF表述进行追溯的。评估者还确定保证要求避免了要求评估者做出主观判定。

已有的ISO/IEC 15408功能和保证要求都可以用作遵从这一要求的模板。

9.3.7.4.6 工作单元 ASE_SRE.1-6

ISO/IEC 15408-3 ASE_SRE.1.6C 明确陈述的IT安全要求应被清楚且无歧义地表述。

评估者***应检查***每个明确陈述的IT安全要求，以确定其表述是清楚且无歧义的。

已有的ISO/IEC 15408功能和保证要求都可以用作遵从这一要求的模板。

9.3.7.4.7 工作单元 ASE_SRE.1-7

ISO/IEC 15408-3 ASE_SRE.1.7C 安全要求基本原理应证实保证要求是适用的，并且适合于支持任何明确陈述的TOE安全功能要求。

评估者***应检查***安全要求基本原理，以确定它证实了保证要求是适用的，并且适合于支持任何明确陈述的TOE安全功能要求。

评估者确定特定保证要求的应用是否会得到关于每个明确陈述的安全功能要求的有意义的评估结果，或者是否应指定其他保证要求。比如，一个明确陈述的功能要求可能隐含要求特殊的文档证据（诸如一个TSP模型）、测试深度或分析（诸如TOE安全功能强度分析或隐蔽通道分析）。

9.3.7.5 行为 ASE_SRE.1.2E

9.3.7.5.1 工作单元 ASE_SRE.1-8

评估者***应检查***IT安全要求陈述，以确定任何明确陈述的IT安全功能要求的所有依赖关系都已被标识。

评估者确认ST作者没有忽略任何可用的依赖关系。

可能存在依赖关系的例子有：如果明确陈述的功能要求提到审计，则可能与FAU“安全审计”类的组件有依赖关系；如果明确陈述的保证要求提到源代码或TOE实现表述，则可能与ADV_IMP“实现表示”有依赖关系。

9.3.8 TOE概要规范的评估（ASE_TSS.1）

9.3.8.1 目的

本子活动的目的是确定TOE概要规范是否为安全功能和安全保障措施提供了清晰的、一致的高层定义，且满足指定的TOE安全要求。

9.3.8.2 输入

本子活动的评估证据是：

a) ST。

9.3.8.3 行为 ASE_TSS.1.1E

9.3.8.3.1 工作单元 ASE_TSS.1-1

ISO/IEC 15408-3 ASE_TSS.1.1C TOE 概要规范应描述 TOE 的 IT 安全功能和保证措施。

评估者***应核查***TOE 概要规范，是否描述了 TOE 的 IT 安全功能和保证措施。

评估者确认 TOE 概要规范提供了声称满足 TOE 安全功能要求的安全功能高层定义和声称满足 TOE 安全保证要求的保证措施高层定义。

保证措施可以通过引用满足安全保证要求的文件（如相关质量计划、生命周期计划、管理计划）来明确陈述或定义。

9.3.8.3.2 工作单元 ASE_TSS.1-2

ISO/IEC 15408-3 ASE_TSS.1.2C TOE 概要规范应把 IT 安全功能追溯到 TOE 安全功能要求，这样就能看出哪个 IT 安全功能满足了哪个 TOE 安全功能要求，以及每个 IT 安全功能是否至少满足一个 TOE 安全功能要求。

评估者***应核查***TOE 概要规范，以确定每个 IT 安全功能是否至少回溯到了一个 TOE 安全功能要求。

如果不能追溯，则表明 TOE 概要规范是不完备的，或 TOE 安全功能要求是不完备的，或 IT 安全功能没有实际意义。

9.3.8.3.3 工作单元 ASE_TSS.1-3

ISO/IEC 15408-3 ASE_TSS.1.3C 应用一个非形式化的方式定义 IT 安全功能，其详细程度需达到其意图可被理解的水平。

评估者***应检查***每个 IT 安全功能，以确定它是否以非形式化的方式进行描述，且详细程度达到了可以理解其意图的水平。

有时，一个 IT 安全功能并不比对应的一个或多个 TOE 安全功能要求提供更详细的信息。此外，ST 作者可能包括一些 TOE 特定细节，例如用 TOE 的特定术语来代替诸如“安全特性”这类一般术语。

注意，此处不允许对 IT 安全功能做半形式化或形式化的描述，除非对同一安全功能还伴有一个非形式化描述。此处目的是要理解功能的含义，而不是确定诸如功能的完整性或正确性之类的属性。

9.3.8.3.4 工作单元 ASE_TSS.1-4

ISO/IEC 15408-3 ASE_TSS.1.4C 对 ST 中所包含安全机制的所有引用，应追溯到相应的安全功能，这样就能看出在每个功能实现中使用了哪些安全机制。

评估者***应检查***TOE 概要规范，以确定 ST 中安全机制的所有引用都可追溯到 IT 安全功能。

在 ST 中对安全机制的引用是可选的，比如在要求实现特殊协议或算法（如特定的口令产生或加密算法）时才适用。如果 ST 没有包含安全机制的引用，则本工作单元不适用，并视为已经满足。

评估者确定 ST 所引用的每个安全机制都能追溯到至少一个 IT 安全功能。

如果不能追溯，则表明 TOE 概要规范是不完备的，或者安全机制没有实际意义。

9.3.8.3.5 工作单元 ASE_TSS.1-5

ISO/IEC 15408-3 ASE_TSS.1.5C TOE 概要规范的基本原理应证实 IT 安全功能恰好满足 TOE 安全功能要求。

评估者***应检查***TOE 概要规范基本原理，以确定对于每个 TOE 安全功能要求而言，它都包含了证明 IT 安全功能恰好满足 TOE 安全功能要求的合适理由。

如果没有 IT 安全功能追溯到 TOE 安全功能要求，则本工作单元为“不通过”。

评估者确定有关 TOE 安全功能要求的证明阐明了：如果所有追溯到 TOE 安全功能要求的 IT 安全功能都已实现，则该 TOE 安全功能要求就得到满足。

评估者还确定每个可追溯到 TOE 安全功能要求的 IT 安全功能，当其实现时，实际上促成了 TOE 安全功能要求的满足。

注意，将 TOE 概要规范中提供的 IT 安全功能追溯到 TOE 安全功能要求，可以作为证明的一部分，但其本身并不构成证明。

9.3.8.3.6 工作单元 ASE_TSS.1-6

评估者***应检查***TOE 概要规范的基本原理，以确定为 IT 安全功能声称的功能强度与 TOE 安全功能要求的功能强度是一致的。

本工作单元利用 ASE_TSS.1-10 工作单元的评估结果。

评估者确定每个 IT 安全功能的功能强度声明都是适当的，且 TOE 概要规范基本原理证明了该声明对所有它可追溯到的 TOE 安全功能要求都是足够的。

通常足够的含义是指 IT 安全功能的功能强度声明相当于或高于所有 TOE 安全功能要求的功能强度，但是可能有例外。比如，在鉴别中，连续使用多个低强度的功能实现一个中等强度的鉴别要求（如生物测定和 PIN）。

9.3.8.3.7 工作单元 ASE_TSS.1-7

ISO/IEC 15408-3 ASE_TSS.1.6C TOE 概要规范的基本原理应证实特定的 IT 安全功能组合在一起能够满足 TOE 安全功能要求。

评估者***应检查***TOE 概要规范的基本原理，以确定它证明了特定的 IT 安全功能组合在一起能够满足 TOE 安全功能要求。

本工作单元建立在工作单元 ASE_REQ.1-23 中对 TOE 安全功能要求实施互相支持决定的基础上。在分析时，评估者应该评价包含在 IT 安全功能中附加信息的影响，以确定包含这类信息不会引入潜在的安全脆弱性，如绕过、篡改和使其他安全功能失效。

9.3.8.3.8 工作单元 ASE_TSS.1-8

ISO/IEC 15408-3 ASE_TSS.1.7C TOE 概要规范应把保证措施追溯到保证要求，这样就能看出哪个措施有助于满足哪个要求。

评估者***应核查***TOE 概要规范，以确定每个保证措施至少能追溯到一个 TOE 安全保证要求。

如果不能追溯，则表明 TOE 概要规范或 TOE 安全保证要求的陈述是不完备的，或者保证措施没有实际意义。

9.3.8.3.9 工作单元 ASE_TSS.1-9

ISO/IEC 15408-3 ASE_TSS.1.8C TOE 概要规范的基本原理应证实保证措施满足 TOE 所有的保证要求。

评估者***应检查***TOE概要规范基本原理，以确定对于每个TOE保证要求而言，它都包含了证明保证措施满足对应的TOE安全保证要求的适当理由。

如果没有保证措施追溯到TOE安全保证要求，则本工作单元为“不通过”。

评估者确定有关TOE安全保证要求的证明阐明了：如果所有追溯到TOE安全保证要求的保证措施都已实现，那么该TOE安全保证要求就得到满足。

评估者还确定每个可追溯到TOE安全保证要求的保证措施，当其实现时，实际上促成了TOE安全保证要求的满足。

保证措施描述了开发者如何处理保证要求。本工作单元的目的是确定特定的保证措施恰好满足保证要求。

注意，将TOE概要规范中提供的保证措施追溯TOE安全保证要求，可以作为证明的一部分，但其本身并不构成证明。

9.3.8.3.10 工作单元 ASE_TSS.1-10

ISO/IEC 15408-3 ASE_TSS.1.9C 适当时，TOE概要规范应标识所有由概率或置换机制实现的IT安全功能。

评估者***应核查***TOE概要规范，是否标识了所有由概率或置换机制实现的IT安全功能。

如果TOE安全保证要求不包括AVA_SOF.1“TOE安全功能强度评估”，则本工作单元不适用，并视为已经满足。

如果对其他评估证据分析后，发现置换或概率机制并不像ST中标识出那样的话，可以再次使用本工作单元。

9.3.8.3.11 工作单元 ASE_TSS.1.11

ISO/IEC 15408-3 ASE_TSS.1.10C TOE概要规范应对每一个适当的IT安全功能提出其功能强度声明，要么为一个特定的尺度，要么为基本级功能强度、中级功能强度、高级功能强度中的一个。

评估者***应核查***每个IT安全功能是否适于规定一个功能强度声明，TOE概要规范提出功能强度声明要么为一个特定的尺度，要么为基本级功能强度、中级功能强度、高级功能强度中的一个。

如果TOE安全保证要求不包括AVA_SOF.1“TOE安全功能强度评估”，则本工作单元不适用，并视为已经满足。

9.3.8.4 行为 ASE_TSS.1.2E

9.3.8.4.1 工作单元 ASE_TSS.1-12

评估者***应检查***TOE概要规范，以确定它是完备的。

如果评估者判定IT安全功能和保证措施足以保证所有指定的TOE安全要求都已满足，那么TOE概要规范是完备的。本工作单元应与工作单元ASE_TSS.1-5和ASE_TSS.1-9一起使用。

9.3.8.4.2 工作单元 ASE_TSS.1-13

评估者***应检查***TOE概要规范，以确定它是有条理的。

如果TOE概要规范的文本和结构都能被其目标读者（例如：评估者和开发者）理解的，TOE概要规范就是有条理的。

9.3.8.4.3 工作单元 ASE_TSS.1-14

评估者***应检查***TOE概要规范，以确定它是内在一致的。

如果评估者确定 IT 安全功能或保证措施之间没有冲突,因为冲突的话 TOE 安全要求就不能被完全满足,那么 TOE 概要规范就是内在一致的。

一致性分析指南见 A.3“一致性分析”。

10 EAL1 评估

10.1 简介

EAL1 提供了一种基本级别的保证。评估者使用功能规范和指导性文档,对安全功能进行分析,以理解安全行为,并进行 TOE 安全功能子集的独立性测试。

10.2 目的

本章的目的是定义达到 EAL1 级评估所需的最少的评估工作,并对完成评估的方式方法提供指导。

10.3 EAL1 评估相互关系

EAL1 评估包括以下活动:

a) 评估输入任务(第 7 章)。

b) EAL1 评估活动包括:

1) ST 评估(第 9 章);

2) 配置管理评估(10.4);

3) 交付和运行文档评估(10.5);

4) 开发文档评估(10.6);

5) 指导性文档评估(10.7);

6) 测试(10.8)。

c) 评估输出任务(第 7 章)。

评估活动源于 ISO/IEC 15408-3 所包含的 EAL1 保证要求。

ST 评估应在所有 TOE 评估子活动之前启动,因为 ST 为执行这些评估子活动提供了基础和背景。

本章描述了构成 EAL1 评估的子活动。尽管各子活动通常可以不同程度的并行,但评估者应考虑子活动间的依赖关系。

有关依赖关系的指南见附录 A。

10.4 配置管理活动

配置管理活动的目的是帮助用户识别被评估的 TOE。

10.4.1 CM 能力评估(ACM_CAP.1)

10.4.1.1 目的

本子活动的目的是确定开发者是否已清楚地标识了 TOE。

10.4.1.2 输入

本子活动的评估证据是:

a) ST;

b) 适于测试的 TOE。

10.4.1.3 行为 ACM_CAP.1.1E

10.4.1.3.1 工作单元 1:ACM_CAP.1-1

ISO/IEC 15408-3 ACM_CAP.1.1C TOE 参照号对 TOE 的每个版本都应当是唯一的。

评估者***应核查***用于评估的 TOE 版本有唯一的参照号。

该保证组件除了要求唯一的参照号外,并不要求开发者使用 CM 系统。因此评估者可以通过核查其他可采购的 TOE 版本有没有相同的参照号,来核实 TOE 版本的唯一性。如果评估中采用了高于 ISO/IEC 15408 要求的 CM 系统,那么评估者可通过核查配置清单来确认参照号的唯一性。如果在评估过程中仅仅检查了一个版本,该项评估证据是不完备的,因此评估者应该查找能够支持唯一参照号的参照系统(比如使用数字、字母或日期)。除非评估者确信该 TOE 能够被唯一标识,否则缺少任何一项参照都将导致对这项要求裁定为“不通过”。

评估者应该设法检查多个 TOE 版本(比如,修正某个漏洞后的版本),以核查两个版本参照号的不同。

10.4.1.3.2 工作单元 1:ACM_CAP.1-2

ISO/IEC 15408-3 ACM_CAP.1.2C 应给 TOE 标记上参照号。

评估者***应核查***所提交评估的 TOE 是否标记了参照号。

评估者应确保 TOE 包含唯一的参照号,以便区分 TOE 的不同版本。这可以通过提供在包装或介质上粘贴标签,或让 TOE 在运行时显示标记等措施来实现,以保证客户在购买或使用时能够识别出 TOE。

TOE 可提供某种方式使得它易于识别。例如,软件形式的 TOE 可以在其启动例程中,或者在响应命令行输入时,显示其名称和版本号。硬件或固件形式的 TOE 可以通过将部件号铭刻在 TOE 上来标识。

10.4.1.3.3 工作单元 1:ACM_CAP.1-3

评估者***应核查***所使用的 TOE 参照号的一致性。

如果 TOE 要多处标记,所有的标记应当是一致的。例如,作为 TOE 一部分而提交的任何一份已标记过的指导性文档都应与被评估的、使用的 TOE 相关。这样就可以确保客户能确认自己所购买和安装的 TOE 版本是经过评估的,并且他们所使用的指南与 ST 一致,可以正确的指导自己使用 TOE。

评估者还应验证该 TOE 参照号是否与 ST 一致。

有关一致性分析的指南参见 A.3“一致性分析”。

10.5 交付和运行活动

交付和运行活动的目的是判断描述用以确保按照开发者期望的方式安装、生成和启动 TOE 程序的文档内容是否充分。

10.5.1 安装、生成和启动评估(ADO_IGS.1)

10.5.1.1 目的

本子活动的目的是确定 TOE 的安全安装、生成和启动程序与步骤是否都已文档化,并最终形成安全的配置。

10.5.1.2 输入

本子活动的评估证据是：

a) 管理员指南；

b) 安全安装、生成和启动程序；

c) 适于测试的 TOE。

10.5.1.3 应用注释

安装、生成和启动程序是指配置 TOE 达到在 ST 中所描述的安全配置所必需的所有安装、生成和启动过程，无论它们是运行在用户现场，还是运行在开发现场。

10.5.1.4 行为 ADO_IGS.1.1E

10.5.1.4.1 工作单元 1：ADO_IGS.1-1

ISO/IEC 15408-3 ADO_IGS.1.1C 安装、生成和启动文档应描述 TOE 安全的安装、生成和启动所必需的所有步骤。

评估者***应核查***是否已经提供了 TOE 安全安装、生成和启动所必需的所有程序。

如果不期望安装、生成和启动程序再次使用(例如，TOE 已经在运行状态下交付)，本工作单元(或者与此相关的部分)就不再适用，并视为已经满足。

10.5.1.5 行为 ADO_IGS.1.2E

10.5.1.5.1 工作单元 1：ADO_IGS.1-2

评估者***应检查***所提供的安装、生成和启动程序，以确认其描述了 TOE 安全安装、生成和启动所需的步骤。

如果不期望安装、生成、启动程序再次使用(例如，TOE 已经在运行状态下交付)，本工作单元(或者与此相关的部分)就不再适用，并视为已经满足。

安装、生成和启动程序可以提供以下详细信息：

a) 对 TSF 控制下相关实体的特定安全特性所做的修改；

b) 对异常情况和问题的处理；

c) 如果适用，列出安全安装所需的最低系统要求。

为了确认安装、生成和启动程序能够形成安全配置，评估者可以只使用所提供的指导性文档，按照开发者的程序，实施客户通常执行的活动以完成对 TOE 的安装、生成和启动(在适用于 TOE 的情况下)。本工作单元可以与工作单元 ATE_IND.1-2 一起被执行。

10.6 开发活动

开发活动的目的是评价设计文档，根据设计文档的充分性来理解 TSF 是如何提供 TOE 安全功能，以此来进行评价。这种理解是通过检查功能规范(描述 TOE 的外部接口)和表示对应性(将功能规范映射到 TOE 的概要规范，以保证一致性)来获得的。

10.6.1 应用注释

ISO/IEC 15408 要求设计文档根据形式化程度来分级。ISO/IEC 15408 将文档的形式化程度分为非形式化、半形式化、形式化三级。非形式化文档是指用自然语言来描述的文档。评估方法没有规定应采用某种语言，这个问题留给评估体制来解决。以下段落分别说明了不同的非形式化文档内容的差别。

一个非形式化功能规范包括一个安全功能描述(类似于 TOE 概要规范的安全功能描述)和一个 TSF 外部可见接口描述。例如,如果操作系统提供给用户一些功能来进行自我身份标识,创建、修改或删除文件,设置文件的访问权限,与远程的机器进行通信,那么它的功能规范应包含对上述每一个功能的描述。如果还有检测和记录这些事件发生的审计功能,那么关于这些审计功能的描述也应该包含在功能规范中;尽管这些审计功能不直接被用户在外部接口所触发,但用户在外部接口的行为的确会对审计功能产生影响。

非形式化的对应性分析不需要采用叙述的方式,一个简单的二维映射就足够了。例如,一个矩阵,沿一个轴的方向列出了模块,沿另一个方向列出了子系统,其中的元素表示两者的对应性,这将在高层设计和低层设计之间提供足够的非形式化对应性。

10.6.2 功能规范评估(ADV_FSP.1)

10.6.2.1 目的

本子活动的目的是确认开发者对 TOE 安全功能是否作了充分描述,以及 TOE 提供的安全功能是否充分足以满足 ST 的安全功能要求。

10.6.2.2 输入

本子活动的评估证据是:

a) ST;
b) 功能规范;
c) 用户指南;
d) 管理员指南。

10.6.2.3 行为 ADV_FSP.1.1E

10.6.2.3.1 工作单元 1:ADV_FSP.1-1

ISO/IEC 15408-3ADV_FSP.1.1C 功能规范应使用非形式化风格来描述 TSF 及其外部接口。

评估者***应检查***功能规范,以确定其包括了所有必需的非形式化解释文本。

如果整个功能规范都是非形式化的,则本工作单元不适用,并视为已经满足要求。

对于那些只采用半形式化或形式化语言进行描述,难以被人理解的功能规范的某些组成部分(例如,为解释任何形式化符号的含义),有必要使用辅助性的叙述描述来帮助理解。

10.6.2.3.2 工作单元 1:ADV_FSP.1-2

ISO/IEC 15408-3ADV_FSP.1.2C 功能规范应是内在一致的。

评估者***应检查***功能规范,以确定它是内在一致的。

评估者通过检查 TSFI 接口描述与 TSF 功能描述是否一致来验证功能规范的一致性。

10.6.2.3.3 工作单元 1:ADV_FSP.1-3

ISO/IEC 15408-3 ADV_FSP.1.3C 功能规范应描述所有外部 TSF 接口的用途与使用方法,适当时应提供效果、例外情况和错误消息的细节。

评估者***应检查***功能规范,以确定其标识了所有的外部 TOE 安全功能接口。

术语"外部"指对用户而言是可见的。TOE 的外部接口或者是 TSF 的直接接口,或者是 TOE 的非 TSF 部分的接口。不过,这些非 TSF 接口可能最终通向 TSF。这些直接或间接通向 TSF 的外部接口共同组成了 TOE 安全功能接口(TSFI)。图 6 表示一个包含 TSF 部分(阴影部分)和非 TSF 部分(空白

部分)的 TOE。该 TOE 有三个外部接口:接口 c 是 TSF 的直接接口;接口 b 是 TSF 的间接接口;接口 a 是 TOE 非 TSF 部分的接口。因此,接口 b 和 c 组成了 TSFI。

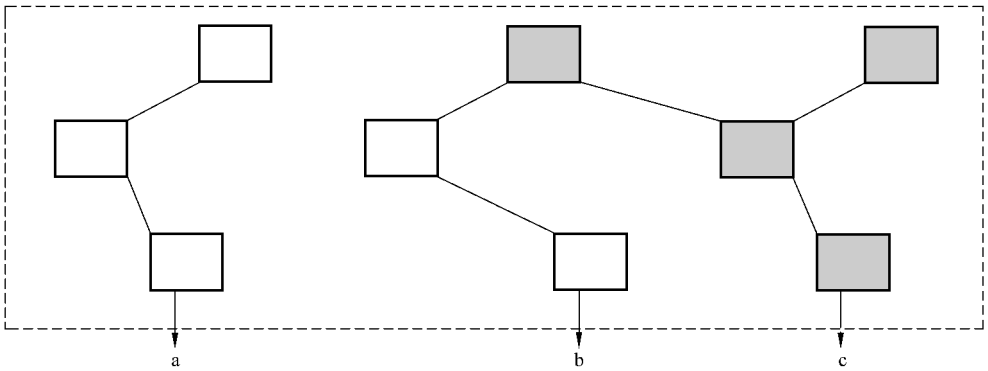

图 6　TSF 接口

应该注意的是,所有反映 ISO/IEC 15408-2 功能要求(或者在其扩展组件中)的安全功能应该有某种外部可见的表现形式。尽管有些安全功能不一定能通过其接口来验证,但由于它们在某种程度上是外部可见的,因此也应包含在功能规范中。

10.6.2.3.4　工作单元 1:ADV_FSP.1-4

评估者***应检查***功能规范,以确定其描述了所有外部的 TOE 安全功能接口。

对于一个没有恶意用户威胁的 TOE(即 FPT_PHP“TSF 物理保护”、FPT_RVM“参照仲裁”和 FPT_SEP“域分离”都被排除在 ST 之外),功能规范中描述的(和在其他 TSF 表示描述中进行了扩展的)只是那些通向和来自 TSF 的接口。缺少 FPT_PHP“TSF 物理保护”、FPT_RVM“参照仲裁”和 FPT_SEP“域分离”,就假设没有考虑任何安全特性的旁路,因而不用考虑其他接口可能施加给 TSF 的任何可能的影响。

另一方面,如果 TOE 存在恶意用户或旁路之类的威胁(即 FPT_PHP“TSF 物理保护”、FPT_RVM“参照仲裁”和 FPT_SEP“域分离”被包含在 ST 中),所有外部接口都需要在功能规范中进行描述,但是仅需描述到每一种影响都已明确的程度:安全功能的接口(即图 6 中的接口 b 和 c)都被描述了,然而其他接口仅仅描述到明确 TSF 不能通过这些接口(即图 6 中的接口 a,而不是 b)访问的程度。包含 FPT_PHP“TSF 物理保护”、FPT_RVM“参照仲裁”和 FPT_SEP“域分离”,意味着所有的接口将对 TSF 有某些影响。由于每一个外部接口都是潜在的 TSF 接口,因此,功能规范应对每一个接口进行详细的描述,以使得评估者能够确定接口是否与安全相关。

某些体系结构易于为外部接口群提供足够详细的描述。例如,在内核结构中所有对操作系统的调用都由内核程序来处理;任何有可能违反 TSP 的调用应由具备这种特权的程序来调用。所有实行特权的程序应被包含在功能规范中。任何在内核之外的没有实行特权的程序是无能力影响 TSP 的(即,这种程序是图 6 中的 a 类的接口,而不是 b 类),因而,可以被排除在功能规范之外。如果是基于上述的内核结构,而且评估者对这种结构能够顺利的了解,那么这种结构不是必需的。

10.6.2.3.5　工作单元 1:ADV_FSP.1-5

评估者***应检查***对 TSFI 的陈述,以确定其正确并充分地描述了每个表示效果、异常和出错信息的外部接口处的 TOE 行为。

为了评估接口描述的充分性和正确性,评估者使用功能规范、ST 的 TOE 概要规范以及用户和管理员指南来评估以下因素:

a) 应标识所有与安全相关的用户输入参数(或这些参数的特性)。为了全面起见,宜标识出管理员可用而普通用户无法直接控制的参数。

b) 对功能规范中语义的描述应当反映所审查指南中描述的所有安全相关行为。它包括一系列通过事件及其影响所表示的行为标识。例如,如果一个操作系统提供了丰富的文件系统接口,并对请求文件无法打开的各种原因(如拒绝访问、文件不存在、文件正被另一个用户使用、用户无权在下午 5 点后打开文件等)提供了不同的错误代码,功能规范应当解释该文件或者在请求下被打开,如不能打开则返回错误代码。(虽然功能规范可以列举所有错误的原因,但不需要提供细节描述)。对语义的描述应当包括安全要求如何应用于接口(例如,是否可以审计接口的使用情况,假如这样的话,应包含能够记录的信息)。

c) 应描述所有可能操作模式下的所有接口。如果 TSF 提供了特权的概念,对接口的描述应分别解释特权模式或非特权模式时,接口的工作方式。

d) 整个文档中安全相关参数的描述和接口的语法所包含的信息应当是一致的。

对以上因素的核实,是通过审核安全规范和 ST 的 TOE 概要规范、开发者提供的用户和管理员指南来完成的。例如,如果 TOE 是一个操作系统及其底层硬件,评估者可以查找用户可访问的程序的讨论、用于指导程序活动的协议的描述、用于指导程序活动的用户可访问数据库的描述,并查找适用于 TOE 的用户接口(例如命令、应用程序接口)。评估者还要确定处理器的指令集已进行描述。

这种核查可以反复进行,直到包含参数和出错信息的设计、源代码或其他证据都被检查为止,以避免发生功能规范描述不全的情况被评估者忽略。

10.6.2.3.6 工作单元 1:ADV_FSP.1-6

ISO/IEC 15408-3 ADV_FSP.1.4C 功能规范应完备地表示 TSF。

评估者***应检查***功能规范,以确定 TSF 已被完全表示。

为了评估 TSF 表示的完备性,评估者可查阅 ST 的 TOE 概要规范、用户指南和管理员指南。它们应当没有描述在功能规范的 TSF 表示中没有的安全功能。

10.6.2.4 行为 ADV_FSP.1.2E

10.6.2.4.1 工作单元 1:ADV_FSP.1-7

评估者***应检查***功能规范,以确定它是 TOE 安全功能要求的一个完备地实例。

为了确保功能规范涵盖了所有的 ST 安全功能要求,评估者应当建立 TOE 概要规范和功能规范之间的映射。为了满足(ADV_RCR.*“表示对应性”)的对应要求,开发者可能已经提交了这种映射证据;这时评估者只需要验证映射的完备性,确定所有的安全功能要求都映射到功能规范中适当的 TSFI 表示。

10.6.2.4.2 工作单元 1:ADV_FSP.1-8

评估者***应检查***功能规范,以确定它是 TOE 安全功能要求的一个准确实例化。

对于每个具有某种特性的安全功能的接口,功能规范中的详细信息应与 ST 中的相关信息所表述准确一致。例如,如果 ST 中的用户鉴别要求规定了口令长度应为 8 个字符,那么 TOE 应有 8 个字符的口令;如果功能规范描述的是 6 字符的固定长度口令,那么功能规范就不是 TOE 安全功能要求的一个准确实例化。

功能规范中对在受控资源上运行的每个接口,评估者应确定它是否返回了一个错误代码,该错误代码是因为某个安全要求的实施失败而导致的,如果没有返回错误代码,评估者应确定是否需要返回一个错误代码。例如,操作系统可以提供一个接口用于打开一个受控对象,该接口描述中可包含因对受控对

象作了未授权的访问而产生的一个错误代码。如果没有这种错误代码,评估者应当确认是否合理(因为,也许访问仲裁是针对读、写的操作执行的,而不是针对打开的)。

10.6.3 表示对应性评估(ADV_RCR.1)

10.6.3.1 目的

本子活动的目的是确定开发者是否在功能规范中正确且完备地执行了 ST 的要求。

10.6.3.2 输入

本子活动的评估证据是:

a) ST;

b) 功能规范;

c) TOE 概要规范和功能规范之间的对应性分析。

10.6.3.3 行为 ADV_RCR.1.1E

ISO/IEC 15408-3 ADV_RCR.1.1C 对于所提供 TSF 表示的每个相邻对,分析应证实,较为抽象的 TSF 表示的所有相关安全功能都在较不抽象的 TSF 表示中得到正确且完备地细化。

10.6.3.3.1 工作单元 1:ADV_RCR.1-1

评估者***应检查***TOE 概要规范和功能规范之间的对应性分析,以确认功能规范是 TOE 安全功能的一个正确且完备的表示。

本工作单元中,评估者的目的是确定 TOE 概要规范中标识的所有安全功能都在功能规范中得到了体现并且是准确地体现。

评估者审核 TOE 概要规范中的 TOE 安全功能和功能规范中的 TOE 安全功能之间的对应性。评估者检查对应的一致性和准确性。当对应性分析中指明了 TOE 概要规范中的一个安全功能和功能规范中一个接口描述之间的关系时,评估者应验证两者中描述的是同一个安全功能。如果 TOE 概要规范的安全功能在所对应的接口中能够正确且完备地实现,那么本工作单元将被视为满足。

本工作单元可与工作单元 ADV_FSP.1-7 和 ADV_FSP.1-8 关联使用。

10.7 指导性文档活动

指导性文档活动的目的是判断该文档是否充分描述了应如何操作 TOE。这些文档针对两类用户:一类是可信的管理员和非管理员用户,他们的不正确行为可能影响 TOE 安全性,另一类是那些不可信用户,他们的不正确行为可能影响其拥有的数据的安全性。

10.7.1 应用注释

指导性文档活动关注那些与 TOE 安全性相关的功能和接口。TOE 的安全配置在 ST 中进行了描述。

10.7.2 管理员指南评估(AGD_AMD.1)

10.7.2.1 目的

本子活动的目的是确定管理员指南是否描述了如何以安全方式管理 TOE。

10.7.2.2 输入

本子活动的评估证据是:

a) ST；
b) 功能规范；
c) 用户指南；
d) 管理员指南；
e) 安全安装、生成和启动程序；
f) 生命周期定义。

10.7.2.3 应用注释

术语“管理员”指在 TOE 中执行关键安全操作(例如,设置 TOE 配置参数)的可信人员。这些操作可能影响 TSP 的执行,因此管理员拥有特殊的权限来执行这些操作。管理员角色应当与 TOE 中的非管理员用户角色明确区分开。

在 ST 中可定义有不同的管理员角色或管理员组,这些角色和组能可被 TOE 识别并可执行 TOE 的安全功能,例如审计员、管理员或日常管理者。每个角色可能具备多种或一种能力。这些角色的能力和相应的特权在 FMT 类中进行描述。管理员指南中应考虑不同的管理员角色和管理员组。

10.7.2.4 行为 AGD_ADM.1.1E

10.7.2.4.1 工作单元 1:AGD_ADM.1-1

ISO/IEC 15408-3 AGD_ADM.1.1C 管理员指南应描述 TOE 管理员可使用的管理功能和接口。

评估者***应检查***管理员指南,以确定其描述了 TOE 管理员可用的管理性安全功能和接口。

管理员指南应包含安全功能的概述,这些安全功能在管理员界面中是可见的。

管理员指南应标识并描述管理性安全接口与功能的用途、行为和相互关系。

对于每个管理性安全接口和功能,管理员指南应当:

a) 描述调用接口的方法(如命令行、程序语言系统调用、菜单选择、命令按钮);
b) 描述由管理员设置的参数及其有效值和默认值;
c) 描述即时的 TSF 响应、消息或返回代码。

10.7.2.4.2 工作单元 1:AGD_ADM.1-2

ISO/IEC 15408-3 AGD_ADM.1.2C 管理员指南应描述如何以安全的方式管理 TOE。

评估者***应检查***管理员指南,以确定它描述了如何以安全的方式管理 TOE。

管理员指南描述如何在 IT 环境中依照 TSP 运行 TOE,这应与 ST 所描述的情况一致。

10.7.2.4.3 工作单元 1:AGD_ADM.1-3

ISO/IEC 15408-3 AGD_ADM.1.3C 管理员指南应包含了在安全处理环境中受控的功能和特权的警示信息。

评估者***应检查***管理员指南,以确定其包含了在安全处理环境中受控的功能和特权的警示信息。

TOE 的配置可以允许用户拥有不同的特权来使用 TOE 的不同功能,这意味着可以授权某些用户执行某些功能,而其他用户无权执行,这些功能和特权应在管理员指南中进行描述。

管理员指南应标识出应控制的功能和特权、控制的类型以及控制的理由。警告应说明预期的效果、可能的负面影响以及与其他功能和特权可能的相互作用。

10.7.2.4.4 工作单元 1:AGD_ADM.1-4

ISO/IEC 15408-3 AGD_ADM.1.4C 管理员指南应描述所有与安全操作 TOE 有关的用户行为假设。

评估者*应检查*管理员指南,以确定它描述了所有与安全操作 TOE 有关的用户行为假设。

关于用户行为的假设可以在 ST 的 TOE 安全环境陈述中比较详细的描述,而只有涉及安全操作 TOE 的信息才需要包含在管理员指南中。

例如,要安全操作 TOE 用户有责任对他们的口令进行保密。

10.7.2.4.5 工作单元 1:AGD_ADM.1-5

ISO/IEC 15408-3 AGD_ADM.1.5C 管理员指南应描述所有受管理员控制的安全参数,并说明适当的安全值。

评估者*应检查*管理员指南,以确定它描述了所有受管理员控制的安全参数,并说明适当的安全值。

对于每个安全参数,管理员指南应描述参数的用途、参数的有效值和缺省值,以及这些参数安全与非安全的使用设置。这些参数可以分别描述,也可以综合起来描述。

10.7.2.4.6 工作单元 1:AGD_ADM.1-6

ISO/IEC 15408-3 AGD_ADM.1.6C 管理员指南应描述每一种与需要执行的管理功能有关的安全相关事件,包括改变在 TSF 控制下的实体的安全特性。

评估者*应检查*管理员指南,以确定它描述了每一种与需要执行的管理功能有关的安全相关事件,包括改变在 TSF 控制下的实体的安全特性。

应详尽描述所有类型的安全相关事件,以便管理员知道可能发生什么事件以及为保持安全管理员应采取哪些动作。应充分定义在 TOE 的操作过程中可能发生的安全相关事件(例如,审计迹的溢出、系统崩溃、用户记录的更新——如当用户离开组织时撤消该用户账号),以允许管理员介入来保持安全。

10.7.2.4.7 工作单元 1:AGD_ADM.1-7

ISO/IEC 15408-3 AGD_ADM.1.7C 管理员指南应与评估提交的所有其他文档保持一致。

评估者*应检查*管理员指南,以确定它与评估提交的所有其他文档是一致的。

特别是在 ST 中可能包含一些对 TOE 管理员提出的关于 TOE 安全环境和安全目的的详细的警告信息。

有关一致性分析的指南参见 A.3“一致性分析”。

10.7.2.4.8 工作单元 1:AGD_ADM.1-8

ISO/IEC 15408-3 AGD_ADM.1.8C 管理员指南应描述所有与管理员有关的 IT 环境安全要求。

评估者*应检查*管理员指南,以确定它描述了所有与管理员有关的 TOE 的 IT 环境安全要求。

如果 ST 中不包含 IT 环境的 IT 安全要求,本工作单元不适用,并视为已经满足。

本工作单元仅与 IT 安全要求有关,而与组织安全策略无关。

评估者应当分析关于 TOE 的 IT 环境安全要求(ST 中的可选陈述),并与管理员指南比较,以确保 ST 中与管理员有关的所有安全要求都在管理员指南中得到适当的描述。

10.7.3 用户指南评估(AGD_USR.1)

10.7.3.1 目的

本子活动的目的是为了确定用户指南是否描述了由 TSF 提供的安全功能和接口,以及指南是否提供了安全使用 TOE 的相关说明和指导。

10.7.3.2 输入

本子活动的评估证据是：

a) ST；
b) 功能规范；
c) 高层设计；
d) 用户指南；
e) 管理员指南；
f) 安全安装、生成和启动程序。

10.7.3.3 应用注释

在 ST 中可定义不同的用户角色或用户组，这些角色和组能被 TOE 识别并可执行 TOE 的安全功能。这些角色的能力和相应的特权在 FMT 类中进行描述。用户指南中应考虑不同的用户角色和组。

10.7.3.4 行为 AGD_USR.1.1E

10.7.3.4.1 工作单元 1：AGD_USR.1-1

ISO/IEC 15408-3 AGD_USR.1.1C 用户指南应描述 TOE 的非管理员用户可使用的功能和接口。

评估者***应检查***用户指南，以确定其描述了 TOE 的非管理员用户可使用的安全功能和接口。

用户指南应包含安全功能的概述，这些安全功能在用户界面中可见的。

用户指南应当标识和描述安全接口和功能的用途。

10.7.3.4.2 工作单元 1：AGD-USR.1-2

ISO/IEC 15408-3 AGD_USR.1.2C 用户指南应描述用户可访问的由 TOE 提供的安全功能的使用。

评估者***应检查***用户指南，以确定它描述了用户可访问的由 TOE 提供的安全功能的使用。

用户指南应标识和描述用户可用安全接口和功能的行为及其相互关系。

如果允许用户调用 TOE 安全功能，用户指南应为用户提供该功能接口的描述。

对每个接口和功能，用户指南应当：

a) 描述调用接口的方法（如命令行、程序语言系统调用、菜单选择、命令按钮）；
b) 描述由用户设置的参数及其有效值和默认值；
c) 描述即时的 TSF 响应、消息或返回代码。

10.7.3.4.3 工作单元 1：AGD-USR.1-3

ISO/IEC 15408-3 AGD_USR.1.3C 用户指南应包含了在安全处理环境中受控的用户可访问功能和特权的警示信息。

评估者***应检查***用户指南，以确定其包含了在安全处理环境中受控的用户可访问功能和特权的警示信息。

TOE 的配置可以允许用户拥有不同的特权来使用 TOE 的不同功能，这意味着可以授权某些用户执行某些功能，而其他用户无权执行，这些用户可访问的功能和特权应在用户指南应中进行描述。

用户指南应标识可用的功能和特权、所需命令的类型以及使用这些命令的理由。用户指南应当包含使用受控的功能和特权时的警告。警告应当说明预期的效果、可能的负面影响以及与其他功能和特权可能的相互作用。

10.7.3.4.4 工作单元 1:AGD_USR.1-4

ISO/IEC 15408-3 AGD_USR.1.4C 用户指南应清晰地阐述安全操作 TOE 所必需的所有用户职责，这些职责包括那些在 TOE 安全环境陈述中的与用户行为相关的假设。

评估者***应检查***用户指南，以确定其阐述了安全操作 TOE 所必需的所有用户职责，这些职责包括那些在 TOE 安全环境陈述中的与用户行为相关的假设。

关于用户行为的假设可以在 ST 的 TOE 安全环境陈述中有比较详细的描述，在用户指南中只需包含涉及 TOE 安全操作的信息。

用户指南应当提供关于有效使用这些安全功能的建议（如审查口令组合的习惯、对用户文件备份频率的建议、对改变用户访问特权所产生影响的讨论）。

例如，要安全操作 TOE 用户有责任对他们的口令进行保密。

用户指南应指出用户是否能够调用某项功能，或者用户是否需要管理员的帮助。

10.7.3.4.5 工作单元 1:AGD-USR.1-5

ISO/IEC 15408-3 AGD_USR.1.5C 用户指南应与评估提交的所有其他文档保持一致。

评估者***应检查***用户指南，以确定其与评估提交的所有其他文档是一致的。

评估者要确保用户指南和评估提交的所有其他文档不会相互矛盾。如果 ST 包含任何对 TOE 用户提出的关于 TOE 安全环境和安全目的的详细警告信息，这一点就尤其重要。

有关一致性分析的指南参见 A.3“一致性分析”。

10.7.3.4.6 工作单元 1:AGD-USR.1-6

ISO/IEC 15408-3 AGD_USR.1.6C 用户指南应描述所有与用户有关的 IT 环境安全要求。

评估者***应检查***用户指南，以确定其描述了所有与用户有关的 TOE 的 IT 环境安全要求。

如果 ST 中不包含 IT 环境的 IT 安全要求，本工作单元不适用，并视为已经满足。

本工作单元仅与 IT 安全要求相关，而与组织安全策略无关。

评估者应分析 TOE 的 IT 环境安全要求（ST 中的可选陈述），并与用户指南比较，以确保所有与用户有关的 ST 安全要求都在用户指南中得到了恰当的描述。

10.8 测试活动

本活动的目的是通过对 TSF 的一个子集进行独立测试，确定 TOE 的行为是否与设计文档中所规定的一样，并且与 ST 中规定的 TOE 安全功能要求一致。

10.8.1 应用注释

评估者测试子集的构成和大小依赖于独立测试子活动（ATE_IND.1“独立测试——一致性”）中所讨论的几个因素。已知的公开弱点便是该类因素之一，评估者需访问这些信息（例如，从评估体制获取）。

为了建立测试，评估者应理解安全功能在其满足要求的情况下所期望的预期行为。评估者可以每次选择 TSF 的某个安全功能，检查 ST 要求以及功能规范和指导性文档中的相关部分，以获得对 TOE 的预期行为方式的理解。

10.8.2 独立测试评估（ATE_IND.1）

10.8.2.1 目的

本子活动的目的是通过对 TSF 的一个子集进行独立测试，确定 TOE 是否按规定执行。

10.8.2.2 输入

本子活动的评估证据是：

a) ST；
b) 功能规范；
c) 用户指南；
d) 管理员指南；
e) 安全安装、生成和启动程序；
f) 适于测试的 TOE。

10.8.2.3 行为 ATE_IND.1.1E

10.8.2.3.1 工作单元 1：ATE_IND.1-1

ISO/IEC 15408-3 ATE_IND.2.1C TOE 应适合测试。

评估者***应检查***TOE，以确定测试配置与所评估的 ST 中规定的配置是一致的。

用于评估者测试的 TOE，其唯一参照号应与 CM 能力（ACM-CAP.＊）子活动建立的唯一参照号相同。

ST 有可能指定不止一个评估配置，TOE 可能由多个不同的硬件和软件实现组成，应根据 ST 对它们进行测试。评估者的 TOE 测试配置应与 ST 中所描述的每个评估配置相一致。

评估者应考虑 ST 中所描述的可用于测试环境的关于 TOE 环境安全方面的假设。ST 中可能有一些假设不适用于测试环境。例如，关于用户许可方面的假设可能就不适用，但关于网络单点接入的假设就适用。

如果使用了任何测试资源（例如仪表、分析仪），评估者有责任保证这些资源是校准正确的。

10.8.2.3.2 工作单元 1：ATE_IND.1-2

评估者***应检查***TOE，以确定它已被正确安装并处于一个已知状态。

评估者可能以多种方式来确定 TOE 的状态。例如，只要评估者仍然相信正在用于测试的 TOE 是正确安装的并且处于一个已知状态，先前的 ADO_IGS.1“安装、生成和启动程序”子活动的成功完成将满足本工作单元。如果情况不是这样，那么评估者只需根据提供的指南按照开发者的规程来安装、生成和启动 TOE。

如果由于 TOE 处于未知状态，评估者不得不执行安装过程，在成功完成后即可满足工作单元 ADO_IGS.1-2 的要求。

10.8.2.4 行为 ATE_IND.1.2E

10.8.2.4.1 工作单元 1：ATE_IND.1-3

评估者***应设计***一个测试子集。

评估者选择一个适合于 TOE 的测试子集和测试策略。一个极端的测试策略是让测试子集包含尽可能多的安全功能，但不是很严格地测试它们。另一个极端的测试策略是根据觉察到的相关性，让测试子集包含少数几个安全功能，并严格地测试这些安全功能。

评估者采用的测试方法一般会处于这两种极端情况之间。评估者应至少使用一项测试来试验 ST 中标明的大部分安全功能要求，但不必进行所有的规范测试。

评估者在选择被测 TSF 子集时应该考虑以下因素：

a) 测试子集中包括的安全功能个数。如果 TOE 只包含少量安全功能，就要对所有安全功能进

行严格测试。如果 TOE 包含很多安全功能，执行全班测试将是不合算的，此时可执行抽样测试。

b) 维持评估活动的平衡。通常，在评估过程中，测试占评估者工作的 20%～30%。

评估者选择安全功能组成测试子集。这种选择依赖于很多因素，对这些因素的考虑也可能影响测试子集大小的选择：

a) 与 TOE 的类型（例如，操作系统、防火墙）相关的已知公共域中的弱点。这些弱点将影响测试子集的选择过程。评估者应将涉及这些弱点的安全功能包含在子集中（这里的已知公共域中的弱点并不是指脆弱性，而是该类 TOE 所带有的不充分的情况或问题区）。如果不知道这样的弱点，那么采用选择更宽范围安全功能的这一通用方法可能更合适。

b) 安全功能的重要性。根据 TOE 的安全目的，那些较重要的安全功能应包含在测试子集中。

c) 安全功能的复杂性。复杂的安全功能可能需要复杂的测试，这些测试对开发者或评估者施以更繁重的要求，这将不利用提高评估效率。相反，从更易找出错误的角度，复杂的安全功能又是子集的一个理想候选对象。因此，评估者需要在这些考虑因素之间寻求一种平衡。

d) 隐含的测试。某些安全功能的测试可能往往隐含着需要测试其他安全功能，把它们包括在子集中可以使被测安全功能数最大化（虽然是隐含的）。典型地，某些特定接口被用于提供多种安全功能特性，这是一种有效的测试方法。

e) TOE 的接口类型（例如，编程的、命令行的、协议的）。评估者应考虑在子集中包括 TOE 支持的所有不同接口类型的测试。

f) 创新的或不寻常的功能。当 TOE 包含有创新的或不寻常的安全功能时，这些功能在市场宣传中可能颇具分量，应该成为测试的重点候选对象。

这一部分指南清楚地说明了在选择合适的测试子集过程中应考虑的因素，但不代表已详述了所有因素。

有关抽样指南参见 A.2“抽样”。

10.8.2.4.2 工作单元 1：ATE_IND.1-4

评估者***应***为测试子集生成足够详细的测试文档，以便测试情况是可再现的。

参照 ST 和功能规范，在对一个安全功能的预期行为有了一定了解后，评估者应确定测试该功能的最可行的方法。

评估者应特别考虑以下几点：

a) 将采用的方法，例如，是否在外部接口上测试安全功能，是否使用测试设备在内部接口上测试安全功能，或者使用其他测试方法（例如：在异常情况下，代码检查）；

b) 用于激发安全功能并观察响应的安全功能接口；

c) 测试所需的初始条件（例如，任何需要具备的特殊客体或主体以及它们需要拥有的安全属性）；

d) 激发安全功能或观察安全功能所需的专用测试设备（例如，包发生器、网络分析仪）。

评估者可能发现，使用一系列测试用例测试每个安全功能是切实可行的，而每个测试用例将测试预期行为的某个特定的方面。

评估者的测试文档应指明每个测试的出处，如有必要，将其追溯到相关的设计规范和 ST。

10.8.2.4.3 工作单元 1：ATE_IND.1-5

评估者***应实施***测试。

评估者使用测试文档作为对 TOE 进行测试的基础。测试文档用作测试的基础，但是这并不排除评估者执行附加的特别测试。基于测试中发现的 TOE 行为，评估者可以设计新的测试，这些新的测试应记录在测试文档中。

10.8.2.4.4 工作单元 1:ATE_IND.1-6

评估者***应记录***包含在测试子集中的如下测试信息:

a) 待测试的安全功能行为的标识;
b) 测试设备的连接说明与设置说明;
c) 测试所需初始条件的说明;
d) 激发安全功能的说明;
e) 观察安全功能行为的说明;
f) 所有预期结果的描述,以及用以比较预期结果的必要分析;
g) 总结测试和为 TOE 建立必要的测试后状态的说明;
h) 实际测试结果。

测试文档中的细节描述应达到这样的程度:使其他评估者能重复测试并获得相同的结果,尽管测试结果的某些特定细节可能不同(例如审计记录中的时间和日期字段),但整体结果应该是相同的。

有些情况可以不必提供本工作单元中出现的全部信息(例如,在可以与预期结果做比较前,可能不需要对实际测试结果进行任何分析)。这些信息的省略由评估者决定,这样才合理。

10.8.2.4.5 工作单元 1:ATE_IND.1-7

评估者***应核查***所有的实际测试结果,是否与预期测试结果一致。

实际测试结果和预期测试结果间的任何差别可能表明 TOE 与其规定不一致,或者评估者的测试文档是错误的。出现意料之外的实际测试结果,可能需要对 TOE 或测试文档进行纠正维护,也许需要重新运行受到影响的测试,并且修改测试样本的数量和组成。该决定由评估者作出,这样才合理。

10.8.2.4.6 工作单元 1:ATE_IND.1-8

评估者***应***在 ETR 中***报告***评估者的测试成果、测试大纲、配置、深度和结果。

在 ETR 中报告的评估者测试信息允许评估者告知总体测试方法和在评估过程中测试活动所付出的效果。提供这种信息的目的是对测试工作给出一个有意义的概述,这并不是为了精确再现特定的测试说明或个别测试结果。其目的是要提供足够的细节,以便允许其他评估者和监督者了解评估者所选择的测试方法、执行的评估者测试数量、执行的开发者测试数量、TOE 测试配置和测试活动的总体结果。

一般可在 ETR 中找到关于评估者测试工作的信息有:

a) TOE 测试配置。被测 TOE 的特殊配置;
b) 所选子集的大小。在评估中要被测试的安全功能的数量和确定子集大小的理由;
c) 构成子集的安全功能选择标准。简要说明在选择组成子集的安全功能时考虑的因素;
d) 被测的安全功能。包含在子集中的安全功能的简表;
e) 活动的裁定。对测试结果的总体判断。

以上列出的信息并不全面,只是为应呈现在 ETR 中的关于评估期间评估者所做测试的信息类型提供借鉴。

11 EAL2 评估

11.1 简介

EAL2 提供低级别到中等级别的独立保证的安全性。使用功能规范、指导性文档以及 TOE 的高层设计,对安全功能进行分析以理解安全行为。这种分析由 TOE 安全功能子集的独立测试、开发者基于

功能规范进行测试的证据、对开发者测试结果的选择性确认、功能强度分析、开发者搜索明显脆弱性的证据等来支持。通过 TOE 配置列表和安全交付程序的证据,可获得进一步的保证。

11.2 目的

本章的目的是定义达到 EAL2 级评估所需的最少评估工作,并对完成评估的方式方法提供指导。

11.3 EAL2 评估相互关系

EAL2 级评估包括以下活动:

a) 评估输入任务(第 7 章)。

b) EAL2 评估活动包括:

1) ST 评估(第 9 章);

2) 配置管理评估(11.4);

3) 交付和运行文档评估(11.5);

4) 开发文档评估(11.6);

5) 指导性文档评估(11.7);

6) 测试评估(11.8);

7) 测试(11.8);

8) 脆弱性评定评估(11.9)。

c) 评估输出任务(第 7 章)。

评估活动源于 ISO/IEC 15408-3 所包含的 EAL2 保证要求。

ST 评估应在所有 TOE 评估子活动之前启动,因为 ST 为执行这些评估子活动提供了基础和背景。

本章描述了构成 EAL2 评估的子活动。尽管各个子活动通常可以或多或少的同时进行,但评估者应考虑子活动间的依赖关系。

有关依赖关系的指南见附录 A。

11.4 配置管理活动

配置管理活动的目的是帮助客户识别被评估 TOE,并确保配置项都已被唯一标识。

11.4.1 CM 能力评估(ACM_CAP.2)

11.4.1.1 目的

本子活动的目的是确定开发者是否已清楚地标识了 TOE 及其相关配置项。

11.4.1.2 输入

本子活动的评估证据是:

a) ST;

b) 适于测试的 TOE;

c) 配置管理文档。

11.4.1.3 应用注释

该组件包含了隐含的评估者行为,以便确定该 CM 系统正在使用。由于这里的要求只限于标识 TOE 和提供配置清单,因此该行为包含于现有工作单元并受之限制。在 ACM_CAP.3“鉴别控制”中的要求不仅扩展了这两项内容,还需要更多明确的运行证据。

11.4.1.4 行为 ACM_CAP.2.1E

11.4.1.4.1 工作单元 2:ACM_CAP.2-1

ISO/IEC 15408-3 ACM_CAP.2.1C TOE 参照号对 TOE 的每个版本都应当是唯一的。

评估者***应核查***用于评估的 TOE 版本有唯一的参照号。

评估者应当使用开发者的 CM 系统来确认参照号的唯一性,通过核查配置清单确认配置项是被唯一标识的。如果在评估过程中仅仅检查了一个版本,该项评估的证据是不完备的,因此评估者应该查找能够支持唯一参照号的参照系统(如,使用数字、字母或日期)。除非评估者确信该 TOE 能够被唯一标识,否则缺少任何一项参照都将导致对这项要求裁定为“不通过”。

评估者应该设法检查多个 TOE 版本(如,修正某个漏洞后的版本),以核查两个版本参照号的不同。

11.4.1.4.2 工作单元 2:ACM_CAP.2-2

ISO/IEC 15408-3 ACM_CAP.2.2C 应给 TOE 标记上参照号。

评估者***应核查***所提交评估的 TOE 是否标记了参照号。

评估者应确保 TOE 包含唯一的参照号,以便区分 TOE 的不同版本。这可以通过提供在包装或介质上粘贴标签,或让 TOE 在运行时显示标记等措施来实现,以保证客户(例如:在购买或使用时)能够识别出。

TOE 可提供某种方式使得它易于识别。例如,软件形式的 TOE 可以在启动例程中,或者在响应命令行输入时,显示其名称和版本号。硬件或固件形式的 TOE 可以通过将零件号码铭刻在 TOE 上来标识。

11.4.1.4.3 工作单元 2:ACM_CAP.2-3

评估者***应核查***所使用的 TOE 参照号是一致的。

如果 TOE 要多处标记,所有的标记应当是一致的。例如,作为 TOE 一部分而提交的任何一份已标记过的指导性文档都应与被评估的、使用的 TOE 相关。这样就可以确保客户能确认自己所购买和安装的 TOE 版本是经过评估的,并且他们所使用的指南与 ST 一致,可以正确的指导自己使用 TOE。评估者可以通过 CM 文档中的配置清单来验证标记使用的一致性。

评估者还应验证该 TOE 的参照号是否与 ST 一致。

有关一致性分析的指南参见 A.3“一致性分析”。

11.4.1.4.4 工作单元 2:ACM_CAP.2-4

ISO/IEC 15408-3 ACM_CAP.2.3C CM 文档应包含一份配置清单。

评估者***应核查***所提交的 CM 文档是否包含了一份配置清单。

配置清单标识了在配置管理控制下维护的配置项。

11.4.1.4.5 工作单元 2:ACM_CAP.2-5

ISO/IEC 15408-3 ACM_CAP.2.4C 配置清单应唯一标识组成 TOE 的所有配置项。

评估者***应核查***配置清单,确认其唯一标识了每个配置项。

配置清单包括组成 TOE 的配置项列表,以及足以唯一标识所使用的每个配置项的版本信息(例如:版本号)。评估者使用该清单来进行核查,确认在评估过程中使用了正确的配置项和正确的版本。

11.4.1.4.6 工作单元 2:ACM_CAP.2-6

ISO/IEC 15408-3 ACM_CAP.2.5C 配置清单应描述组成 TOE 的配置项。

评估者***应检查***配置清单,以确定其标识了组成 TOE 的配置项。

配置清单所涵盖配置项的最小范围由 ACM_SCP“CM 范围”给出。如果没有包括 ACM_SCP 组件,评估者应根据开发者使用的 CM 方法,将 ACM_SCP.1“TOE CM 覆盖”的要求作为上限(超出这个范围是不合理的),评价该配置清单内容是否充分。例如,当 TOE 或任何文档配置项被改动时,评估者应观察或询问这些重新发布项的修改粒度,该粒度需应与配置清单中相应的内容相一致。

11.4.1.4.7 工作单元 2:ACM_CAP.2-7

ISO/IEC 15408-3 ACM_CAP.2.6C CM 文档应描述用于唯一标识 TOE 所包含配置项的方法。

评估者***应检查***标识配置项的方法,以确定其描述了如何唯一地标识配置项。

11.4.1.4.8 工作单元 2:ACM_CAP.2-8

ISO/IEC 15408-3 ACM_CAP.2.7C CM 系统应唯一标识 TOE 所包含的所有配置项。

评估者***应核查***配置项,以确定它们是用一种与 CM 文档一致的方式来标识的。

通过核查配置项的标识来确认 CM 系统唯一标识了所有配置项。无论是组成 TOE 的所有配置项还是开发者作为评估证据提交的配置项初稿,评估者确认每个配置项具有一个唯一的标识,并且在一定程度上是与 CM 文档所描述的唯一标识方法相一致。

11.5 交付和运行活动

交付和运行活动的目的是判断描述用于确保是以开发者期望的方式安装、生成和启动 TOE,以及 TOE 在交付过程中没有被更改的相关程序文档的内容是否充分。这里既包含括运输过程使用的程序又包括安装、生成和启动程序。

11.5.1 交付评估(ADO_DEL.1)

11.5.1.1 目的

本子活动的目的是确定交付文档是否描述了在将 TOE 分发到用户方时,用于维护其安全性的所有程序。

11.5.1.2 输入

本子活动的评估证据是:

a) 交付文档。

11.5.1.3 行为 ADO_DEL.1.1E

11.5.1.3.1 工作单元 2:ADO_DEL.1-1

ISO/IEC 15408-3 ADO_DEL.1.1C 交付文档应描述,在向用户方分发 TOE 版本时,用以维护其安全性所必需的所有程序。

评估者***应检查***交付文档,以确定其描述了将 TOE 或其一部分提交给用户方时,为维护其安全性所必需的所有程序。

对术语“必需的”的解释应考虑 TOE 的自身属性和 ST 中包含的信息。提供的保护措施程度应与 ST 中标识的假设、威胁、组织安全策略以及安全目的相称。在某些情况下,ST 中的这些内容可能没有

明确的说明与交付相关。评估者应当确定是否已采取了一种均衡手段,使得在非安全开发过程中交付也不存在明显弱点。

交付程序应描述 TOE 或其一部分在传输过程中为确定 TOE 的标识和维持其安全性而采取的相关程序。程序应当描述 TOE 的哪些部分需要按这些程序执行。适当时还应包括物理或电子的分发程序(例如:从因特网下载)。交付程序涉及整个 TOE,包括应用软件、硬件、固件和文档。

交付文档的重点很可能是完整性度量的相关措施,如在 TOE 交付过程中所使用的验证其完整性的技术措施。然而,在某些 TOE 的交付过程中,交付的保密性和可用性却是重点,因而相关内容也应在交付程序中论述。

交付程序应适用于从生产环境到安装环境的整个交付过程(例如,包装、存储和分发)的各个阶段。

标准的商业化包装和交付惯例是可以接受的。这包括紧压包装、安全带或密封套。对于分发而言,邮寄或私人快递都是可以接受的。

交付程序选择是否适当受 TOE(例如,是软件还是硬件产品)和安全目的的影响。即使 TOE 的不同部分,交付程序不相同,但全部程序应适于满足全部安全目的。

11.5.1.4 隐含的评估者行为

11.5.1.4.1 工作单元 2:ADO_DEL.1-2

ISO/IEC 15408-3 ADO_DEL.1.2D 开发者应使用交付程序。

评估者***应检查***交付过程的各个方面,以确定交付程序得到了应用。

评估者检查交付程序执行情况所采取的方法,取决于 TOE 的种类和交付过程自身。除检查交付程序本身外,评估者还应当确保程序得到切实执行。可采取的核查方法如下:

a) 对可观察到程序实际运行情况的分发场所进行现场核查;

b) 在交付的中间阶段,或在用户现场对 TOE 进行检查(例如检查篡改封条);

c) 评估者通过从常规渠道获得 TOE 来观察交付过程是否在实际中得到使用;

d) 询问最终用户 TOE 是如何被交付的。

有关现场检查的指南参见 A.5“现场核查”。

可能有这样的情况:新开发的 TOE,交付程序还尚未实施。对于这种情况,评估者应确信有适当的程序和设施供以后的交付使用,而且所有相关人员都清楚各自的责任。可行的话,评估者可以要求演习交付过程。如果开发者还生产了其他类似产品,评估者还可以通过对这些产品交付程序的检查来进行确认。

11.5.2 安装、生成和启动评估(ADO_IGS.1)

11.5.2.1 目的

本子活动的目的是确定 TOE 的安全安装、生成和启动的程序与步骤是否都已文档化,并最终形成安全的配置。

11.5.2.2 输入

本子活动的评估证据是:

a) 管理员指南;

b) 安全安装、生成和启动程序;

c) 适于测试的 TOE。

11.5.2.3 应用注释

安装、生成和启动程序是指配置 TOE 达到在 ST 中所描述的安全配置所必需的所有安装、生成和启动程序，无论它们是运行在用户现场，还是运行在开发现场。

11.5.2.4 行为 ADO_IGS.1.1E

11.5.2.4.1 工作单元 2：ADO_IGS.1-1

ISO/IEC 15408-3 ADO_IGS.1.1C 安装、生成和启动文档应描述 TOE 安全地安装、生成和启动所必需的所有步骤。

评估者***应核查***是否已经提供了 TOE 安全安装、生成和启动所必需的所有程序。

如果不期望安装、生成和启动程序再次使用(例如，TOE 已经在运行状态下交付)，本工作单元(或者与此相关的部分)就不再适用，并视为已经满足。

11.5.2.5 行为 ADO_IGS.1.2E

11.5.2.5.1 工作单元 2：ADO_IGS.1-2

评估者***应检查***所提供的安装、生成和启动程序，以确认其描述了 TOE 安全安装、生成和启动所需的步骤。

如果不期望安装、生成、启动程序再次使用(例如，TOE 已经在运行状态下交付)，本工作单元(或者与此相关的部分)就不再适用，并视为已经满足。

安装、生成和启动程序可以提供以下详细信息：

a) 对 TSF 控制下相关实体的特定安全特性所做的修改；

b) 对异常情况和问题的处理；

c) 如果适用，列出安全安装所需的最低系统要求。

为了确认安装、生成和启动程序能够形成安全配置，评估者可以只使用所提供的指导性文档，按照开发者的程序，实施客户通常执行的活动以完成对 TOE 的安装、生成和启动(在适用于 TOE 的情况下)。本工作单元可以与工作单元 ATE_IND.1-2 一起被执行。

11.6 开发活动

开发活动的目的是评价设计文档，根据设计文档的充分性来理解 TSF 是如何提供 TOE 安全功能，以此来进行评价。这种理解是通过检查功能规范(描述 TOE 的外部接口)和表示对应性(将功能规范映射到 TOE 的概要规范，以保证一致性)来获得的。

11.6.1 应用注释

ISO/IEC 15408 要求设计文档根据形式化程度来分级。ISO/IEC 15408 将文档的形式化程度分为非形式化、半形式化、形式化三级。非形式化文档是指用自然语言来描述的文档。评估方法没有规定应采用某种语言，这个问题留给评估体制。以下段落分别说明了不同的非形式化文档内容的差别。

一个非形式化功能规范包括一个安全功能描述(类似于 TOE 概要规范的安全功能描述)和一个 TSF 外部可见接口描述。例如，如果操作系统提供给用户一些功能来进行自我身份标识，创建、修改或删除文件，设置文件的访问权限，与远程的机器进行通信，那么它的功能规范应包含对上述每一个功能的描述。如果还有检测和记录这些事件发生的审计功能，那么关于这些审计功能的描述也应该包含在功能规范中；尽管这些审计功能不直接被用户在外部接口所触发，但用户在外部接口的行为的确会对审计功能产生影响。

每个子系统在其接口触发的响应行为有先后顺序,非形式化高层设计就是按照这种顺序来描述的。例如,一个防火墙可能包含一些处理包过滤、远程管理、审计和传输层过滤的子系统。防火墙的高层设计应当按照当一个输入包到达防火墙时,每个子系统所采取的行为来对防火墙采取的行为加以描述。

非形式化的对应性分析不需要采用叙述的方式,一个简单的二维映射就足够了。例如,一个矩阵,沿一个轴的方向列出了模块,沿另一个方向列出了子系统,其中的元素表示两者的对应性,这将在高层设计和低层设计之间提供足够的非形式化对应性。

11.6.2 功能规范评估(ADV_FSP.1)

11.6.2.1 目的

本子活动的目的是确认开发者对 TOE 安全功能是否作了充分描述,以及 TOE 提供的安全功能是否充分足以满足 ST 的安全功能要求。

11.6.2.2 输入

本子活动的评估证据是:

a) ST;
b) 功能规范;
c) 用户指南;
d) 管理员指南。

11.6.2.3 行为 ADV_FSP.1.1E

11.6.2.3.1 工作单元 2:ADV_FSP.1-1

ISO/IEC 15408-3ADV_FSP.1.1C 功能规范应使用非形式化风格来描述 TSF 及其外部接口。

评估者***应检查***功能规范,以确定其包括了所有必需的非形式化解释文本。

如果整个功能规范都是非形式化的,则本工作单元不适用,并视为已经满足要求。

对于那些只采用半形式化或形式化语言进行描述,难以被人理解的功能规范的某些组成部分(例如,为解释任何形式化符号的含义),有必要使用辅助性的叙述描述来帮助理解。

11.6.2.3.2 工作单元 2:ADV_FSP.1-2

ISO/IEC 15408-3ADV_FSP.1.2C 功能规范应是内在一致的。

评估者***应检查***功能规范,以确定它是内在一致的。

评估者通过检查 TSFI 接口描述与 TSF 功能描述是否一致来验证功能规范的一致性。

11.6.2.3.3 工作单元 2:ADV_FSP.1-3

ISO/IEC 15408-3 ADV_FSP.1.3C 功能规范应描述所有外部 TSF 接口的用途与使用方法,适当时应提供效果、例外情况和错误消息的细节。

评估者***应检查***功能规范,以确定其标识了所有的外部 TOE 安全功能接口。

术语“外部”指对用户而言是可见的。TOE 的外部接口或者是 TSF 的直接接口,或者是 TOE 的非 TSF 部分的接口。不过,这些非 TSF 接口可能最终通向 TSF。这些直接或间接通向 TSF 的外部接口共同组成了 TOE 安全功能接口(TSFI)。图 7 表示一个包含 TSF 部分(阴影部分)和非 TSF 部分(空白部分)的 TOE。该 TOE 有三个外部接口:接口 c 是 TSF 的直接接口;接口 b 是 TSF 的间接接口;接口 a 是 TOE 非 TSF 部分的接口。因此,接口 b 和 c 组成了 TSFI。

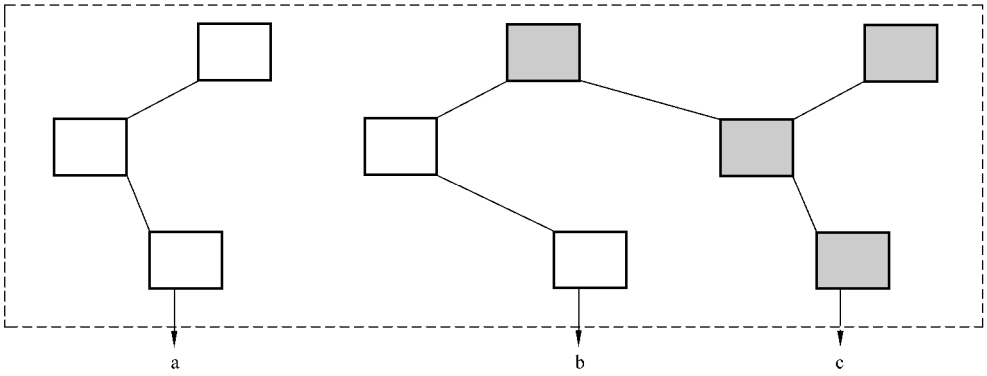

图 7　TSF 接口

应该注意的是，所有反映 ISO/IEC 15408-2 功能要求（或者在其扩展组件中）的安全功能应该有某种外部可见的表现形式。尽管有些安全功能不一定能通过其接口来验证，但由于它们在某种程度上是外部可见的，因此也应包含在功能规范中。

11.6.2.3.4　工作单元 2：ADV_FSP.1-4

评估者***应检查***功能规范，以确定其描述了所有外部的 TOE 安全功能接口。

对于一个没有恶意用户威胁的 TOE（即 FPT_PHP“TSF 物理保护”、FPT_RVM“参照仲裁”和 FPT_SEP“域分离”都被排除在 ST 之外），功能规范中描述的（和在其他 TSF 表示描述中进行了扩展的）只是那些通向和来自 TSF 的接口。缺少 FPT_PHP“TSF 物理保护”、FPT_RVM“参照仲裁”和 FPT_SEP“域分离”，就假设没有考虑任何安全特性的旁路，因而不用考虑其他接口可能施加给 TSF 的任何可能的影响。

另一方面，如果 TOE 存在恶意用户或旁路之类的威胁（即 FPT_PHP“TSF 物理保护”、FPT_RVM“参照仲裁”和 FPT_SEP“域分离”被包含在 ST 中），所有外部接口都需要在功能规范中进行描述，但是仅需描述到每一种影响都已明确的程度：安全功能的接口（即图 7 中的接口 b 和 c）都被描述了，然而其他接口仅仅描述到明确 TSF 不能通过这些接口（即图 7 中的接口 a，而不是 b）访问的程度。包含 FPT_PHP“TSF 物理保护”、FPT_RVM“参照仲裁”和 FPT_SEP“域分离”，意味着所有的接口将对 TSF 有某些影响。由于每一个外部接口都是潜在的 TSF 接口，因此，功能规范应对每一个接口进行详细的描述，以使得评估者能够确定接口是否与安全相关。

某些体系结构易于为外部接口群提供足够详细的描述。例如，在内核结构中所有对操作系统的调用都由内核程序来处理；任何有可能违反 TSP 的调用应由具备这种特权的程序来调用。所有实行特权的程序应被包含在功能规范中。任何在内核之外的没有实行特权的程序是无能力影响 TSP 的（即，这种程序是图 7 中的 a 类的接口，而不是 b 类），因而，可以被排除在功能规范之外。如果是基于上述的内核结构，而且评估者对这种结构能够顺利的了解，那么这种结构不是必需的。

11.6.2.3.5　工作单元 2：ADV_FSP.1-5

评估者***应检查***对 TSFI 的陈述，以确定其正确并充分地描述了每个表示效果、异常和出错信息的外部接口处的 TOE 行为。

为了评估接口描述的充分性和正确性，评估者使用功能规范、ST 的 TOE 概要规范以及用户和管理员指南来评估以下因素：

a）　应标识所有与安全相关的用户输入参数（或这些参数的特性）。为了全面起见，宜标识出管理员可用而普通用户无法直接控制的参数。

b) 对功能规范中语义的描述应当反映所审查指南中描述的所有安全相关行为。它包括一系列通过事件及其影响所表示的行为标识。例如,如果一个操作系统提供了丰富的文件系统接口,并对请求文件无法打开的各种原因(如拒绝访问、文件不存在、文件正被另一个用户使用、用户无权在下午 5 点后打开文件等)提供了不同的错误代码,功能规范应当解释该文件或者在请求下被打开,如不能打开则返回错误代码。(虽然功能规范可以列举所有错误的原因,但不需要提供细节描述)。对语义的描述应当包括安全要求如何应用于接口(例如,是否可以审计接口的使用情况,假如这样的话,应包含能够记录的信息)。

c) 应描述所有可能操作模式下的所有接口。如果 TSF 提供了特权的概念,对接口的描述应分别解释特权模式或非特权模式时,接口的工作方式。

d) 整个文档中安全相关参数的描述和接口的语法所包含的信息应当是一致的。

对以上因素的核实,是通过审核安全规范和 ST 的 TOE 概要规范、开发者提供的用户和管理员指南来完成的。例如,如果 TOE 是一个操作系统及其底层硬件,评估者可以查找用户可访问的程序的讨论、用于指导程序活动的协议的描述、用于指导程序活动的用户可访问数据库的描述,并查找适用于 TOE 的用户接口(例如命令、应用程序接口)。评估者还要确定处理器的指令集已进行描述。

这种核查可以反复进行,直到包含参数和出错信息的设计、源代码或其他证据都被检查为止,以避免发生功能规范描述不全的情况被评估者忽略。

11.6.2.3.6 工作单元 2:ADV_FSP.1-6

ISO/IEC 15408-3 ADV_FSP.1.4C 功能规范应完备地表示 TSF。

评估者***应检查***功能规范,以确定 TSF 已被完全表示。

为了评估 TSF 表示的完备性,评估者可查阅 ST 的 TOE 概要规范、用户指南和管理员指南。它们应当没有描述在功能规范的 TSF 表示中没有的安全功能。

11.6.2.4 行为 ADV_FSP.1.2E

11.6.2.4.1 工作单元 2:ADV_FSP.1-7

评估者***应检查***功能规范,以确定它是 TOE 安全功能要求的一个完备地实例。

为了确保功能规范涵盖了所有的 ST 安全功能要求,评估者应当建立 TOE 概要规范和功能规范之间的映射。为了满足(ADV_RCR.*“表示对应性”)的对应要求,开发者可能已经提交了这种映射证据;这时评估者只需要验证映射的完备性,确定所有的安全功能要求都映射到功能规范中适当的 TSFI 表示。

11.6.2.4.2 工作单元 2:ADV_FSP.1-8

评估者***应检查***功能规范,以确定它是 TOE 安全功能要求的一个准确实例化。

对于每个具有某种特性的安全功能的接口,功能规范中的详细信息应与 ST 中的相关信息所表述准确一致。例如,如果 ST 中的用户鉴别要求规定了口令长度应为 8 个字符,那么 TOE 应有 8 个字符的口令;如果功能规范描述的是 6 字符的固定长度口令,那么功能规范就不是 TOE 安全功能要求的一个准确实例化。

功能规范中对在受控资源上运行的每个接口,评估者应确定它是否返回了一个错误代码,该错误代码是因为某个安全要求的实施失败而导致的,如果没有返回错误代码,评估者应确定是否需要返回一个错误代码。例如,操作系统可以提供一个接口用于打开一个受控对象,该接口描述中可包含因对受控对象作了未授权的访问而产生的一个错误代码。如果没有这种错误代码,评估者应当确认是否合理。(因为,也许访问仲裁是针对读、写的操作执行的,而不是针对打开的)。

11.6.3 高层设计评估（ADV_HLD.1）

11.6.3.1 目的

本子活动的目的是确定高层设计是否按照主要架构单元(如子系统)的方式对 TSF 进行描述,并确定高层设计是功能规范的一个正确实现。

11.6.3.2 输入

本子活动的评估证据是:

a) ST;

b) 功能规范;

c) 高层设计。

11.6.3.3 行为 ADV_HLD.1.1E

11.6.3.3.1 工作单元 2:ADV_HLD.1-1

ISO/IEC 15408-3 ADV_HLD.1.1C 高层设计的表示应是非形式化的。

评估者***应检查***高层设计,以确定它包括了所有必需的非形式化解释性文本。

如果整个高层设计都是非形式化的,则本工作单元被视为不适用,并认为已经满足要求。

对于功能规范中那些仅以半形式化或形式化描述难以理解的部分(例如,为解释清楚任何形式化符号的含义),那么起辅助作用的叙述性描述是必需的。

11.6.3.3.2 工作单元 2:ADV_HLD.1-2

ISO/IEC 15408-3 ADV_HLD.1.2C 高层设计应是内在一致的。

评估者***应检查***高层设计的表示,以确定它是内在一致的。

有关一致性分析的指南见 A.3“一致性分析”。

评估者应确认子系统的接口规范,以确定接口规范与子系统用途的描述相一致。

11.6.3.3.3 工作单元 2:ADV_HLD.1-3

ISO/IEC 15408-3 ADV_HLD.1.3C 高层设计应按子系统方式描述 TSF 的结构。

评估者***应检查***高层设计,以确定 TSF 是按子系统方式描述的。

关于高层设计中的术语“子系统”指的是大的相关单元(如内存管理、文件管理、进程管理)。通过把一个设计分成多个基本功能区,有助于理解设计思路。

检查高层设计的主要目的是帮助评估者理解 TOE。开发者对子系统定义的选择以及各个子系统中 TSF 分组的选择,是使高层设计有益于理解 TOE 预期运行的一个重要方面。作为本工作单元的一部分,评估者应当评估开发者列举的子系统数目是否恰当,各个子系统中功能分组的选择是否恰当。评估者应确定把 TSF 分解成子系统,足以使评估者从高层的角度来理解 TSF 的功能是如何提供的。

不必非得用“子系统”这个术语来描述高层设计中子系统这个概念,子系统应当代表一类相似级别的分解。例如,可以使用“层”“管理器”对设计进行分解。

11.6.3.3.4 工作单元 2:ADV_HLD.1-4

ISO/IEC 15408-3 ADV_HLD.1.4C 高层设计应描述每个 TSF 子系统所提供的安全功能性。

评估者***应检查***高层设计,以确定它描述了每个子系统的安全功能。

子系统的安全功能行为是对子系统“做些什么”进行的描述。不仅要对子系统直接执行其功能的行

为进行描述，而且还要将子系统对 TOE 的安全状态可能产生的影响进行描述（例如，改变主体、对象、安全数据库）。

11.6.3.3.5 工作单元 2：ADV_HLD.1-5

ISO/IEC 15408-3 ADV_HLD.1.5C 高层设计应标识 TSF 所要求的任何基础性硬件、固件或软件，以及在这些硬件、固件或软件中实现的支持性保护机制所提供功能的一个表示。

评估者***应核查***高层设计，以确定它标识了 TSF 所需的所有硬件、固件和软件。

如果 ST 中没有对 IT 环境的安全要求，则本工作单元被视为不适用，并视为已经满足。

如果 ST 包含可选的 IT 环境安全要求，评估者比较高层设计中陈述的 TSF 所需硬件、固件或软件列表与 IT 环境安全要求的陈述，以确定两者的一致性。ST 中的信息刻画了 TOE 赖以运行的底层抽象机。

如果高层设计中的 IT 环境安全要求不属于 ST 中的已定义的 IT 环境安全要求，或者它们与包含在 ST 中的要求不同，那么评估者应根据 ADV_HLD.1.2E 评估行为对这种不一致性进行评估。

11.6.3.3.6 工作单元 2：ADV_HLD.1-6

评估者***应检查***高层设计，以确定它涵盖那些可以通过在底层硬件、固件或软件而实现的支持性保护机制功能的表示。

如果 ST 中没有 IT 环境安全要求，则本工作单元被视为不适用，并视为已经满足。

TOE 赖以运行的“根本抽象机”所提供功能的介绍，不需要像作为 TSF 组成部分的功能那样详细，而应解释 TOE 如何使用硬件、固件或软件提供的功能，这些硬件、固件或软件实现了 TOE 用来支持 TOE 安全目的的 IT 环境安全要求。

IT 环境安全要求的陈述可以是抽象的，特别是当它由各种硬件、固件或软件的不同组合来满足时。作为测试活动的一部分，当能够为评估者提供至少一个声称满足 IT 环境安全要求的“根本机”的实例时，评估者就能够确定其是否为 TOE 提供了必要的安全功能。评估者的这种确认不需要测试和分析“根本机”，只需要确定期望其提供的功能确实存在。

11.6.3.3.7 工作单元 2：ADV_HLD.1-7

ISO/IEC 15408-3 ADV_HLD.1.6C 高层设计应标识 TSF 子系统的所有接口。

评估者***应核查***高层设计是否标识了 TSF 子系统的接口。

对每个子系统，高层设计应当包括它的每个入口点的名称。

11.6.3.3.8 作单元 2：ADV_HLD.1-8

ISO/IEC 15408-3 ADV_HLD.1.7C 高层设计应标识 TSF 子系统的哪些接口是外部可见的。

评估者***应核查***高层设计是否标识了 TSF 子系统的哪些接口是外部可见的。

11.6.3.4 行为 ADV_HLD.1.2E

11.6.3.4.1 工作单元 2：ADV_HLD.1-9

评估者***应检查***高层设计，以确认它是 TOE 安全功能要求的一个准确实例化。

评估者应分析高层设计中每个 TOE 的安全功能，以确定功能描述是准确的。评估者还应确定功能都包含在高层设计的依赖关系中。

评估者还分析在 ST 和高层设计中的 IT 环境安全要求，以确定它们是一致的。例如，如果 ST 包含了关于审计踪迹存储的 TOE 安全功能要求，但高层设计规定审计踪迹存储是由 IT 环境提供的，那么

高层设计就不是 TOE 安全功能要求的一个准确实例化。

11.6.3.4.2 工作单元 2:ADV_HLD.1-10

评估者*应检查*高层设计,以确认它是 TOE 安全功能要求的一个完备实例化。

为确保高层设计涵盖了所有的 ST 安全功能要求,评估者可以在 TOE 安全功能要求和高层设计之间建立映射。

11.6.4 表示对应性评估(ADV_RCR.1)

11.6.4.1 目的

本子活动的目的是确定开发者是否在高层设计中正确且完备地执行了 ST 和功能规范中的要求。

11.6.4.2 输入

本子活动的评估证据是:

a) ST;
b) 功能规范;
c) 高层设计;
d) TOE 概要规范和功能规范之间的对应性分析;
e) 功能规范和高层设计之间的对应性分析。

11.6.4.3 行为 ADV_RCR.1.1E

11.6.4.3.1 工作单元 2:ADV_RCR1-1

ISO/IEC 15408-3 ADV_RCR.1.1C 对于所提供 TSF 表示的每个相邻对,分析应证实,较为抽象的 TSF 表示的所有相关安全功能都在较不抽象的 TSF 表示中得到正确且完备地细化。

评估者*应检查*TOE 概要规范和功能规范之间的对应性分析,以确认功能规范是 TOE 安全功能的一个正确且完备的表示。

本工作单元中,评估者的目的是确定 TOE 概要规范中标识的所有安全功能都在功能规范中得到了体现并且是准确地体现。

评估者审核 TOE 概要规范中的 TOE 安全功能和功能规范中的 TOE 安全功能之间的对应性。评估者检查对应的一致性和准确性。当对应性分析中指明了 TOE 概要规范中的一个安全功能和功能规范中一个接口描述之间的关系时,评估者应验证两者中描述的是同一个安全功能。如果 TOE 概要规范的安全功能在所对应的接口中能够正确且完备地实现,那么本工作单元将被视为满足。

本工作单元可与工作单元 ADV_FSP.1-7 和 ADV_FSP.1-8 关联使用。

11.6.4.3.2 工作单元 2:ADV_RCR1-2

评估者*应检查*功能规范与高层设计之间的对应性分析,以确定高层设计是功能规范的一个正确且完备的表示。

评估者通过使用对应性分析、功能规范以及高层设计来确定将功能规范中标识的每项安全功能映射到高层设计中所描述的一个 TSF 子系统是可行的。并且对于每个 TOE 安全功能,对应性还可以指明该功能涵盖了哪些子系统。评估者应审核高层设计所涵盖的每一个安全功能得以正确实现的描述。

11.7 指导性文档活动

指导性文档活动的目的是判断该文档是否充分描述了应如何操作 TOE。这些文档针对两类用户:

一类是可信的管理员和非管理员用户,他们的不正确行为可能影响 TOE 安全性,另一类是那些不可信用户,他们的不正确行为可能影响其拥有的数据的安全性。

11.7.1 应用注释

指导性文档活动关注那些与 TOE 安全性相关的功能和接口。TOE 的安全配置在 ST 中进行了描述。

11.7.2 管理员指南评估(AGD_AMD.1)

11.7.2.1 目的

本子活动的目的是确定管理员指南是否描述了如何以安全方式管理 TOE。

11.7.2.2 输入

本子活动的评估证据是:

a) ST;
b) 功能规范;
c) 高层设计;
d) 用户指南;
e) 管理员指南;
f) 安全安装、生成和启动程序;
g) 生命周期定义。

11.7.2.3 应用注释

术语"管理员"指在 TOE 中执行关键安全操作(例如,设置 TOE 配置参数)的可信人员。这些操作可能影响 TSP 的执行,因此管理员拥有特殊的权限来执行这些操作。管理员角色应当与 TOE 中的非管理员用户角色明确区分开。

在 ST 中可定义有不同的管理员角色或管理员组,这些角色和组能可被 TOE 识别并可执行 TOE 的安全功能,例如审计员、管理员或日常管理者。每个角色可能具备多种或一种能力。这些角色的能力和相应的特权在 FMT 类中进行描述。管理员指南中应考虑不同的管理员角色和管理员组。

11.7.2.4 行为 AGD_ADM.1.1E

11.7.2.4.1 工作单元 2:AGD_ADM.1-1

ISO/IEC 15408-3 AGD_ADM.1.1C 管理员指南应描述 TOE 管理员可使用的管理功能和接口。

评估者***应检查***管理员指南,以确定其描述了 TOE 管理员可用的管理性安全功能和接口。

管理员指南应包含安全功能的概述,这些安全功能在管理员界面中是可见的。

管理员指南应标识并描述管理性安全接口与功能的用途、行为和相互关系。

对于每个管理性安全接口和功能,管理员指南应当:

a) 描述调用接口的方法(如命令行、程序语言系统调用、菜单选择、命令按钮);
b) 描述由管理员设置的参数及其有效值和默认值;
c) 描述即时的 TSF 响应、消息或返回代码。

11.7.2.4.2 工作单元 2:AGD_ADM.1-2

ISO/IEC 15408-3 AGD_ADM.1.2C 管理员指南应描述如何以安全的方式管理 TOE。

评估者*应检查*管理员指南，以确定它描述了如何以安全的方式管理 TOE。

管理员指南描述如何在 IT 环境中依照 TSP 运行 TOE，这应与 ST 所描述的情况一致。

11.7.2.4.3 工作单元 2：AGD_ADM.1-3

ISO/IEC 15408-3 AGD_ADM.1.3C 管理员指南应包含了在安全处理环境中受控的功能和特权的警示信息。

评估者*应检查*管理员指南，以确定其包含了在安全处理环境中受控的功能和特权的警示信息。

TOE 的配置可以允许用户拥有不同的特权来使用 TOE 的不同功能，这意味着可以授权某些用户执行某些功能，而其他用户无权执行，这些功能和特权应在管理员指南中进行描述。

管理员指南应标识出应控制的功能和特权、控制的类型以及控制的理由。警告应说明预期的效果、可能的负面影响以及与其他功能和特权可能的相互作用。

11.7.2.4.4 工作单元 2：AGD_ADM.1-4

ISO/IEC 15408-3 AGD_ADM.1.4C 管理员指南应描述所有与安全操作 TOE 有关的用户行为假设。

评估者*应检查*管理员指南，以确定它描述了所有与安全操作 TOE 有关的用户行为假设。

关于用户行为的假设可以在 ST 的 TOE 安全环境陈述中比较详细的描述，而只有涉及安全操作 TOE 的信息才需要包含在管理员指南中。

例如，要安全操作 TOE 用户有责任对他们的口令进行保密。

11.7.2.4.5 工作单元 2：AGD_ADM.1-5

ISO/IEC 15408-3 AGD_ADM.1.5C 管理员指南应描述所有受管理员控制的安全参数，并说明适当的安全值。

评估者*应检查*管理员指南，以确定它描述了所有受管理员控制的安全参数，并说明适当的安全值。

对于每个安全参数，管理员指南应描述参数的用途、参数的有效值和缺省值，以及这些参数安全与非安全的使用设置。这些参数可以分别描述，也可以综合起来描述。

11.7.2.4.6 工作单元 2：AGD_ADM.1-6

ISO/IEC 15408-3 AGD_ADM.1.6C 管理员指南应描述每一种与需要执行的管理功能有关的安全相关事件，包括改变在 TSF 控制下的实体的安全特性。

评估者*应检查*管理员指南，以确定它描述了每一种与需要执行的管理功能有关的安全相关事件，包括改变在 TSF 控制下的实体的安全特性。

应详尽描述所有类型的安全相关事件，以便管理员知道可能发生什么事件以及为保持安全管理员应采取哪些动作。应充分定义在 TOE 的操作过程中可能发生的安全相关事件（例如，审计迹的溢出、系统崩溃、用户记录的更新——如当用户离开组织时撤消该用户账号），以允许管理员介入来保持安全。

11.7.2.4.7 工作单元 2：AGD_ADM.1-7

ISO/IEC 15408-3 AGD_ADM.1.7C 管理员指南应与评估提交的所有其他文档保持一致。

评估者*应检查*管理员指南，以确定它与评估提交的所有其他文档是一致的。

特别是在 ST 中可能包含一些对 TOE 管理员提出的关于 TOE 安全环境和安全目的的详细的警告信息。

有关一致性分析的指南参见 A.3“一致性分析”。

11.7.2.4.8 工作单元 2:AGD_ADM.1-8

ISO/IEC 15408-3 AGD_ADM.1.8C 管理员指南应描述所有与管理员有关的 IT 环境安全要求。

评估者***应检查***管理员指南,以确定它描述了所有与管理员有关的 TOE 的 IT 环境安全要求。

如果 ST 中不包含 IT 环境的 IT 安全要求,本工作单元不适用,并视为已经满足。

本工作单元仅与 IT 安全要求有关,而与组织安全策略无关。

评估者应当分析关于 TOE 的 IT 环境安全要求(ST 中的可选陈述),并与管理员指南比较,以确保 ST 中与管理员有关的所有安全要求都在管理员指南中得到适当的描述。

11.7.3 用户指南评估(AGD_USR.1)

11.7.3.1 目的

本子活动的目的是为了确定用户指南是否描述了由 TSF 提供的安全功能和接口,以及指南是否提供了安全使用 TOE 的相关说明和指导。

11.7.3.2 输入

本子活动的评估证据是:

a) ST;
b) 功能规范;
c) 高层设计;
d) 用户指南;
e) 管理员指南;
f) 安全安装、生成和启动程序。

11.7.3.3 应用注释

在 ST 中可定义不同的用户角色或用户组,这些角色和组能被 TOE 识别并可执行 TOE 的安全功能。这些角色的能力和相应的特权在 FMT 类中进行描述。用户指南中应考虑不同的用户角色和组。

11.7.3.4 行为 AGD_USR.1.1E

11.7.3.4.1 工作单元 2:AGD_USR.1-1

ISO/IEC 15408-3 AGD_USR.1.1C 用户指南应描述 TOE 的非管理员用户可使用的功能和接口。

评估者***应检查***用户指南,以确定其描述了 TOE 的非管理员用户可使用的安全功能和接口。

用户指南应包含安全功能的概述,这些安全功能在用户界面中可见的。

用户指南应当标识和描述安全接口和功能的用途。

11.7.3.4.2 工作单元 2:AGD-USR.1-2

ISO/IEC 15408-3 AGD_USR.1.2C 用户指南应描述用户可访问的由 TOE 提供的安全功能的使用。

评估者***应检查***用户指南,以确定它描述了用户可访问的由 TOE 提供的安全功能的使用。

用户指南应标识和描述用户可用安全接口和功能的行为及其相互关系。

如果允许用户调用 TOE 安全功能,用户指南应为用户提供该功能接口的描述。

对每个接口和功能,用户指南应当:

a) 描述调用接口的方法(如命令行、程序语言系统调用、菜单选择、命令按钮);
b) 描述由用户设置的参数及其有效值和默认值;

c) 描述即时的 TSF 响应、消息或返回代码。

11.7.3.4.3 工作单元 2:AGD-USR.1-3

ISO/IEC 15408-3 AGD_USR.1.3C 用户指南应包含了在安全处理环境中受控的用户可访问功能和特权的警示信息。

评估者***应检查***用户指南,以确定其包含了在安全处理环境中受控的用户可访问功能和特权的警示信息。

TOE 的配置可以允许用户拥有不同的特权来使用 TOE 的不同功能,这意味着可以授权某些用户执行某些功能,而其他用户无权执行,这些用户可访问的功能和特权应在用户指南应中进行描述。

用户指南应标识可用的功能和特权、所需命令的类型以及使用这些命令的理由。用户指南应当包含使用受控的功能和特权时的警告。警告应当说明预期的效果、可能的负面影响以及与其他功能和特权可能的相互作用。

11.7.3.4.4 工作单元 2:AGD_USR.1-4

ISO/IEC 15408-3 AGD_USR.1.4C 用户指南应清晰地阐述安全操作 TOE 所必需的所有用户职责,这些职责包括那些在 TOE 安全环境陈述中的与用户行为相关的假设。

评估者***应检查***用户指南,以确定其阐述了安全操作 TOE 所必需的所有用户职责,这些职责包括那些在 TOE 安全环境陈述中的与用户行为相关的假设。

关于用户行为的假设可以在 ST 的 TOE 安全环境陈述中有比较详细的描述,在用户指南中只需包含涉及 TOE 安全操作的信息。

用户指南应当提供关于有效使用这些安全功能的建议(如审查口令组合的习惯、对用户文件备份频率的建议、对改变用户访问特权所产生影响的讨论)。

例如,要安全操作 TOE 用户有责任对他们的口令进行保密。

用户指南应指出用户是否能够调用某项功能,或者用户是否需要管理员的帮助。

11.7.3.4.5 工作单元 2:AGD-USR.1-5

ISO/IEC 15408-3 AGD_USR.1.5C 用户指南应与评估提交的所有其他文档保持一致。

评估者***应检查***用户指南,以确定其与评估提交的所有其他文档是一致的。

评估者要确保用户指南和评估提交的所有其他文档不会相互矛盾。如果 ST 包含任何对 TOE 用户提出的关于 TOE 安全环境和安全目的的详细警告信息,这一点就尤其重要。

有关一致性分析的指南参见 A.3“一致性分析”。

11.7.3.4.6 工作单元 2:AGD-USR.1-6

ISO/IEC 15408-3 AGD_USR.1.6C 用户指南应描述所有与用户有关的 IT 环境安全要求。

评估者***应检查***用户指南,以确定其描述了所有与用户有关的 TOE 的 IT 环境安全要求。

如果 ST 中不包含 IT 环境的 IT 安全要求,本工作单元不适用,并视为已经满足。

本工作单元仅与 IT 安全要求相关,而与组织安全策略无关。

评估者应分析 TOE 的 IT 环境安全要求(ST 中的可选陈述),并与用户指南比较,以确保所有与用户有关的 ST 安全要求都在用户指南中得到了恰当的描述。

11.8 测试活动

本活动的目的是通过对 TSF 的一个子集进行独立测试,确定 TOE 的行为是否与设计文档中所规定的一样,并且与 ST 中规定的 TOE 安全功能要求一致。

11.8.1 应用注释

评估者分析开发者的测试，以确定该测试足以证实安全功能按照规范执行，并理解开发者的测试方法。评估者也执行开发者测试的一个子集，以确信开发者的测试结果。评估者将使用该分析结果作为对 TSF 一个子集进行独立测试的输入。对于该子集，评估者应采取不同于开发者测试的测试方法，特别是当开发者测试有缺陷时。

评估者测试子集的构成和大小依赖于独立测试子活动（ATE_IND.2“独立测试——抽样”）中所讨论的几个因素。已知的公开弱点便是这类因素之一，评估者需得到这些信息（例如，从评估体制获取）。

为了确定开发者的测试文档是否充分，或者为了建立新的测试，评估者应理解安全功能在其满足要求的情况下所期望的预期行为。评估者可以每次选择 TSF 的某个安全功能，检查 ST 要求以及功能规范和指导性文档中的相关部分，以获得对 TOE 的预期行为方式的理解。

1.8.2 覆盖评估（ATE_COV.1）

11.8.2.1 目的

本子活动的目的是确定开发者的测试覆盖证据是否说明了测试文档中标识的测试与功能规范之间的对应性。

11.8.2.2 输入

本子活动的评估证据是：

a） 功能规范；

b） 测试文档；

c） 测试覆盖证据。

11.8.2.3 应用注释

要求开发者提供的覆盖分析应说明作为评估证据的测试与功能规范之间的对应性。不过，覆盖分析不必表明所有的安全功能都已被测试，也不必表明 TSF 的所有外部接口都已被测试。评估者在独立测试（ATE_IND.2“独立测试——抽样”）子活动中应考虑到这些不足之处。

11.8.2.4 行为 ATE_COV1.1E

11.8.2.4.1 工作单元 2：ATE_COV.1-1

ISO/IEC 15408-3 ATE_COV.1.1C 测试覆盖的证据应说明测试文档中所标识的测试与功能规范中所描述的 TSF 之间的对应性。

评估者***应检查***测试覆盖的证据，以确定测试文档中所标识的测试与功能规范之间的对应性是准确的。

对应性可采用表格或矩阵的形式来表示。该组件需要的证据应显示出覆盖的广度，而不需显示出全部覆盖。如果测试覆盖不足，评估者应提高独立测试的级别来作补偿。

图 8 显示了功能规范中所描述的安全功能与测试文档中概括的测试之间对应关系的概念性框架。测试中可能包括一项或几项安全功能，这取决于测试依赖性或实施测试的总体目标。

测试标识和测试覆盖证据中所列出的安全功能应当是明确无误的，并且在已标识的测试和所测试安全功能的功能规范之间提供了明确的对应关系。

图 8 中没有对 SF-3 进行测试，所以关于功能规范的覆盖是不完备的。但不完备的覆盖并不影响本子活动的裁定，因为测试覆盖证据没有必要显示出功能规范中所标识安全功能的完全覆盖。

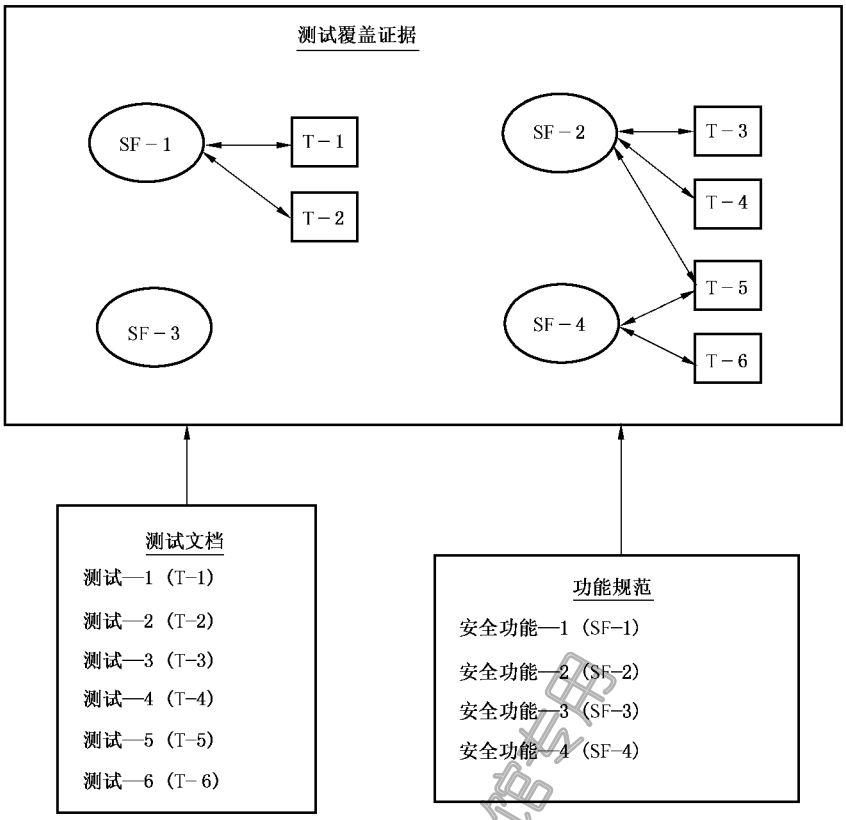

图 8　测试覆盖证据的概念框架

11.8.3　功能测试评估（ATE_FUN.1）

11.8.3.1　目的

本子活动的目的是确定开发者的功能测试文档是否可充分地证实安全功能都以按规定实现。

11.8.3.2　输入

本子活动的评估证据是：

a）　ST；

b）　功能规范；

c）　测试文档；

d）　测试流程。

11.8.3.3　应用注释

测试文档应覆盖 TSF 的程度依赖于覆盖保证组件。

对于开发者提供的测试，评估者确定测试是否是可复验的，并确定开发者的测试在多大程度上可用于评估者的独立测试工作。开发者测试结果中表明可能有未按照规定执行的安全功能，评估者应对其进行独立测试，以确定情况是否属实。

测试文档应标识为测试建立测试条件或为后续测试清除相关条件而使用特权模式的情况。测试文档要描述为什么必需使用特权模式以获得必要的条件（例如，测试套件的效率、产生测试所需的非特权用户不能创建的特殊对象），以及在执行 TOE 安全功能测试步骤前如何退出特权模式。因此，虽然在

建立测试条件时,测试配置可能与 ST 中描述的 TOE 不一致,但是测试文档应描述如何使配置返回到与 ST 所描述配置相一致的状态,以便执行测试步骤。

11.8.3.4 行为 ATE_FUN.1.1E

11.8.3.4.1 工作单元 2:ATE_FUN.1-1

ISO/IEC 15408-3 ATE_FUN.1.1C 测试文档应包括测试计划、测试流程描述、预期测试结果和实际测试结果。

评估者***应检查***测试文档是否包括测试计划、测试流程描述、预期测试结果和实际测试结果。

11.8.3.4.2 工作单元 2:ATE_FUN.1-2

ISO/IEC 15408-3 ATE_FUN.1.2C 测试计划应标识要测试的安全功能,并应描述测试的目标。

评估者***应核查***测试计划是否标识了待测安全功能。

用于标识待测安全功能的一种方法是可参考规定特定安全功能的功能规范中所描述的相应部分。

在执行本工作单元时,评估者可能希望采用抽样的策略。

关于抽样的指南参见 A.2“抽样”。

11.8.3.4.3 工作单元 2:ATE_FUN.1-3

评估者***应检查***测试计划,以确定它描述了测试的目标。

测试计划提供了关于安全功能如何测试的信息以及测试过程中的测试配置信息。

在执行本工作单元时,评估者可能希望采用抽样的策略。

关于抽样的指南参见 A.2“抽样”。

11.8.3.4.4 工作单元 2:ATE_FUN.1-4

评估者***应检查***测试计划,以确定 TOE 测试配置是否与在 ST 中列出的评估配置一致。

开发者测试计划中所提到的 TOE,其唯一参照号应与 CM 能力(ACM-CAP.*)子活动建立的唯一参照号相同。

ST 有可能指定不止一个评估配置,TOE 可能由多个不同的硬件和软件实现组成,应根据 ST 对它们进行测试。评估者要核实在开发者测试文档中所标识的测试配置是否与 ST 中描述的每个评估配置相一致。

评估者应考虑 ST 中描述的可适用于测试环境的关于 TOE 环境安全方面的假设。ST 中的某些假设可能不适用于测试环境。例如,关于用户许可方面的假设就可能不适用,但关于网络单点接入的假设就适用。

11.8.3.4.5 工作单元 2:ATE_FUN.1-5

评估者***应检查***测试计划,以确定它是否与测试流程描述一致。

在执行本工作单元时,评估者可能希望采用抽样的策略。

关于抽样的指南参见 A.2“抽样”,关于一致性分析的指南参见附录 A.3“一致性分析”。

11.8.3.4.6 工作单元 2:ATE_FUN.1-6

ISO/IEC 15408-3 ATE_FUN.1.3C 测试流程描述应标识要执行的测试和描述每个安全功能的测试情景。这些情景应包括对于其他测试结果的任何顺序依赖性。

评估者***应核查***测试流程描述是否标识了每一个待测安全功能行为。

用于标识待测安全功能行为的一种方法是引用设计规范中规定特定待测行为的相应部分。

在执行本工作单元时,评估者可能希望采用抽样的策略。

关于抽样的指南见 A.2“抽样”。

11.8.3.4.7 工作单元 2:ATE_FUN.1-7

评估者***应检查***测试流程描述,以确定是否提供了足够的命令以建立可重复的测试初始条件,有时也包括顺序依赖关系。

为建立初始条件可能要采取一些步骤。例如,用户账号应在其能被删除前添加。对于与其他测试结果有顺序依赖关系的一个例子是,在依靠审计功能对其他安全机制如访问控制产生审计记录之前,需要测试审计功能。另一个顺序依赖关系的例子是,某个测试用例所产生的数据文件被用作其他测试用例的输入。

在执行本工作单元时,评估者可能希望采用抽样的策略。

关于抽样的指南参见 A.2“抽样”。

11.8.3.4.8 工作单元 2:ATE_FUN.1-8

评估者***应检查***测试流程描述,以确定是否提供了足够的命令,以便拥有可重复的手段来激发安全功能和观察安全功能行为。

激励通常通过 TSFI 从外部提供给安全功能。一旦输入(激励)传给了 TSFI,安全功能行为就可以在 TSFI 观察到。除非测试流程包含足够的细节以明确无误地描述激励和期望作为该激励结果的行为,否则不能保证测试是可重复执行的。

在执行本工作单元时,评估者可能希望采用抽样的策略。

关于抽样的指南参见 A.2“抽样”。

11.8.3.4.9 工作单元 2:ATE_FUN.1-9

评估者***应检查***测试流程描述,以确定它们与实际测试流程是一致的。

如果两者一致,那么本工作单元就不适用,并认为已经满足要求。

在执行本工作单元时,评估者可能希望采用抽样的策略。

关于抽样的指南参见 A.2“抽样”,关于一致性分析的指南参见 A.3“一致性分析”。

11.8.3.4.10 工作单元 2:ATE_FUN.1-10

ISO/IEC 15408-3 ATE_FUN.1.4C 预期测试结果应指出测试成功执行后的预期输出。

评估者***应检查***测试文档,以确定其包括了足够的预期测试结果。

预期的测试结果用以确定测试是否成功执行。如果预期测试结果是明确无误的并且与给定测试方法的预期行为是一致的,那么该预期结果就足够了。

在执行本工作单元时,评估者可能希望采用抽样的策略。

关于抽样的指南参见 A.2“抽样”。

11.8.3.4.11 工作单元 2:ATE_FUN.1-11

ISO/IEC 15408-3 ATE_FUN.1.5C 开发者执行测试所得到的测试结果应证实每个被测试的安全性功能都按照规定执行。

评估者***应检查***测试文档中的预期测试结果,是否与给出的实际测试结果一致。

由开发者提供的实际测试结果和预期测试结果的比较将揭示出二者间的任何不一致。

只有当对某些数据进行约减或综合后,方可进行实际结果的直接比较。在这种情况下,开发者的测

试文档应描述约减或综合真实数据的过程。

例如,开发者可能需要在网络连接建立后测试消息缓冲区以确定缓冲区中的内容。消息缓冲区将包含一个二进制数。这个二进制数应被转换为其他的数据表现形式以使测试更有意义。开发者应足够详细地描述从数据的二进制表示到更高级表示的转换,以便评估者能够实施转换过程(例如,同步或异步传输、停止位位数、奇偶校验位数等)。。

应当注意,评估者使用约减或综合真实数据过程的描述,不是实际执行必要的修改,而是评定这一过程是否正确。开发者负责把预期测试结果转换为容易与实际测试结果相比较的格式。

在执行本工作单元时,评估者可能希望采用抽样的策略。

关于抽样的指南参见 A.2“抽样”。

如果任何测试的预期结果和实际结果不相同,那么表明安全功能没有正确执行。这种情况将会影响评估者的独立测试努力,包括隐含安全功能的测试。评估者要考虑增加本工作单元执行的证据样本。

11.8.3.4.12 工作单元 2:ATE_FUN.1-12

评估者***应报告***开发者测试工作,概述测试方法、配置、深度和结果。

对于在 ETR 中报告的开发者测试信息,可以允许评估者转述开发者测试 TOE 时的方法和成果。提供这种信息的目的是为了对开发者的测试工作给出一个有意义的概述,在 ETR 中关于开发者测试的信息不是为了精确再现特定的测试步骤或个别测试结果。其目的是要提供足够的细节,以便允许其他评估者和监督者了解开发者的测试方法、执行的测试数量、TOE 测试配置和开发者测试的总体结果。

一般可在 ETR 中找到关于开发者测试工作的信息有:

a) TOE 测试配置,被测 TOE 的特殊配置;
b) 测试方法,开发者全部测试策略的账目;
c) 开发者执行的测试数量,开发者测试覆盖和深度的描述;
d) 测试结果,开发者测试结果的整体描述。

以上列出的信息并不全面,只是为应呈现在 ETR 中的关于开发者所做测试的信息类型提供借鉴。

11.8.4 独立测试评估(ATE_IND.2)

11.8.4.1 目的

本子活动的目的是通过对 TSF 的一个子集进行独立测试,确定 TOE 是否按规定执行。同时,通过抽样执行开发者的测试,以获得对开发者测试结果的信任。

11.8.4.2 输入

本子活动的评估证据是:

a) ST;
b) 功能规范;
c) 用户指南;
d) 管理员指南;
e) 安全安装、生成和启动程序;
f) 测试文档;
g) 测试覆盖分析;
h) 测试深度分析;
i) 适于测试的 TOE。

11.8.4.3 行为 ATE_IND.2.1E

11.8.4.3.1 工作单元 2:ATE_IND.2-1

ISO/IEC 15408-3 ATE_IND.2.1C TOE 应适合测试。

评估者***应检查***TOE,以确定测试配置与所评估的 ST 中规定的配置是一致的。

用于评估者测试的 TOE,其唯一参照号应与 CM 能力(ACM-CAP.*)子活动建立的唯一参照号相同。

ST 有可能指定不止一个评估配置,TOE 可能由多个不同的硬件和软件实现组成,应根据 ST 对它们进行测试。评估者的 TOE 测试配置应与 ST 中所描述的每个评估配置相一致。

评估者应考虑 ST 中所描述的可用于测试环境的关于 TOE 环境安全方面的假设。ST 中可能有一些假设不适用于测试环境。例如,关于用户许可方面的假设可能就不适用,但关于网络单点接入的假设就适用。

如果使用了任何测试资源(例如仪表、分析仪),评估者有责任保证这些资源是校准正确的。

11.8.4.3.2 工作单元 2:ATE_IND.2-2

评估者***应检查***TOE,以确定它已被正确安装并处于一个已知状态。

评估者可能以多种方式来确定 TOE 的状态。例如,只要评估者仍然相信正在用于测试的 TOE 是正确安装的并且处于一个已知状态,先前的 ADO_IGS.1"安装、生成和启动程序"子活动的成功完成将满足本工作单元。如果情况不是这样,那么评估者只需根据提供的指南按照开发者的规程来安装、生成和启动 TOE。

如果由于 TOE 处于未知状态,评估者不得不执行安装过程,在成功完成后即可满足工作单元 ADO_IGS.1-2 的要求。

11.8.4.3.3 工作单元 2:ATE_IND.2-3

ISO/IEC 15408-3 ATE_IND.2.2C 开发者应提供一组相当的资源,该资源曾被用于开发者的 TSF 功能测试。

评估者***应检查***开发者提供的资源集,以确认它们与开发者做 TSF 功能测试时使用的资源集等同。

资源集可能包括实验室和专用测试设备等。这里的资源与开发者所使用的资源不一定完全相同,但在对测试结果的影响方面上,两者应是等同的。

11.8.4.4 行为 ATE_IND.2.2E

11.8.4.4.1 工作单元 2:ATE_IND.2-4

评估者***应设计***一个测试子集。

评估者选择一个适合于 TOE 的测试子集和测试策略。一个极端的测试策略是让测试子集包含尽可能多的安全功能,但不是很严格地测试它们。另一个极端的测试策略是根据觉察到的相关性,让测试子集包含少数几个安全功能,并严格地测试这些安全功能。

评估者采用的测试方法一般会处于这两种极端情况之间。评估者应至少使用一项测试来试验 ST 中标明的大部分安全功能要求,但不必进行所有的规范测试。

评估者在选择被测 TSF 子集时应该考虑以下因素:

a) 开发者测试证据。开发者测试证据包括测试覆盖分析、测试深度分析和测试文档。开发者测试证据将使评估者了解有关安全功能是如何被开发者测试的。当评估者在开发新的测试来对

TOE 进行独立性测试时会用到这一信息。评估者应特别考虑：

1） 针对特定安全功能，增加开发者测试。评估者或许希望通过修改参数进行多个同类测试，以便更严格地测试安全功能；

2） 针对特定安全功能，补充开发者测试策略。评估者或许希望通过使用另外一个测试策略测试某个特定的安全功能，以改变对该安全功能的测试方法。

b） 测试子集中包括的安全功能个数。如果 TOE 只包含少量安全功能，就要对所有安全功能进行严格测试。如果 TOE 包含很多安全功能，执行全班测试将是不合算的，此时可执行抽样测试。

c） 维持评估活动的平衡。评估者花费在测试活动上的工作应与花费在其他评估活动上的工作相称。

评估者选择安全功能组成测试子集。这种选择依赖于很多因素，对这些因素的考虑也可能影响测试子集大小的选择：

a） 开发者对安全功能测试的严格性。根据 ATE_COV.2“覆盖分析”的要求，在功能规范中所标识的所有安全功能应具有开发者测试证据。评估者决定需要补充测试的那些安全功能应包括在测试子集中。

b） 开发者测试结果。如果开发者的测试结果导致评估者对某个安全功能或某个方面产生怀疑，那么评估者应该将这些安全功能包括在测试子集中。

c） 与 TOE 的类型（例如，操作系统、防火墙）相关的已知公共域中的弱点。这些弱点将影响测试子集的选择过程。评估者应将涉及这些弱点的安全功能包含在子集中（这里的已知公共域中的弱点并不是指脆弱性，而是该类 TOE 所带有的不充分的情况或问题区）。如果不知道这样的弱点，那么采用选择更宽范围安全功能的这一通用方法可能更合适。

d） 安全功能的重要性。根据 TOE 的安全目的，那些较重要的安全功能应包含在测试子集中。

e） ST 中给出的 SOF 声明。所有有 SOF 声明的安全功能应包括在测试子集中。

f） 安全功能的复杂性。复杂的安全功能可能需要复杂的测试，这些测试对开发者或评估者施以更繁重的要求，这将不利用提高评估效率。相反，从更易找出错误的角度，复杂的安全功能又是子集的一个理想候选对象。因此，评估者需要在这些考虑因素之间寻求一种平衡。

g） 隐含的测试。某些安全功能的测试可能往往隐含着需要测试其他安全功能，把它们包括在子集中可以使被测安全功能数最大化（虽然是隐含的）。典型地，某些特定接口被用于提供多种安全功能特性，这是一种有效的测试方法。

h） TOE 的接口类型（例如，编程的、命令行的、协议的）。评估者应考虑在子集中包括 TOE 支持的所有不同接口类型的测试。

i） 创新的或不寻常的功能。当 TOE 包含有创新的或不寻常的安全功能时，这些功能在市场宣传中可能颇具分量，应该成为测试的重点候选对象。

这一部分指南清楚地说明了在选择合适的测试子集过程中应考虑的因素，但不代表已详述了所有因素。

有关抽样指南参见 A.2“抽样”。

11.8.4.4.2 工作单元 2：ATE_IND.2-5

评估者**应**为测试子集生成足够详细的测试文档，以便测试情况是可再现的。

参照 ST 和功能规范，在对一个安全功能的预期行为有了一定了解后，评估者应确定测试该功能的最可行的方法。

评估者应特别考虑以下几点：

a） 将采用的方法，例如，是否在外部接口上测试安全功能，是否使用测试设备在内部接口上测试安

全功能,或者使用其他测试方法(例如在异常情况下,代码检查);

b) 用于激发安全功能并观察响应的安全功能接口;

c) 测试所需的初始条件(例如,任何需要具备的特殊客体或主体以及它们需要拥有的安全属性);

d) 激发安全功能或观察安全功能所需的专用测试设备(例如,包发生器、网络分析仪)。

评估者可能发现,使用一系列测试用例测试每个安全功能是切实可行的,而每个测试用例将测试预期行为的某个特定的方面。

评估者的测试文档应指明每个测试的出处,如有必要,将其追溯到相关的设计规范和 ST。

11.8.4.4.3 工作单元 2:ATE_IND.2-6

评估者***应实施***测试。

评估者使用测试文档作为对 TOE 进行测试的基础。测试文档用作测试的基础,但是这并不排除评估者执行附加的特别测试。基于测试中发现的 TOE 行为,评估者可以设计新的测试,这些新的测试应记录在测试文档中。

11.8.4.4.4 工作单元 2:ATE_IND.2-7

评估者***应记录***包含在测试子集中的如下测试信息:

a) 待测试的安全功能行为的标识;

b) 测试设备的连接说明与设置说明;

c) 测试所需初始条件的说明;

d) 激发安全功能的说明;

e) 观察安全功能行为的说明;

f) 所有预期结果的描述,以及用以比较预期结果的必要分析;

g) 总结测试和为 TOE 建立必要的测试后状态的说明;

h) 实际测试结果。

测试文档中的细节描述应达到这样的程度:使其他评估者能重复测试并获得相同的结果,尽管测试结果的某些特定细节可能不同(例如,审计记录中的时间和日期字段),但整体结果应该是相同的。

有些情况可以不必提供本工作单元中出现的全部信息(例如,在可以与预期结果做比较前,可能不需要对实际测试结果进行任何分析)。这些信息的省略由评估者决定,这样才合理。

11.8.4.4.5 工作单元 2:ATE_IND.2-8

评估者***应核查***所有的实际测试结果,是否与预期测试结果一致。

实际测试结果和预期测试结果间的任何差别可能表明 TOE 与其规定不一致,或者评估者的测试文档是错误的。出现意料之外的实际测试结果,可能需要对 TOE 或测试文档进行纠正维护,也许需要重新运行受到影响的测试,并且修改测试样本的数量和组成。该决定由评估者作出,这样才合理。

11.8.4.5 行为 ATE_IND.2.3E

11.8.4.5.1 工作单元 2:ATE_IND.2-9

评估者***应***使用在开发者测试计划和测试流程中抽取的测试样本***实施***测试。

本工作单元的总体目的是要实施足够数量的开发者测试,以确认开发者的测试结果的有效性。评估者必需确定样本量和构成样本的开发者测试。

考虑到整个测试活动的评估工作,通常应该完成 20%的开发者测试,当然这可以根据 TOE 的特性和所提交的测试证据而改变。

所有的开发者测试都能被追溯到特定的安全功能。因此,在选择构成样本的测试时,所需考虑的因素要相似于在工作单元 ATE_IND.2-4 中为子集选择列出的那些因素。此外,评估者可以使用一个随机抽样的方法来选择构成样本的开发者测试。

有关抽样的指南参见 A.2“抽样”。

11.8.4.5.2 工作单元 2:ATE_IND.2-10

评估者***应核查***所有的实际测试结果,是否与预期测试结果一致。

开发者的预期测试结果和实际测试结果之间的不一致将迫使评估者解决这个差异。评估者最初遇到的不一致性可由开发者提供的合理解释和不一致性解决办法予以解决。

如果没有一个满意的解释或解决办法,评估者可能会降低对开发者测试结果的信任,并且有必要增加试样量,以便重新获取对开发者测试的信任。如果增加试样量还不能满足评估者的要求,就有必要重复整个开发者测试集。最后,就充分测试在工作单元 ATE_IND.2-4 中所标识的 TSF 子集而言,开发者测试的不足将导致要么需要对开发者测试进行纠正,要么由评估者产生新的测试。

11.8.4.5.3 工作单元 2:ATE_IND.2-11

评估者***应***在 ETR 中***报告***评估者的测试成果、测试大纲、配置、深度和结果。

在 ETR 中报告的评估者测试信息允许评估者告知总体测试方法和在评估过程中测试活动所付出的效果。提供这种信息的目的是对测试工作给出一个有意义的概述,这并不是为了精确再现特定的测试说明或个别测试结果。其目的是要提供足够的细节,以便允许其他评估者和监督者了解评估者所选择的测试方法、执行的评估者测试数量、执行的开发者测试数量、TOE 测试配置和测试活动的总体结果。

一般可在 ETR 中找到关于评估者测试工作的信息有:

a) TOE 测试配置。被测 TOE 的特殊配置;
b) 所选子集的大小。在评估中要被测试的安全功能的数量和确定子集大小的理由;
c) 构成子集的安全功能选择标准。简要说明在选择组成子集的安全功能时考虑的因素;
d) 被测的安全功能。包含在子集中的安全功能的简表;
e) 所执行的开发者测试。所执行的开发者测试的数量和对用于选择测试标准的一个简要描述;
f) 活动的裁定。对测试结果的总体判断。

以上列出的信息并不全面,只是为应呈现在 ETR 中的关于评估期间评估者所做测试的信息类型提供借鉴。

11.9 脆弱性评定活动

脆弱性评定活动的目的是确定 TOE 在预期使用环境下的缺陷或弱点的可利用性。这种确定是基于开发者所进行的分析,并由评估者的穿透性测试予以支持。

11.9.1 TOE 安全功能强度评估(AVA_SOF.1)

11.9.1.1 目的

本子活动的目的是确定,在 ST 中是否为所有概率或置换机制作出了 SOF 声明,以及开发者在 ST 中所作的 SOF 声明是否都是有正确的分析予以支持。

11.9.1.2 输入

本子活动的评估证据是:

a) ST；
b) 功能规范；
c) 高层设计；
d) 用户指南；
e) 管理员指南；
f) TOE 安全功能强度分析。

11.9.1.3 应用注释

对 SOF 进行的分析在本质上是针对概率或置换的机制(例如,口令机制或生物识别)而实施的。尽管密码机制在本质上也是概率性的并且经常用“强度”来描述,但是 AVA_SOF.1“TOE 安全功能强度评估”却不适用于密码机制。对这种情况,评估者应遵循评估体制的规定来执行。

尽管 SOF 分析是在单个机制的基础上进行的,但是对 SOF 的总体判断却是基于功能的。当采用多个概率或置换机制来实现一个安全功能时,应分析每个不同的机制。提供安全功能的这些机制的组合方式将决定这个功能的总体 SOF 级别。评估者需要设计信息以理解这些机制如何协同工作才能实现一个功能,并且依据 ADV_HLD.1“描述性高层设计”给出这些信息的最小级别。评估者可获得由 EAL 确定的实际的设计信息,并且在必要时这些信息应能被用于支持评估者的分析。

对于涉及多个 TOE 域的 SOF 的讨论参见 ASE_REQ.1“IT 安全要求评估”。

11.9.1.4 行为 AVA_SOF.1.1E

11.9.1.4.1 工作单元 2:AVA_SOF.1-1

ISO/IEC 15408-3 AVA_SOF.1.1C 对于每个具有 TOE 安全功能强度声明的安全机制,TOE 安全功能强度分析应说明该机制达到或超过 PP/ST 中定义的最低强度级别。

评估者***应核查***开发者是否已为每个具有 SOF 声明的安全机制提供了 SOF 分析,该声明在 ST 中是以 SOF 级别的方式予以表示的。

如果仅以 SOF 度量标准的方式来声明 SOF,那么本工作单元是不适用的,视为已满足要求

SOF 级别分为基本级功能强度、中级功能强度或高级功能强度,这些级别是根据攻击潜力来定义的,参见 ISO/IEC 15408-1 第 2 章。表示成一个级别的最小整体 SOF 要求适用于所有非密码的概率或置换安全机制。但个别机制可能具有一个被表示成超出整体 SOF 要求级别的 SOF 声明。

确定实现一个攻击所必需的攻击潜力,从而确定出 SOF 级别的指南参见 A.8“功能强度和脆弱性分析”。

SOF 分析中要包含基本原理以证明 ST 中所作的 SOF 声明。

11.9.1.4.2 工作单元 2:AVA_SOF.1-2

ISO/IEC 15408-3 AVA_SOF.1.2C 对于每个具有特定 TOE 安全功能强度声明的安全机制,TOE 安全功能强度分析应说明该机制达到或超过 PP/ST 中定义的特定功能强度度量标准。

评估者***应核查***开发者是否已为每个具有 SOF 声明的安全机制提供了 SOF 分析,该声明在 ST 中是以度量标准的方式予以表示的。

如果仅以 SOF 级别的方式来声明 SOF,那么本工作单元是不适用的,视为已满足要求。

表示成一个级别的最小整体 SOF 要求适用于所有非密码的概率或置换机制。但个别机制可能具有一个被表示成满足或超出整体 SOF 要求度量的 SOF 声明。

SOF 分析中要包含基本原理以证明 ST 中所作的 SOF 声明。

11.9.1.4.3 工作单元 2:AVA_SOF.1-3

评估者*应核查*SOF 分析,以确定支持分析的任何主张或假设都是有效的。

例如,认为伪随机数发生器的特定实现将拥有必要的熵,该熵是产生与 SOF 分析相关的安全机制所必需的,那么该假设就是有缺陷的。

支持 SOF 分析的假设应该反映"最差情形",除非"最差情形"被 ST 确定是无效的。当许多不同的情形存在时,并且这些情形都是依赖于人类用户或攻击者行为时,代表最低强度的情形应被假设,除非如以上所述该情况无效。

例如,基于最大理论口令空间(例如所有可打印的 ASCII 码)的强度声明,就不是"最差情形",因为人类习惯于使用自然语言口令,但这样的行为却大大地减少了口令空间和相关强度。然而,如果在 ST 中列出了 TOE 使用的 IT 措施,例如用口令过滤器将自然语言口令的使用降至最少,那么这样的假设就是适当的。

11.9.1.4.4 工作单元 2:AVA_SOF.1-4

评估者*应检查*SOF 分析,以确定用以支持分析的任何算法、原理、性质和计算都是正确的。

本工作单元高度依赖于所考虑的机制类型。A.8"功能强度和脆弱性分析"提供了一个使用口令机制实现标识和鉴别功能的 SOF 分析实例;该分析考虑用最大口令空间以最终达到一个 SOF 级别。对于生物测量学,该分析应考虑解决方法和其他影响机制的欺骗敏感性的因素。

SOF 表示成一个级别,该级别是基于可击败安全机制所必需的最小攻击潜力。SOF 级别是在 ISO/IEC 15408-1 第 2 章中以攻击潜力进行定义的。

关于攻击潜力的指南参见 A.8"功能强度和脆弱性分析"。

11.9.1.4.5 工作单元 2:AVA_SOF.1-5

评估者*应检查*SOF 分析,以确定每个 SOF 声明被满足或超过。

关于 SOF 声明级别的指南参见 A.8"功能强度和脆弱性分析"。

11.9.1.4.6 工作单元 2:AVA_SOF.1-6

评估者*应检查*SOF 分析,以确定所有带有 SOF 声明的功能都达到了 ST 中所定义的最低强度级别。

11.9.1.5 行为 AVA_SOF.1.2E

11.9.1.5.1 工作单元 2:AVA_SOF.1-7

评估者*应检查*功能规范、高层设计、低层设计、用户指南和管理员指南,以确定所有的概率或置换机制都具有相应的 SOF 声明。

通过概率或置换机制实现的安全功能应由开发者予以标识,该标识应在 ST 评估活动期间予以验证。但是,由于 TOE 概要规范可能是执行此项活动的唯一有效证据,因此这种机制的识别可能是不完备的。作为本子活动输入的附加评估证据,可能识别出未在 ST 中列出的额外的概率或置换机制。如果是这样的话,那么应适当地更新 ST 以反映附加的 SOF 声明,而且开发者需提供额外的分析以证明该声明合理的,其可以作为评估者行为 AVA_SOF.1.1E 的输入。

11.9.1.5.2 工作单元 2:AVA_SOF.1-8

评估者*应检查*SOF 声明,以确定它们是正确的。

当 SOF 分析包括断言或假设时(例如,每分钟可能有多少次鉴别尝试),评估者应独立地确认它们是正确的。这可通过测试或独立的分析来完成。

11.9.2 脆弱性分析评估(AVA_VLA.1)

11.9.2.1 目的

本子活动的目的是确定在其预期使用环境中的 TOE 是否存在可利用的明显脆弱性。

11.9.2.2 输入

本子活动的评估证据是:

a) ST;
b) 功能规范;
c) 高层设计;
d) 用户指南;
e) 管理员指南;
f) 安全安装、生成和启动程序;
g) 脆弱性分析;
h) 功能强度声明分析;
i) 适于测试的 TOE。

本子活动的其他输入有:

a) 关于明显脆弱性的当前信息(例如:来自监督者)。

11.9.2.3 应用注释

术语“指南”在本子活动中指用户指南、管理员指南和安全安装、生成和启动程序。

对可利用脆弱性的考虑是由 ST 中安全目的和功能要求确定的。例如,如果 ST 中不要求描述防止安全功能被旁路的措施(不选 FPT_PHP“TSF 物理保护”、FPT_RVM“参照仲裁”和 FPT_SEP“域分离”),那么基于旁路的脆弱性就无需考虑。

脆弱性可能存在于公共域中,也可能不在,并且利用它可能需要技巧,也可能不要。这两方面是相关的,但是有区别的。不应仅仅因为脆弱性存在于公共域中而认为其容易被利用。

指南中的以下术语具有特定含义:

a) 脆弱性:在一定条件下能被利用来违反安全策略的 TOE 的弱点;
b) 脆弱性分析:系统地搜寻 TOE 中的脆弱性并且对所寻找到的脆弱性进行评判,以确定它们与 TOE 预期使用环境的关系;
c) 明显脆弱性:只要求对 TOE 有最低程度的了解、最小的技术复杂性和最少的资源就可公开利用的脆弱性;
d) 潜在脆弱性:怀疑在 TOE 中存在(根据假定的攻击途径)但并未被证实的脆弱性;
e) 可利用的脆弱性:在 TOE 预期使用环境下可被利用的脆弱性;
f) 不可利用的脆弱性:在 TOE 预期使用环境下不能被利用的脆弱性;
g) 残余脆弱性:一种几乎无法利用的脆弱性,但是在 TOE 预期使用环境下却能够被那些在预计之外的具备更大攻击潜力的攻击者所利用;
h) 穿透性测试:在 TOE 的预期使用环境下进行的测试,以确定已标识的 TOE 潜在脆弱性的可利用程度。

11.9.2.4 行为 AVA_VLA.1.1E

11.9.2.4.1 工作单元 2:AVA_VLA.1-1

ISO/IEC 15408-3 AVA_VLA.1.1C 脆弱性分析文档应描述对 TOE 交付件的分析,以寻找用户能够违反 TSP 的明显途径。

ISO/IEC 15408-3 AVA_VLA.1.2C 脆弱性分析文档应描述如何处理明显的脆弱性。

ISO/IEC 15408-3 AVA_VLA.1.3C 脆弱性分析文档应针对所有已标识的脆弱性,说明该脆弱性不能在 TOE 的预期使用环境中被利用。

评估者***应检查***开发者的脆弱性分析,以确定对明显脆弱性的搜索是否已经考虑了所有相关的信息。

开发者的脆弱性分析应涵盖开发者在所有评估交付件和公共域信息源中搜索到的明显脆弱性。评估者应使用交付件,不是执行独立的脆弱性分析(AVA_VLA.1"开发者脆弱性分析"中没有要求),而是将其作为评价开发者搜索明显脆弱性的基础。

公共域中的信息是高度动态的。因此,在开发者执行脆弱性分析和评估完成之间的这一段时间内可能在公共域中有新的脆弱性报告。具体在那一个点停止对公共域信息的监测是评估授权机构的问题,因此相应的指南和协议应从评估授权机构得到。

11.9.2.4.2 工作单元 2:AVA_VLA.1-2

评估者***应检查***开发者的脆弱性分析,以确定每个明显的脆弱性都已被描述,并就它在 TOE 的预期使用环境中为什么是不可利用的给出合理的解释。

希望开发者基于对 TOE 和公共域信息源的了解来寻找明显的脆弱性。如果指定的要求是仅识别明显脆弱性,则不需要进行详细的脆弱性分析。开发者根据以上的定义将信息过滤整理,从而说明在预期使用环境中明显的脆弱性是不可利用的。

评估者需要关注开发者脆弱性分析的以下三个方面:

a) 开发者的分析是否已考虑所有的评估交付件;

b) 在预期使用环境中是否有适当的措施来防止明显脆弱性被利用;

c) 是否有一些明显的脆弱性仍然未被识别。

评估者不宜过分关注已识别的脆弱性本身是不是明显的,除非其被开发者用来作为确定脆弱性是不可利用的依据。在这种情况下,对于已识别的脆弱性,评估者可通过确定是否可阻止拥有低攻击潜力的攻击者的攻击来验证这种论断。

明显脆弱性的概念与攻击潜力无关,后者由评估者在独立的脆弱性分析中确定。因为 AVA_VLA.1"开发者脆弱性分析"并不进行这样的活动,通常评估者不是以攻击潜力为基础对脆弱性进行搜索和过滤。然而,评估者仍可以在评估期间发现潜在的脆弱性,并且可通过参照明显脆弱性的定义和低攻击潜力的概念,确定应如何描述这些潜在的脆弱性。

只能限于评价开发者分析的有效性、对获得自公共域脆弱性信息的比较和对评估者在其他评估活动过程中所标识的其他脆弱性的比较,来确定是否仍然存在未识别的明显脆弱性。

如果存在下列条件中的一个或多个,那么脆弱性就是不可利用的:

a) (IT 或非 IT)环境中的安全功能或措施防止了在预期使用环境中脆弱性的利用。例如,限定只有授权用户可对 TOE 进行物理访问,可以有效地致使一个 TOE 脆弱性成为不可利用的脆弱性。

b) 脆弱性只能被拥有中级或高级攻击潜力的攻击者利用。例如,对于分布式 TOE 的会话劫持攻击的脆弱性来说,就需要一个高于能够利用明显脆弱性的攻击者才能利用该脆弱性。然而,

这样的脆弱性在 ETR 中被报告为残余脆弱性。

c) 在 ST 中既没有声明要抵抗的威胁，也没有声明要满足的组织安全策略。例如，一个防火墙，其 ST 中没有作有效性策略声明并易受到 TCP SYN 攻击(一种基于通用 Internet 协议的攻击，使得主机无法为连接请求提供服务)，不应仅基于这种脆弱性认为该评估活动失败。

关于确定利用某个脆弱性所应具备的攻击潜力的指南，请参见 A.8“功能强度和脆弱性分析”。

11.9.2.4.3 工作单元 2:AVA_VLA.1-3

评估者***应检查***开发者的脆弱性分析，以确定其与 ST 和指南都是一致的。

开发者的脆弱性分析可通过建议对 TOE 功能进行特殊配置或设置来处理一个脆弱性。如果认为这样的操作限制是有效的并与 ST 是一致的，那么所有这样的配置/设置都应该在指南中得到充分描述，这样才可能被用户使用。

11.9.2.5 行动 AVA_VLA.1.2E

11.9.2.5.1 工作单元 2:AVA_VLA.1-4

评估者***应***基于开发者的脆弱性分析***设计***穿透性测试。

评估者准备穿透性测试：

a) 当需尝试驳斥开发者的分析，质疑开发者关于脆弱性为什么不可利用的解释时；

b) 当需确定 TOE 在其预期使用环境中对未被开发者考虑到的脆弱性的敏感程度时。评估者应有权使用关于公共域中开发者尚未考虑到的明显脆弱性的最新信息(例如，来自监督者的信息)，也可拥有一些作为执行其他评估活动的结果而识别出的潜在脆弱性。

不能期望评估者对除明显脆弱性之外的脆弱性进行测试(即使那些脆弱性包括在公共域中)。然而，许多情况下，在确定可利用性之前，应先进行测试。如果作为评估专家意见，评估者发现一个明显脆弱性之外的脆弱性，则这样的脆弱性在 ETR 中被报告为残余脆弱性。

在理解可疑脆弱性的基础上，评估者决定出最合理的方法测试 TOE 是否存在这样的脆弱性。评估者应特别考虑：

a) 用于激发 TSF 和观察反应的安全功能接口；

b) 测试所需的初始条件(例如：任何需要存在的特殊客体或主体及它们需要拥有的安全属性)；

c) 激发安全功能或观察安全功能所需的专用测试设备(尽管不可能要求使用专门设备来利用一个明显的脆弱性)。

评估者可能会将发现采用一系列测试用例来进行穿透性测试是可行的，其中每个测试用例将测试一个特定的脆弱性。

11.9.2.5.2 工作单元 2:AVA_VLA.1-5

评估者***应***基于开发者的脆弱性分析***编制***穿透性测试文档，并且应足够详尽使得测试可重复。测试文档应包括：

a) 标识被测 TOE 的明显脆弱性；

b) 进行穿透性测试所需的所有测试设备连接和设置的说明；

c) 建立所有穿透性测试的必备条件的说明；

d) 激发 TSF 的说明；

e) 观察 TSF 行为的说明；

f) 所有预期结果的描述，并对用于比较预期结果的观察行为进行必要的分析；

g) 总结测试和为 TOE 建立必要的测试后状态的说明。

测试文档中的细节描述应达到这种程度:其他的评估者能再现测试并获得相同的结果。

11.9.2.5.3 工作单元 2:AVA_VLA.1-6

评估者*应*基于开发者的脆弱性分析*实施*穿透性测试。

评估者使用工作单元 4:AVA_VLA.1-4 产生的穿透性测试文档作为对 TOE 进行穿透性测试的基础,但这并不排除评估者执行其他特别的穿透性测试。如果有必要的话,评估者可根据在穿透性测试期间(如果由评估者执行)所获得的信息设计特别的测试,这些测试应记录在穿透性测试文档中。这些测试有必要深入研究意外的结果或观察结果,或在预先测试计划阶段评估者所要研究的潜在脆弱性。

11.9.2.5.4 工作单元 2:AVA_VLA.1-7

评估者*应记录*穿透性测试的实际结果。

尽管实际测试结果的某些特定细节可能与预期的不同(例如:审计记录中的时间和日期字段),但整体结果应该是相同的。任何差异都应被证明是合理的。

11.9.2.5.5 工作单元 2:AVA_VLA.1-8

评估者*应检查*所有的穿透性测试结果和所有脆弱性分析的结论,以确定 TOE 在其预期环境中没有可被利用的明显脆弱性。

如果结果显示 TOE 在预期环境中有可被利用的明显脆弱性,则评估者活动裁定为“不通过”。

11.9.2.5.6 工作单元 2:AVA_VLA.1-9

评估者*应*在 ETR 中*报告*穿透性测试工作、测试方法大纲、配置、深度和结果。

在 ETR 中报告的穿透性测试信息允许评估者描述全部穿透性测试方法和本子活动所做的工作。提供该信息的目的是对评估者的穿透性测试工作给出一个有意义的概述。这不意味着 ETR 中关于穿透性测试的信息完全复制于单个穿透性测试的具体测试步骤或测试结果。其目的是提供足够的细节,以便其他评估者和监督者了解所选择的穿透性测试方法、执行穿透性测试的数量、TOE 测试配置和穿透性测试活动的总体结果。

在 ETR 中,在有关评估者穿透性测试工作的章节中通常应包括以下信息:

a) TOE 测试配置。进行穿透性测试的 TOE 的特殊配置;

b) 进行穿透性测试的安全功能。穿透性测试所关注的安全功能简单列表;

c) 子活动的裁定。穿透性测试结果的总体判断。

以上列出的并不全面,只是为应在 ETR 中出现的,在评估期间评估者所做穿透性测试的信息的类型提供一些借鉴。

11.9.2.5.7 工作单元 2:AVA_VLA.1-10

评估者*应*在 ETR 中*报告*所有可利用的脆弱性和残余脆弱性,每种脆弱性应包括以下细节:

a) 来源(例如,在进行评估方法活动时构想到的、评估者知晓的、出版物上读到的);

b) 牵涉到哪些或哪个安全功能,哪些或哪个目的没有满足,违反了哪些或哪个组织安全策略和实现了哪些或哪个威胁;

c) 描述;

d) 在其预期环境中是否可被利用(例如,可利用的,还是残余的);

e) 识别出该脆弱性的评估方(例如开发者、评估者)的标识。

12 EAL3 评估

12.1 简介

EAL3 提供中等级别的保证级别。使用功能规范、指导性文档以及 TOE 的高层设计，对安全功能进行分析以理解安全行为。这种分析由 TOE 安全功能子集的独立测试、开发者基于功能规范和高层设计进行测试的证据、对开发者测试结果的选择性确认、功能强度分析、开发者搜索明显脆弱性的证据等来支持。通过开发环境控制措施的使用、TOE 配置管理和安全交付程序的证据，可获得进一步的保证。

12.2 目的

本章的目的是定义达到 EAL3 级评估所需的最少评估努力，并对完成评估的方式方法加以指导。

12.3 EAL3 评估相互关系

EAL3 级评估包括以下活动：

a) 评估输入任务(第 7 章)。

b) EAL3 评估活动包括：

1) ST 评估(第 9 章)；
2) 配置管理评估(12.4)；
3) 交付和运行文档评估(12.5)；
4) 开发文件评估(12.6)；
5) 指导性文档评估(12.7)；
6) 生命周期支持评估(12.8)；
7) 测试评估(12.9)；
8) 测试(12.9)；
9) 脆弱性评定评估(12.10)。

c) 评估输出任务(第 7 章)。

评估活动源于 ISO/IEC 15408-3 所包含的 EAL3 保证要求。

ST 评估应在所有 TOE 评估子活动之前启动，因为 ST 为执行这些评估子活动提供了基础和背景。

本章描述了构成 EAL3 评估的子活动。尽管各子活动通常可以或多或少的同时进行，但评估者应考虑子活动间的依赖关系。

有关依赖关系的指南参见附录 A。

12.4 配置管理活动

配置管理活动的目的是帮助用户识别被评估 TOE，确保配置项都已被唯一标识，并确保开发者用于控制和跟踪 TOE 改变的程序是充分的。这包括跟踪哪些改变、潜在的改变如何体现等方面的详细信息。

12.4.1 CM 能力评估（ACM_CAP.3）

12.4.1.1 目的

本子活动的目的是确定开发者是否已清楚地标识了 TOE 及其相关配置项，以及改变这些配置项的能力是否被适当的控制。

12.4.1.2 输入

本子活动的评估证据是：

a) ST；

b) 适于测试的 TOE；

c) 配置管理文档。

12.4.1.3 行为 ACM_CAP.3.1E

12.4.1.3.1 工作单元 3:ACM_CAP.3-1

ISO/IEC 15408-3 ACM_CAP.3.1C TOE 参照号对 TOE 的每个版本都应是唯一的。

评估者应当使用开发者的 CM 系统来确认参照号的唯一性，通过核查配置清单确认配置项是被唯一标识的。如果在评估过程中仅仅检查了一个版本，该项评估的证据是不完备的，因此评估者应该查找能够支持唯一参照号的参照系统（如，使用数字、字母或日期）。除非评估者确信该 TOE 能够被唯一标识，否则缺少任何一项参照都将导致对这项要求裁定为“不通过”。

评估者应该设法检查多个 TOE 版本（如，修正某个漏洞后的版本），以核查两个版本参照号的不同。

12.4.1.3.2 工作单元 3:ACM_CAP.3-2

ISO/IEC 15408-3 ACM_CAP.3.2C 应给 TOE 标记上参照号。

评估者***应核查***提交评估的 TOE 是否标记了参照号。

评估者应确保 TOE 包含唯一的参照号，以便区分 TOE 的不同版本。这可以通过提供在包装或介质上粘贴标签，或让 TOE 在运行时显示标记等措施来实现，以保证客户（例如在购买或使用时）能够识别出。

TOE 可提供某种方式使得它易于识别。例如，软件形式的 TOE 可以在启动例程中，或者在响应命令行输入时，显示其名称和版本号。硬件或固件形式的 TOE 可以通过将部件号以物理方式铭刻在 TOE 上来标识。

12.4.1.3.3 工作单元 3:ACM_CAP.3-3

评估者***应核查***所使用的 TOE 参照号是一致的。

如果 TOE 要多处标记，所有的标记应当是一致的。例如，作为 TOE 一部分而提交的任何一份已标记过的指导性文档都应与被评估的、使用的 TOE 相关。这样就可以确保客户能确认自己所购买和安装的 TOE 版本是经过评估的，并且他们所使用的指南与 ST 一致，可以正确的指导自己使用 TOE。评估者可以通过 CM 文档中的配置清单来验证标记使用的一致性。

评估者还应验证该 TOE 的参照号是否与 ST 一致。

有关一致性分析的指南参见 A.3“一致性分析”。

12.4.1.3.4 工作单元 3:ACM_CAP.3-4

ISO/IEC 15408-3 ACM_CAP.3.3C CM 文档应包含一个配置清单和一个 CM 计划。

评估者***应检查***所提交的 CM 文档是否包含了一份配置清单。

配置清单标识了在配置管理控制下进行维护的配置项。

12.4.1.3.5 工作单元 3:ACM_CAP.3-5

评估者***应核查***所提交的 CM 文档是否包含了一份 CM 计划。

12.4.1.3.6 工作单元 3:ACM_CAP.3-6

ISO/IEC 15408-3 ACM_CAP.3.4C 配置清单应唯一标识组成 TOE 的所有配置项。

评估者***应核查***配置清单,确认其唯一标识了每个配置项。

配置清单包括组成 TOE 的配置项列表,以及足以唯一标识所使用的每个配置项的版本信息(例如版本号)。评估者使用该清单来进行核查,确认在评估过程中使用了正确的配置项和正确的版本。

12.4.1.3.7 工作单元 3:ACM_CAP.3-7

ISO/IEC 15408-3 ACM_CAP.3.5C 配置清单应描述组成 TOE 的配置项。

评估者***应检查***配置清单,以确认其标识了组成 TOE 的配置项。

配置清单所涵盖配置项的最小范围由 ACM_SCP“CM 范围”给出。

12.4.1.3.8 工作单元 3:ACM_CAP.3-8

ISO/IEC 15408-3 ACM_CAP.3.6C CM 文档应描述用于唯一标识 TOE 所包含配置项的方法。

评估者***应检查***标识配置项的方法,以确定其描述了如何唯一地标识配置项。

12.4.1.3.9 工作单元 3:ACM_CAP.3-9

ISO/IEC 15408-3 ACM_CAP.3.7C CM 系统应唯一标识 TOE 所包含的所有配置项。

评估者***应核查***配置项,以确定它们是用一种与 CM 文档一致的方式来标识的。

通过核查配置项的标识来确认 CM 系统唯一标识了所有配置项。无论是组成 TOE 的所有配置项还是开发者作为评估证据提交的配置项草初稿,评估者确认每个配置项具有一个唯一的标识,并且在一定程度上是与 CM 文档所描述的唯一标识方法相一致。

12.4.1.3.10 工作单元 3:ACM_CAP.3-10

ISO/IEC 15408-3 ACM_CAP.3.8C CM 计划应描述 CM 系统是如何使用的。

评估者***应检查***CM 计划,以确定其描述了怎样使用 CM 系统以保持 TOE 配置项的完整性。

CM 计划应包括:

a) 在配置管理程序控制之下的开发环境中执行的所有活动(例如,配置项的建立、修改和删除);
b) 需要对配置项进行操作的人员角色及其责任(对于不同类型的配置项(如设计文档或源代码)标识不同的角色);
c) 用于确保只有授权人员才能够修改配置项的程序;
d) 用于确保多个配置项同时修改而不会导致并发问题的程序;
e) 由于程序的应用而产生的证据。例如,对于某个配置项的修改,CM 系统应记录所做的修改、修改的说明、受影响的所有配置项的标识、状态(例如:挂起或完成)、修改的日期和时间,这些内容可以记录在所作修改的审计迹或修改控制记录中;
f) TOE 版本的版本控制和确定唯一参照号的方法(例如,包括操作系统补丁的发布以及随后对其使用的检测)。

12.4.1.3.11 工作单元 3:ACM_CAP.3-11

ISO/IEC 15408-3 ACM_CAP.3.9C 证据应证实 CM 系统的运行与 CM 计划是一致的。

评估者***应核查***CM 文档,以确定其包括了 CM 计划中所标识的 CM 系统记录。

由 CM 系统产生的输出应向评估者提供所需的证据,使其确信 CM 计划正在被执行,而且所有的配置项都是按照 ACM_CAP.4.10C 所要求的那样,由 CM 系统进行维护的。输出一般包括修改控制表

格或者配置项访问批准表格。

12.4.1.3.12 工作单元 3:ACM_CAP.3-12

评估者*应检查*证据,以确定 CM 系统的使用方式与 CM 计划中描述的一致。

评估者应选取并检查对一个配置项执行了各种 CM 相关操作(例如,创建、修改、删除、恢复到以前版本)的证据样本,以证实 CM 系统的所有操作都已经完全按照文档化的程序执行。评估者确认这些证据包括了 CM 计划中所标识操作的全部信息。核查证据时评估者可以要求使用 CM 工具,可以选择对证据抽样。

有关抽样的指南参见 A.2“抽样”。

通过与选定的开发人员进行访谈,可以建立对 CM 系统正确运行和配置项有效维护的进一步信任。通过进行访谈,评估者可以进一步理解 CM 系统如何在实际中应用,并确认 CM 程序与 CM 文档中描述的一致。值得注意的是,这种访谈只能是对核查的补充而不能取代对文档证据的核查;如果单独进行文档核查即可满足要求,就没有必要再进行访谈。然而,对于一个内容范围很宽泛的 CM 计划,单从 CM 计划和记录来确认某些方面(例如角色和职责)不是很清楚的情况下,就有必要通过访谈来确认。

建议评估者通过核查开发现场以支持本活动。

有关现场检查的指南参见 A.5“现场核查”。

12.4.1.3.13 工作单元 3:ACM_CAP.3-13

ISO/IEC 15408-3 ACM_CAP.3.10C CM 文档应提供所有配置项都已经和正在 CM 系统下有效地进行维护的证据。

评估者*应核查*配置清单中标识的配置项是否正在 CM 系统下进行维护。

开发者使用的 CM 系统应当维持 TOE 的完整性。评估者应核查,对配置清单中的每类配置项(例如高层设计或源代码模块),都存在由 CM 计划所描述程序产生的证据样本。在这种情况下,抽样方法依赖于 CM 系统中用于控制 CM 项的粒度等级。例如,在配置清单中标识了 10000 个源代码模块,与只有 5 个或甚至只有 1 个源代码模块的情况相比,应采用不同的抽样策略。该活动应着重于确保 CM 系统的正确运行,而不是检测小错误。

有关抽样的指南参见 A.2“抽样”。

12.4.1.3.14 工作单元 3:ACM_CAP.3-14

ISO/IEC 15408-3 ACM_CAP.3.11C CM 系统应提供措施使得只能对配置项进行授权改变。

评估者*应检查*CM 计划中描述的访问控制措施,以确定其能够有效地防止对配置项的非授权访问。

评估者可使用多种方法确定 CM 访问控制措施的有效性。例如,评估者可以实施访问控制措施,以验证该程序措施不会被旁路。评估者可以使用由 CM 系统程序的输出结果,以及在工作单元 ACM_CAP.3-12 中核查的部分结果。评估者还可通过 CM 系统现场演示,确保所使用的访问控制措施得到有效执行。

12.4.2 CM 范围评估(ACM_SCP.1)

12.4.2.1 目的

本子活动的目的是确定开发者是否对 TOE 的实现表示、设计、测试、用户和管理员指南、CM 文档执行了配置管理。

12.4.2.2 输入

本子活动的评估证据是：

a) 配置项列表。

12.4.2.3 行为 ACM_SCP.1.1E

12.4.2.3.1 工作单元 3:ACM_SCP.1-1

ISO/IEC 15408-3 ACM_SCP.1.1C 配置项列表应包括：实现表示和 ST 中其他保证组件所要求的评估证据。

评估者***应核查***配置项列表是否包括了 ISO/IEC 15408 所要求的一组配置项。

该列表包括以下内容：

a) TOE 实现表示(即组成 TOE 的部件或子系统)。对纯软件 TOE 而言，实现表示可以只包括源代码；对包括硬件平台的 TOE 而言，实现表示就会是软件、固件以及相关硬件描述的结合体；

b) ST 中保证组件所要求的评估证据。

记录与实现相关并已报告的安全缺陷细节相关文档(例如，从开发者问题数据库中获得的问题现状报告)。

12.5 交付和运行活动

交付和运行活动的目的是判断程序文档是否齐全，该程序用于确保是以开发者期望的方式安装、生成和启动 TOE 的，以及 TOE 在交付过程中没有被修改。这里包含两个程序：运输过程使用的程序以及安装、生成和启动程序。

12.5.1 交付评估（ADO_DEL.1）

12.5.1.1 目的

本子活动的目的是确定交付文档是否描述了在将 TOE 分发到用户方时，用于维护其安全性的所有程序。

12.5.1.2 输入

本子活动的评估证据是：

a) 交付文档。

12.5.1.3 行为 ADO_DEL.1.1E

12.5.1.3.1 工作单元 3:ADO_DEL.1-1

ISO/IEC 15408-3 ADO_DEL.1.1C 交付文档应描述，在分发 TOE 版本到用户现场时用以维持其安全性所必需的所有程序。

评估者***应检查***交付文档，以确定其描述了将 TOE 或其一部分提交给用户方时，为维护其安全性所必需的所有程序。

对术语“必需的”的解释应考虑 TOE 的自身属性和 ST 中包含的信息。提供的保护措施程度应与 ST 中标识的假设、威胁、组织安全策略以及安全目的相称。在某些情况下，ST 中的这些内容可能没有明确的说明与交付相关。评估者应当确定是否已采取了一种均衡手段，使得在非安全开发过程中交付

也不存在明显弱点。

交付程序应描述 TOE 或其一部分在传输过程中为确定 TOE 的标识和维持其安全性而采取的相关程序。程序应当描述 TOE 的哪些部分需要按这些程序执行。适当时还应包括物理或电子的分发程序(例如从因特网下载)。交付程序涉及整个 TOE,包括应用软件、硬件、固件和文档。

交付文档的重点很可能是完整性度量的相关措施,如在 TOE 交付过程中所使用的验证其完整性的技术措施。然而,在某些 TOE 的交付过程中,交付的保密性和可用性却是重点,因而相关内容也应在交付程序中论述。

交付程序应适用于从生产环境到安装环境的整个交付过程(例如,包装、存储和分发)的各个阶段。

标准的商业化包装和交付惯例是可以接受的。这包括紧压包装、安全带或密封套。对于分发而言,邮寄或私人快递都是可以接受的。

交付程序选择是否适当受 TOE(例如,是软件还是硬件产品)和安全目的的影响。即使 TOE 的不同部分,交付程序不相同,但全部程序应适于满足全部安全目的。

12.5.1.4 隐含的评估者行为

12.5.1.4.1 工作单元 2:ADO_DEL.1-2

ISO/IEC 15408-3 ACM_DEL.1.2D 开发者应使用交付程序。

评估者***应检查***交付过程的各个方面,以确定交付程序得到了应用。

评估者检查交付程序执行情况所采取的方法,取决于 TOE 的种类和交付过程自身。除检查交付程序本身外,评估者还应当确保程序得到切实执行。可采取的核查方法如下:

a) 对可观察到程序实际运行情况的分发场所进行现场核查;

b) 在交付的中间阶段,或在用户现场对 TOE 进行检查(例如检查篡改封条);

c) 评估者通过从常规渠道获得 TOE 来观察交付过程是否在实际中得到使用;

d) 询问最终用户 TOE 是如何被交付的。

有关现场检查的指南参见 A.5“现场核查”。

可能有这样的情况:新开发的 TOE,交付程序还尚未实施。对于这种情况,评估者应确信有适当的程序和设施供以后的交付使用,而且所有相关人员都清楚各自的责任。可行的话,评估者可以要求演习交付过程。如果开发者还生产了其他类似产品,评估者还可以通过对这些产品交付程序的检查来进行确认。

12.5.2 安装、生成和启动评估(ADO_IGS.1)

12.5.2.1 目的

本子活动的目的是确定 TOE 的安全安装、生成和启动的程序和步骤是否都已文档化,并最终形成了一个安全的配置。

12.5.2.2 输入

本子活动的评估证据是:

a) 管理员指南;

b) 安全安装、生成和启动程序;

c) 适于测试的 TOE。

12.5.2.3 应用注释

安装、生成和启动程序是指配置 TOE 达到在 ST 中所描述的安全配置所必需的所有安装、生成和启动程序，不管它们是运行在用户现场，还是运行在开发现场。

12.5.2.4 行为 ADO_IGS.1.1E

12.5.2.4.1 工作单元 3：ADO_IGS.1-1

ISO/IEC 15408-3 ADO_IGS.1.1C 安装、生成和启动文档应描述 TOE 安全地安装、生成和启动必需的所有步骤。

评估者***应核查***是否已经提供了 TOE 安全安装、生成和启动所必需的所有程序。

如果不期望安装、生成和启动程序再次使用(例如，TOE 已经在运行状态下交付)，本工作单元(或者与此相关的部分)就不再适用，并视为已经满足。

12.5.2.5 行为 ADO_IGS.1.2E

12.5.2.5.1 工作单元 3：ADO_IGS.1-2

评估者***应检查***所提供的安装、生成和启动程序，以确认其描述了 TOE 安全安装、生成和启动所需的步骤。

如果不期望安装、生成、启动程序再次使用(例如，TOE 已经在运行状态下交付)，本工作单元(或者与此相关的部分)就不再适用，并视为已经满足。

安装、生成和启动程序可以提供以下详细信息：

a) 对 TSF 控制下相关实体的特定安全特性所做的修改；

b) 对异常情况和问题的处理；

c) 如果适用，列出安全安装所需的最低系统要求。

为了确认安装、生成和启动程序能够形成安全配置，评估者可以只使用所提供的指导性文档，按照开发者的程序，实施客户通常执行的活动以完成对 TOE 的安装、生成和启动(在适用于 TOE 的情况下)。本工作单元可以与工作单元 ATE_IND.1-2 一起被执行。

12.6 开发活动

开发活动的目的是评价设计文档，根据设计文档的充分性来理解 TSF 是如何提供 TOE 安全功能，以此来进行评价。这种理解是通过检查功能规范(描述 TOE 的外部接口)和表示对应性(将功能规范映射到 TOE 的概要规范，以保证一致性)来获得的。

12.6.1 应用注释

ISO/IEC 15408 要求设计文档根据形式化程度来分级。ISO/IEC 15408 将文档的形式化程度分为非形式化、半形式化、形式化三级。非形式化文档是指用自然语言来描述的文档。评估方法没有规定应采用某种语言，这个问题留给评估体制。以下段落分别说明了不同的非形式化文档内容的差别。

一个非形式化功能规范包括一个安全功能描述(类似于 TOE 概要规范的安全功能描述)和一个 TSF 外部可见接口描述。例如，如果操作系统提供给用户一些功能来进行自我身份标识，创建、修改或删除文件，设置文件的访问权限，与远程的机器进行通信，那么它的功能规范应包含对上述每一个功能的描述。如果还有检测和记录这些事件发生的审计功能，那么关于这些审计功能的描述也应该包含在功能规范中；尽管这些审计功能不直接被用户在外部接口所触发，但用户在外部接口的行为的确会对审

计功能产生影响。

每个子系统在其接口触发的响应行为有先后顺序,非形式化高层设计就是按照这种顺序来描述的。例如,一个防火墙可能包含一些处理包过滤、远程管理、审计和传输层过滤的子系统。防火墙的高层设计应当按照当一个输入包到达防火墙时,每个子系统所采取的行为来对防火墙采取的行为加以描述。

非形式化的对应性分析不需要采用叙述的方式,一个简单的二维映射就足够了。例如,一个矩阵,沿一个轴的方向列出了模块,沿另一个方向列出了子系统,其中的元素表示两者的对应性,这将在高层设计和低层设计之间提供足够的非形式化对应性。

12.6.2 功能规范评估(ADV_FSP.1)

12.6.2.1 目的

本子活动的目的是确认开发者对 TOE 安全功能是否作了充分描述,以及 TOE 提供的安全功能是否充分足以满足 ST 的安全功能要求。

12.6.2.2 输入

本子活动的评估证据是:

a) ST;
b) 功能规范;
c) 用户指南;
d) 管理员指南。

12.6.2.3 行为 ADV_FSP.1.1E

12.6.2.3.1 工作单元 3:ADV_FSP.1-1

ISO/IEC 15408-3ADV_FSP.1.1C 功能规范应使用非形式化风格来描述 TSF 及其外部接口。

评估者***应检查***功能规范,以确定其包括了所有必需的非形式化解释文本。

如果整个功能规范都是非形式化的,则本工作单元不适用,并视为已经满足要求。

对于那些只采用半形式化或形式化语言进行描述,难以被人理解的功能规范的某些组成部分(例如,为解释任何形式化符号的含义),有必要使用辅助性的叙述描述来帮助理解。

12.6.2.3.2 工作单元 3:ADV_FSP.1-2

ISO/IEC 15408-3ADV_FSP.1.2C 功能规范应是内在一致的。

评估者***应检查***功能规范,以确定它是内在一致的。

评估者通过检查 TSFI 接口描述与 TSF 功能描述是否一致来验证功能规范的一致性。

12.6.2.3.3 工作单元 3:ADV_FSP.1-3

ISO/IEC 15408-3 ADV_FSP.1.3C 功能规范应描述所有外部 TSF 接口的用途与使用方法,适当时应提供效果、例外情况和错误消息的细节。

评估者***应检查***功能规范,以确定其标识了所有的外部 TOE 安全功能接口。

术语"外部"指对用户而言是可见的。TOE 的外部接口或者是 TSF 的直接接口,或者是 TOE 的非 TSF 部分的接口。不过,这些非 TSF 接口可能最终通向 TSF。这些直接或间接通向 TSF 的外部接口共同组成了 TOE 安全功能接口(TSFI)。图 9 表示一个包含 TSF 部分(阴影部分)和非 TSF 部分(空白部分)的 TOE。该 TOE 有三个外部接口:接口 c 是 TSF 的直接接口;接口 b 是 TSF 的间接接口;接口 a 是 TOE 非 TSF 部分的接口。因此,接口 b 和 c 组成了 TSFI。

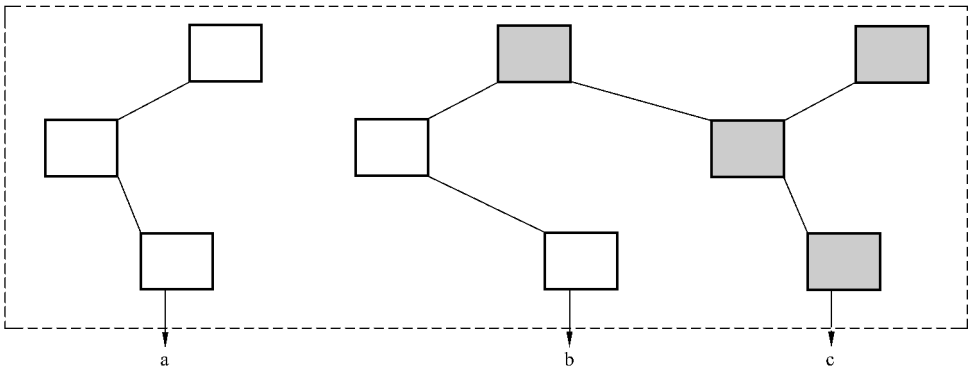

图 9　TSF 接口

应该注意的是，所有反映 ISO/IEC 15408-2 功能要求（或者在其扩展组件中）的安全功能应该有某种外部可见的表现形式。尽管有些安全功能不一定能通过其接口来验证，但由于它们在某种程度上是外部可见的，因此也应包含在功能规范中。

12.6.2.3.4　工作单元 3：ADV_FSP.1-4

评估者***应检查***功能规范，以确定其描述了所有外部的 TOE 安全功能接口。

对于一个没有恶意用户威胁的 TOE（即 FPT_PHP“TSF 物理保护”、FPT_RVM“参照仲裁”和 FPT_SEP“域分离”都被排除在 ST 之外），功能规范中描述的（和在其他 TSF 表示描述中进行了扩展的）只是那些通向和来自 TSF 的接口。缺少 FPT_PHP“TSF 物理保护”、FPT_RVM“参照仲裁”和 FPT_SEP“域分离”，就假设没有考虑任何安全特性的旁路，因而不用考虑其他接口可能施加给 TSF 的任何可能的影响。

另一方面，如果 TOE 存在恶意用户或旁路之类的威胁（即 FPT_PHP“TSF 物理保护”、FPT_RVM“参照仲裁”和 FPT_SEP“域分离”被包含在 ST 中），所有外部接口都需要在功能规范中进行描述，但是仅需描述到每一种影响都已明确的程度：安全功能的接口（即图 9 中的接口 b 和 c）都被描述了，然而其他接口仅仅描述到明确 TSF 不能通过这些接口（即图 9 中的接口 a，而不是 b）访问的程度。包含 FPT_PHP“TSF 物理保护”、FPT_RVM“参照仲裁”和 FPT_SEP“域分离”，意味着所有的接口将对 TSF 有某些影响。由于每一个外部接口都是潜在的 TSF 接口，因此，功能规范应对每一个接口进行详细的描述，以使得评估者能够确定接口是否与安全相关。

某些体系结构易于为外部接口群提供足够详细的描述。例如，在内核结构中所有对操作系统的调用都由内核程序来处理；任何有可能违反 TSP 的调用应由具备这种特权的程序来调用。所有实行特权的程序应被包含在功能规范中。任何在内核之外的没有实行特权的程序是无能力影响 TSP 的（即，这种程序是图 9 中的 a 类的接口，而不是 b 类），因而，可以被排除在功能规范之外。如果是基于上述的内核结构，而且评估者对这种结构能够顺利的了解，那么这种结构不是必需的。

12.6.2.3.5　工作单元 3：ADV_FSP.1-5

评估者***应检查***对 TSFI 的陈述，以确定其正确并充分地描述了每个表示效果、异常和出错信息的外部接口处的 TOE 行为。

为了评估接口描述的充分性和正确性，评估者使用功能规范、ST 的 TOE 概要规范以及用户和管理员指南来评估以下因素：

a) 应标识所有与安全相关的用户输入参数(或这些参数的特性)。为了全面起见,宜标识出管理员可用而普通用户无法直接控制的参数。

b) 对功能规范中语义的描述应当反映所审查指南中描述的所有安全相关行为。它包括一系列通过事件及其影响所表示的行为标识。例如,如果一个操作系统提供了丰富的文件系统接口,并对请求文件无法打开的各种原因(如拒绝访问、文件不存在、文件正被另一个用户使用、用户无权在下午 5 点后打开文件等)提供了不同的错误代码,功能规范应当解释该文件或者在请求下被打开,如不能打开则返回错误代码。(虽然功能规范可以列举所有错误的原因,但不需要提供细节描述)。对语义的描述应当包括安全要求如何应用于接口(例如,是否可以审计接口的使用情况,假如这样的话,应包含能够记录的信息)。

c) 应描述所有可能操作模式下的所有接口。如果 TSF 提供了特权的概念,对接口的描述应分别解释特权模式或非特权模式时,接口的工作方式。

d) 整个文档中安全相关参数的描述和接口的语法所包含的信息应当是一致的。

对以上因素的核实,是通过审核安全规范和 ST 的 TOE 概要规范、开发者提供的用户和管理员指南来完成的。例如,如果 TOE 是一个操作系统及其底层硬件,评估者可以查找用户可访问的程序的讨论、用于指导程序活动的协议的描述、用于指导程序活动的用户可访问数据库的描述,并查找适用于 TOE 的用户接口(例如命令、应用程序接口)。评估者还要确定处理器的指令集已进行描述。

这种核查可以反复进行,直到包含参数和出错信息的设计、源代码或其他证据都被检查为止,以避免发生功能规范描述不全的情况被评估者忽略。

12.6.2.3.6 工作单元 3:ADV_FSP.1-6

ISO/IEC 15408-3 ADV_FSP.1.4C 功能规范应完备地表示 TSF。

评估者***应检查***功能规范,以确定 TSF 已被完全表示。

为了评估 TSF 表示的完备性,评估者可查阅 ST 的 TOE 概要规范、用户指南和管理员指南。它们应当没有描述在功能规范的 TSF 表示中没有的安全功能。

12.6.2.4 行为 ADV_FSP.1.2E

12.6.2.4.1 工作单元 3:ADV_FSP.1-7

评估者***应检查***功能规范,以确定它是 TOE 安全功能要求的一个完备地实例。

为了确保功能规范涵盖了所有的 ST 安全功能要求,评估者应当建立 TOE 概要规范和功能规范之间的映射。为了满足(ADV_RCR.*“表示对应性”)的对应要求,开发者可能已经提交了这种映射证据;这时评估者只需要验证映射的完备性,确定所有的安全功能要求都映射到功能规范中适当的 TSFI 表示。

12.6.2.4.2 工作单元 3:ADV_FSP.1-8

评估者***应检查***功能规范,以确定它是 TOE 安全功能要求的一个准确实例化。

对于每个具有某种特性的安全功能的接口,功能规范中的详细信息应与 ST 中的相关信息所表述准确一致。例如,如果 ST 中的用户鉴别要求规定了口令长度应为 8 个字符,那么 TOE 应有 8 个字符的口令;如果功能规范描述的是 6 字符的固定长度口令,那么功能规范就不是 TOE 安全功能要求的一个准确实例化。

功能规范中对在受控资源上运行的每个接口,评估者应确定它是否返回了一个错误代码,该错误代码是因为某个安全要求的实施失败而导致的,如果没有返回错误代码,评估者应确定是否需要返回一个

错误代码。例如,操作系统可以提供一个接口用于打开一个受控对象,该接口描述中可包含因对受控对象作了未授权的访问而产生的一个错误代码。如果没有这种错误代码,评估者应当确认是否合理。(因为,也许访问仲裁是针对读、写的操作执行的,而不是针对打开的)。

12.6.3 高层设计评估(ADV_HLD.2)

12.6.3.1 目的

本子活动的目的是确定高层设计是否按照主要结构单元(例如子系统)提供了对 TSF 的描述,提供了这些结构单元接口的描述,并确定高层设计是功能规范的一个正确实现。

12.6.3.2 输入

本子活动的评估证据是:

a) ST;

b) 功能规范;

c) 高层设计。

12.6.3.3 行为 ADV_HLD.2.1E

12.6.3.3.1 工作单元 3:ADV_HLD.2-1

ISO/IEC 15408-3 ADV_HLD.2.1C 高层设计的表示应是非形式化的。

评估者***应检查***高层设计,以确定它包括了所有必需的非形式化解释性文本。

如果整个高层设计都是非形式化的,则本工作单元被视为不适用,并认为已经满足要求。

对于高层设计中那些仅以半形式化或形式化描述难以理解的部分(例如,为解释清楚任何形式化符号的含义),那么起辅助作用的叙述性描述是必需的。

12.6.3.3.2 工作单元 3:ADV_HLD.2-2

ISO/IEC 15408-3 ADV_HLD.2.2C 高层设计应是内在一致的。

评估者***应检查***高层设计的表述,以确定它是内在一致的。

有关一致性分析的指南见 A.3“一致性分析”。

评估者通过确定接口规范都是与子系统的用途描述相一致,来验证子系统的接口规范。

12.6.3.3.3 工作单元 3:ADV_HLD.2-3

ISO/IEC 15408-3 ADV_HLD.2.3C 高层设计应按子系统描述 TSF 的结构。

评估者***应检查***高层设计,以确定 TSF 是按子系统方式描述的。

关于高层设计中的术语“子系统”指的是大的相关单元(如内存管理、文件管理、进程管理)。通过把一个设计分成多个基本功能区,有助于理解设计思路。

检查高层设计的主要目的是帮助评估者理解 TOE。开发者对子系统定义的选择以及各个子系统中 TSF 分组的选择,是使高层设计有益于理解 TOE 预期运行的一个重要方面。作为本工作单元的一部分,评估者应当评估开发者列举的子系统数目是否恰当,各个子系统中功能分组的选择是否恰当。评估者应确定把 TSF 分解成子系统,足以使评估者从高层的角度来理解 TSF 的功能是如何提供的。

不必非得用“子系统”这个术语来描述高层设计中子系统这个概念,子系统应当代表一类相似级别的分解。例如,可以使用“层”“管理器”对设计进行分解。

在子系统定义的选择和评估者分析范围之间可能存在某些相互影响。对这种相互影响的讨论见工

作单元 3:ADV_HLD.2-10。

12.6.3.3.4 工作单元 3:ADV_HLD.2-4

ISO/IEC 15408-3 ADV_HLD.2.4C 高层设计应描述每个 TSF 子系统所提供的安全功能性。

评估者***应检查***高层设计,以确定它描述了每个子系统的安全功能。

子系统的安全功能行为是对子系统"做些什么"进行的描述。不仅要对子系统直接执行其功能的行为进行描述,而且还要将子系统对 TOE 的安全状态可能产生的影响进行描述(例如,改变主体、对象、安全数据库)。

12.6.3.3.5 工作单元 3:ADV_HLD.2-5

ISO/IEC 15408-3 ADV_HLD.2.5C 高层设计应标识 TSF 所需的任何基础性硬件、固件或软件,以及在这些硬件、固件或软件中实现的支持性保护机制所提供功能的一个表示。

评估者***应核查***高层设计,以确定它标识了 TSF 所需的所有硬件、固件和软件。

如果 ST 中没有对 IT 环境的安全要求,则本工作单元被视为不适用,并视为已经满足。

如果 ST 包含可选的 IT 环境安全要求,评估者比较高层设计中陈述的 TSF 所需硬件、固件或软件列表与 IT 环境安全要求的陈述,以确定两者的一致性。ST 中的信息刻画了 TOE 赖以运行的底层抽象机。

如果高层设计中的 IT 环境安全要求不属于 ST 中的已定义的 IT 环境安全要求,或者它们与包含在 ST 中的要求不同,那么评估者应根据 ADV_HLD.2.2E 评估行为对这种不一致性进行评估。

12.6.3.3.6 工作单元 3:ADV_HLD.2-6

评估者***应检查***高层设计,以确定它涵盖那些可以通过在底层硬件、固件或软件而实现的支持性保护机制功能的表示。

如果 ST 中没有 IT 环境安全要求,则本工作单元被视为不适用,并视为已经满足。

TOE 赖以运行的"根本抽象机"所提供功能的表示,不必象作为 TSF 组成部分的功能的表示那样详细。表示应当解释 TOE 如何使用硬件、固件或软件提供的功能,这些硬件、固件或软件实现了 TOE 用来支持 TOE 安全目的的 IT 环境安全要求。

IT 环境安全要求的陈述可以是抽象的,特别是当它打算由各种硬件、固件或软件的不同组合来满足时。作为测试活动的一部分,当能够为评估者提供至少一个声称满足 IT 环境安全要求的"根本机"的实例时,评估者就能够确定其是否为 TOE 提供了必要的安全功能。评估者的这种确认不需要测试和分析"根本机",只需要确定期望它提供的功能确实存在。

12.6.3.3.7 工作单元 3:ADV_HLD.2-7

ISO/IEC 15408-3 ADV_HLD.2.6C 高层设计应标识 TSF 子系统的所有接口。

评估者***应核查***高层设计是否标识了 TSF 子系统的接口。

对每个子系统,高层设计应当包括它的每个入口点的名称。

12.6.3.3.8 工作单元 3:ADV_HLD.2-8

ISO/IEC 15408-3 ADV_HLD.2.7C 高层设计应标识 TSF 子系统的哪些接口是外部可见的。

评估者***应核查***高层设计是否标识了 TSF 子系统的哪些接口是外部可见的。

正如在工作单元 3:ADV_FSP.1-3 所讨论的那样,外部接口(例如:那些用户可见的接口)可以直接或间接访问 TSF,任何直接或间接访问 TSF 的外部接口都应该包含在本工作单元的标识范围内,而那

些不能访问 TSF 的外部接口则不必包含在内。

12.6.3.3.9 工作单元 3:ADV_HLD.2-9

ISO/IEC 15408-3 ADV_HLD.2.8C 高层设计应描述 TSF 子系统所有接口的用途与使用方法,适当时应提供效果、例外情况和错误消息的细节。

评估者***应检查***高层设计,以确定它按照接口的用途和使用方法描述了每个子系统的接口,并且适当地提供了效果、例外情况和错误消息的详细描述。

高层设计应当包括按照用途和使用方法对每个子系统所有接口提供描述。可以对某些接口笼统地提供这样的描述,而对其他的接口提供更详细的描述。在决定应提供的效果、例外情况和错误信息的详细程度时,评估者应当考虑该分析的目的和 TOE 对接口的使用。例如,评估者需要理解子系统间交互作用的本质,以确认 TOE 设计是合理的,并能够通过子系统间某些接口的通用描述来获得这种理解。尤其是不被其他子系统调用的内部子系统入口点通常不需要进行详细描述。

描述的详细程度还依赖于为达到 ATE_DPT“深度”的要求而采用的测试方法。例如,只使用外部接口进行测试,和同时使用子系统的内外部接口相比,对描述的详细程度要求是不同的。

详细描述应当包括所有输入输出参数、接口的效果、接口产生的任何例外情况或错误信息的细节。对于外部接口,所需的描述很可能包括在功能规范中,可以在高层设计中引用而无需复制。

12.6.3.3.10 工作单元 3:ADV_HLD.2-10

ISO/IEC 15408-3 ADV_HLD.2.9C 高层设计应把 TOE 分成 TSP-实施和其他子系统来描述。

评估者***应核查***高层设计是否把 TOE 分成 TSP-实施和其他子系统来描述。

TSF 包括了 TSP 赖以实施的所有 TOE 组成部分。因为 TSF 既包括直接实施 TSP 的功能,又包括间接实施 TSP 的功能,所以 TSF 中包括了所有的 TSP-实施子系统。子系统如果不参与 TSP 的实施,就不是 TSF 的组成部分。如果子系统的任何部分都是 TSF 的组成部分,那么整个子系统就是 TSF 的组成部分。

正如在工作单元 3:ADV_HLD2-3 中所说明的那样,开发者对子系统定义的选择以及每个子系统内 TSF 分组的选择是使高层设计有益于理解 TOE 预期运行的一个重要方面。但是,子系统内 TSF 分组的选择也会影响到 TSF 的范围,因为一个具有直接或间接实施 TSP 功能的子系统是 TSF 的组成部分。尽管可理解性是很重要的,但限制 TSF 范围以减少所需分析的数量也同样重要。可理解性和范围减少有时相互矛盾,评估者在评估子系统定义的选择时,应牢记这一点。

12.6.3.4 行为 ADV_HLD.2.2E

12.6.3.4.1 工作单元 3:ADV_HLD.2-11

评估者***应检查***高层设计,以确认它是 TOE 安全功能要求的一个准确实例化。

评估者应分析高层设计中每个 TOE 的安全功能,以确定功能描述是准确的。评估者还应确定功能都包含在高层设计的依赖关系中。

评估者还分析在 ST 和高层设计中的 IT 环境安全要求,以确定它们是一致的。例如,如果 ST 包含了关于审计踪迹存储的 TOE 安全功能要求,但高层设计陈述审计踪迹存储是由 IT 环境提供的,那么高层设计就不是 TOE 安全功能要求的一个准确实例化。

评估者应通过确定接口规范和子系统用途描述是一致的,来证实子系统接口规范。

12.6.3.4.2 工作单元 3:ADV_HLD.2-12

评估者***应检查***高层设计,以确定它是 TOE 安全功能要求的一个完备实例化。

为了确保高层设计涵盖了所有的ST安全功能要求,评估者可以在TOE安全功能要求和高层设计之间建立映射。

12.6.4 表示对应性评估(ADV_RCR.1)

12.6.4.1 目的

本子活动的目的是确定开发者是否在高层设计中正确且完备地执行了ST和功能规范中的要求

12.6.4.2 输入

本子活动的评估证据是:

a) ST;
b) 功能规范;
c) 高层设计;
d) TOE概要规范和功能规范之间的对应性分析;
e) 功能规范和高层设计之间的对应性分析。

12.6.4.3 行为 ADV_RCR.1.1E

12.6.4.3.1 工作单元3:ADV_RCR.1-1

ISO/IEC 15408-3 ADV_RCR.1.1C 对于所提供 TSF 表示的每个相邻对,分析应证实,较为抽象的 TSF 表示的所有相关安全功能都在较不抽象的 TSF 表示中得到正确且完备地细化。

评估者***应检查***TOE概要规范和功能规范之间的对应性分析,以确认功能规范是TOE安全功能的一个正确且完备的表示。

本工作单元中,评估者的目的是确定TOE概要规范中标识的所有安全功能都在功能规范中得到了体现并且是准确地体现。

评估者审核TOE概要规范中的TOE安全功能和功能规范中的TOE安全功能之间的对应性。评估者检查对应的一致性和准确性。当对应性分析中指明了TOE概要规范中的一个安全功能和功能规范中一个接口描述之间的关系时,评估者应验证两者中描述的是同一个安全功能。如果TOE概要规范的安全功能在所对应的接口中能够正确且完备地实现,那么本工作单元将被视为满足。

本工作单元可与工作单元ADV_FSP.1-7和ADV_FSP.1-8关联使用。

12.6.4.3.2 工作单元3:ADV_RCR.1-2

评估者***应检查***功能规范与高层设计之间的对应性分析,以确定高层设计是功能规范的一个正确且完备的表示。

评估者通过使用对应性分析、功能规范以及高层设计来确定将功能规范中标识的每项安全功能映射到高层设计中所描述的一个TSF子系统是可行的。并且对于每个TOE安全功能,对应性还可以指明该功能涵盖了哪些子系统。评估者应审核高层设计所涵盖的每一个安全功能得以正确实现的描述。

12.7 指导性文档活动

指导性文档活动的目的是判断该文档是否充分描述了应如何操作TOE。这些文档针对两类用户:一类是可信的管理员和非管理员用户,他们的不正确行为可能影响TOE安全性,另一类是那些不可信用户,他们的不正确行为可能影响其拥有的数据的安全性。

12.7.1 应用注释

指导性文档活动关注那些与 TOE 安全性相关的功能和接口。TOE 的安全配置在 ST 中进行了描述。

12.7.2 管理员指南评估（AGD_AMD.1）

12.7.2.1 目的

本子活动的目的是确定管理员指南是否描述了如何以安全方式管理 TOE。

12.7.2.2 输入

本子活动的评估证据是：

a) ST；
b) 功能规范；
c) 高层设计；
d) 用户指南；
e) 管理员指南；
f) 安全安装、生成和启动程序；
g) 生命周期定义。

12.7.2.3 应用注释

术语“管理员”指在 TOE 中执行关键安全操作（例如，设置 TOE 配置参数）的可信人员。这些操作可能影响 TSP 的执行，因此管理员拥有特殊的权限来执行这些操作。管理员角色应当与 TOE 中的非管理员用户角色明确区分开。

在 ST 中可定义有不同的管理员角色或管理员组，这些角色和组能可被 TOE 识别并可执行 TOE 的安全功能，例如审计员、管理员或日常管理者。每个角色可能具备多种或一种能力。这些角色的能力和相应的特权在 FMT 类中进行描述。管理员指南中应考虑不同的管理员角色和管理员组。

12.7.2.4 行为 AGD_ADM.1.1E

12.7.2.4.1 工作单元 3：AGD_ADM.1-1

ISO/IEC 15408-3 AGD_ADM.1.1C 管理员指南应描述 TOE 管理员可使用的管理功能和接口。

评估者***应检查***管理员指南，以确定其描述了 TOE 管理员可用的管理性安全功能和接口。

管理员指南应包含安全功能的概述，这些安全功能在管理员界面中是可见的。

管理员指南应标识并描述管理性安全接口与功能的用途、行为和相互关系。

对于每个管理性安全接口和功能，管理员指南应当：

a) 描述调用接口的方法（如命令行、程序语言系统调用、菜单选择、命令按钮）；
b) 描述由管理员设置的参数及其有效值和默认值；
c) 描述即时的 TSF 响应、消息或返回代码。

12.7.2.4.2 工作单元 3：AGD_ADM.1-2

ISO/IEC 15408-3 AGD_ADM.1.2C 管理员指南应描述如何以安全的方式管理 TOE。

评估者***应检查***管理员指南，以确定它描述了如何以安全的方式管理 TOE。

管理员指南描述如何在 IT 环境中依照 TSP 运行 TOE,这应与 ST 所描述的情况一致。

12.7.2.4.3 工作单元 3:AGD_ADM.1-3

ISO/IEC 15408-3 AGD_ADM.1.3C 管理员指南应包含了在安全处理环境中受控的功能和特权的警示信息。

评估者***应检查***管理员指南,以确定其包含了在安全处理环境中受控的功能和特权的警示信息。

TOE 的配置可以允许用户拥有不同的特权来使用 TOE 的不同功能,这意味着可以授权某些用户执行某些功能,而其他用户无权执行,这些功能和特权应在管理员指南中进行描述。

管理员指南应标识出应控制的功能和特权、控制的类型以及控制的理由。警告应说明预期的效果、可能的负面影响以及与其他功能和特权可能的相互作用。

12.7.2.4.4 工作单元 3:AGD_ADM.1-4

ISO/IEC 15408-3 AGD_ADM.1.4C 管理员指南应描述所有与安全操作 TOE 有关的用户行为假设。

评估者***应检查***管理员指南,以确定它描述了所有与安全操作 TOE 有关的用户行为假设。

关于用户行为的假设可以在 ST 的 TOE 安全环境陈述中比较详细的描述,而只有涉及安全操作 TOE 的信息才需要包含在管理员指南中。

例如,要安全操作 TOE 用户有责任对他们的口令进行保密。

12.7.2.4.5 工作单元 3:AGD_ADM.1-5

ISO/IEC 15408-3 AGD_ADM.1.5C 管理员指南应描述所有受管理员控制的安全参数,并说明适当的安全值。

评估者***应检查***管理员指南,以确定它描述了所有受管理员控制的安全参数,并说明适当的安全值。

对于每个安全参数,管理员指南应描述参数的用途、参数的有效值和缺省值,以及这些参数安全与非安全的使用设置。这些参数可以分别描述,也可以综合起来描述。

12.7.2.4.6 工作单元 3:AGD_ADM.1-6

ISO/IEC 15408-3 AGD_ADM.1.6C 管理员指南应描述每一种与需要执行的管理功能有关的安全相关事件,包括改变在 TSF 控制下的实体的安全特性。

评估者***应检查***管理员指南,以确定它描述了每一种与需要执行的管理功能有关的安全相关事件,包括改变在 TSF 控制下的实体的安全特性。

应详尽描述所有类型的安全相关事件,以便管理员知道可能发生什么事件以及为保持安全管理员应采取哪些动作。应充分定义在 TOE 的操作过程中可能发生的安全相关事件(例如,审计迹的溢出、系统崩溃、用户记录的更新——如当用户离开组织时撤消该用户账号),以允许管理员介入来保持安全。

12.7.2.4.7 工作单元 3:AGD_ADM.1-7

ISO/IEC 15408-3 AGD_ADM.1.7C 管理员指南应与评估提交的所有其他文档保持一致。

评估者***应检查***管理员指南,以确定它与评估提交的所有其他文档是一致的。

特别是在 ST 中可能包含一些对 TOE 管理员提出的关于 TOE 安全环境和安全目的的详细的警告信息。

有关一致性分析的指南参见 A.3“一致性分析”。

12.7.2.4.8 工作单元 3:AGD_ADM.1-8

ISO/IEC 15408-3 AGD_ADM.1.8C 管理员指南应描述所有与管理员有关的 IT 环境安全要求。

评估者***应检查***管理员指南,以确定它描述了所有与管理员有关的 TOE 的 IT 环境安全要求。

如果 ST 中不包含 IT 环境的 IT 安全要求,本工作单元不适用,并视为已经满足。

本工作单元仅与 IT 安全要求有关,而与组织安全策略无关。

评估者应当分析关于 TOE 的 IT 环境安全要求(ST 中的可选陈述),并与管理员指南比较,以确保 ST 中与管理员有关的所有安全要求都在管理员指南中得到适当的描述。

12.7.3 用户指南评估(AGD_USR.1)

12.7.3.1 目的

本子活动的目的是为了确定用户指南是否描述了由 TSF 提供的安全功能和接口,以及指南是否提供了安全使用 TOE 的相关说明和指导。

12.7.3.2 输入

本子活动的评估证据是:

a) ST;
b) 功能规范;
c) 高层设计;
d) 用户指南;
e) 管理员指南;
f) 安全安装、生成和启动程序。

12.7.3.3 应用注释

在 ST 中可定义不同的用户角色或用户组,这些角色和组能被 TOE 识别并可执行 TOE 的安全功能。这些角色的能力和相应的特权在 FMT 类中进行描述。用户指南中应考虑不同的用户角色和组。

12.7.3.4 行为 AGD_USR.1.1E

12.7.3.4.1 工作单元 3:AGD_USR.1-1

ISO/IEC 15408-3 AGD_USR.1.1C 用户指南应描述 TOE 的非管理员用户可使用的功能和接口。

评估者***应检查***用户指南,以确定其描述了 TOE 的非管理员用户可使用的安全功能和接口。用户指南应包含安全功能的概述,这些安全功能在用户界面中可见的。

用户指南应当标识和描述安全接口和功能的用途。

12.7.3.4.2 工作单元 3:AGD_USR.1-2

ISO/IEC 15408-3 AGD_USR.1.2C 用户指南应描述用户可访问的由 TOE 提供的安全功能的使用。

评估者***应检查***用户指南,以确定它描述了用户可访问的由 TOE 提供的安全功能的使用。

用户指南应标识和描述用户可用安全接口和功能的行为及其相互关系。

如果允许用户调用 TOE 安全功能,用户指南应为用户提供该功能接口的描述。

对每个接口和功能,用户指南应当:

a) 描述调用接口的方法(如命令行、程序语言系统调用、菜单选择、命令按钮);

b) 描述由用户设置的参数及其有效值和默认值；

c) 描述即时的 TSF 响应、消息或返回代码。

12.7.3.4.3 工作单元 3：AGD_USR.1-3

ISO/IEC 15408-3 AGD_USR.1.3C 用户指南应包含了在安全处理环境中受控的用户可访问功能和特权的警示信息。

评估者***应检查***用户指南，以确定其包含了在安全处理环境中受控的用户可访问功能和特权的警示信息。

TOE 的配置可以允许用户拥有不同的特权来使用 TOE 的不同功能，这意味着可以授权某些用户执行某些功能，而其他用户无权执行，这些用户可访问的功能和特权应在用户指南应中进行描述。

用户指南应标识可用的功能和特权、所需命令的类型以及使用这些命令的理由。用户指南应当包含使用受控的功能和特权时的警告。警告应当说明预期的效果、可能的负面影响以及与其他功能和特权可能的相互作用。

12.7.3.4.4 工作单元 3：AGD_USR.1-4

ISO/IEC 15408-3 AGD_USR.1.4C 用户指南应清晰地阐述安全操作 TOE 所必需的所有用户职责，这些职责包括那些在 TOE 安全环境陈述中的与用户行为相关的假设。

评估者***应检查***用户指南，以确定其阐述了安全操作 TOE 所必需的所有用户职责，这些职责包括那些在 TOE 安全环境陈述中的与用户行为相关的假设。

关于用户行为的假设可以在 ST 的 TOE 安全环境陈述中有比较详细的描述，在用户指南中只需包含涉及 TOE 安全操作的信息。

用户指南应当提供关于有效使用这些安全功能的建议（如审查口令组合的习惯、对用户文件备份频率的建议、对改变用户访问特权所产生影响的讨论）。

例如，要安全操作 TOE 用户有责任对他们的口令进行保密。

用户指南应指出用户是否能够调用某项功能，或者用户是否需要管理员的帮助。

12.7.3.4.5 工作单元 3：AGD_USR.1-5

ISO/IEC 15408-3 AGD_USR.1.5C 用户指南应与评估提交的所有其他文档保持一致。

评估者***应检查***用户指南，以确定其与评估提交的所有其他文档是一致的。

评估者要确保用户指南和评估提交的所有其他文档不会相互矛盾。如果 ST 包含任何对 TOE 用户提出的关于 TOE 安全环境和安全目的的详细警告信息，这一点就尤其重要。

有关一致性分析的指南参见 A.3“一致性分析”。

12.7.3.4.6 工作单元 3：AGD_USR.1-6

ISO/IEC 15408-3 AGD_USR.1.6C 用户指南应描述所有与用户有关的 IT 环境安全要求。

评估者***应检查***用户指南，以确定其描述了所有与用户有关的 TOE 的 IT 环境安全要求。

如果 ST 中不包含 IT 环境的 IT 安全要求，本工作单元不适用，并视为已经满足。

本工作单元仅与 IT 安全要求相关，而与组织安全策略无关。

评估者应分析 TOE 的 IT 环境安全要求（ST 中的可选陈述），并与用户指南比较，以确保所有与用户有关的 ST 安全要求都在用户指南中得到了恰当的描述。

12.8 生命周期支持活动

生命周期支持活动的目的是确定开发者在 TOE 开发和维护期间所使用程序的充分性。这些程序是为了保护 TOE 及其相关的设计信息,以防它们受到干扰或暴露。开发过程中的干扰使故意引入脆弱性成为可能。而设计信息的暴露可能导致脆弱性更容易被人利用。这些程序的充分性依赖于 TOE 的性质和开发过程。

12.8.1 开发安全评估(ALC_DVS.1)

12.8.1.1 目的

本子活动的目的是确定开发者对开发环境的安全控制是否足以提供 TOE 设计和实现的保密性和完整性,这是保证 TOE 的安全操作不受危害所必需的。

12.8.1.2 输入

本子活动的评估证据是:

a) ST;

b) 开发安全文档。

此外,评估者可以检查其他交付件,以确定安全控制定义明确且得到了遵循。评估者特别要检查开发者的配置管理文件(用作 ACM_CAP.4"产生支持和接受程序"和 ACM_SCP.2"问题跟踪 CM 覆盖"子活动的输入)。此过程使用的证据也是必需的。

12.8.1.3 行为 ALC_DVS.1.1E

12.8.1.3.1 工作单元 3:ALC_DVS.1-1

ISO/IEC 15408-3 ALC_DVS.1.1C 开发安全文档应描述用于保护 TOE 设计和实现中保密性和完整性所必需的所有物理的、程序的、人员的及其他在 TOE 的开发环境中的安全措施。

评估者***应检查***开发安全文档,以确定其详细描述了在 TOE 的开发环境中使用的用于保护 TOE 设计和实现保密性与完整性所必需的所有安全措施。

评估者要确定哪些是必需的,这可首先从 ST 中,特别是关于威胁、组织安全策略和假设等章节中查阅可帮助确定必要保护的任何信息(也可能找不到明确提及的信息)。在这方面,环境安全目的陈述也可能有用。

如果从 ST 中得不到明确的信息,评估者就需要根据对 TOE 预期使用环境的考虑,确定必要的措施。如果开发者的措施考虑得不够全面,开发者就应该根据潜在的可利用脆弱性,为评估提供一份清晰的理由说明。

评估者在检查文档时应该考虑下面几种安全措施类型:

a) 物理上的,例如,用于阻止对 TOE 开发环境未授权访问(在正常工作时间和其他时间里)的物理访问控制方法。

b) 过程上的,例如涵盖:

——准许对开发环境或者环境中特定部分(如开发设备)的访问;

——在开发者离开开发团队时撤消其访问权;

——将受保护的材料转移出开发环境;

——容许并陪同来访者参观开发环境;

——建立角色和责任以确保持续地采取安全措施并检查安全违背情况。

c) 人员上的,例如为建立对新开发成员的信任所采取的任何控制或检查。

d) 其他安全措施,例如对所有开发设备的逻辑保护。

开发安全文档应明确开发的场所,并描述执行哪方面的开发以及在每个场所使用的安全措施。比如说,开发行为可能发生在一幢建筑内的多个设备上、同一场所的多个建筑内,或者分布在多个场所。开发工作也包括诸如创建多个 TOE 拷贝之类的任务(若可行的话)。本工作单元不应与 ADO_DEL“交付”的工作单元重叠,但评估者应确保所有的方面都被某个子活动或其他子活动覆盖。

此外,开发安全文档可以描述不同的安全措施,按照能力和所需的输入与输出的特点,这些措施可被运用到开发的不同方面。例如,不同的过程可能被运用到 TOE 不同部分的开发中,或者开发过程的不同阶段。

12.8.1.3.2 工作单元 3:ALC_DVS.1-2

评估者***应检查***开发的保密性和完整性策略,以确定所使用安全措施的充分性。

包括的策略管理有:

a) 与 TOE 开发相关的哪些信息需要保证保密性,以及允许哪些开发成员访问这些材料;

b) 为了保持 TOE 的完整性,应保护哪些材料,以防止其被未授权修改,以及允许哪些开发成员修改这些材料。

评估者应确定在开发安全文档中描述了这些策略,所使用的安全措施与策略是一致的,并且策略是完备的。

应注意,配置管理程序有助于保护 TOE 的完整性,评估者应避免与 ACM_CAP“CM 能力”子活动导出的工作单元相重叠。例如,CM 文档可以描述控制可访问开发环境和修改 TOE 的角色或个人的安全程序。

虽然 ACM_CAP“CM 能力”要求是固定的,但那些关于 ALC_DVS“开发安全”的要求,若仅强制执行必需的措施,将主要依赖于 TOE 的性质和 ST 的安全环境部分所提供的信息。例如,ST 可以标识组织安全策略,以要求 TOE 由具有安全许可的人员来开发。这样,评估者就可以确定这一策略是应用在本子活动中的。

12.8.1.3.3 工作单元 3:ALC_DVS.1-3

ISO/IEC 15408-3 ALC_DVS.1.2C 开发安全文档应提供在 TOE 的开发和维护过程中执行安全措施的证据。

评估者***应核查***开发安全文档,以确定作为程序应用结果的文档证据都已经产生。

评估者检查文档证据的产生,以确认其是否遵守程序。例如,证据产生可能包括登录日志和审计迹。评估者可以选择抽样检查证据。

有关抽样的指南见 A.2“抽样”。

12.8.1.4 行为 ALC_DVS.1.2E

12.8.1.4.1 工作单元 3:ALC_DVS.1-4

评估者***应检查***开发安全文档和相关的证据,以确定正在采取安全措施。

本工作单元要求评估者确定在开发安全文档中描述的安全措施都已被采用,以确定 TOE 的完整性和相关文档的保密性正受到充分保护。例如,可以通过检查所提供的文档证据来确认这一点,并通过

检查开发环境来补充文件证据。对开发环境的现场核查将允许评估者：

a) 观察安全措施(如物理措施)的应用状况；

b) 检查程序应用的文档证据；

c) 会见开发人员，检查其对开发安全策略、程序以及他们责任的认识。

对开发场所的现场核查是信任措施正在使用的一个有用方法。任何不采用这种检查而作出的决定都应该在和监督者商议后作出。

有关检查开发场所的指南参见 A.5“现场核查”。

12.9 测试活动

本活动的目的是通过独立测试 TSF 的一个子集来确定在设计文档中规定的 TSF 行为是否与在 ST 中规定的 TOE 安全功能要求一致。本活动是通过确定开发者已经根据 TSF 的功能规范及其高层设计测试了 TSF 来完成的，可以通过对开发者的测试进行抽样验证和独立测试 TSF 的一个子集而获得对开发者测试结果的信任。

12.9.1 应用注释

评估者测试子集的构成和大小依赖于独立测试子活动(ATE_IND.2“独立测试——抽样”)中所讨论的几个因素。已知的公开弱点便是这类因素之一，评估者需访问这些信息(例如，从评估体制获取)。

ISO/IEC 15408 已经将覆盖和深度从功能测试中分离出来，以增强使用族中组件的灵活性。但希望这些族的要求被一起应用，以确认 TSF 是根据规范进行运行的。这些族的紧密结合已经导致评估工作的子活动有一些重复，以下的这些应用注释将使相同的子活动与 EAL 之间的文本重复减到最少。

12.9.1.1 理解 TOE 的预期行为

在正确评估测试文档是否充分之前，或在新的测试创建之前，评估者应理解安全功能在其满足要求的情况下所期望的预期行为。

评估者可以选择每一次只关注 TSF 的一个安全功能。对于每个安全功能，评估者检查 ST 要求和功能规范、高层设计与指导性文档的相关部分，以获得对 TOE 预期行为方式的理解。

在理解预期行为之后，评估者要检查测试计划，以获得对测试方法的理解。在大多数情况下，测试方法要通过在外部或内部接口处激发一个安全功能并观察其反应来进行。但有些情况下安全功能不能在一个接口处被充分测试(比如对于残余信息的保护功能而言)，此时需要使用其他的方法。

12.9.1.2 测试与验证安全功能预期行为的替代方法

如果在接口处不能进行测试或者没有充分测试，测试计划应确定其他替代方法验证预期行为。评估者有责任确定替代方法的适用性。但是，在评估替代方法的适用性时应考虑以下几个方面：

a) 对实现表示进行分析，确定 TOE 应该执行的必要行为就是一个可接受的替代方法。这意味着可以检查一个软件 TOE 的代码，或者可以对一个硬件 TOE 进行芯片掩膜检查；

b) 即使 EAL 与低层设计或实现的评估结论不匹配时，使用开发者集成或模块化测试的证据也是可接受的。如果在检验一个安全功能的预期行为时使用了开发者集成或模块化测试的证据，应注意确认测试证据是否反映了 TOE 的当前实现。如果因为测试导致子系统或者模块发生了改变，那么通常需要通过分析或进一步测试来跟踪和处理证据的变化。

应该强调的是，应该只有在开发者和评估者都确认不存在其他实际手段对某一安全功能的预期行为进行测试时，方可用替代方法进行补充测试。这种替代使开发者可以把在上述环境下测试的开销(时

间或金钱)减少到最小;这并不是为赋予评估者更多自由,索要不必要的 TOE 附加信息而设计的,也不会取代原有测试计划。

12.9.1.3 确认测试的充分性

测试的前提条件是应建立测试所需的初始条件,可用应设置的参数形式表示,也可用测试顺序表示,即以一个测试的完成作为另一个测试的必备条件。为了使观察测试结果不偏向预期测试结果,评估者应确定初始条件是完备的、适当的。

测试步骤和预期结果描述了用于接口的行为和参数,以及预期结果应该是什么样的以及怎样被验证。评估者应确定测试步骤和预期结果与功能规范和高层设计是一致的。测试应验证规范中确定的行为。这意味着每个在功能规范和高层设计中明确描述的安全功能行为特征都应具有可测性和预期结果,以验证其行为。

虽然开发者应测试所有 TSF,但不必要求对接口的所有规范进行测试。本活动的总体目的是确定已经依据功能规范和高层设计中的行为声明,对每个安全功能进行了充分测试。测试程序将提供了解开发者在测试中是如何检验安全功能的方法。当评估者开发附加测试进行 TOE 独立测试时,可以使用这种信息。

12.9.2 覆盖评估(ATE_COV.2)

12.9.2.1 目的

本子活动的目的是确定测试(像文件说明的那样)是否充分保证已经依据功能规范系统地测试过 TSF。

12.9.2.2 输入

本子活动的评估证据是:

a) ST;
b) 功能规范;
c) 测试文档;
d) 测试覆盖分析。

12.9.2.3 行为 ATE_COV.2.1E

12.9.2.3.1 工作单元 3:ATE_COV.2-1

ISO/IEC 15408-3 ATE_COV.2.1C 测试覆盖的分析应证实测试文档中所标识的测试与功能规范中所描述的 TSF 之间的对应性。

评估者***应检查***测试覆盖分析,以确定测试文档中所标识的测试与功能规范之间的对应是准确的。

对应性可采用表格或矩阵的形式来表示。有时映射关系足以表明测试的对应关系;但有时,开发者提供的基本原理(一般性描述)应补充对应关系的分析。

图 10 示意了功能规范中所描述的安全功能与测试文档中概括的测试之间对应关系的概念框架。测试中可能包括一项或几项安全功能,取决于测试依赖性或实施测试的总体目标。

测试覆盖分析中列出的测试和安全功能的标识应是明确无误的。测试覆盖分析可使评估者把所标识的测试追溯到测试文档,并把被测试的特殊安全功能追溯到功能规范。

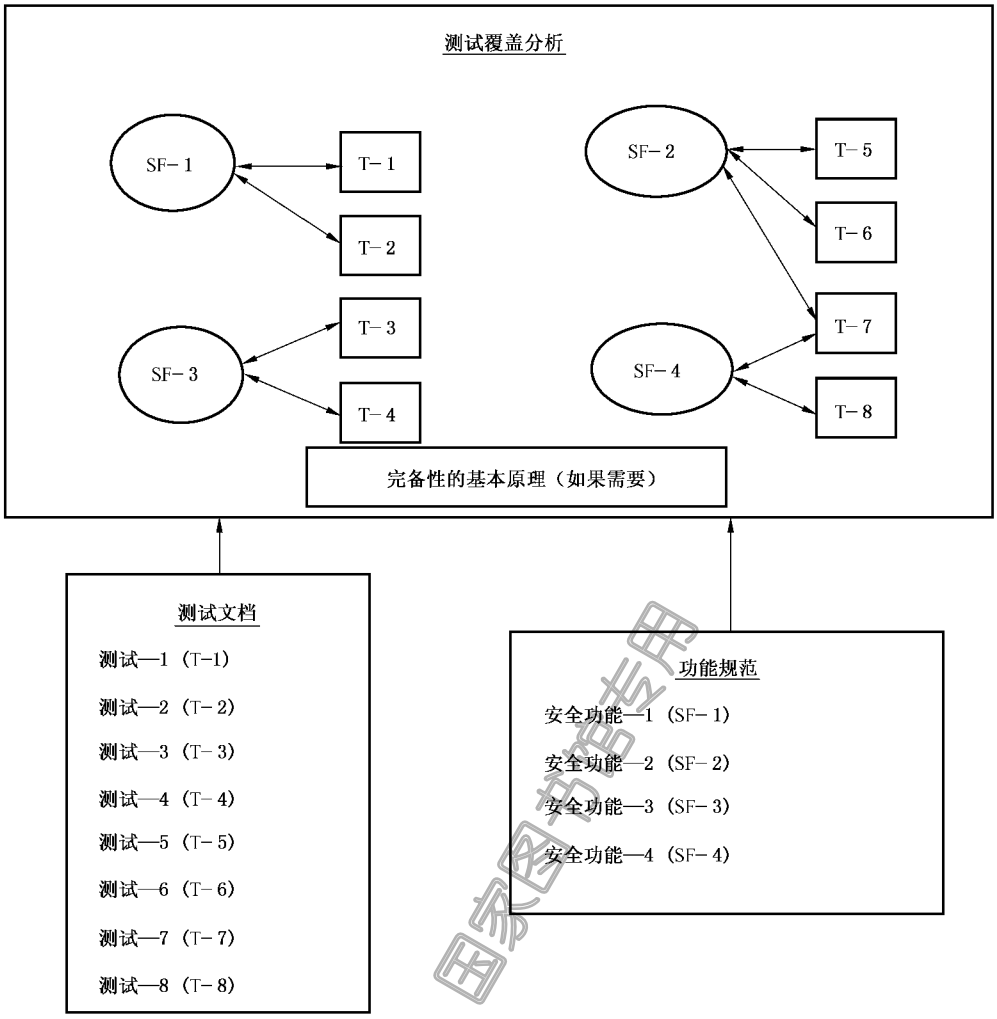

图 10　测试覆盖分析的概念框架

12.9.2.3.2　工作单元 3:ATE_COV.2-2

评估者***应检查***测试计划,以确定关于 TSF 每个安全功能的测试方法适于证实预期行为。

本工作单元的指南参见:

a)　12.9.1.1 应用注释“理解 TOE 的预期行为”;

b)　12.9.1.2 应用注释“测试与验证安全功能预期行为的替代方法”。

12.9.2.3.3　工作单元 3:ATE_COV.2-3

评估者***应检查***测试程序,以确定测试的初始条件、测试步骤和预期结果足以测试每个安全功能。

本工作单元的指南与功能规范相关,可参见:

a)　12.9.1.3 应用注释“确认测试的充分性”。

12.9.2.3.4 工作单元 3:ATE_COV.2-4

ISO/IEC 15408-3 ATE_COV.2.2C 测试覆盖的分析应证实功能规范中所描述 TSF 与测试文档所标识的测试之间的对应性是完备的。

评估者***应检查***测试覆盖的分析,以确定功能规范中所描述的 TSF 与测试文档中列出的测试之间的对应性是完备的。

尽管不要求详尽的接口测试,但所有在功能规范中描述的安全功能和接口应在测试覆盖分析中说明,并映射到测试中,以满足完备性要求。如图 10 所示,所有的安全功能具有相应的测试,因此在这个例子中描述了完整的测试覆盖。如果测试覆盖分析中列出的安全功能没有属于它的测试,那么说明覆盖不是完备的。

12.9.3 深度评估(ATE_DPT.1)

12.9.3.1 目的

本子活动的目的是要确定开发者是否已经对照高层设计测试了 TSF。

12.9.3.2 输入

本子活动的评估证据是:

a) ST;
b) 功能规范;
c) 高层设计;
d) 测试文档;
e) 测试深度分析。

12.9.3.3 行为 ATE_DPT.1.1E

12.9.3.3.1 工作单元 3:ATE_DPT.1-1

ISO/IEC 15408-3 ATE_DPT.1.1C 深度分析应证实测试文档中所标识的测试足以证实该 TSF 是依照其高层设计运行的。

评估者***应检查***测试深度分析,是否在测试文档所标识的测试和高层设计之间建立了一个映射关系。

测试深度分析标识在高层设计中描述的所有子系统,并提供了测试到这些子系统的一个映射关系。对应性可以采用表格或矩阵形式来表示。在有些情况下,映射关系可以充分说明测试的对应性。在其他情况下,开发者有必要用一个基本原理(一般的描述)来补充映射关系的证据。

在高层设计中可映射到并满足 TOE 安全要求的设计细节都应该经过测试,从而应映射到测试文档。图 11 展示了在高层设计中描述的子系统和用于测试这些子系统的 TOE 测试文档中所描述测试之间映射关系的一个概念框架。测试可涉及一个或多个安全功能,这依赖于测试依赖性或执行测试的总体目标。

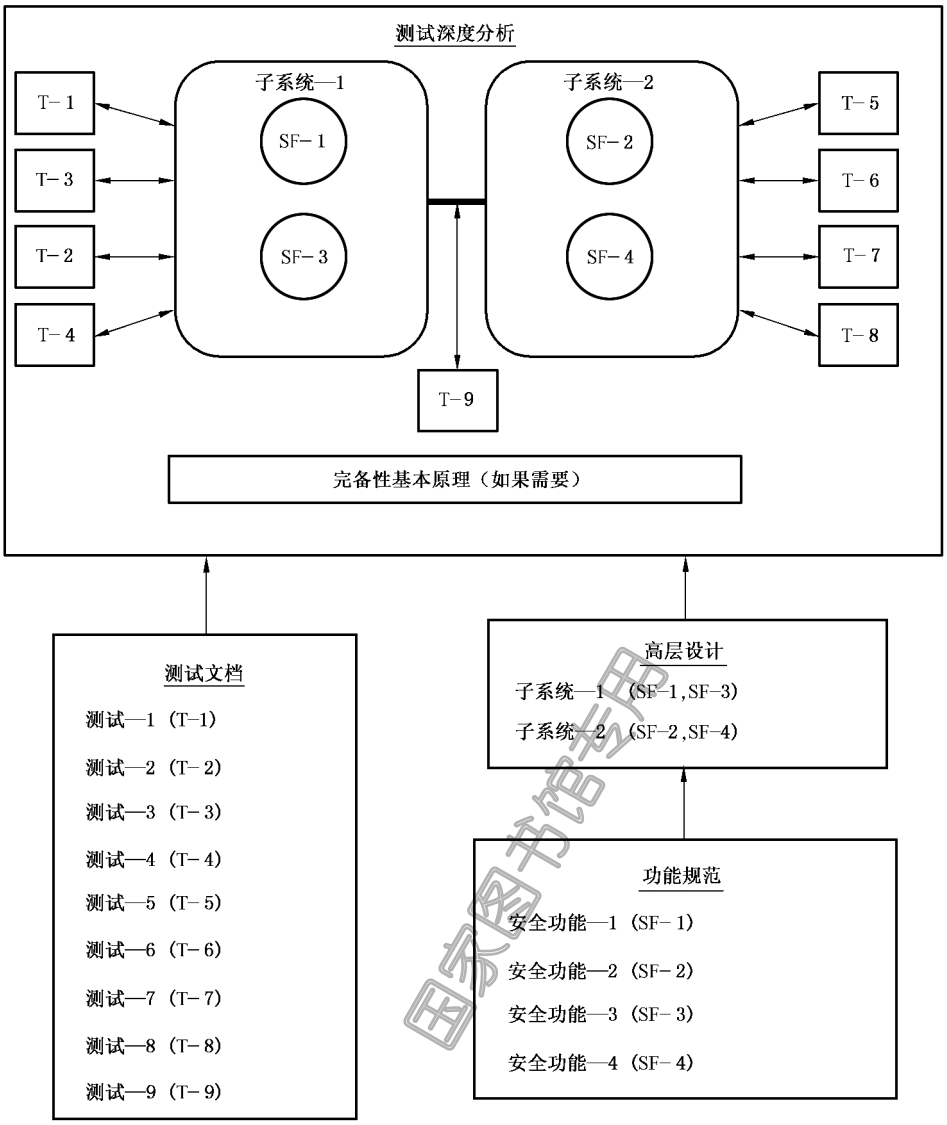

图 11 测试深度分析的概念框架

12.9.3.3.2 工作单元 3:ATE_DPT.1-2

评估者***应检查***开发者的测试计划,以确定 TSF 每个安全功能的测试方法适用于证实预期的行为。

本工作单元的指南参见:

a) 12.9.1.1 应用注释“理解 TOE 的预期行为”;

b) 12.9.1.2 应用注释“测试与验证安全功能预期行为的替代方法”。

TSF 的测试可以在外部接口、内部接口或两处同时执行。无论何种情况,评估者都应考虑其对充分测试安全功能的适当性,特别要确定对某个安全功能内部接口的测试是否有必要,或者能否通过操纵外部接口的方式来充分地测试这些内部接口(虽然是隐含的)。出于公正的目的,这个决定留给评估者。

12.9.3.3.3 工作单元 3:ATE_DPT.1-3

评估者***应检查***测试程序,以确定测试的前提条件,测试步骤和期望结果足以测试每个安全功能。

本工作单元的指南与高层设计相关,可参见:

a) 12.9.1.3 应用注释“确认测试的充分性”。

12.9.3.3.4 工作单元 3:ATE_DPT.1-4

评估者***应检查***测试深度分析,以确保高层设计中定义的 TSF 完全对应于测试文档中的测试。

测试深度分析提供了高层设计和测试计划与程序之间对应性的一个完备陈述。在高层设计中描述的所有子系统和内部接口应在测试深度分析中说明。所有在测试深度分析中说明的子系统和内部接口应有对应的测试,从而满足完备性要求。如图 11 所示,所有的子系统和内部接口都有属于它们的测试,因此这个例子描述了完整的测试深度。如果测试深度分析中标识的子系统或内部接口没有属于它们的测试,那么说明覆盖不是完备的。

12.9.4 功能测试评估(ATE_FUN.1)

12.9.4.1 目的

本子活动的目的是确定开发者的功能测试文档是否可充分地证实安全功能都以按规定实现。

12.9.4.2 输入

本子活动的评估证据是:

a) ST;
b) 功能规范;
c) 测试文档;
d) 测试流程。

12.9.4.3 应用注释

测试文档应覆盖 TSF 的程度依赖于覆盖保证组件。

对于开发者提供的测试,评估者确定测试是否是可复验的,并确定开发者的测试在多大程度上可用于评估者的独立测试工作。开发者测试结果中表明可能有未按照规定执行的安全功能,评估者应对其进行独立测试,以确定情况是否属实。

测试文档应标识为测试建立测试条件或为后续测试清除相关条件而使用特权模式的情况。测试文档要描述为什么必需使用特权模式以获得必要的条件(例如,测试套件的效率、产生测试所需的非特权用户不能创建的特殊对象),以及在执行 TOE 安全功能测试步骤前如何退出特权模式。因此,虽然在建立测试条件时,测试配置可能与 ST 中描述的 TOE 不一致,但是测试文档应描述如何使配置返回到与 ST 所描述配置相一致的状态,以便执行测试步骤。

12.9.4.4 行为 ATE_FUN.1.1C

12.9.4.4.1 工作单元 3:ATE_FUN.1-1

ISO/IEC 15408-3 ATE_FUN.1.1C 测试文档应包括测试计划、测试流程描述、预期测试结果和实际测试结果。

评估者***应检查***测试文档是否包括测试计划、测试流程描述、预期测试结果和实际测试结果。

12.9.4.4.2 工作单元 3:ATE_FUN.1-2

ISO/IEC 15408-3 ATE_FUN.1.2C 测试计划应标识要测试的安全功能,并应描述测试的目标。

评估者***应核查***测试计划是否标识了待测安全功能。

用于标识待测安全功能的一种方法是可参考规定特定安全功能的功能规范中所描述的相应部分。

在执行本工作单元时,评估者可能希望采用抽样的策略。

关于抽样的指南参见 A.2“抽样”。

12.9.4.4.3 工作单元 3:ATE_FUN.1-3

评估者***应检查***测试计划,以确定它描述了测试的目标。

测试计划提供了关于安全功能如何测试的信息以及测试过程中的测试配置信息。

在执行本工作单元时,评估者可能希望采用抽样的策略。

关于抽样的指南参见 A.2“抽样”。

12.9.4.4.4 工作单元 3:ATE_FUN.1-4

评估者***应检查***测试计划,以确定 TOE 测试配置是否与在 ST 中列出的评估配置一致。

开发者测试计划中所提到的 TOE,其唯一参照号应与 CM 能力(ACM-CAP.*)子活动建立的唯一参照号相同。

ST 有可能指定不止一个评估配置,TOE 可能由多个不同的硬件和软件实现组成,应根据 ST 对它们进行测试。评估者要核实在开发者测试文档中所标识的测试配置是否与 ST 中描述的每个评估配置相一致。

评估者应考虑 ST 中描述的可适用于测试环境的关于 TOE 环境安全方面的假设。ST 中的某些假设可能不适用于测试环境。例如,关于用户许可方面的假设就可能不适用,但关于网络单点接入的假设就适用。

12.9.4.4.5 工作单元 3:ATE_FUN.1-5

评估者***应检查***测试计划,以确定它是否与测试流程描述一致。

在执行本工作单元时,评估者可能希望采用抽样的策略。

关于抽样的指南参见 A.2“抽样”,关于一致性分析的指南参见 A.3“一致性分析”。

12.9.4.4.6 工作单元 3:ATE_FUN.1-6

ISO/IEC 15408-3 ATE_FUN.1.3C 测试流程描述应标识要执行的测试和描述每个安全功能的测试情景。这些情景应包括对于其他测试结果的任何顺序依赖性。

评估者***应核查***测试流程描述是否标识了每一个待测安全功能行为。

用于标识待测安全功能行为的一种方法是引用设计规范中规定特定待测行为的相应部分。

在执行本工作单元时,评估者可能希望采用抽样的策略。

关于抽样的指南参见 A.2“抽样”。

12.9.4.4.7 工作单元 3:ATE_FUN.1-7

评估者***应检查***测试流程描述,以确定是否提供了足够的命令以建立可重复的测试初始条件,有时也包括顺序依赖关系。

为建立初始条件可能要采取一些步骤。例如,用户账号应在其能被删除前添加。对于与其他测试结果有顺序依赖关系的一个例子是,在依靠审计功能对其他安全机制如访问控制产生审计记录之前,需要测试审计功能。另一个顺序依赖关系的例子是,某个测试用例所产生的数据文件被用作其他测试用例的输入。

在执行本工作单元时,评估者可能希望采用抽样的策略。

关于抽样的指南参见 A.2“抽样”。

12.9.4.4.8 工作单元 3:ATE_FUN.1-8

评估者***应检查***测试流程描述,以确定是否提供了足够的命令,以便拥有可重复的手段来激发安全功能和观察安全功能行为。

激励通常通过 TSFI 从外部提供给安全功能。一旦输入(激励)传给了 TSFI,安全功能行为就可以在 TSFI 观察到。除非测试流程包含足够的细节以明确无误地描述激励和期望作为该激励结果的行为,否则不能保证测试是可重复执行的。

在执行本工作单元时,评估者可能希望采用抽样的策略。

关于抽样的指南参见 A.2“抽样”。

12.9.4.4.9 工作单元 3:ATE_FUN.1-9

评估者***应检查***测试流程描述,以确定它们与实际测试流程是一致的。

如果两者一致,那么本工作单元就不适用,并认为已经满足要求。

在执行本工作单元时,评估者可能希望采用抽样的策略。

关于抽样的指南参见 A.2“抽样”,关于一致性分析的指南参见 A.3“一致性分析”。

12.9.4.4.10 工作单元 3:ATE_FUN.1-10

ISO/IEC 15408-3 ATE_FUN.1.4C 预期测试结果应指出测试成功执行后的预期输出。

评估者***应检查***测试文档,以确定其包括了足够的预期测试结果。

预期的测试结果用以确定测试是否成功执行。如果预期测试结果是明确无误的并且与给定测试方法的预期行为是一致的,那么该预期结果就足够了。

在执行本工作单元时,评估者可能希望采用抽样的策略。

关于抽样的指南参见 A.2“抽样”。

12.9.4.4.11 工作单元 3:ATE_FUN.1-11

ISO/IEC 15408-3 ATE_FUN.1.5C 开发者执行测试所得到的测试结果应证实每个被测试的安全性功能都按照规定执行。

评估者***应检查***测试文档中的预期测试结果,是否与给出的实际测试结果一致。

由开发者提供的实际测试结果和预期测试结果的比较将揭示出二者间的任何不一致。

只有当对某些数据进行约减或综合后,方可进行实际结果的直接比较。在这种情况下,开发者的测试文档应描述约减或综合真实数据的过程。

例如,开发者可能需要在网络连接建立后测试消息缓冲区以确定缓冲区中的内容。消息缓冲区将包含一个二进制数。这个二进制数应被转换为其他的数据表现形式以使测试更有意义。开发者应足够详细地描述从数据的二进制表示到更高级表示的转换,以便评估者能够实施转换过程(例如,同步或异步传输、停止位位数、奇偶校验位数等)。

应当注意,评估者使用约减或综合真实数据过程的描述,不是实际执行必要的修改,而是评定这一过程是否正确。开发者负责把预期测试结果转换为容易与实际测试结果相比较的格式。

在执行本工作单元时,评估者可能希望采用抽样的策略。

关于抽样的指南参见 A.2“抽样”。

如果任何测试的预期结果和实际结果不相同,那么表明安全功能没有正确执行。这种情况将会影响评估者的独立测试努力,包括隐含安全功能的测试。评估者要考虑增加本工作单元执行的证据样本。

12.9.4.4.12 工作单元 3:ATE_FUN.1-12

评估者***应报告***开发者测试工作,概述测试方法、配置、深度和结果。

对于在 ETR 中报告的开发者测试信息,可以允许评估者转述开发者测试 TOE 时的方法和成果。提供这种信息的目的是为了对开发者的测试工作给出一个有意义的概述,在 ETR 中关于开发者测试的信息不是为了精确再现特定的测试步骤或个别测试结果。其目的是要提供足够的细节,以便允许其他评估者和监督者了解开发者的测试方法、执行的测试数量、TOE 测试配置和开发者测试的总体结果。

一般可在 ETR 中找到关于开发者测试工作的信息有:

a) TOE 测试配置。被测 TOE 的特殊配置;

b) 测试方法,开发者全部测试策略的账目;

c) 开发者执行的测试数量,开发者测试覆盖和深度的描述;

d) 测试结果,开发者测试结果的整体描述。

以上列出的信息并不全面,只是为应呈现在 ETR 中的关于开发者所做测试的信息类型提供借鉴。

12.9.5 独立测试评估(ATE_IND.2)

12.9.5.1 目的

本子活动的目的是通过对 TSF 的一个子集进行独立测试,确定 TOE 是否按规定执行。同时,通过抽样执行开发者的测试,以获得对开发者测试结果的信任。

12.9.5.2 输入

本子活动的评估证据是:

a) ST;

b) 功能规范;

c) 用户指南;

d) 管理员指南;

e) 安全安装、生成和启动程序;

f) 测试文档;

g) 测试覆盖分析;

h) 测试深度分析;

i) 适于测试的 TOE。

12.9.5.3 行为 ATE_IND.2.1E

12.9.5.3.1 工作单元 3:ATE_IND.2-1

ISO/IEC 15408-3 ATE_IND.2.1C TOE 应适合测试。

评估者***应检查***TOE,以确定测试配置与所评估的 ST 中规定的配置是一致的。

用于评估者测试的 TOE,其唯一参照号应与 CM 能力(ACM-CAP.*)子活动建立的唯一参照号相同。

ST 有可能指定不止一个评估配置,TOE 可能由多个不同的硬件和软件实现组成,应根据 ST 对它们进行测试。评估者的 TOE 测试配置应与 ST 中所描述的每个评估配置相一致。

评估者应考虑 ST 中所描述的可用于测试环境的关于 TOE 环境安全方面的假设。ST 中可能有一些假设不适用于测试环境。例如,关于用户许可方面的假设可能就不适用,但关于网络单点接入的假设就适用。

如果使用了任何测试资源(例如仪表、分析仪),评估者有责任保证这些资源是校准正确的。

12.9.5.3.2 工作单元 3:ATE_IND.2-2

评估者*应检查*TOE,以确定它已被正确安装并处于一个已知状态。

评估者可能以多种方式来确定 TOE 的状态。例如,只要评估者仍然相信正在用于测试的 TOE 是正确安装的并且处于一个已知状态,先前的 ADO_IGS.1"安装、生成和启动程序"子活动的成功完成将满足本工作单元。如果情况不是这样,那么评估者只需根据提供的指南按照开发者的规程来安装、生成和启动 TOE。

如果由于 TOE 处于未知状态,评估者不得不执行安装过程,在成功完成后即可满足工作单元 ADO_IGS.1-2 的要求。

12.9.5.3.3 工作单元 3:ATE_IND.2-3

ISO/IEC 15408-3 ATE_IND.2.2C 开发者应提供一组相当的资源,该资源曾被用于开发者的 TSF 功能测试。

评估者*应检查*开发者提供的资源集,以确认它们与开发者做 TSF 功能测试时使用的资源集等同。

资源集可能包括实验室和专用测试设备等。这里的资源与开发者所使用的资源不一定完全相同,但在对测试结果的影响方面上,两者应是等同的。

12.9.5.4 行为 ATE_IND.2.2E

12.9.5.4.1 工作单元 3:ATE_IND.2-4

评估者*应设计*一个测试子集。

评估者选择一个适合于 TOE 的测试子集和测试策略。一个极端的测试策略是让测试子集包含尽可能多的安全功能,但不是很严格地测试它们。另一个极端的测试策略是根据觉察到的相关性,让测试子集包含少数几个安全功能,并严格地测试这些安全功能。

评估者采用的测试方法一般会处于这两种极端情况之间。评估者应至少使用一项测试来试验 ST 中标明的大部分安全功能要求,但不必进行所有的规范测试。

评估者在选择被测 TSF 子集时应该考虑以下因素:

a) 开发者测试证据。开发者测试证据包括:测试覆盖分析、测试深度分析和测试文档。开发者测试证据将使评估者了解有关安全功能是如何被开发者测试的。当评估者在开发新的测试来对 TOE 进行独立性测试时会用到这一信息。评估者应特别考虑:
   1) 针对特定安全功能,增加开发者测试。评估者或许希望通过修改参数进行多个同类测试,以便更严格地测试安全功能;
   2) 针对特定安全功能,补充开发者测试策略。评估者或许希望通过使用另外一个测试策略测试某个特定的安全功能,以改变对该安全功能的测试方法。
b) 测试子集中包括的安全功能个数。如果 TOE 只包含少量安全功能,就要对所有安全功能进行严格测试。如果 TOE 包含很多安全功能,执行全班测试将是不合算的,此时可执行抽样测试。
c) 维持评估活动的平衡。评估者花费在测试活动上的工作应与花费在其他评估活动上的工作相称。

评估者选择安全功能组成测试子集。这种选择依赖于很多因素,对这些因素的考虑也可能影响测试子集大小的选择:

a) 开发者对安全功能测试的严格性。根据 ATE_COV.2"覆盖分析"的要求,在功能规范中所标识的所有安全功能应具有开发者测试证据。评估者决定需要补充测试的那些安全功能应包括

在测试子集中。

b) 开发者测试结果。如果开发者的测试结果导致评估者对某个安全功能或某个方面产生怀疑，那么评估者应该将这些安全功能包括在测试子集中。

c) 与 TOE 的类型(例如，操作系统、防火墙)相关的已知公共域中的弱点。这些弱点将影响测试子集的选择过程。评估者应将涉及这些弱点的安全功能包含在子集中(这里的已知公共域中的弱点并不是指脆弱性，而是该类 TOE 所带有的不充分的情况或问题区)。如果不知道这样的弱点，那么采用选择更宽范围安全功能的这一通用方法可能更合适。

d) 安全功能的重要性。根据 TOE 的安全目的，那些较重要的安全功能应包含在测试子集中。

e) ST 中给出的 SOF 声明。所有有 SOF 声明的安全功能应包括在测试子集中。

f) 安全功能的复杂性。复杂的安全功能可能需要复杂的测试，这些测试对开发者或评估者施以更繁重的要求，这将不利用提高评估效率。相反，从更易找出错误的角度，复杂的安全功能又是子集的一个理想候选对象。因此，评估者需要在这些考虑因素之间寻求一种平衡。

g) 隐含的测试。某些安全功能的测试可能往往隐含着需要测试其他安全功能，把它们包括在子集中可以使被测安全功能数最大化(虽然是隐含的)。典型地，某些特定接口被用于提供多种安全功能特性，这是一种有效的测试方法。

h) TOE 的接口类型(例如，编程的、命令行的、协议的)。评估者应考虑在子集中包括 TOE 支持的所有不同接口类型的测试。

i) 创新的或不寻常的功能。当 TOE 包含有创新的或不寻常的安全功能时，这些功能在市场宣传中可能颇具分量，应该成为测试的重点候选对象。

这一部分指南清楚地说明了在选择合适的测试子集过程中应考虑的因素，但不代表已详述了所有因素。

关于抽样的指南参见 A.2“抽样”。

12.9.5.4.2 工作单元 3:ATE_IND.2-5

评估者***应***为测试子集生成足够详细的测试文档，以便测试情况是可再现的。

参照 ST 和功能规范，在对一个安全功能的预期行为有了一定了解后，评估者应确定测试该功能的最可行的方法。

评估者应特别考虑以下几点：

a) 将采用的方法，例如，是否在外部接口上测试安全功能，是否使用测试设备在内部接口上测试安全功能，或者使用其他测试方法(例如，在异常情况下，代码检查)；

b) 用于激发安全功能并观察响应的安全功能接口；

c) 测试所需的初始条件(例如，任何需要具备的特殊客体或主体以及它们需要拥有的安全属性)；

d) 激发安全功能或观察安全功能所需的专用测试设备(例如，包发生器、网络分析仪)。

评估者可能发现，使用一系列测试用例测试每个安全功能是切实可行的，而每个测试用例将测试预期行为的某个特定的方面。

评估者的测试文档应指明每个测试的出处，如有必要，将其追溯到相关的设计规范和 ST。

12.9.5.4.3 工作单元 3:ATE_IND.2-6

评估者***应实施***测试。

评估者使用测试文档作为对 TOE 进行测试的基础。测试文档用作测试的基础，但是这并不排除评估者执行附加的特别测试。基于测试中发现的 TOE 行为，评估者可以设计新的测试，这些新的测试应记录在测试文档中。

12.9.5.4.4 工作单元 3:ATE_IND.2-7

评估者***应记录***包含在测试子集中的如下测试信息:

a) 待测试的安全功能行为的标识;

b) 测试设备的连接说明与设置说明;

c) 测试所需初始条件的说明;

d) 激发安全功能的说明;

e) 观察安全功能行为的说明;

f) 所有预期结果的描述,以及用以比较预期结果的必要分析;

g) 总结测试和为 TOE 建立必要的测试后状态的说明;

h) 实际测试结果。

测试文档中的细节描述应达到这样的程度:使其他评估者能重复测试并获得相同的结果,尽管测试结果的某些特定细节可能不同(例如审计记录中的时间和日期字段),但整体结果应该是相同的。

有些情况可以不必提供本工作单元中出现的全部信息(例如,在可以与预期结果做比较前,可能不需要对实际测试结果进行任何分析)。这些信息的省略由评估者决定,这样才合理。

12.9.5.4.5 工作单元 3:ATE_IND.2-8

评估者***应核查***所有的实际测试结果,是否与预期测试结果一致。

实际测试结果和预期测试结果间的任何差别可能表明 TOE 与其规定不一致,或者评估者的测试文档是错误的。出现意料之外的实际测试结果,可能需要对 TOE 或测试文档进行纠正维护,也许需要重新运行受到影响的测试,并且修改测试样本的数量和组成。该决定由评估者作出,这样才合理。

12.9.5.5 行为 ATE_IND.2.3E

12.9.5.5.1 工作单元 3:ATE_IND.2-9

评估者***应***使用在开发者测试计划和测试流程中抽取的测试样本***实施***测试。

本工作单元的总体目的是要实施足够数量的开发者测试,以确认开发者的测试结果的有效性。评估者必须确定样本量和构成样本的开发者测试。

考虑到整个测试活动的评估工作,通常应该完成 20%的开发者测试,当然这可以根据 TOE 的特性和所提交的测试证据而改变。

所有的开发者测试都能被追溯到特定的安全功能。因此,在选择构成样本的测试时,所需考虑的因素要相似于在工作单元 ATE_IND.2-4 中为子集选择列出的那些因素。此外,评估者可以使用一个随机抽样的方法来选择构成样本的开发者测试。

关于抽样的指南参见 A.2“抽样”。

12.9.5.5.2 工作单元 3:ATE_IND.2-10

评估者***应核查***所有的实际测试结果,是否与预期测试结果一致。

开发者的预期测试结果和实际测试结果之间的不一致将迫使评估者解决这个差异。评估者最初遇到的不一致性可由开发者提供的合理解释和不一致性解决办法予以解决。

如果没有一个满意的解释或解决办法,评估者可能会降低对开发者测试结果的信任,并且有必要增加试样量,以便重新获取对开发者测试的信任。如果增加试样量还不能满足评估者的要求,就有必要重复整个开发者测试集。最后,就充分测试在工作单元 ATE_IND.2-4 中所标识的 TSF 子集而言,开发者

测试的不足将导致要么需要对开发者测试进行纠正,要么由评估者产生新的测试。

12.9.5.5.3 工作单元 3:ATE_IND.2-11

评估者*应*在 ETR 中*报告*评估者的测试成果、测试大纲、配置、深度和结果。

在 ETR 中报告的评估者测试信息允许评估者告知总体测试方法和在评估过程中测试活动所付出的效果。提供这种信息的目的是对测试工作给出一个有意义的概述,这并不是为了精确再现特定的测试说明或个别测试结果。其目的是要提供足够的细节,以便允许其他评估者和监督者了解评估者所选择的测试方法、执行的评估者测试数量、执行的开发者测试数量、TOE 测试配置和测试活动的总体结果。

一般可在 ETR 中找到关于评估者测试工作的信息有:

a) TOE 测试配置。被测 TOE 的特殊配置;

b) 所选子集的大小。在评估中要被测试的安全功能的数量和确定子集大小的理由;

c) 构成子集的安全功能选择标准。简要说明在选择组成子集的安全功能时考虑的因素;

d) 被测的安全功能。包含在子集中的安全功能的简表;

e) 所执行的开发者测试。所执行的开发者测试的数量和对用于选择测试标准的一个简要描述;

f) 活动的裁定。对测试结果的总体判断。

以上列出的信息并不全面,只是为应呈现在 ETR 中的关于评估期间评估者所做测试的信息类型提供借鉴。

12.10 脆弱性评定活动

脆弱性评定活动的目的是确定 TOE 在预期使用环境下的缺陷或弱点的存在性和可利用性。这种确定是基于开发者和评估者所进行的分析,并由评估者的测试予以支持。

12.10.1 误用评估(AVA_MSU.1)

12.10.1.1 目的

本子活动的目的是确定指南是否是令人误解的、不合理的或是自相矛盾的,是否已经提出了关于所有操作方式的安全流程,以及指南的使用是否便于防止和检测到不安全的 TOE 状态。

12.10.1.2 输入

本子活动的评估证据是:

a) ST;

b) 功能规范;

c) 高层设计;

d) 用户指南;

e) 管理员指南;

f) 安全安装、生成和启动程序;

g) 测试文档。

12.10.1.3 应用注释

术语“指南”在本子活动中指用户指南、管理员指南和安全安装、生成和启动程序。安装、生成和启动程序指管理员负责执行的使 TOE 从交付状态进入运行状态的全部流程。

12.10.1.4 行为 AVA_MSU.1.1E

12.10.1.4.1 工作单元 3:AVA_MSU.1-1

ISO/IEC 15408-3 AVA_MSU.2.1C 指导性文档应标识所有可能的 TOE 操作模式(包括失败或操作失误后的操作)、它们的后果以及对于保持安全运行的意义。

评估者***应检查***指南和其他评估证据,以确定指南标识了所有可能的 TOE 操作模式(例如:失败或操作失误后的操作)、它们的后果以及对于保持安全运行的意义。

其他评估证据,特别是功能规范和测试文档,为评估者提供了信息源。评估使用这些信息确认指南是否包含了足够的指导信息。

评估者应每次只关注单个安全功能,并将其他评估证据与指南中有关安全地使用安全功能的部分相比较,从而确定指南中有关安全功能的部分足以保证安全功能的安全使用(即与 TSP 一致)。评估者也应考虑安全功能之间的关系,并寻找潜在的冲突。

12.10.1.4.2 工作单元 3:AVA_MSU.1-2

ISO/IEC 15408-3 AVA_MSU.2.2C 指导性文档应是完备的、清晰的、一致的、合理的。

评估者***应检查***指南,以确定它是清晰的和内在一致的。

如果指南可能能被管理员或用户曲解,并且以有害于 TOE 或 TOE 安全的方式使用,那么这个指南就是不清晰的。

关于一致性的指南参见 A.3“一致性分析”。

12.10.1.4.3 工作单元 3:AVA_MSU.1-3

评估者***应检查***指南和其他评估证据,以确认指南是完备的和合理的。

评估者应利用从其他评估活动中所获得的对 TOE 的熟悉程度来确认指南是完备的。

评估者特别要考虑功能规范和 TOE 概要规范。所有这些文档中描述的安全功能应在指南中加以描述,以便安全地管理和使用。评估者也可以在指南和这些文件之间找出非形式化的映射关系。在这个映射关系中任何省略都意味着不全面。

如果指南对 TOE 的使用或运行环境要求与 ST 不一致,或者维持安全的负担过于繁重,那么这个指南就是不合理的。

评估者应注意到,执行 AGD_ADM 子活动的工作单元所得到的结果将对此检查提供有用的输入。

12.10.1.4.4 工作单元 3:AVA_MSU.1-4

ISO/IEC 15408-3 AVA_MSU.2.3C 指导性文档应列出关于预期使用环境的所有假设。

评估者***应检查***指南,以确定其列出了关于预期使用环境的所有假设。

评估者分析 ST 中预期 TOE 安全环境的假设,并且与指南相比较,以确保在指南中适当地描述了所有与管理员和用户有关的 ST 预期 TOE 安全环境的假设。

12.10.1.4.5 工作单元 3:AVA_MSU.1-5

ISO/IEC 15408-3 AVA_MSU.2.4C 指导性文档应列出对外部安全措施(包括外部程序的、物理的或人员的控制)的所有要求。

评估者***应检查***指南,以确定其列出了所有外部安全措施要求。

评估者分析指南,以确保其列出了所有的外部程序的、物理的、人员的和连接控制。ST 中非 IT 环境的安全目的将指出什么是必需的。

12.10.1.5 行为 AVA_MSU.1.2E

12.10.1.5.1 工作单元 3:AVA_MSU.1-6

评估者***应执行***所有管理员和用户(可用的话)流程,这些流程对于 TOE 的配置和安装是必要的,从而确定只要利用所提供的指南就能配置并安全地使用 TOE。

配置和安装要求评估者将 TOE 从一个可交付状态,推进到 TOE 运行的状态,并促使 TSP 与 ST 中规定的安全目的一致。

评估者应仅遵循正式提交给 TOE 使用者的用户和管理员指南中给出的开发者制定的流程。在操作中遇到任何困难都说明指南是不完备的、不清晰的、不一致的或者不合理的。

注意,满足本工作单元的工作,同时也满足评估者行为 ADO_IGS.1-2E 的要求。

12.10.1.6 行为 AVA_MSU.1.3E

12.10.1.6.1 工作单元 3:AVA_MSU.1-7

评估者***应检查***指南,以确定其给用户提供了足够的指导信息,使得他们能有效地管理和使用 TOE 的安全功能,并能检测不安全的状态。

TOE 可能使用多种方法来帮助用户安全地使用 TOE。在 TOE 处于不安全的状态时,TOE 可以使用某种功能(特性)来警告用户。同时 TOE 可以在带有增强型指南的情况下被交付,其中增强型指南包括建议、提示、流程等内容,以更有效使用现有安全特性。例如,关于使用审计特性的指南就有助于检测不安全的状态。

为作出对本工作单元的裁定,评估者考虑 TOE 的功能性、目的、预期使用环境,以及关于使用方法或用户的假设。如果 TOE 可能会转变到不安全状态,但使用指南可以一种及时的方式检测到不安全状态,对此情况,评估者应给出结论。可使用诸如 ST、TSF 的功能规范和高层设计这样的评估交付件来确定 TOE 转换到不安全状态的可能性。

12.10.2 TOE 安全功能强度评估(AVA_SOF.1)

12.10.2.1 目的

本子活动的目的是确定,在 ST 中是否为所有概率或置换机制作出了 SOF 声明,以及开发者在 ST 中所作的 SOF 声明是否都是有正确的分析予以支持。

12.10.2.2 输入

本子活动的评估证据是:

a) ST;
b) 功能规范;
c) 高层设计;
d) 用户指南;
e) 管理员指南;
f) TOE 安全功能强度分析。

12.10.2.3 应用注释

对 SOF 进行的分析在本质上是针对概率或置换的机制(例如:口令机制或生物识别)而实施的。尽管密码机制在本质上也是概率性的并且经常用“强度”来描述,但是 AVA_SOF.1“TOE 安全功能强度

评估”却不适用于密码机制。对这种情况,评估者应遵循评估体制的规定来执行。

尽管 SOF 分析是在单个机制的基础上进行的,但是对 SOF 的总体判断却是基于功能的。当采用多个概率或置换机制来实现一个安全功能时,应分析每个不同的机制。提供安全功能的这些机制的组合方式将决定这个功能的总体 SOF 级别。评估者需要设计信息以理解这些机制如何协同工作才能实现一个功能,并且依据 ADV_HLD.1“描述性高层设计”给出这些信息的最小级别。评估者可获得由 EAL 确定的实际的设计信息,并且在必要时这些信息应能被用于支持评估者的分析。

对于涉及多个 TOE 域的 SOF 的讨论参见 ASE_REQ.1“IT 安全要求评估”。

12.10.2.4 行为 AVA_SOF.1.1E

12.10.2.4.1 工作单元 3:AVA_SOF.1-1

ISO/IEC 15408-3 AVA_SOF.1.1C 对于每个具有 TOE 安全功能强度声明的安全机制,TOE 安全功能强度分析应说明该机制达到或超过 PP/ST 中定义的最低强度级别。

评估者***应核查***开发者是否已为每个具有 SOF 声明的安全机制提供了 SOF 分析,该声明在 ST 中是以 SOF 级别的方式予以表示的。

如果仅以 SOF 度量标准的方式来声明 SOF,那么本工作单元是不适用的,视为已满足要求

SOF 级别分为基本级功能强度、中级功能强度或高级功能强度,这些级别是根据攻击潜力来定义的,参见 ISO/IEC 15408-1 第 2 章。表示成一个级别的最小整体 SOF 要求适用于所有非密码的概率或置换安全机制。但个别机制可能具有一个被表示成超出整体 SOF 要求级别的 SOF 声明。

确定实现一个攻击所必需的攻击潜力,从而确定出 SOF 级别的指南参见附录 A.8“功能强度和脆弱性分析”。

SOF 分析中要包含基本原理以证明 ST 中所作的 SOF 声明。

12.10.2.4.2 工作单元 3:AVA_SOF.1-2

ISO/IEC 15408-3 AVA_SOF.1.2C 对于每个具有特定 TOE 安全功能强度声明的安全机制,TOE 安全功能强度分析应说明该机制达到或超过 PP/ST 中定义的特定功能强度度量标准。

评估者***应核查***开发者是否已为每个具有 SOF 声明的安全机制提供了 SOF 分析,该声明在 ST 中是以度量标准的方式予以表示的。

如果仅以 SOF 级别的方式来声明 SOF,那么本工作单元是不适用的,视为已满足要求。

表示成一个级别的最小整体 SOF 要求适用于所有非密码的概率或置换机制。但个别机制可能具有一个被表示成满足或超出整体 SOF 要求度量的 SOF 声明。

SOF 分析中要包含基本原理以证明 ST 中所作的 SOF 声明。

12.10.2.4.3 工作单元 3:AVA_SOF.1-3

评估者***应核查***SOF 分析,以确定支持分析的任何主张或假设都是有效的。

例如,认为伪随机数发生器的特定实现将拥有必要的熵,该熵是产生与 SOF 分析相关的安全机制所必需的,那么该假设就是有缺陷的。

支持 SOF 分析的假设应该反映“最差情形”,除非“最差情形”被 ST 确定是无效的。当许多不同的情形存在时,并且这些情形都是依赖于人类用户或攻击者行为时,代表最低强度的情形应被假设,除非如以上所述该情况无效。

例如,基于最大理论口令空间(例如所有可打印的 ASCII 码)的强度声明,就不是“最差情形”,因为人类习惯于使用自然语言口令,但这样的行为却大大地减少了口令空间和相关强度。然而,如果在 ST 中列出了 TOE 使用的 IT 措施,例如用口令过滤器将自然语言口令的使用降至最少,那么这样的假设

就是适当的。

12.10.2.4.4 工作单元 3:AVA_SOF.1-4

评估者*应检查*SOF 分析,以确定用以支持分析的任何算法、原理、性质和计算都是正确的。

本工作单元高度依赖于所考虑的机制类型。A.8“功能强度和脆弱性分析”提供了一个使用口令机制实现标识和鉴别功能的 SOF 分析实例;该分析考虑用最大口令空间以最终达到一个 SOF 级别。对于生物测量学,该分析应考虑解决方法和其他影响机制的欺骗敏感性的因素。

SOF 表示成一个级别,该级别是基于可击败安全机制所必需的最小攻击潜力。SOF 级别是在 ISO/IEC 15408-1 第 2 章中以攻击潜力进行定义的。

关于攻击潜力的指南参见 A.8“功能强度和脆弱性分析”。

12.10.2.4.5 工作单元 3:AVA_SOF.1-5

评估者*应检查*SOF 分析,以确定每个 SOF 声明被满足或超过。

关于 SOF 声明级别的指南参见 A.8“功能强度和脆弱性分析”。

12.10.2.4.6 工作单元 3:AVA_SOF.1-6

评估者*应检查*SOF 分析,以确定所有带有 SOF 声明的功能都达到了 ST 中所定义的最低强度级别。

12.10.2.5 行为 AVA_SOF.1.2E

12.10.2.5.1 工作单元 3:AVA_SOF.1-7

评估者*应检查*功能规范、高层设计、低层设计、用户指南和管理员指南,以确定所有的概率或置换机制都具有相应的 SOF 声明。

通过概率或置换机制实现的安全功能应由开发者予以标识,该标识应在 ST 评估活动期间予以验证。但是,由于 TOE 概要规范可能是执行此项活动的唯一有效证据,因此这种机制的识别可能是不完备的。作为本子活动输入的附加评估证据,可能识别出未在 ST 中列出的额外的概率或置换机制。如果是这样的话,那么应适当地更新 ST 以反映附加的 SOF 声明,而且开发者需提供额外的分析以证明该声明合理的,其可以作为评估者行为 AVA_SOF.1.1E 的输入。

12.10.2.5.2 工作单元 3:AVA_SOF.1-8

评估者*应检查*SOF 声明,以确定它们是正确的。

当 SOF 分析包括断言或假设时(例如,每分钟可能有多少次鉴别尝试),评估者应独立地确认它们是正确的。这可通过测试或独立的分析来完成。

12.10.3 脆弱性分析评估(AVA_VLA.1)

12.10.3.1 目的

本子活动的目的是确定在其预期使用环境中的 TOE 是否存在可利用的明显脆弱性。

12.10.3.2 输入

本子活动的评估证据是:

a) ST;

b) 功能规范;

c) 高层设计；
d) 用户指南；
e) 管理员指南；
f) 安全安装、生成和启动程序；
g) 脆弱性分析；
h) 功能强度声明分析；
i) 适于测试的 TOE。

本子活动的其他输入有：

a) 关于明显脆弱性的当前信息(例如来自监督者)。

12.10.3.3 应用注释

术语“指南”在本子活动中指用户指南、管理员指南和安全安装、生成和启动程序。

对可利用脆弱性的考虑是由 ST 中安全目的和功能要求确定的。例如，如果 ST 中不要求描述防止安全功能被旁路的措施(不选 FPT_PHP“TSF 物理保护”、FPT_RVM“参照仲裁”和 FPT_SEP“域分离”)，那么基于旁路的脆弱性就无需考虑。

脆弱性可能存在于公共域中，也可能不在，并且利用它可能需要技巧，也可能不要。这两方面是相关的，但是有区别的。不应仅仅因为脆弱性存在于公共域中而认为其容易被利用。

指南中的以下术语具有特定含义：

a) 脆弱性：在一定条件下能被利用来违反安全策略的 TOE 的弱点；
b) 脆弱性分析：系统地搜寻 TOE 中的脆弱性并且对所寻找到的脆弱性进行评判，以确定它们与 TOE 预期使用环境的关系；
c) 明显脆弱性：只要求对 TOE 有最低程度的了解、最小的技术复杂性和最少的资源就可公开利用的脆弱性；
d) 潜在脆弱性：怀疑在 TOE 中存在(根据假定的攻击途径)但并未被证实的脆弱性；
e) 可利用的脆弱性：在 TOE 预期使用环境下可被利用的脆弱性；
f) 不可利用的脆弱性：在 TOE 预期使用环境下不能被利用的脆弱性；
g) 残余脆弱性：一种几乎无法利用的脆弱性，但是在 TOE 预期使用环境下却能够被那些在预计之外的具备更大攻击潜力的攻击者所利用；
h) 穿透性测试：在 TOE 的预期使用环境下进行的测试，以确定已标识的 TOE 潜在脆弱性的可利用程度。

12.10.3.4 行为 AVA_VLA.1.1E

12.10.3.4.1 工作单元 3：AVA_VLA.1-1

ISO/IEC 15408-3 AVA_VLA.1.1C 脆弱性分析文档应描述对 TOE 交付件的分析，以寻找用户能够违反 TSP 的明显途径。

ISO/IEC 15408-3 AVA_VLA.1.2C 脆弱性分析文档应描述如何处理明显的脆弱性。

ISO/IEC 15408-3 AVA_VLA.1.3C 脆弱性分析文档应针对所有已标识的脆弱性，说明该脆弱性不能在 TOE 的预期使用环境中被利用。

评估者***应检查***开发者的脆弱性分析，以确定对明显脆弱性的搜索是否已经考虑了所有相关的信息。

开发者的脆弱性分析应涵盖开发者在所有评估交付件和公共域信息源中搜索到的明显脆弱性。评估者应使用交付件，不是执行独立的脆弱性分析(AVA_VLA.1“开发者脆弱性分析”中没有要求)，而是

将其作为评价开发者搜索明显脆弱性的基础。

公共域中的信息是高度动态的。因此,在开发者执行脆弱性分析和评估完成之间的这一段时间内可能在公共域中有新的脆弱性报告。具体在那一个点停止对公共域信息的监测是评估授权机构的问题,因此相应的指南和协议应从评估授权机构得到。

12.10.3.4.2 工作单元 3:AVA_VLA.1-2

评估者**应检查**开发者的脆弱性分析,以确定每个明显的脆弱性都已被描述,并就它在 TOE 的预期使用环境中为什么是不可利用的给出合理的解释。

希望开发者基于对 TOE 和公共域信息源的了解来寻找明显的脆弱性。如果指定的要求是仅识别明显脆弱性,则不需要进行详细的脆弱性分析。开发者根据以上的定义将信息过滤整理,从而说明在预期使用环境中明显的脆弱性是不可利用的。

评估者需要关注开发者脆弱性分析的以下三个方面:

a) 开发者的分析是否已考虑所有的评估交付件;

b) 在预期使用环境中是否有适当的措施来防止明显脆弱性被利用;

c) 是否有一些明显的脆弱性仍然未被识别。

评估者不宜过分关注已识别的脆弱性本身是不是明显的,除非其被开发者用来作为确定脆弱性是不可利用的依据。在这种情况下,对于已识别的脆弱性,评估者可通过确定是否可阻止拥有低攻击潜力的攻击者的攻击来验证这种论断。

明显脆弱性的概念与攻击潜力无关,后者由评估者在独立的脆弱性分析中确定。因为 AVA _VLA.1 "开发者脆弱性分析"并不进行这样的活动,通常评估者不是以攻击潜力为基础对脆弱性进行搜索和过滤。然而,评估者仍可以在评估期间发现潜在的脆弱性,并且可通过参照明显脆弱性的定义和低攻击潜力的概念,确定应如何描述这些潜在的脆弱性。

只能限于评价开发者分析的有效性、对获得自公共域脆弱性信息的比较和对评估者在其他评估活动过程中所标识的其他脆弱性的比较,来确定是否仍然存在未识别的明显脆弱性。

如果存在下列条件中的一个或多个,那么脆弱性就是不可利用的:

a) (IT 或非 IT)环境中的安全功能或措施防止了在预期使用环境中脆弱性的利用。例如,限定只有授权用户可对 TOE 进行物理访问,可以有效地致使一个 TOE 脆弱性成为不可利用的脆弱性。

b) 脆弱性只能被拥有中级或高级攻击潜力的攻击者利用。例如,对于分布式 TOE 的会话劫持攻击的脆弱性来说,就需要一个高于能够利用明显脆弱性的攻击者才能利用该脆弱性。然而,这样的脆弱性在 ETR 中被报告为残余脆弱性。

c) 在 ST 中既没有声明要抵抗的威胁,也没有声明要满足的组织安全策略。例如,一个防火墙,其 ST 中没有作有效性策略声明并易受到 TCP SYN 攻击(一种基于通用 Internet 协议的攻击,使得主机无法为连接请求提供服务),不应仅基于这种脆弱性认为该评估活动失败。

关于确定利用某个脆弱性所应具备的攻击潜力的指南,请参见 A.8"功能强度和脆弱性分析"。

12.10.3.4.3 工作单元 3:AVA_VLA.1-3

评估者**应检查**开发者的脆弱性分析,以确定其与 ST 和指南都是一致的。

开发者的脆弱性分析可通过建议对 TOE 功能进行特殊配置或设置来处理一个脆弱性。如果认为这样的操作限制是有效的并与 ST 是一致的,那么所有这样的配置/设置都应该在指南中得到充分描述,这样才可能被用户使用。

12.10.3.5 行动 AVA_VLA.1.2E

12.10.3.5.1 工作单元 3:AVA_VLA.1-4

评估者***应***基于开发者的脆弱性分析***设计***穿透性测试。

评估者准备穿透性测试:

a) 当需尝试驳斥开发者的分析,质疑开发者关于脆弱性为什么不可利用的解释时;

b) 当需确定 TOE 在其预期使用环境中对未被开发者考虑到的脆弱性的敏感程度时。评估者应有权使用关于公共域中开发者尚未考虑到的明显脆弱性的最新信息(例如,来自监督者的信息),也可拥有一些作为执行其他评估活动的结果而识别出的潜在脆弱性。

不能期望评估者对除明显脆弱性之外的脆弱性进行测试(即使那些脆弱性包括在公共域中)。然而,许多情况下,在确定可利用性之前,应先进行测试。如果作为评估专家意见,评估者发现一个明显脆弱性之外的脆弱性,则这样的脆弱性在 ETR 中被报告为残余脆弱性。

在理解可疑脆弱性的基础上,评估者决定出最合理的方法测试 TOE 是否存在这样的脆弱性。评估者应特别考虑:

a) 用于激发 TSF 和观察反应的安全功能接口;

b) 测试所需的初始条件(例如任何需要存在的特殊客体或主体及它们需要拥有的安全属性);

c) 激发安全功能或观察安全功能所需的专用测试设备(尽管不可能要求使用专门设备来利用一个明显的脆弱性)。

评估者可能会将发现采用一系列测试用例来进行穿透性测试是可行的,其中每个测试用例将测试一个特定的脆弱性。

12.10.3.5.2 工作单元 3:AVA_VLA.1-5

评估者***应***基于开发者的脆弱性分析***编制***穿透性测试文档,并且应足够详尽使得测试可重复。测试文档应包括:

a) 标识被测 TOE 的明显脆弱性;

b) 进行穿透性测试所需的所有测试设备连接和设置的说明;

c) 建立所有穿透性测试的必备条件的说明;

d) 激发 TSF 的说明;

e) 观察 TSF 行为的说明;

f) 所有预期结果的描述,并对用于比较预期结果的观察行为进行必要的分析;

g) 总结测试和为 TOE 建立必要的测试后状态的说明。

测试文档中的细节描述应达到这种程度:其他的评估者能再现测试并获得相同的结果。

12.10.3.5.3 工作单元 3:AVA_VLA.1-6

评估者***应***基于开发者的脆弱性分析***实施***透性测试。

评估者使用工作单元 4:AVA_VLA.1-4 产生的穿透性测试文档作为对 TOE 进行穿透性测试的基础,但这并不排除评估者执行其他特别的穿透性测试。如果有必要的话,评估者可根据在穿透性测试期间(如果由评估者执行)所获得的信息设计特别的测试,这些测试应记录在穿透性测试文档中。这些测试有必要深入研究意外的结果或观察结果,或在预先测试计划阶段评估者所要研究的潜在脆弱性。

12.10.3.5.4 工作单元 3:AVA_VLA.1-7

评估者***应记录***穿透性测试的实际结果。

尽管实际测试结果的某些特定细节可能与预期的不同(例如审计记录中的时间和日期字段),但整体结果应该是相同的。任何差异都应被证明是合理的。

12.10.3.5.5 工作单元 3:AVA_VLA.1-8

评估者***应检查***所有的穿透性测试结果和所有脆弱性分析的结论,以确定 TOE 在其预期环境中没有可被利用的明显脆弱性。

如果结果显示 TOE 在预期环境中有可被利用的明显脆弱性,则评估者活动裁定为"不通过"。

12.10.3.5.6 工作单元 3:AVA_VLA.1-9

评估者***应***在 ETR 中***报告***穿透性测试工作、测试方法大纲、配置、深度和结果。

在 ETR 中报告的穿透性测试信息允许评估者描述全部穿透性测试方法和本子活动所做的工作。提供该信息的目的是对评估者的穿透性测试工作给出一个有意义的概述。这不意味着 ETR 中关于穿透性测试的信息完全复制于单个穿透性测试的具体测试步骤或测试结果。其目的是提供足够的细节,以便其他评估者和监督者了解所选择的穿透性测试方法、执行穿透性测试的数量、TOE 测试配置和穿透性测试活动的总体结果。

在 ETR 中,在有关评估者穿透性测试工作的章节中通常应包括以下信息:

a) TOE 测试配置。进行穿透性测试的 TOE 的特殊配置;
b) 进行穿透性测试的安全功能。穿透性测试所关注的安全功能简单列表;
c) 子活动的裁定。穿透性测试结果的总体判断。

以上列出的并不全面,只是为应在 ETR 中出现的,在评估期间评估者所做穿透性测试的信息的类型提供一些借鉴。

12.10.3.5.7 工作单元 3:AVA_VLA.1-10

评估者***应***在 ETR 中***报告***所有可利用的脆弱性和残余脆弱性,每种脆弱性应包括以下细节:

a) 来源(例如,在进行评估方法活动时构想到的、评估者知晓的、出版物上读到的);
b) 牵涉到哪些或哪个安全功能,哪些或哪个目的没有满足,违反了哪些或哪个组织安全策略和实现了哪些或哪个威胁;
c) 描述;
d) 在其预期环境中是否可被利用(例如,可利用的,还是残余的);
e) 识别出该脆弱性的评估方(例如开发者、评估者)的标识。

13 EAL4 评估

13.1 简介

EAL4 提供了一个中到高的保证级。使用功能规范、指导性文档、TOE 的高层设计和低层设计以及实现的子集,对安全功能进行分析,以理解安全行为。这种分析由 TOE 安全功能子集的独立测试、开发者基于功能规范和高层设计进行测试的证据、对开发者测试结果的选择性确认、功能强度分析、开发者搜索脆弱性的证据以及可抵御具有低攻击潜力的穿透性攻击者攻击进行论证的独立脆弱性分析等来支持。通过 TOE 安全策略非形式化模型的使用和开发环境控制措施的使用、自动化 TOE 配置管理和安全交付程序的证据,也可获得进一步的保证。

13.2 目的

本章目的是定义达到 EAL4 级评估所需的最少评估努力,并对完成评估的方式方法提供指导。

13.3 EAL4 评估相互关系

EAL4 级评估包括以下任务：

a) 评估输入任务(第 7 章)。

b) EAL4 评估活动包括：

1) ST 评估(第 9 章)；

2) 配置管理评估(13.4)；

3) 交付和运行文档评估(13.5)；

4) 开发文档评估(13.6)；

5) 指导性文档评估(13.7)；

6) 生命周期支持评估(13.8)；

7) 测试评估(13.9)；

8) 测试(13.9)；

9) 脆弱性评定评估(13.10)。

c) 评估输出任务(第 7 章)。

评估活动源于 ISO/IEC 15408-3 所包含的 EAL4 保证要求。

ST 评估应在所有 TOE 评估子活动之前启动，因为 ST 为执行这些评估子活动提供了基础和背景。

本章描述了构成 EAL4 评估的子活动。尽管各子活动通常可以或多或少的同时进行，但评估者应考虑子活动间的依赖关系。

有关依赖关系的指南参见附录 A。

13.4 配置管理活动

配置管理活动的目的是帮助客户识别被评估的 TOE，确保配置项都已被唯一标识，并确保开发者用于控制和跟踪 TOE 改变的程序是充分的。这包括跟踪哪些改变、潜在的改变如何体现以及为减少错误而实现自动化的程度等方面的详细信息。

13.4.1 CM 自动化评估(ACM_AUT.1)

13.4.1.1 目的

本子活动的目的是确定实现表示的更改是否在自动化工具的支持下受到控制，从而减少人为错误和疏忽对 CM 系统的影响。

13.4.1.2 输入

本子活动的评估证据是：

a) 配置管理文档。

13.4.1.3 行为 ACM_AUT.1.1E

13.4.1.3.1 工作单元 4:ACM_AUT.1-1

ISO/IEC 15408-3 ACM_AUT.1.1C CM 系统应提供一种自动方式，通过该方式确保只能对 TOE 的实现表示进行已授权的改变。

评估者***应核查***CM 计划，是否描述自动化的措施，以实现对 TOE 实现表示的访问控制。

13.4.1.3.2 工作单元 4:ACM_AUT.1-2

评估者***应检查***自动访问控制措施,以确定它们有效地阻止了对 TOE 实现表示的非授权修改。

评估者审核配置管理文档,以确认标识了那些对 TOE 实现表示进行了修改的已授权人员或角色。例如,一旦在配置管理之下,仅允许担当软件集成角色的人员访问实现表示的一个元素。

评估者应执行自动访问控制措施来确定他们能否被未授权的角色和用户旁路。做出这一判断仅需执行几个基本测试。

13.4.1.3.3 工作单元 4:ACM_AUT.1-3

ISO/IEC 15408-3 ACM_AUT.1.2C CM 系统应提供一种自动方式来支持 TOE 的生成。

评估者***应核查***CM 文档,确认其支持从实现表示自动的生成 TOE。

本工作单元中,术语"生成"用于那些由开发者采用的,使 TOE 从其实现演变到可交付给最终用户状态的过程。

评估者应核实在 CM 文档中存在自动生成支持程序。

13.4.1.3.4 工作单元 4:ACM_AUT.1-4

评估者***应检查***自动生成程序,以确定它们能用于支持 TOE 的生成。

评估者确定依据生成程序将产生出反映其实现表示的 TOE。客户就能够确信交付安装的 TOE 版本实现了 ST 中所描述的 TSP。例如,在一个软件 TOE 中,可包括检查自动生成程序是否有助于确保所有用来实施 TSP 的源文件和相关库都已包含在编译好的目标代码中。

应注意,这一要求仅是支持性的,例如,将 Unix makefile 置于配置管理之下的方法就足以达到此目的,在这种情况下自动化将对精确产生 TOE 起到显著作用。自动程序能够有助于识别用于产生 TOE 的正确配置项。

13.4.1.3.5 工作单元 4:ACM_AUT.1-5

ISO/IEC 15408-3 ACM_AUT.1.3C CM 计划应描述在 CM 系统中所使用的自动工具。

评估者***应核查***CM 计划,确认其是否包括在 CM 系统中所使用的自动化工具的信息。

13.4.1.3.6 工作单元 4:ACM_AUT.1-6

ISO/IEC 15408-3 ACM_AUT.1.4C CM 计划应描述在 CM 系统中如何使用自动工具。

评估者***应检查***在 CM 计划中提供的有关自动化工具的信息,确定其描述了自动化工具的使用方法。

CM 计划应为 CM 系统的用户提供如何正确操作自动化工具,从而保持 TOE 完整性的必要细节信息。例如,所提供的信息可能包含以下描述:

a) 由工具所提供的功能;

b) 开发者如何使用自动化工具对实现表示的更改进行控制;

c) 开发者如何使用自动化工用于支持 TOE 的生成。

13.4.1.4 隐含的评估者行为

13.4.1.4.1 工作单元 4:ACM_AUT.1-7

ISO/IEC 15408-3 ACM_AUT.1.1D 开发者应使用一个 CM 系统。

评估者***应检查***CM 系统,以确定使用了 CM 计划中所述的自动工具和程序。

本工作单元可视为一个附加活动,该活动可与评估者对 ACM_CAP“CM 能力”要求的 CM 系统使用的核查同时进行。评估者寻找使用工具和程序的相关证据,包括对开发现场的核查以证实这些工具和程序的使用,还应包括对工具和程序使用过程中所产生证据的核查。

有关现场检查的指南参见 A.5“现场核查”。

13.4.2 CM 能力评估(ACM_CAP.4)

13.4.2.1 目的

本子活动的目的是确定开发者是否已清楚地标识了 TOE 及其相关配置项,以及改变这些配置项的能力是否完全受控制。

13.4.2.2 输入

本子活动的评估证据是:

a) ST;

b) 适于测试的 TOE;

c) 配置管理文档。

13.4.2.3 行为 ACM_CAP.4.1E

13.4.2.3.1 工作单元 4:ACM_CAP.4-1

ISO/IEC 15408-3 ACM_CAP.4.1C TOE 参照号对 TOE 的每一个版本应是唯一的。

评估者***应核查***用于评估的 TOE 版本有唯一的参照号。

评估者应当使用开发者的 CM 系统来确认参照号的唯一性,通过核查配置清单确认配置项是被唯一标识的。如果在评估过程中仅仅检查了一个版本,该项评估的证据是不完备的,因此评估者应该查找能够支持唯一参照号的参照系统(如,使用数字、字母或日期)。除非评估者确信该 TOE 能够被唯一标识,否则缺少任何一项参照都将导致对这项要求裁定为“不通过”。

评估者应该设法检查多个 TOE 版本(如修正某个漏洞后的版本),以核查两个版本参照号的不同。

13.4.2.3.2 工作单元 4:ACM_CAP.4-2

ISO/IEC 15408-3 ACM_CAP.4.2C 应给 TOE 标记上参照号。

评估者***应核查***提交评估的 TOE 是否标记有参照号。

评估者应确保 TOE 包含唯一的参照号,以便区分 TOE 的不同版本。可以在包装或介质上粘贴标签,也可以让 TOE 在运行时显示标记,以确保客户(例如:在购买或使用时)能够识别出。

TOE 可提供某种方式使得它易于识别。例如,软件形式的 TOE 可以在启动例程中,或者在响应命令行输入时,显示其名称和版本号。硬件或固件形式的 TOE 可以通过将零件号码以物理方式铭刻在 TOE 上来标识。

13.4.2.3.3 工作单元 4:ACM_CAP.4-3

评估者***应核查***所使用的 TOE 参照号是一致的。

如果 TOE 要多处标记,所有的标记应当是一致的。例如,作为 TOE 一部分而提交的任何一份已标记过的指导性文档都应与被评估的、使用的 TOE 相关。这样就可以确保客户能确认自己所购买和安装的 TOE 版本是经过评估的,并且他们所使用的指南与 ST 一致,可以正确的指导自己使用 TOE。评估者可以通过 CM 文档中的配置清单来验证标记使用的一致性。

评估者还应验证该 TOE 的参照号是否与 ST 一致。

有关一致性分析的指南参见 A.3“一致性分析”。

13.4.2.3.4 工作单元 4:ACM_CAP.4-4

ISO/IEC 15408-3 ACM_CAP.4.3C CM 文档应包括一个配置清单、一个 CM 计划和一个接受计划。

评估者***应核查***所提交的 CM 文档包括了一份配置清单。

配置清单标识了在配置管理控制下维护的配置项。

13.4.2.3.5 工作单元 4:ACM_CAP.4-5

评估者***应核查***所提交的 CM 文档包括一份 CM 计划。

13.4.2.3.6 工作单元 4:ACM_CAP.4-6

评估者***应核查***所提交的 CM 文档包括一份接受计划。

13.4.2.3.7 工作单元 4:ACM_CAP.4-7

ISO/IEC 15408-3 ACM_CAP.4.4C 配置清单应唯一标识组成 TOE 的所有配置项。

评估者***应核查***配置清单,确认其唯一标识了每个配置项。

配置清单包括组成 TOE 的配置项列表,以及足以唯一标识所使用的每个配置项的版本信息(例如:版本号)。评估者使用该清单来进行核查,确认在评估过程中使用了正确的配置项和正确的版本。

13.4.2.3.8 工作单元 4:ACM_CAP.4-8

ISO/IEC 15408-3 ACM_CAP.4.5C 配置清单应描述组成 TOE 的配置项。

评估者***应核查***配置清单,确认其标识了组成 TOE 的配置项。

配置清单所涵盖配置项的最小范围由 ACM_SCP“CM 范围”给出。

13.4.2.3.9 工作单元 4:ACM_CAP.4-9

ISO/IEC 15408-3 ACM_CAP.4.6C CM 文档应描述用于唯一标识 TOE 所包含配置项的方法。

评估者***应检查***标识配置项的方法,以确定其描述了如何唯一地标识配置项。

13.4.2.3.10 工作单元 4:ACM_CAP.4-10

ISO/IEC 15408-3 ACM_CAP.4.7C CM 系统应唯一标识 TOE 所包含的所有配置项。

评估者***应核查***配置项,以确定它们是用一种与 CM 文档一致的方式来标识的。

通过核查配置项的标识来确认 CM 系统唯一标识了所有配置项。无论是组成 TOE 的所有配置项还是开发者作为评估证据提交的配置项初稿,评估者确认每个配置项具有一个唯一的标识,并且在一定程度上是与 CM 文档所描述的唯一标识方法相一致。

13.4.2.3.11 工作单元 4:ACM_CAP.4-11

ISO/IEC 15408-3 ACM_CAP.4.8C CM 计划应描述 CM 系统是如何使用的。

评估者***应检查***CM 计划,以确定其描述了怎样使用 CM 系统以保持 TOE 配置项的完整性。

CM 计划应包括:

a) 在配置管理程序控制之下的开发环境中执行的所有活动(例如:配置项的建立、修改和删除);

b) 需要对配置项进行操作的人员角色及其责任(对于不同类型的配置项(如设计文档或源代码)标识不同的角色);

c) 用于确保只有授权人员才能够修改配置项的程序；
d) 用于确保多个配置项同时修改而不会导致并发问题的程序；
e) 由于程序的应用而产生的证据。例如，对于某个配置项的修改，CM 系统应记录所做的修改、修改的说明、受影响的所有配置项的标识、状态（例如：挂起或完成）、修改的日期和时间，这些内容可以记录在所作修改的审计迹或修改控制记录中；
f) TOE 版本的版本控制和确定唯一参照号的方法（例如，操作系统补丁的发布以及随后对其使用的检测）。

13.4.2.3.12 工作单元 4：ACM_CAP.4-12

ISO/IEC 15408-3 ACM_CAP.4.9C 证据应证实 CM 系统的运行与 CM 计划是一致的。

评估者***应核查***CM 文档，以确定其包括了 CM 计划中所标识的 CM 系统记录。

由 CM 系统产生的输出应向评估者提供所需的证据，使其确信 CM 计划正在被执行，而且所有的配置项都是按照 ACM_CAP.4.10C 所要求的那样，由 CM 系统进行维护的。输出一般包括修改控制表格或者配置项访问批准表格。

13.4.2.3.13 工作单元 4：ACM_CAP.4-13

评估者***应检查***证据，以确定 CM 系统的使用方式与 CM 计划中描述的一致。

评估者应选取并检查对一个配置项执行了各种 CM 相关操作（例如：创建、修改、删除、恢复到以前版本）的证据样本，以证实 CM 系统的所有操作都已经完全按照文档化的程序执行。评估者确认这些证据包括了 CM 计划中所标识操作的全部信息。核查证据时评估者可以要求使用 CM 工具，可以选择对证据抽样。

有关抽样的指南参见 A.2“抽样”。

通过与选定的开发人员进行访谈，可以建立对 CM 系统正确运行和配置项有效维护的进一步信任。通过进行访谈，评估者可以进一步理解 CM 系统如何在实际中应用，并确认 CM 程序与 CM 文档中描述的一致。值得注意的是，这种访谈只能是对核查的补充而不能取代对文档证据的核查；如果单独进行文档核查即可满足要求，就没有必要再进行访谈。然而，对于一个内容范围很宽泛的 CM 计划，单从 CM 计划和记录来确认某些方面（例如：角色和职责）不是很清楚的情况下，就有必要通过访谈来确认。

建议评估者通过核查开发现场以支持本活动。

有关现场检查的指南参见 A.5“现场核查”。

13.4.2.3.14 工作单元 4：ACM_CAP.4-14

ISO/IEC 15408-3 ACM_CAP.4.10C CM 文档应提供所有配置项都已经和正在 CM 系统下有效地进行维护的证据。

评估者***应核查***配置清单中标识的配置项是否正在 CM 系统下进行维护。

开发者使用的 CM 系统应当维持 TOE 的完整性。评估者应核查，对配置清单中的每类配置项（例如：高层设计或源代码模块），都存在由 CM 计划所描述程序产生的证据样本。在这种情况下，抽样方法依赖于 CM 系统中用于控制 CM 项的粒度等级。例如，在配置清单中标识了 10000 个源代码模块，与只有 5 个或甚至只有 1 个源代码模块的情况相比，应采用不同的抽样策略。该活动应着重于确保 CM 系统的正确运行，而不是检测小错误。

有关抽样的指南参见 A.2“抽样”。

13.4.2.3.15 工作单元 4：ACM_CAP.4-15

ISO/IEC 15408-3 ACM_CAP.4.11C CM 系统应提供措施使得只能对配置项进行授权改变。

评估者***应检查***CM 计划中描述的访问控制措施，以确定其能够有效地防止对配置项的非授权访问。

评估者可使用多种方法确定 CM 访问控制措施的有效性。例如，评估者可以实施访问控制措施，以验证该程序措施不会被旁路。评估者可以使用由 CM 系统程序的输出结果，以及在工作单元 ACM_CAP.4-13 中核查的部分结果。评估者还可通过 CM 系统现场演示，确保所使用的访问控制措施得到有效执行。

开发者可能提供的 CM 系统访问控制措施是自动化的，严格意义上这样的访问控制措施的适宜性需要在 ACM_AUT.1“部分 CM 自动化”组件下进行验证。

13.4.2.3.16 工作单元 4：ACM_CAP.4-16

ISO/IEC 15408-3 ACM_CAP.4.12C CM 系统应支持 TOE 的生成。

评估者***应核查***支持 TOE 生成程序的 CM 文档。

本工作单元中，术语“生成”用于那些由开发者采用的、使 TOE 从其实现演变到可交付给最终用户状态的过程。

评估者应核实 CM 文档中是否存在支持 TOE 生成的程序。由开发者提供的生成支持程序可能是自动的，严格意义上他们的存在性需要在 ACM-AUT.1.2C 组件下进行验证。

13.4.2.3.17 工作单元 4：ACM_CAP.4-17

评估者***应检查***TOE 生成程序，以确定它们有助于确保正确的配置项被用于生成 TOE。

评估者确定依据生成支持程序将会生成用户所期望的 TOE 版本（即与 TOE 的 ST 所描述的一致并且由正确的配置项构成），并且同一版本的 TOE 也被交付到客户现场进行安装。例如，对于一个软件 TOE，应确保所有源文件和相关库的生成程序都已包含在编译好的目标代码中。

评估者应谨记 CM 系统不一定非要具有生成 TOE 的能力，但应为 TOE 生成过程减少人为错误提供支持。

13.4.2.3.18 工作单元 4：ACM_CAP.4-18

ISO/IEC 15408-3 ACM_CAP.4.13C 接受计划应描述用来接受修改过的或新建的作为 TOE 组成部分的配置项的程序。

评估者***应检查***接受程序以确定其描述了用于接受新创建的或已修改的配置项的所依据的标准。

接受计划描述了确保 TOE 组成部分在被集成到 TOE 之前都具有良好质量的程序。接受计划描述的接受程序被应用于以下情况：

a) 构造 TOE 的每个阶段（例如，模块阶段、集成阶段和系统阶段）；
b) 对软件、固件和硬件部件的接受；
c) 对以前评估过的部件的接受。

接受标准的描述应包括以下内容：

a) 负责接受配置项的开发者角色或相关人员；
b) 在配置项被接受前应通过的接受标准（例如，通过文档审查或通过软件级、固件级或硬件级的测试）。

13.4.3 CM 范围评估（ACM_SCP.2）

13.4.3.1 目的

本子活动的目的是确定开发者是否对 TOE 的实现表示、设计、测试、用户和管理员指南、CM 文档及安全缺陷执行了配置管理。

13.4.3.2 输入

本子活动的评估证据是：

a) 配置项列表。

13.4.3.3 行为 ACM_SCP.2.1E

13.4.3.3.1 工作单元 4：ACM_SCP.2-1

ISO/IEC 15408-3 ACM_SCP.2.1C 配置项列表应包括：TOE 实现表示、安全缺陷和 ST 中的保证组件所要求的评估证据。

评估者***应核查***配置项列表是否包括了 ISO/IEC 15408 所要求的一组配置项。

该列表包括以下内容：

a) TOE 实现表示(即组成 TOE 的部件或子系统)。对纯软件 TOE 而言，实现表示可以只包括源代码；对包括硬件平台的 TOE 而言，实现表示就会是软件、固件以及相关硬件描述的结合体；

b) ST 中保证组件所要求的评估证据；

c) 记录与实现相关并已报告的安全缺陷细节相关文档(例如，从开发者问题数据库中获得的问题现状报告)。

13.5 交付和运行活动

交付和运行活动的目的是判断描述用于确保是以开发者期望的方式安装、生成和启动 TOE，以及 TOE 在交付过程中没有被更改的相关程序文档的内容是否充分。这里既包含括运输过程使用的程序又包括安装、生成和启动程序。

13.5.1 交付评估(ADO_DEL.2)

13.5.1.1 目的

本子活动的目的是确定交付文档是否描述了在将 TOE 分发到用户方时，用于维护其安全性并对 TOE 更改或替代情况进行检测的所有程序。

13.5.1.2 输入

本子活动的评估证据是：

a) 交付文档。

13.5.1.3 行为 ADO_DEL.2.1E

13.5.1.3.1 工作单元 4：ADO_DEL.2-1

ISO/IEC 15408-3 ADO_DEL.2.1C 交付文档应描述，在向用户方分发 TOE 版本时，用以维护其安全性所必需的所有程序。

评估者***应检查***交付文档，以确定其描述了将 TOE 或其一部分提交给用户方时，为维护其安全性所必需的所有程序。

对术语“必需的”的解释应考虑 TOE 的自身属性和 ST 中包含的信息。提供的保护措施程度应与 ST 中标识的假设、威胁、组织安全策略以及安全目的相称。在某些情况下，ST 中的这些内容可能没有明确的说明与交付相关。评估者应当确定是否已采取了一种均衡手段，使得在非安全开发过程中交付

也不存在明显弱点。

交付程序应描述 TOE 或其一部分在传输过程中为确定 TOE 的标识和维持其安全性而采取的相关程序。程序应当描述 TOE 的哪些部分需要按这些程序执行。适当时还应包括物理或电子的分发程序(例如:从因特网下载)。交付程序涉及整个 TOE,包括应用软件、硬件、固件和文档。

交付文档的重点很可能是完整性度量的相关措施,如在 TOE 交付过程中所使用的验证其完整性的技术措施。然而,在某些 TOE 的交付过程中,交付的保密性和可用性却是重点,因而相关内容也应在交付程序中论述。

交付程序应适用于从生产环境到安装环境的整个交付过程(例如:包装、存储和分发)的各个阶段。

标准的商业化包装和交付惯例是可以接受的。这包括紧压包装、安全带或密封套。对于分发而言,邮寄或私人快递都是可以接受的。

交付程序选择是否适当受 TOE(例如,是软件还是硬件产品)和安全目的的影响。即使 TOE 的不同部分,交付程序不相同,但全部程序应适于满足全部安全目的。

13.5.1.3.2 工作单元 4:ADO_DEL.2-2

ISO/IEC 15408-3 ADO_DEL.2.2C 交付文档应描述不同的程序和技术措施如何检测修改,或检测开发者的主拷贝和用户方所收到版本之间的任何差异。

评估者***应检查***交付文档,以确定其描述了不同的程序和技术措施如何检测开发者主拷贝和用户方所接收版本间的修改或任何差异。

开发者可使用校验和程序、软件签名或防篡改封条来确保篡改能够被检测出来。开发者也可使用其他程序(例如:有记录的交付服务),登记发送方姓名并将其提供给接收方。

交付程序应描述用于检测开发者主拷贝和用户方所接收版本之间任何差异的技术措施。

13.5.1.3.3 工作单元 4:ADO_DEL.2-3

ISO/IEC 15408-3 ADO_DEL.2.3C 交付文档应描述不同的程序如何检测试图伪装成开发者的情况,甚至在开发者没有向用户方发送任何东西的情况下。

评估者***应检查***交付文档,以确定其描述了如何检测试图伪装的不同机制和程序,甚至在开发者没有向用方发送任何东西的情况下。

这一要求可通过 TOE 或部分 TOE 的交付方式来满足(例如,通过一个开发者和用户都了解并信任的代理)。对软件 TOE 而言,交付过程可采用数字签名机制。

如果 TOE 可以电子形式下载,则可通过使用数字签名、完整性校验和或加密来保证其安全性。

13.5.1.4 隐含的评估者行为

13.5.1.4.1 工作单元 4:ADO_DEL.2-4

ISO/IEC 15408-3 ADO_DEL.2.2D 开发者应使用交付程序。

评估者***应检查***交付过程的各个方面,以确定交付程序得到了应用。

评估者检查交付程序执行情况所采取的方法,取决于 TOE 的种类和交付过程自身。除检查交付程序本身外,评估者还应当确保程序得到切实执行。可采取的核查方法如下:

a) 对可观察到程序实际运行情况的分发场所进行现场核查;

b) 在交付的中间阶段,或在用户现场对 TOE 进行检查(例如,检查篡改封条);

c) 评估者通过从常规渠道获得 TOE 来观察交付过程是否在实际中得到使用;

d) 询问最终用户 TOE 是如何被交付的。

有关现场检查的指南参见 A.5“现场核查”。

可能有这样的情况:新开发的 TOE,交付程序还尚未实施。对于这种情况,评估者应确信有适当的程序和设施供以后的交付使用,而且所有相关人员都清楚各自的责任。可行的话,评估者可以要求演习交付过程。如果开发者还生产了其他类似产品,评估者还可以通过对这些产品交付程序的检查来进行确认。

13.5.2 安装、生成和启动评估(ADO_IGS.1)

13.5.2.1 目的

本子活动的目的是确定 TOE 的安全安装、生成和启动的程序和步骤是否都已文档化,并最终形成了一个安全的配置。

13.5.2.2 输入

本子活动的评估证据是:

a) 管理员指南;

b) 安全安装、生成和启动程序;

c) 适于测试的 TOE。

13.5.2.3 应用注释

安装、生成和启动程序是指配置 TOE 达到在 ST 中所描述的安全配置的所必需的所有安装、生成和启动程序,不管它们是运行在用户现场,还是运行在开发现场。

13.5.2.4 行为 ADO_IGS.1.1E

13.5.2.4.1 工作单元 4:ADO_IGS.1-1

ISO/IEC 15408-3 ADO_IGS.1.1C 安装、生成和启动文档应描述 TOE 安全地安装、生成和启动必需的所有步骤。

评估者***应核查***是否已经提供了 TOE 安全安装、生成和启动所必需的所有程序。

如果不期望安装、生成和启动程序再次使用(例如,TOE 已经在运行状态下交付),本工作单元(或者与此相关的部分)就不再适用,并视为已经满足。

13.5.2.5 行为 ADO_IGS.1.2E

13.5.2.5.1 工作单元 4:ADO_IGS.1-2

评估者***应检查***所提供的安装、生成和启动程序,以确认其描述了 TOE 安全安装、生成和启动所需的步骤。

如果不期望安装、生成、启动程序再次使用(例如,TOE 已经在运行状态下交付),本工作单元(或者与此相关的部分)就不再适用,并视为已经满足。

安装、生成和启动程序可以提供以下详细信息:

a) 对 TSF 控制下相关实体的特定安全特性所做的修改;

b) 对异常情况和问题的处理;

c) 如果适用,列出安全安装所需的最低系统要求。

为了确认安装、生成和启动程序能够形成安全配置,评估者可以只使用所提供的指导性文档,按照开发者的程序,实施客户通常执行的活动以完成对 TOE 的安装、生成和启动(在适用于 TOE 的情况下)。本工作单元可以与工作单元 ATE_IND.1-2 一起被执行。

13.6 开发活动

开发活动的目的是根据对 TSF 是如何提供 TOE 安全功能的充分理解来评价设计文档。这种理解是通过检查 TSF 设计文档的逐步完善的描述来获得的。设计文档包括一个功能规范(描述 TOE 的外部接口)和一个高层设计(按照内部子系统描述 TOE 的结构)、低层设计(按照内部模块描述 TOE 的结构)。此外还有实现描述(源码级描述)、安全策略模型(描述 TOE 实施的安全策略)和表示对应性(将 TOE 的一种表示映射到另一种表示,以保证一致性)。

13.6.1 应用注释

ISO/IEC 15408 要求设计文档根据形式化程度来分级。ISO/IEC 15408 将文档的形式化程度分为非形式化、半形式化、形式化三级。非形式化文档是指用自然语言来描述的文档。评估方法没有规定应采用某种语言,这个问题留给评估方案。以下段落分别描述不同非形式化文档内容上的差别。

一个非形式化功能规范包括一个安全功能描述(类似于 TOE 概要规范的安全功能描述)和一个 TSF 外部可见接口描述。例如,如果一个操作系统提供给用户一些方法来进行自我身份鉴别、创建文件、修改或删除文件、设置允许哪些其他用户可以访问文件、与远程的机器进行通信,那么它的功能规范应包含对上述每一个功能的描述。如果还有检测和记录这些事件发生的审计功能,那么关于这些审计功能的描述也应该包含在功能规范中;尽管这些审计功能在技术上不直接被用户在外部接口调用,但确实受到了在用户外部接口所发生事件的影响。

一个非形式化高层设计就是按照每个子系统在其接口激发响应行为的先后顺序来描述的。例如,一个防火墙可能包含一些处理包过滤、远程管理、审计和传输层过滤的子系统。防火墙的高层设计应当按照当一个输入包到达防火墙时,每个子系统所采取的行为来对防火墙采取的行为加以描述。

一个非形式化低层设计就是按照每个模块对其接口激发响应行为的先后顺序来描述的。例如,一个 VPN 子系统可能包含如下模块:生成会话密钥、加密通信、解密通信、决定通信是否需要加密。加密模块的低层描述应描述当模块接收到需要加密的信息流时该模块所采取的步骤。

当功能规范描述功能和服务时,模型描述这些功能和服务执行的策略。非形式化模型是对外部接口处可用的服务或功能所执行的安全策略的简单描述。例如,访问控制策略描述受保护资源和访问所应满足的许可条件;审计策略描述 TOE 的可审计事件,标识出哪些事件可以由管理员选择,哪些事件总是被审计;标识和鉴别策略描述用户如何被标识,那些宣称的标识如何被鉴别,以及任何影响标识如何被鉴别的规则(如公司内联网的用户不需要鉴别,而外部用户需要一次性口令鉴别)。

对应性的非形式化证实不需要采用叙述的方式,一个简单的二维映射就足够了。例如,一个矩阵,沿一个轴的方向列出了模块,沿另一个方向列出了子系统,其中的单元(cell)表示两者的对应性,这将在高层设计和底层设计之间提供足够的非形式化对应性。

13.6.2 功能规范评估(ADV_FSP.2)

13.6.2.1 目的

本子活动的目的是确认开发者对 TOE 安全功能是否作了充分描述,以及 TOE 提供的安全功能是否充分足以满足 ST 的安全功能要求。

13.6.2.2 输入

本子活动的评估证据是:

a) ST;

b) 功能规范;

c) 用户指南；

d) 管理员指南。

13.6.2.3 行为 ADV_FSP.2.1E

13.6.2.3.1 工作单元 4:ADV_FSP.2-1

ISO/IEC 15408-3 ADV_FSP.2.1C 功能规范应使用非形式化风格来描述 TSF 及其外部接口。

评估者***应检查***功能规范，以确定其包括了所有必需的非形式化解释文本。

如果整个功能规范都是非形式化的，则本工作单元不适用，并视为已经满足要求。

对于那些只采用半形式化或形式化语言进行描述，难以被人理解的功能规范的某些组成部分（例如，为解释任何形式化符号的含义），有必要使用辅助性的叙述描述来帮助理解。

13.6.2.3.2 工作单元 4:ADV_FSP.2-2

ISO/IEC 15408-3 ADV_FSP.2.2C 功能规范应是内在一致的。

评估者***应检查***功能规范，以确定它是内在一致的。

评估者通过检查 TSFI 接口描述与 TSF 功能描述是否一致来验证功能规范的一致性。

13.6.2.3.3 工作单元 4:ADV_FSP.2-3

ISO/IEC 15408-3 ADV_FSP.2.3C 功能规范应描述所有外部 TSF 接口的用途与使用方法，适当时应提供效果、例外情况和错误消息的细节。

评估者***应检查***功能规范，以确定其标识了所有的外部 TOE 安全功能接口。

术语“外部”指对用户而言是可见的。TOE 的外部接口或者是 TSF 的直接接口，或者是 TOE 的非 TSF 部分的接口。不过，这些非 TSF 接口可能最终通向 TSF。这些直接或间接通向 TSF 的外部接口共同组成了 TOE 安全功能接口（TSFI）。图 12 表示一个包含 TSF 部分（阴影部分）和非 TSF 部分（空白部分）的 TOE。该 TOE 有三个外部接口：接口 c 是 TSF 的直接接口；接口 b 是 TSF 的间接接口；接口 a 是 TOE 非 TSF 部分的接口。因此，接口 b 和 c 组成了 TSFI。

应该注意的是，所有反映 ISO/IEC 15408-2 功能要求（或者在其扩展组件中）的安全功能应该有某种外部可见的表现形式。尽管有些安全功能不一定能通过其接口来验证，但由于它们在某种程度上是外部可见的，因此也应包含在功能规范中。

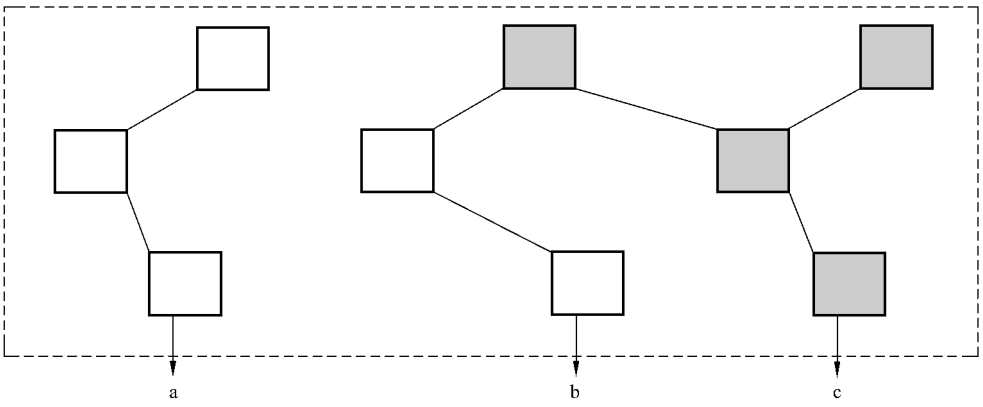

图 12 TSF 接口

13.6.2.3.4 工作单元 4:ADV_FSP.2-4

评估者*应检查*功能规范,以确定其描述了所有外部的 TOE 安全功能接口。

对于一个没有恶意用户威胁的 TOE(即 FPT_PHP“TSF 物理保护”、FPT_RVM“参照仲裁”和 FPT_SEP“域分离”都被排除在 ST 之外),功能规范中描述的(和在其他 TSF 表示描述中进行了扩展的)只是那些通向和来自 TSF 的接口。缺少 FPT_PHP“TSF 物理保护”、FPT_RVM“参照仲裁”和 FPT_SEP“域分离”,就假设没有考虑任何安全特性的旁路,因而不用考虑其他接口可能施加给 TSF 的任何可能的影响。

另一方面,如果 TOE 存在恶意用户或旁路之类的威胁(即 FPT_PHP“TSF 物理保护”、FPT_RVM“参照仲裁”和 FPT_SEP“域分离”被包含在 ST 中),所有外部接口都需要在功能规范中进行描述,但是仅需描述到每一种影响都已明确的程度:安全功能的接口(即图 12 中的接口 b 和 c)都被描述了,然而其他接口仅仅描述到明确 TSF 不能通过这些接口(即图 12 中的接口 a,而不是 b)访问的程度。包含 FPT_PHP“TSF 物理保护”、FPT_RVM“参照仲裁”和 FPT_SEP“域分离”,意味着所有的接口将对 TSF 有某些影响。由于每一个外部接口都是潜在的 TSF 接口,因此,功能规范应对每一个接口进行详细的描述,以使得评估者能够确定接口是否与安全相关。

某些体系结构易于为外部接口群提供足够详细的描述。例如,在内核结构中所有对操作系统的调用都由内核程序来处理;任何有可能违反 TSP 的调用应由具备这种特权的程序来调用。所有实行特权的程序应被包含在功能规范中。任何在内核之外的没有实行特权的程序是无能力影响 TSP 的(即,这种程序是图 12 中的 a 类的接口,而不是 b 类),因而,可以被排除在功能规范之外。如果是基于上述的内核结构,而且评估者对这种结构能够顺利的了解,那么这种结构不是必需的。

13.6.2.3.5 工作单元 4:ADV_FSP.2-5

评估者*应检查*对 TSFI 的陈述,以确定其正确并充分地描述了每个表示效果、异常和出错信息的外部接口处的 TOE 行为。

为了评估接口描述的充分性和正确性,评估者使用功能规范、ST 的 TOE 概要规范以及用户和管理员指南来评估以下因素:

a) 应标识所有与安全相关的用户输入参数(或这些参数的特性)。为了全面起见,宜标识出管理员可用而普通用户无法直接控制的参数。

b) 对功能规范中语义的描述应当反映所审查指南中描述的所有安全相关行为。它包括一系列通过事件及其影响所表示的行为标识。例如,如果一个操作系统提供了丰富的文件系统接口,并对请求文件无法打开的各种原因(如拒绝访问、文件不存在、文件正被另一个用户使用、用户无权在下午 5 点后打开文件等等)提供了不同的错误代码,功能规范应当解释该文件或者在请求下被打开,如不能打开则返回错误代码。(虽然功能规范可以列举所有错误的原因,但不需要提供细节描述)。对语义的描述应当包括安全要求如何应用于接口(例如,是否可以审计接口的使用情况,假如这样的话,应包含能够记录的信息)。

c) 应描述所有可能操作模式下的所有接口。如果 TSF 提供了特权的概念,对接口的描述应分别解释特权模式或非特权模式时,接口的工作方式。

d) 整个文档中安全相关参数的描述和接口的语法所包含的信息应当是一致的。

对以上因素的核实,是通过审核安全规范和 ST 的 TOE 概要规范、开发者提供的用户和管理员指南来完成的。例如,如果 TOE 是一个操作系统及其底层硬件,评估者可以查找用户可访问的程序的讨论、用于指导程序活动的协议的描述、用于指导程序活动的用户可访问数据库的描述,并查找适用于 TOE 的用户接口(例如命令、应用程序接口)。评估者还要确定处理器的指令集已进行描述。

这种核查可以反复进行,直到包含参数和出错信息的设计、源代码或其他证据都被检查为止,以避

免发生功能规范描述不全的情况被评估者忽略。

13.6.2.3.6 工作单元 4:ADV_FSP.2-6

ISO/IEC 15408-3 ADV_FSP.1.4C 功能规范应完备地表示 TSF。

评估者***应检查***功能规范,以确定 TSF 已被完全表示。

为了评估 TSF 表示的完备性,评估者可查阅 ST 的 TOE 概要规范、用户指南和管理员指南。它们应当没有描述在功能规范的 TSF 表示中没有的安全功能。

13.6.2.3.7 工作单元 4:ADV_FSP.2-7

ISO/IEC 15408-3 ADV_FSP.2.5C 功能规范应包括 TSF 是完备地表示的基本原理。

评估者***应检查***功能规范,以确定其涵盖一个可以证明 TSF 能被功能规范完备地表示这样一个令人信服的证据。

评估者确定功能规范涵盖一个可以证明 TSFI 所有接口都包含在功能规范中这样一个令人信服的证据。该证据应涵盖一个开发者用以确定所有外部接口都能被覆盖所使用的程序或方法的描述。如果评估者在其他评估证据中发现诸如命令、参数、错误信息或其他通向 TSF 的接口,而这些都没有包含在功能规范中,则该证据就是不充分的。

13.6.2.4 行为 ADV_FSP2.2E

13.6.2.4.1 工作单元 4:ADV_FSP.2-8

评估者***应检查***功能规范,以确定它是 TOE 安全功能要求的一个完备地实例。

为了确保功能规范涵盖了所有的 ST 安全功能要求,评估者应当建立 TOE 概要规范和功能规范之间的映射。为了满足(ADV_RCR.*“表示对应性”)的对应要求,开发者可能已经提交了这种映射证据;这时评估者只需要验证映射的完备性,确定所有的安全功能要求都映射到功能规范中适当的 TSFI 表示。

13.6.2.4.2 工作单元 4:ADV_FSP.2-9

评估者***应检查***功能规范,以确定它是 TOE 安全功能要求的一个准确实例化。

对于每个具有某种特性的安全功能的接口,功能规范中的详细信息应与 ST 中的相关信息所表述准确一致。例如,如果 ST 中的用户鉴别要求规定了口令长度应为 8 个字符,那么 TOE 应有 8 个字符的口令;如果功能规范描述的是 6 字符的固定长度口令,那么功能规范就不是 TOE 安全功能要求的一个准确实例化。

功能规范中对在受控资源上运行的每个接口,评估者应确定它是否返回了一个错误代码,该错误代码是因为某个安全要求的实施失败而导致的,如果没有返回错误代码,评估者应确定是否需要返回一个错误代码。例如,操作系统可以提供一个接口用于打开一个受控对象,该接口描述中可包含因对受控对象作了未授权的访问而产生的一个错误代码。如果没有这种错误代码,评估者应当确认是否合理。(因为,也许访问仲裁是针对读、写的操作执行的,而不是针对打开的)。

13.6.3 高层设计评估(ADV_HLD.2)

13.6.3.1 目的

本子活动的目的是确定高层设计是否按照主要结构单元(如子系统)提供了 TSF 的描述,提供了这些结构单元接口的描述,并是功能规范的一个正确实现。

13.6.3.2 输入

本子活动的评估证据是：

a) ST；

b) 功能规范；

c) 高层设计。

13.6.3.3 行为 ADV_HLD.2.1E

13.6.3.3.1 工作单元 4：ADV_HLD.2-1

ISO/IEC 15408-3 ADV_HLD.2.1C 高层设计的表示应是非形式化的。

评估者***应检查***高层设计，以确定它包括了所有必需的非形式化解释性文本。

如果整个高层设计都是非形式化的，则本工作单元被视为不适用，并认为已经满足要求。

对于高层设计中那些仅以半形式化或形式化描述难以理解的部分（例如，为解释清楚任何形式化符号的含义），那么起辅助作用的叙述性描述是必需的。

13.6.3.3.2 工作单元 4：ADV_HLD.2-2

ISO/IEC 15408-3 ADV_HLD.2.2C 高层设计应是内在一致的。

评估者***应检查***高层设计的表述，以确定它是内在一致的。

有关一致性分析的指南见 A.3“一致性分析”。

评估者通过确定接口规范都是与子系统的用途描述一致的，来验证子系统的接口规范。

13.6.3.3.3 工作单元 4：ADV_HLD.2-3

ISO/IEC 15408-3 ADV_HLD.2.3C 高层设计应按子系统描述 TSF 的结构。

评估者***应检查***高层设计，以确定 TSF 是按子系统描述的。

关于高层设计中的术语“子系统”指的是大的相关单元（如内存管理、文件管理、进程管理）。通过把一个设计分成多个基本功能区，有助于理解设计思路。

检查高层设计的主要目的是帮助评估者理解 TOE。开发者对子系统定义的选择以及各个子系统中 TSF 分组的选择，是使高层设计有益于理解 TOE 预期运行的一个重要方面。作为本工作单元的一部分，评估者应当评估开发者列举的子系统数目是否恰当，各个子系统中功能分组的选择是否恰当。评估者应确定把 TSF 分解成子系统，足以使评估者从高层的角度来理解 TSF 的功能是如何提供的。

不必非得用“子系统”这个术语来描述高层设计中子系统这个概念，子系统应当代表一类相似级别的分解。例如，可以使用“层”、“管理器”对设计进行分解。

在子系统定义的选择和评估者分析范围之间可能存在某些相互影响。对这种相互影响的讨论见工作单元 4：ADV_HLD.2-10。

13.6.3.3.4 工作单元 4：ADV_HLD.2-4

ISO/IEC 15408-3 ADV_HLD.2.4C 高层设计应描述每个 TSF 子系统所提供的安全功能性。

评估者***应检查***高层设计，以确定它描述了每个子系统的安全功能。

子系统的安全功能行为是对子系统“做些什么”进行的描述。不仅要对子系统直接执行其功能的行为进行描述，而且还要将子系统对 TOE 的安全状态可能产生的影响进行描述（例如：改变主体、对象、安全数据库）。

13.6.3.3.5 工作单元 4:ADV_HLD.2-5

ISO/IEC 15408-3 ADV_HLD.2.5C 高层设计应标识 TSF 所要求的任何基础性硬件、固件或软件,以及在这些硬件、固件或软件中实现的支持性保护机制所提供功能的一个表示。

评估者***应核查***高层设计,以确定它标识了 TSF 所需的所有硬件、固件和软件。

如果 ST 中没有对 IT 环境的安全要求,则本工作单元被视为不适用,并视为已经满足。

如果 ST 包含可选的 IT 环境安全要求,评估者比较高层设计中陈述的 TSF 所需硬件、固件或软件列表与 IT 环境安全要求的陈述,以确定两者的一致性。ST 中的信息刻画了 TOE 赖以运行的底层抽象机。

如果高层设计中的 IT 环境安全要求不属于 ST 中的已定义的 IT 环境安全要求,或者它们与包含在 ST 中的要求不同,那么评估者应根据 ADV_HLD.2.2E 评估行为对这种不一致性进行评估。

13.6.3.3.6 工作单元 4:ADV_HLD.2-6

评估者***应检查***高层设计,以确认它描述了在底层硬件、固件、软件中实现的保护支持机制提供的功能。

如果 ST 中没有 IT 环境安全要求,则本工作单元不适用,并视为已经满足。

TOE 赖以运行的"根本抽象机"所提供功能的表示,不必像作为 TSF 组成部分的功能的表示那样详细。表示应当解释 TOE 如何使用硬件、固件或软件提供的功能,这些硬件、固件或软件实现了 TOE 用来支持 TOE 安全目的的 IT 环境安全要求。

IT 环境安全要求的陈述可以是抽象的,特别是当它打算由各种硬件、固件或软件的不同组合来满足时。作为测试活动的一部分,当能够为评估者提供至少一个声称满足 IT 环境安全要求的"根本机"的实例时,评估者就能够确定其是否为 TOE 提供了必要的安全功能。评估者的这种确认不需要测试和分析"根本机",只需要确定期望它提供的功能确实存在。

13.6.3.3.7 工作单元 4:ADV_HLD.2-7

ISO/IEC 15408-3 ADV_HLD.2.6C 高层设计应标识 TSF 子系统的所有接口。

评估者***应核查***高层设计是否标识了 TSF 子系统的接口。

对每个子系统,高层设计应当包括它的每个入口点的名称。

13.6.3.3.8 工作单元 4:ADV_HLD.2-8

ISO/IEC 15408-3 ADV_HLD.2.7C 高层设计应标识 TSF 子系统的哪些接口是外部可见的。

评估者***应核查***高层设计是否标识了 TSF 子系统的哪些接口是外部可见的。

正如在工作单元 4:ADV_FSP.1-3 所讨论的那样,外部接口(即用户可见的接口)可以直接或间接访问 TSF,任何直接或间接访问 TSF 的外部接口都应该包含在本工作单元的标识范围内,而那些不能访问 TSF 的外部接口则不必包含在内。

13.6.3.3.9 工作单元 4:ADV_HLD.2-9

ISO/IEC 15408-3 ADV_HLD.2.8C 高层设计应描述 TSF 子系统所有接口的用途与使用方法,适当时应提供效果、例外情况和错误消息的细节。

评估者***应检查***高层设计,以确定它按照接口的用途和使用方法描述了每个子系统的接口,并且适当地提供了效果、例外情况和错误消息的详细描述。

高层设计应当按照用途和使用方法对每个子系统所有接口提供描述。这样的描述对某些接口可能是使用通用术语,而对其他的接口则可能提供更详细的描述。在决定应提供的效果、例外情况和错误消

息的详细程度时,评估者应当考虑该分析的目的和 TOE 对接口的使用。例如,评估者需要理解子系统间交互作用的本质,以确认 TOE 设计是合理的,并能够通过子系统间某些接口的通用描述来获得这种理解。尤其是不被其他子系统调用的内部子系统入口点通常不需要进行详细描述。

描述的详细程度还依赖于为达到 ATE_DPT“深度”的要求而采用的测试方法。例如,只使用外部接口进行测试,和同时使用子系统的内外部接口相比,对描述的详细程度要求是不同的。

详细描述应当包括所有输入输出参数、接口的效果、接口产生的任何例外情况或错误消息的细节。对于外部接口,所需的描述很可能包括在功能规范中,可以在高层设计中引用而无需复制。

13.6.3.3.10 工作单元 4:ADV_HLD.2-10

ISO/IEC 15408-3 ADV_HLD.2.9C 高层设计应把 TOE 分成 TSP-实施和其他子系统来描述。

评估者***应核查***高层设计是否把 TOE 分成 TSP-实施和其他子系统来描述。

TSF 包括了 TSP 赖以实施的所有 TOE 组成部分。因为 TSF 既包括直接实施 TSP 的功能,也包括间接实施 TSP 的功能,所以 TSF 中包括了所有的 TSP-实施子系统。子系统如果不参与 TSP 的实施,就不是 TSF 的组成部分。如果子系统的任何部分都是 TSF 的组成部分,那么整个子系统就是 TSF 的组成部分。

正如在工作单元 4:ADV_HLD2-3 中所说明的那样,开发者对子系统定义的选择以及每个子系统内 TSF 分组的选择是使高层设计有益于理解 TOE 的预期运作的一个重要方面。但是,子系统内 TSF 分组的选择也会影响到 TSF 的范围,因为一个具有直接或间接实施 TSP 功能的子系统是 TSF 的组成部分。尽管可理解性是很重要的,但限制 TSF 范围以减少所需分析的数量也同样重要。可理解性和范围减少有时相互矛盾,评估者在评估子系统定义的选择时,应牢记这一点。

13.6.3.4 行为 ADV_HLD.2.2E

13.6.3.4.1 工作单元 4:ADV_HLD.2-11

评估者***应检查***高层设计,以确定它是 TOE 安全功能要求的一个准确实例化。

评估者分析每个 TOE 安全功能的高层设计,确定功能被准确的描述。评估者还应确定没有依赖关系的功能都没有被包含在高层设计中。

评估者还分析在 ST 和高层设计中的 IT 环境安全要求,以确定它们是一致的。例如,如果 ST 包含了关于审计踪迹存储的 TOE 安全功能要求,但高层设计规定审计踪迹存储是由 IT 环境提供的,那么高层设计就不是 TOE 安全功能要求的一个准确实例化。

评估者应通过确定接口规范和子系统用途描述是一致的,来确认子系统接口的规范。

13.6.3.4.2 工作单元 4:ADV_HLD.2-12

评估者***应检查***高层设计,以确定它是 TOE 安全功能要求的一个完备实例化。

为了确保高层设计涵盖了所有的 ST 安全功能要求,评估者可以在 TOE 安全功能要求和高层设计之间建立映射。

13.6.4 实现表示评估(ADV_IMP.1)

13.6.4.1 目的

本子活动的目的是确定实现表示是否足以满足 ST 的功能要求并且是低层设计的正确实现。

13.6.4.2 输入

本子活动的评估证据是:

a) ST；
b) 低层设计；
c) 实现表示的子集。

13.6.4.3 行为 ADV_IMP.1.1E

13.6.4.3.1 工作单元 4:ADV_IMP.1-1

ISO/IEC 15408-3 ADV_IMP.1.1C 实现表示应无歧义地定义 TSF,且详细程度达到无需进一步设计就能生成 TSF 的程度。

评估者***应检查***实现表示,以确定其无歧义地定义了 TSF,且详细程度达到了不需要进一步的设计就能生成 TSF 的程度。

本工作单元要求评估者确认实现表示适于分析。评估者应考虑从提供的表示生成 TSF 时所需要的过程。如果过程是明确定义的,无需作进一步的设计(例如,仅需编译源代码,或根据硬件图制作硬件),那么实现表示就是合适的。

所使用的任何编程语言应明确定义,所有的陈述都是无歧义的,以及用于产生目标码的编译器选项也是明确定义的。这一确定应作为 ALC_TAT.1"明确定义的开发工具"子活动的一部分。

13.6.4.3.2 工作单元 4:ADV_IMP.1-2

评估者***应检查***开发者提供的实现表示,以确定它是充分表示的。

要求开发者仅为 TSF 的一个子集提供实现表示。如果 PP 或 ST 指定了一个已选子集,那么也要求开发者提供该子集。开发者可选择并提供一个初始子集,然而评估者可要求提供额外的部分,甚至可以是不同的子集。

评估者通过抽样原理的应用来确认子集的充分性和适合性。

关于抽样的指南见 A.2"抽样"

为确保子集的适合性,评估者决定子集是否有助于评估者理解并确信 TSF 机制实现的正确性。在作决定时,评估者应考虑开发者所用表示方式的不同,以便评估者满意所选的表示子集。

例如,对于以传统操作系统方式实现的 TOE,为源代码所选的子集应包括来自内核或核心的样本以及内核外的样本,如命令或应用程序。如果已知某些源代码来自于不同的开发组织,那么所选子集应包括每个来自不同开发组织的样本。如果实现表示源码包括不同形式的编程语言,那么子集应包括每种不同语言的样本。

如果实现表示包括硬件图,那么 TOE 的几个不同部分应包括在子集内。例如,一个 TOE 如果包含桌面计算机,所选子集应包括外围控制器以及计算机主板的样本。

可能影响子集确定的其他因素包括:

a) 设计的复杂性(如果 TOE 中设计的复杂性多样化,那么子集应包括某些高复杂性的部分);
b) 方案要求;
c) 其他设计分析子活动的结果(例如与低层设计或高层设计有关的工作单元),这些结果也许能指出 TOE 的某些部分在设计中存在着被混淆的可能性;
d) 评估者对于实现表示部分的判断可能有助于独立脆弱性分析(见 AVA_VLA.2 评估子活动)

13.6.4.3.3 工作单元 4:ADV_IMP.1-3

ISO/IEC 15408-3 ADV_IMP.1.2C 实现表示应是内在一致的。

评估者***应检查***实现表示,以确定它是内在一致的。

由于仅要求开发者提供实现表示的一个子集,本工作单元要求评估者仅通过所提供的子集来确定

一致性。评估者通过比较实现表示的各部分来查找不一致之处。例如对于源代码而言,如果源代码的一个部分包括调用另一部分的子程序,那么评估者应查看调用程序的变量是否与被调用程序处理的变量相匹配。对于硬件图而言,评估者应寻找在电路两端之间性质和特性的约定事项(例如,电压水平、逻辑走向、信号时序要求)。

有关一致性分析的指南见 A.3“一致性分析”。

13.6.4.4 行为 ADV_IMP.1.2E

13.6.4.4.1 工作单元 4:ADV_IMP.1-4

评估者***应检查***实现表示子集,以确定其准确例证了和子集相关的 TOE 安全功能要求。

对于实现表示子集中直接提供安全功能的那些部分,评估者应确定实现是否符合 TOE 的安全功能要求。实现表示子集的其余部分可用于支持某些 TOE 功能要求,在对其余这些部分作决定时,评估者利用低层设计来评估实现表示子集中的这些部分,看他们是否能和低层设计中所作的论述一起例证 TOE 的安全功能要求。

实现表示子集如果有其余部分,那么通常可以忽略,因为它们与实现子集支持的任何 TOE 安全功能要求无关。但是评估者应注意不要忽略在支持 TOE 安全功能方面起间接作用的部分,不管该部分作用多小。例如,通常在操作系统中,核心(或内核)部分的源代码在支持 TOE 安全功能方面可能不起任何直接作用,但能影响内核中起直接作用的那部分的功能。如果发现所提供的实现表示子集中存在任何一个这样的部分,而 ST 要求这些部分互不影响,则应评估这些部分确实和那些起直接作用的部分没有相互影响,这种评估一般不要求与在支持 TOE 安全功能中起直接作用的那些实现表示部分进行相同级别的详细检查。

13.6.5 低层设计评估(ADV_LLD.1)

13.6.5.1 目的

本子活动的目的是确定低层设计是否充分满足 ST 中的功能要求,以及是不是高层设计的一个正确且有效的细化。

13.6.5.2 输入

本子活动的评估证据是:

a) ST;
b) 功能规范;
c) 高层设计;
d) 低层设计。

13.6.5.3 行为 ADV_LLD.1.1E

13.6.5.3.1 工作单元 4:ADV_LLD.1-1

ISO/IEC 15408-3 ADV_LLD.1.1C 低层设计的表示应是非形式化的。

评估者***应检查***低层设计,以确定其包括了所有必需的非形式化的解释性文本。

如果整个低层设计都是非形式化的,则本工作单元不再适用,并认为已满足要求。

对于低层设计中那些仅以半形式化或形式化描述难以理解的部分(例如,为解释清楚任何形式化符号的含义),那么起辅助作用的叙述性描述是必需的。

13.6.5.3.2 工作单元 4:ADV_LLD.1-2

ISO/IEC 15408-3 ADV_LLD.1.2C 低层设计应是内在一致的。

评估者***应检查***低层设计表示,以确定它是内在一致的。

有关一致性分析的指南见 A.3“一致性分析”。

13.6.5.3.3 工作单元 4:ADV_LLD.1-3

ISO/IEC 15408-3 ADV_LLD.1.3C 低层设计应按模块描述 TSF。

评估者***应核查***低层设计,以确定它以模块的方式描述了 TSF。

ISO/IEC 15408 使用术语“模块”来表示比子系统更少抽象的实体,这意味着它包括更多细节,不仅有模块的目的,而且有模块达到目的而采用的方法。理想情况下,低层设计应描述实现模块所必需的所有信息。本子活动中后面的工作单元要求进行特定的分析,以确定已包括足够的细节。对本工作单元来说,评估者只要证实每个模块都被清晰且无歧义地标识就足够了。

13.6.5.3.4 工作单元 4:ADV_LLD.1-4

ISO/IEC 15408-3 ADV_LLD.1.4C 低层设计应描述每一个模块的用途。

评估者***应检查***低层设计,以确定其描述了各个模块的用途。

低层设计包括各个模块用途的描述。这些描述应足够清楚,以告知模块将提供哪些功能,并且应提供模块用途概述,但不必像模块接口规范那样详细。

13.6.5.3.5 工作单元 4:ADV_LLD.1-5

ISO/IEC 15408-3 ADV_LLD.1.5C 低层设计应根据所提供的安全功能性和对其他模块的依赖关系,定义模块间的相互关系。

评估者***应检查***低层设计,以确定低层设计应根据所提供的安全功能性和对其他模块的依赖关系,定义模块间的相互关系。

为达到这一分析的目的,应按下面两种相互作用方式来审核模块:

a) 相互提供服务;

b) 合作支持安全功能。

低层设计应包括这些相互关系的具体信息。例如,如果一个模块执行运算依赖于其他模块的计算结果,应列出所依赖的其他模块。另外,如果一个模块在支持某安全功能运行的同时提供了其他模块可用的服务,这个服务也应被描述。如前一个工作单元分析的那样,模块用途描述有可能足以提供本工作单元所需要的信息。

13.6.5.3.6 工作单元 4:ADV_LLD.1-6

ISO/IEC 15408-3 ADV_LLD.1.6C 低层设计应描述每一个 TSP-实施功能是如何被提供的。

评估者***应检查***低层设计,以确定其描述了每个 TSP-实施功能是如何提供的。

TSP-实施功能是 TSF 中直接或间接实施 TSP 的那些功能。

对于评估来说描述的关键是低层设计是否充分地细化到允许创建一个实现。

评估者应当从实现者的观点来分析这种描述。当评估者使用实现者的观点时,仍不清楚模块的任一方面是如何实现的,这个描述就不是完备的。应注意到一个模块并不要求作为一个独立单元被实现(可以是一个程序、子程序、或硬件元件);但是低层设计应该足够详细,以允许这种实现。

13.6.5.3.7 工作单元 4:ADV_LLD.1-7

ISO/IEC 15408-3 ADV_LLD.1.7C 低层设计应标识 TSF 模块的所有接口。

评估者***应核查***低层设计中所标识的 TSF 模块接口。

对于每个模块而言，低层设计应包括该模块各入口点的名称。

13.6.5.3.8 工作单元 4：ADV_LLD.1-8

ISO/IEC 15408-3 ADV_LLD.1.8C 低层设计应标识 TSF 模块的哪些接口是外部可见的。

评估者***应核查***低层设计，是否标识了哪些 TSF 模块接口是外部可见的。

正如在工作单元 4：ADV_FSP.2-3 中所讨论的那样，外部接口（即用户可见的接口）可以直接或间接访问 TSF。任何直接或间接访问 TSF 的外部接口都应包括在本工作单元的标识中，不能访问 TSF 的外部接口则不需被包含其中。

13.6.5.3.9 工作单元 4：ADV_LLD.1-9

ISO/IEC 15408-3 ADV_LLD.1.9C 低层设计应描述 TSF 模块所有接口的用途和用法，适当时应提供效果、例外情况和错误消息的细节。

评估者***应检查***低层设计，以确定其按照各模块接口的用途和使用方法描述了这些接口，并适当地提供了效果、例外情况和错误消息的细节。

对模块接口的描述中可以对某些接口使用通用术语，而对其他的接口则可提供更详细的描述。为了确定对效果、例外情况和错误消息等细节的程度，评估者应当考虑该分析的目的和 TOE 对接口的使用。例如，评估者需要理解模块间交互作用的本质，以确认 TOE 设计是合理的，并能够通过模块间某些接口的通用描述获得这种理解。尤其是不被其他模块调用的内部入口点通常不需要进行详细描述。

本工作单元可以与评估者独立脆弱性分析一起执行。（独立脆弱性分析是 AVA_VLA“脆弱性分析”子活动的一部分）

详细描述应当包括所有输入输出参数、接口的效果、接口产生的任何例外情况或错误消息的细节。对于外部接口，所需的描述很可能包括在功能规范中，在低层设计中可以引用而不需复制。

13.6.5.3.10 工作单元 4：ADV_LLD.1-10

ISO/IEC 15408-3 ADV_LLD.1.10C 低层设计应把 TOE 分成 TSP-实施模块和其他模块来描述。

评估者***应核查***低层设计是否将 TOE 分解成 TSP-实施和其他模块来描述。

TSF 包括 TSP 实施所依赖的所有 TOE 组成部分。因为 TSF 既包括直接实施 TSP 的功能，也包括虽然不直接实施 TSP 但以更间接方式实施 TSP 的那些功能，所以 TSF 中包括所有 TSP-实施模块。不能影响 TSP 实施的模块就不是 TSF 的组成部分。

13.6.5.4 行为 ADV_LLD.1.2E

13.6.5.4.1 工作单元 4：ADV_LLD.1-11

评估者应检查低层设计，以确定它是 TOE 安全功能要求的一个准确实例化。

评估者应通过确定下列几方面以验证模块接口规范：

a) 接口规范与模块用途描述是一致的；

b) 接口规范与其他模块对其使用是一致的；

c) 已正确规定了支持各 TSP-实施功能所需模块间的相互关系。

13.6.5.4.2 工作单元 4：ADV_LLD.1-12

评估者***应检查***低层设计，以确定它是 TOE 安全功能要求的一个完备实例化。

评估者确定所有 ST 功能要求都被映射到低层设计的适当部分，这一决定应结合子活动 ADV_

RCR.1“非形式化对应性证实”作出。

评估者应分析低层设计以确定每个 TOE 安全功能都被模块规范完全描述，并且没有 TOE 安全功能所依赖的模块，在低层设计中没有规范。

13.6.6 表示对应性评估(ADV_RCR.1)

13.6.6.1 目的

本子活动的目的是确定开发者是否在实现表示中正确且完备地执行了 ST、功能规范、高层设计和低层设计中的要求。

13.6.6.2 输入

本子活动的评估证据包括：

a) ST；
b) 功能规范；
c) 高层设计；
d) 低层设计；
e) 实现表示的子集；
f) TOE 概要规范和功能规范之间的对应性分析；
g) 功能规范和高层设计之间的对应性分析；
h) 高层设计和低层设计之间的对应性分析；
i) 低层设计和实现表示子集之间的对应性分析。

13.6.6.3 行为 ADV_RCR.1.1E

13.6.6.3.1 工作单元 4:ADV_RCR.1-1

ISO/IEC 15408-3 ADV_RCR.1.1C 对于所提供 TSF 表示的每个相邻对，分析应证实，较为抽象的 TSF 表示的所有相关安全功能都在较不抽象的 TSF 表示中得到正确且完备地细化。

评估者***应检查***TOE 概要规范和功能规范之间的对应性分析，以确认功能规范是 TOE 安全功能的一个正确且完备的表示。

本工作单元中，评估者的目的是确定 TOE 概要规范中标识的所有安全功能都在功能规范中得到了体现并且是准确地体现。

评估者审核 TOE 概要规范中的 TOE 安全功能和功能规范中的 TOE 安全功能之间的对应性。评估者检查对应的一致性和准确性。当对应性分析中指明了 TOE 概要规范中的一个安全功能和功能规范中一个接口描述之间的关系时，评估者应验证两者中描述的是同一个安全功能。如果 TOE 概要规范的安全功能在所对应的接口中能够正确且完备地实现，那么本工作单元将被视为满足。

本工作单元可与工作单元 ADV_FSP.2-8 和 ADV_FSP.2-9 关联使用。

13.6.6.3.2 工作单元 4:ADV_RCR.1-2

评估者***应检查***功能规范与高层设计之间的对应性分析，以确定高层设计是功能规范的一个正确且完备的表示。

评估者通过使用对应性分析、功能规范以及高层设计来确定将功能规范中标识的每项安全功能映射到高层设计中所描述的一个 TSF 子系统是可行的。并且对于每个 TOE 安全功能，对应性还可以指明该功能涵盖了哪些子系统。评估者应审核高层设计所涵盖的每一个安全功能得以正确实现的描述。

13.6.6.3.3 工作单元 4:ADV_RCR.1-3

评估者*应检查*高层设计与低层设计之间的对应性分析,以确定低层设计是高层设计的一个正确且完备的表示。

评估者通过使用对性应分析、高层设计和低层设计,确定将低层设计中标识的每一个 TSF 模块映射到高层设计中描述的一个 TSF 子系统是可行的。并且对于每个 TOE 安全功能,对应性还可以指明该功能涵盖了哪些 TSF 模块。评估者应审核低层设计所涵盖的每一个安全功能得以正确实现的描述。

13.6.6.3.4 工作单元 4:ADV_RCR.1-4

评估者*应检查*低层设计和实现表示子集的对应性分析,以确定子集是在实现表示细化后的那些低层设计部分的一个正确且完备的表示。

由于评估者只检查实现表示的子集,那么本工作单元评估的是实现表示子集与低层设计相关部分的对应性分析,而不是试图将每个 TOE 安全功能都能追溯到实现表示。实现表示子集可能覆盖不到某些功能。

13.6.7 安全策略模型评估

13.6.7.1 目的

本子活动的目的是要确定安全策略模型是否一致且清晰地描述了安全策略的规则及特征,并确定这些描述是否与功能规范中对安全功能的描述一致。

13.6.7.2 输入

本子活动的评估证据是:

a) ST;
b) 功能规范;
c) TOE 安全策略模型;
d) 用户指南;
e) 管理员指南。

13.6.7.3 行为 ADV_SPM.1.1E

13.6.7.3.1 工作单元 4:ADV_SPM.1-1

ISO/IEC 15408-3 ADV_SPM.1.1C TSP 模型应是非形式化的。

评估者*应检查*安全策略模型,以确定它包含了所有必要的非形式化解释性文本。

如果整个安全策略模型是非形式化的,则本工作单元不再适用,并视为已经满足。

对于那些只靠半形式化或形式化描述难以理解的模型部分(例如,为说明任何形式化符号的含义),起支撑作用的叙述性描述是必需的。

13.6.7.3.2 工作单元 4:ADV_SPM.1-2

ISO/IEC 15408-3 ADV_SPM.1.2C TSP 模型应描述所有能被模型化的 TSP 策略的规则与特征。

评估者*应核查*安全策略模型,以确定所有明确包含在 ST 中的安全策略都被模型化。

安全策略通过 ST 中功能性安全要求的集合来表述。因此为确定安全策略的性质(策略应被模型化),评估者应分析那些策略所调用的 ST 功能要求(如果包含在 ST 中,可通过 FDP_ACC“访问控制策略”和 FDP_IFC“信息流控制策略”)。

依靠 TOE,对访问控制进行形式/半形式模型化甚至是不可能的(例如,对于一个连在 Internet 上的防火墙来说,访问控制策略就不可能以有效的方式形式化地模型化,因为 Internet 的状态不能被完全定义)。对于任何不能用形式或半形式模型化的安全策略,应以一种非形式化方式提出。

如果 ST 中没有包含明确的策略(因为在 ST 中既没有 FDP_ACC"访问控制策略",也没有 FDP_IFC"信息流控制策略"),则本工作单元不再适用,并视为已经满足要求。

13.6.7.3.3 工作单元 4:ADV_SPM.1-3

评估者***应检查***安全策略模型,以确定所有由在 ST 中所声明的安全功能要求表达的安全策略都被模型化了。

除明确列出的策略(见工作单元 4:ADV_SPM.1-2)外,评估者应针对那些隐含在其他功能性安全要求类中的策略分析 ST 功能要求。例如,包含 FDP "用户数据保护"要求(除了 FDP_ACC"访问控制策略"和 FDP_IFC"信息流控制策略"),需要一个正在实施的数据保护策略描述;包含任何 FIA"标识和鉴别"要求,标识和鉴别策略描述出现在 TSP 模型中是必要的;包含 FAU"安全审计"要求,则需要审计策略的描述等。虽然其他功能要求族和通常所指的安全策略没有明显联系,它们仍然应实施那些应包含在安全策略模型中的安全策略(例如,抗抵赖、参照仲裁、私密性等)。

如果安全策略模型的表示是非形式化的,所有安全策略都能被模型化(即被描述),而且应被包含。当安全策略不能用形式化或半形式化安全策略模型表示时,应以一种非形式化方式提出策略。

如果 ST 没有包含隐含的策略,则本工作单元不再适用,并视为已经满足要求。

13.6.7.3.4 工作单元 4:ADV_SPM.1-4

评估者***应检查***安全策略模型的规则和特点,以确定 TOE 安全行为的模型化是清楚明白的。

规则和特点描述了 TOE 的安全状态。这种描述有可能包括在一个已评估和证实过的 ST 中。出于清晰的考虑,这样的描述应定义 TOE 的安全概念,识别 TOE 所控制实体的安全属性,和识别改变这些属性的 TOE 行为。例如,如果一个策略试图关注数据完整性,那么策略模型应当:

a) 定义 TOE 的完整性概念;
b) 识别那些 TOE 将保护其完整性的数据类型;
c) 识别能够修改数据的实体;
d) 识别潜在的修改者修改数据应遵守的规则。

13.6.7.3.5 工作单元 4:ADV_SPM.1-5

ISO/IEC 15408-3 ADV_SPM.1.3C TSP 模型应包含一个基本原理,证实该模型相对所有能被模型化的 TSP 策略是一致的和完备的。

评估者***应检查***安全策略模型基本原理,以确定被模型化了的行为与安全策略所描述的策略(如 ST 中功能要求明确规定的那样)是一致的。

在判断一致性方面,评估者验证基本原理是否说明了在安全策略模型中描述的每条规则和特征准确地反映了安全策略的意图。例如,如果策略规定访问控制应达到单个个体这样的粒度,那么从控制用户组方面描述 TOE 安全行为的模型就与访问控制策略的描述不是一致的。同样,如果策略规定访问控制应针对用户组,那么从控制单个用户方面描述 TOE 安全行为的模型也与策略就不是一致的。

保证是从策略的明确且概括性陈述中获得的,该策略以 TOE 安全功能要求为基础。保证获得是双重的:聚集每个安全策略的描述到一个简明的整体,有助于理解所实施策略的细节;另外,如此集中描述,使得更容易发现任何差异或不一致之处(作为安全策略模型 ADV_SPM.*.3C 元素的组成部分,应满足),并提供了安全状态的一个清晰特征(作为安全策略模型 ADV_SPM.*.2C 元素的组成部分,应满足)。

信息安全策略模型(ISPM)的要求是由安全策略的一个清晰陈述来满足。关于单独 ISPM 的需求不是绝对的,因为对于特别简单的策略或对于在 ST 中非常清晰地说明了的那些策略,就可以不需要单独的 ISPM。在这种情况下,ST 的不同章节(例如,安全要求、TOE 概要规范)可以组合在一起,提供安全策略的充分细节。但是,不是总是这样。例如,审计要求可以分散到 TOE 安全功能要求的陈述中,不可能提供整个策略的一个明确模型。除非,ST 的另外章节(可能是 TOE 概要规范)将审计要求聚集成一个具有内聚性的整体,这样就需要一个单独的 ISPM,以便允许检测 ST 要求的不一致之处,这种不一致也可通过另外的方式来检测。

当开发者声明关于某些或所有安全策略的 ISPM 要求都由 ST 满足时,评估者需要通过采用 ADV_SPM.1"非形式化安全策略模型"组件的要求,来确定策略是清晰表述的,并且模型与 ST 的其他部分是一致的。作为 ISPM 基本原理的一部分,或许开发者声明 ISPM 完全由 ST 来满足,这样基本原理就可以参考 ST 不同部分间适宜性和对应性的证明。在评估本工作单元时,评估者可以利用 ST 评估在这方面的结果。

关于一致性分析的指南见 A.3"一致性分析"。

13.6.7.3.6 工作单元 4:ADV_SPM.1-6

评估者***应检查***安全策略模型基本原理,以确定模型化的行为对于由安全策略描述的策略是完备的(如 ST 中功能要求明确规定的那样)。

在确定基本原理完备性方面,评估者应考虑安全策略模型的规则和特征,并将这些规则和特征映射到明确的策略陈述中(即功能性要求)。基本原理应说明所有需要被模型化的策略都与安全策略模型中描述的规则和特征相关。

当开发者声明关于某些或所有安全策略的 ISPM 要求都由 ST 满足时,评估者需要通过采用 ADV_SPM.1"非形式化安全策略模型"组件的要求,来确定策略是清晰表述的,并且模型与 ST 的其他部分是完全一致的。在评估本工作单元时,评估者可以利用 ST 评估在这方面的结果。

13.6.7.3.7 工作单元 4:ADV_SPM.1-7

ISO/IEC 15408-3 ADV_SPM.1.4C TSP 模型和功能规范之间对应性的证实应说明功能规范中的所有安全功能相对 TSP 模型是一致的和完备的。

评估者***应检查***功能规范对应的安全策略模型的证实,以确定它标识了在功能规范中描述的所有安全功能,这些功能实现了一部分策略。

在确定完备性时,评估者审查功能规范,标识哪种功能直接支持安全策略模型,并验证这些功能存在于功能规范的安全策略模型的相应说明中。

13.6.7.3.8 工作单元 4:ADV_SPM.1-8

评估者***应检查***功能规范对应安全策略模型的证实,以确定那些被标识为实现模型的功能描述与功能规范的描述是一致的。

为了证实一致性,评估者要验证功能规范对应性,该对应性应说明,那些在功能规范中实现了策略模型的功能的描述,能标识该模型定义的属性和特征,并实施了模型定义的规则。

当对不被信任的用户和管理员实施不同的安全策略时,对用户和管理员实施的安全策略与用户指南和管理员指南中对其各自行为的描述是一致的。例如,针对远程不可信用户所实施的"标识与鉴别"策略,可比那些针对只能访问被物理保护区域的管理员所实施的策略更严格。鉴别的不同应与用户指南和管理员指南中的鉴别描述的差异相一致。

关于一致性分析的指南见 A.3"一致性分析"。

13.7 指导性文档活动

指导性文档活动的目的是判断该文档是否充分描述了应如何操作 TOE。这些文档针对两类用户：一类是可信的管理员和非管理员用户，他们的不正确行为可能影响 TOE 安全性，另一类是那些不可信用户，他们的不正确行为可能影响其拥有的数据的安全性。

13.7.1 应用注释

指导性文档活动关注那些与 TOE 安全性相关的功能和接口。TOE 的安全配置在 ST 中进行了描述。

13.7.2 管理员指南评估（AGD_AMD.1）

13.7.2.1 目的

本子活动的目的是确定管理员指南是否描述了如何以安全方式管理 TOE。

13.7.2.2 输入

本子活动的评估证据是：

a) ST；
b) 功能规范；
c) 高层设计
d) 用户指南；
e) 管理员指南；
f) 安全安装、生成和启动程序；
g) 生命周期定义。

13.7.2.3 应用注释

术语“管理员”指在 TOE 中执行关键安全操作（例如，设置 TOE 配置参数）的可信人员。这些操作可能影响 TSP 的执行，因此管理员拥有特殊的权限来执行这些操作。管理员角色应当与 TOE 中的非管理员用户角色明确区分开。

在 ST 中可定义有不同的管理员角色或管理员组，这些角色和组能可被 TOE 识别并可执行 TOE 的安全功能，例如审计员、管理员或日常管理者。每个角色可能具备多种或一种能力。这些角色的能力和相应的特权在 FMT 类中进行描述。管理员指南中应考虑不同的管理员角色和管理员组。

13.7.2.4 行为 AGD_ADM.1.1E

13.7.2.4.1 工作单元 4：AGD_ADM.1-1

ISO/IEC 15408-3 AGD_ADM.1.1C 管理员指南应描述 TOE 管理员可使用的管理功能和接口。

评估者***应检查***管理员指南，以确定其描述了 TOE 管理员可用的管理性安全功能和接口。

管理员指南应包含安全功能的概述，这些安全功能在管理员界面中是可见的。

管理员指南应标识并描述管理性安全接口与功能的用途、行为和相互关系。

对于每个管理性安全接口和功能，管理员指南应当：

a) 描述调用接口的方法（如命令行、程序语言系统调用、菜单选择、命令按钮）；
b) 描述由管理员设置的参数及其有效值和默认值；
c) 描述即时的 TSF 响应、消息或返回代码。

13.7.2.4.2 工作单元 4:AGD_ADM.1-2

ISO/IEC 15408-3 AGD_ADM.1.2C 管理员指南应描述如何以安全的方式管理 TOE。

评估者***应检查***管理员指南,以确定它描述了如何以安全的方式管理 TOE。

管理员指南描述如何在 IT 环境中依照 TSP 运行 TOE,这应与 ST 所描述的情况一致。

13.7.2.4.3 工作单元 4:AGD_ADM.1-3

ISO/IEC 15408-3 AGD_ADM.1.3C 管理员指南应包含了在安全处理环境中受控的功能和特权的警示信息。

评估者***应检查***管理员指南,以确定其包含了在安全处理环境中受控的功能和特权的警示信息。

TOE 的配置可以允许用户拥有不同的特权来使用 TOE 的不同功能,这意味着可以授权某些用户执行某些功能,而其他用户无权执行,这些功能和特权应在管理员指南中进行描述。

管理员指南应标识出应控制的功能和特权、控制的类型以及控制的理由。警告应说明预期的效果、可能的负面影响以及与其他功能和特权可能的相互作用。

13.7.2.4.4 工作单元 4:AGD_ADM.1-4

ISO/IEC 15408-3 AGD_ADM.1.4C 管理员指南应描述所有与安全操作 TOE 有关的用户行为假设。

评估者***应检查***管理员指南,以确定它描述了所有与安全操作 TOE 有关的用户行为假设。

关于用户行为的假设可以在 ST 的 TOE 安全环境陈述中比较详细的描述,而只有涉及安全操作 TOE 的信息才需要包含在管理员指南中。

例如:要安全操作 TOE 用户有责任对他们的口令进行保密。

13.7.2.4.5 工作单元 4:AGD_ADM.1-5

ISO/IEC 15408-3 AGD_ADM.1.5C 管理员指南应描述所有受管理员控制的安全参数,并说明适当的安全值。

评估者***应检查***管理员指南,以确定它描述了所有受管理员控制的安全参数,并说明适当的安全值。

对于每个安全参数,管理员指南应描述参数的用途、参数的有效值和缺省值,以及这些参数安全与非安全的使用设置。这些参数可以分别描述,也可以综合起来描述。

13.7.2.4.6 工作单元 4:AGD_ADM.1-6

ISO/IEC 15408-3 AGD_ADM.1.6C 管理员指南应描述每一种与需要执行的管理功能有关的安全相关事件,包括改变在 TSF 控制下的实体的安全特性。

评估者***应检查***管理员指南,以确定它描述了每一种与需要执行的管理功能有关的安全相关事件,包括改变在 TSF 控制下的实体的安全特性。

应详尽描述所有类型的安全相关事件,以便管理员知道可能发生什么事件以及为保持安全管理员应采取哪些动作。应充分定义在 TOE 的操作过程中可能发生的安全相关事件(例如,审计迹的溢出、系统崩溃、用户记录的更新——如当用户离开组织时撤消该用户账号),以允许管理员介入来保持安全。

13.7.2.4.7 工作单元 4:AGD_ADM.1-7

ISO/IEC 15408-3 AGD_ADM.1.7C 管理员指南应与评估提交的所有其他文档保持一致。

评估者***应检查***管理员指南,以确定它与评估提交的所有其他文档是一致的。

特别是在 ST 中可能包含一些对 TOE 管理员提出的关于 TOE 安全环境和安全目的的详细的警告

信息。

有关一致性分析的指南参见 A.3“一致性分析”。

13.7.2.4.8 工作单元 4:AGD_ADM.1-8

ISO/IEC 15408-3 AGD_ADM.1.8C 管理员指南应描述所有与管理员有关的 IT 环境安全要求。

评估者***应检查***管理员指南,以确定它描述了所有与管理员有关的 关于 TOE 的 IT 环境的 IT 安全要求。

如果 ST 没有包括关于 IT 环境的 IT 安全要求,则本工作单元不适用,并视为已经满足。

本工作单元仅与 IT 安全要求有关,而与组织安全策略无关。

评估者应当分析关于 TOE 的 IT 环境安全要求(ST 中的可选陈述),并与管理员指南比较,以确保与管理员有关的 ST 的所有安全要求都在管理员指南中得到适当的描述。

13.7.3 用户指南评估(AGD_USR.1)

13.7.3.1 目的

本子活动的目的是为了确定用户指南是否描述了由 TSF 提供的安全功能和接口,以及指南是否提供了安全使用 TOE 的相关说明和指导。

13.7.3.2 输入

本子活动的评估证据是:

a) ST;
b) 功能规范;
c) 高层设计
d) 用户指南;
e) 管理员指南;
f) 安全安装、生成和启动程序。

13.7.3.3 应用注释

在 ST 中可定义不同的用户角色或用户组,这些角色和组能被 TOE 识别并可执行 TOE 的安全功能。这些角色的能力和相应的特权在 FMT 类中进行描述。用户指南中应考虑不同的用户角色和组。

13.7.3.4 行为 AGD_USR.1.1E

13.7.3.4.1 工作单元 4:AGD_USR.1-1

ISO/IEC 15408-3 AGD_USR.1.1C 用户指南应描述 TOE 的非管理员用户可使用的功能和接口。

评估者***应检查***用户指南,以确定其描述了 TOE 的非管理员用户可使用的安全功能和接口。

用户指南应包含安全功能的概述,这些安全功能在用户界面中可见的。

用户指南应当标识和描述安全接口和功能的用途。

13.7.3.4.2 工作单元 4:AGD_USR.1-2

ISO/IEC 15408-3 AGD_USR.1.2C 用户指南应描述用户可访问的由 TOE 提供的安全功能的使用。

评估者***应检查***用户指南,以确定它描述了用户可访问的由 TOE 提供的安全功能的使用。

用户指南应标识和描述用户可用安全接口和功能的行为及其相互关系。

如果允许用户调用 TOE 安全功能,用户指南应为用户提供该功能接口的描述。

对每个接口和功能,用户指南应当:

a) 描述调用接口的方法(如命令行、程序语言系统调用、菜单选择、命令按钮);

b) 描述由用户设置的参数及其有效值和默认值;

c) 描述即时的 TSF 响应、消息或返回代码。

13.7.3.4.3 工作单元 4:AGD_USR.1-3

ISO/IEC 15408-3 AGD_USR.1.3C 用户指南应包含了在安全处理环境中受控的用户可访问功能和特权的警示信息。

评估者***应检查***用户指南,以确定其包含了在安全处理环境中受控的用户可访问功能和特权的警示信息。

TOE 的配置可以允许用户拥有不同的特权来使用 TOE 的不同功能,这意味着可以授权某些用户执行某些功能,而其他用户无权执行,这些用户可访问的功能和特权应在用户指南应中进行描述。

用户指南应标识可用的功能和特权、所需命令的类型以及使用这些命令的理由。用户指南应当包含使用受控的功能和特权时的警告。警告应当说明预期的效果、可能的负面影响以及与其他功能和特权可能的相互作用。

13.7.3.4.4 工作单元 4:AGD_USR.1-4

ISO/IEC 15408-3 AGD_USR.1.4C 用户指南应清晰地阐述安全操作 TOE 所必需的所有用户职责,这些职责包括那些在 TOE 安全环境陈述中的与用户行为相关的假设。

评估者***应检查***用户指南,以确定其阐述了安全操作 TOE 所必需的所有用户职责,这些职责包括那些在 TOE 安全环境陈述中的与用户行为相关的假设。

关于用户行为的假设可以在 ST 的 TOE 安全环境陈述中有比较详细的描述,在用户指南中只需包含涉及 TOE 安全操作的信息。

用户指南应当提供关于有效使用这些安全功能的建议(如审查口令组合的习惯、对用户文件备份频率的建议、对改变用户访问特权所产生影响的讨论)。

例如:要安全操作 TOE 用户有责任对他们的口令进行保密。

用户指南应指出用户是否能够调用某项功能,或者用户是否需要管理员的帮助。

13.7.3.4.5 工作单元 4:AGD_USR.1-5

ISO/IEC 15408-3 AGD_USR.1.5C 用户指南应与评估提交的所有其他文档保持一致。

评估者***应检查***用户指南,以确定其与评估提交的所有其他文档是一致的。

评估者要确保用户指南和评估提交的所有其他文档不会相互矛盾。如果 ST 包含任何对 TOE 用户提出的关于 TOE 安全环境和安全目的的详细警告信息,这一点就尤其重要。

有关一致性分析的指南参见 A.3“一致性分析”。

13.7.3.4.6 工作单元 4:AGD_USR.1-6

ISO/IEC 15408-3 AGD_USR.1.6C 用户指南应描述所有与用户有关的 IT 环境安全要求。

评估者***应检查***用户指南,以确定其描述了所有与用户有关的 TOE 的 IT 环境安全要求。

如果 ST 中不包含 IT 环境的 IT 安全要求,本工作单元不适用,并视为已经满足。

本工作单元仅与 IT 安全要求相关,而与组织安全策略无关。

评估者应分析 TOE 的 IT 环境安全要求(ST 中的可选陈述),并与用户指南比较,以确保所有与用户有关的 ST 安全要求都在用户指南中得到了恰当的描述。

13.8 生命周期支持活动

生命周期支持活动的目的是确定开发者在 TOE 开发和维护期间所使用程序的充分性。这些程序包括 TOE 开发全过程所使用的安全措施、开发者使用的生命周期模型以及开发者在整个 TOE 生命周期中使用的工具。

开发者安全程序是为了保护 TOE 及其相关的设计信息,以防它们受到干扰或暴露。开发过程中的干扰使故意引入脆弱性成为可能。而设计信息的暴露可能导致脆弱性更容易被人利用。这些程序的充分性依赖于 TOE 的性质和开发过程。

如果 TOE 的开发和维护过程没有得到很好的控制,将会带来实现方面的脆弱性。与所定义的生命周期模型一致有助于这方面控制的改进。

使用明确定义的开发工具有助于确保在细化过程中不会不经意地引入脆弱性。

13.8.1 开发安全评估(ALC_DVS.1)

13.8.1.1 目的

本子活动的目的是确定开发者对开发环境的安全控制是否足以提供 TOE 设计和实现的保密性和完整性,这是保证 TOE 的安全操作不受危害所必需的。

13.8.1.2 输入

本子活动的评估证据是:

a) ST;

b) 开发安全文档。

此外,评估者可以检查其他交付件,以确定安全控制定义明确且得到了遵循。评估者特别要检查开发者的配置管理文件(用作 ACM_CAP.4“产生支持和接受程序”和 ACM_SCP.2“问题跟踪 CM 覆盖”子活动的输入)。此过程使用的证据也是必需的。

13.8.1.3 行为 ALC-DVS.1.1E

13.8.1.3.1 工作单元 4:ALC_DVS.1-1

ISO/IEC 15408-3 ALC-DVS.1.1C 开发安全文档应描述用于保护 TOE 设计和实现中保密性和完整性所必需的所有物理的、程序的、人员的及其他在 TOE 的开发环境中的安全措施。

评估者***应检查***开发安全文档,以确定其详细描述了在 TOE 的开发环境中使用的用于保护 TOE 设计和实现保密性与完整性所必需的所有安全措施。

评估者要确定哪些是必需的,这可首先从 ST 中,特别是关于威胁、组织安全策略和假设等章节中查阅可帮助确定必要保护的任何信息,(也可能找不到明确提及的信息)。在这方面,环境安全目的陈述也可能有用。

如果从 ST 中得不到明确的信息,评估者就需要根据对 TOE 预期使用环境的考虑,确定必要的措施。如果开发者的措施考虑得不够全面,开发者就应该根据潜在的可利用脆弱性,为评估提供一份清晰的理由说明。

评估者在检查文档时应该考虑下面几种安全措施类型:

a) 物理上的,例如,用于阻止对 TOE 开发环境未授权访问(在正常工作时间和其他时间里)的物理访问控制。

b) 过程上的,例如涵盖:

——准许对开发环境或者环境中的特定部分(如开发设备)的访问;

——在开发者离开开发团队时撤消其访问权;

——将受保护的材料转移出开发环境;

——容许并陪同来访者参观开发环境;

——建立角色和责任以确保持续地采取安全措施并检查安全违背情况。

c) 人员上的,例如为建立对新开发成员的信任所采取的任何控制或检查。

d) 其他安全措施,例如对所有开发设备的逻辑保护。

开发安全文档应明确开发的场所,并描述执行哪方面的开发以及在每个场所使用的安全措施。比如说,开发行为可能发生在一幢建筑内的多个设备上、同一场所的多个建筑内,或者分布在多个场所。开发工作也包括诸如创建多个 TOE 拷贝之类的任务(若可行的话)。本工作单元不应与 ADO_DEL“交付”的工作单元重叠,但评估者应确保所有的方面都被某个子活动或其他子活动覆盖。

此外,开发安全文档可以描述不同的安全措施,按照功能和所需的输入与输出的特点,这些措施可被运用到开发的不同方面。例如,不同的过程可能被运用到 TOE 不同部分的开发中,或者开发过程的不同阶段。

13.8.1.3.2 工作单元 4:ALC_DVS.1-2

评估者***应检查***开发的保密性和完整性策略,以确定所使用安全措施的充分性。

包括的策略管理有:

a) 与 TOE 开发相关的哪些信息需要保证保密性,以及允许哪些开发成员访问这些材料;

b) 为了保持 TOE 的完整性,应保护哪些材料,以防止其被未授权修改,以及允许哪些开发成员修改这些材料。

评估者应确定在开发安全文档中描述了这些策略,所使用的安全措施与策略是一致的并且策略是完备的。

应注意,配置管理程序有助于保护 TOE 的完整性,评估者应避免与 ACM_CAP“CM 能力”子活动的工作单元相重叠。例如,CM 文档可以描述控制可访问开发环境和修改 TOE 的角色或个人的安全程序。

虽然 ACM_CAP“CM 能力”要求是固定的,但那些关于 ALC_DVS“开发安全”的要求,若仅强制执行必需的措施,将主要依赖于 TOE 的性质和 ST 的安全环境部分所提供的信息。例如,ST 可以标识组织安全策略,以要求 TOE 由具有安全许可的人员来开发。这样,评估者就可以确定这一策略是应用在本子活动中的。

13.8.1.3.3 工作单元 4:ALC_DVS.1-3

ISO/IEC 15408-3 ALC_DVS.1.2C 开发安全文档应提供在 TOE 的开发和维护过程中执行安全措施的证据。

评估者***应核查***开发安全文档,以确定作为程序应用结果的文档证据都已经产生。

评估者检查文档证据的产生,以确定其是否遵守程序。例如,证据产生可能包括登录日志和审计迹。评估者可以选择抽样检查证据。

有关抽样的指南见 A.2“抽样”。

13.8.1.4 行为 ALC_DVS.1.2E

13.8.1.4.1 工作单元 4:ALC_DVS.1-4

评估者***应检查***开发安全文档和相关的证据,以确定开发者正在采取安全措施。

本工作单元要求评估者确定在开发安全文档中描述的安全措施都已被采用,以确定 TOE 的完整性和相关文档的保密性正受到充分保护。例如,可以通过检查所提供的文档证据来确认这一点,并通过检查开发环境来补充文件证据。对开发环境的现场核查将允许评估者:

a) 观察安全措施(如物理措施)的应用状况;

b) 检查程序应用的文档证据;

c) 会见开发人员,检查其对开发安全策略、程序以及他们责任的认识。

对开发场所的现场核查是信任措施正在使用的一个有用方法。任何不采用这种检查而作出的决定都应该在和监督者商议后作出。

有关检查开发场所的指南参见 A.5“现场核查”。

13.8.2 生命周期定义评估(ALC_LCD.1)

13.8.2.1 目的

本子活动的目的是确定开发者是否使用了 TOE 生命周期的一个文档化模型。

13.8.2.2 输入

本子活动的评估证据是:

a) ST;

b) 生命周期定义文档。

13.8.2.3 行为 ALC_LCD.1.1E

13.8.2.3.1 工作单元 4:ALC_LCD.1-1

ISO/IEC 15408-3 ALC_LCD.1.1C 生命周期定义文档应描述用于开发和维护 TOE 的模型。

评估者***应检查***生命周期模型的文档化描述,以确定它是否覆盖了开发和维护过程。

生命周期模型包括 TOE 开发和维护中所使用的程序、工具和技术。生命周期模型的描述应包括开发者使用的程序、工具及技术的信息(如关于设计、编码、测试、缺陷修复),还应描述管理程序应用的总体管理结构(如识别和描述在生命周期模型所涵盖的开发和维护过程所要求的每个程序的个体责任)。ALC_LCD.1“开发者定义的生命周期模型”不要求所使用的模型符合任何标准生命周期模型。

13.8.2.3.2 工作单元 4:ALC_LCD.1-2

ISO/IEC 15408-3 ALC_LCD.1.2C 生命周期模型应提供对 TOE 的开发和维护进行的必要控制。

评估者***应检查***生命周期模型,以确定生命周期模型所描述的程序、工具及技术的使用将对 TOE 的开发和维护作出积极贡献。

生命周期模型中提供的信息使评估者确信已采用的开发和维护程序能使安全缺陷存在的可能性降到最低。比如,如果生命周期模型描述审查过程,而不记录组件的变化,评估者将难以确信 TOE 不会引入错误。通过比较模型描述和从其他与 TOE 开发相关的评估者行为(如 ACM 活动所覆盖的那些行为)中获得对开发过程的理解后,评估者会得到更进一步的保证。如果生命周期中的不足之处可能会在 TOE 中引入缺陷,无论偶然或故意,这些标识出来的不足之处都应该受到关注。

ISO/IEC 15408 不强制要求任何特殊的开发方法,每种方法都有其优点。例如,在受控环境下,可以应用循环法、快速原型法和瀑布法来产生一个高质量的 TOE。

13.8.3 工具与技术评估(ALC_TAT.1)

13.8.3.1 目的

本子活动的目的是确定开发者是否使用了明确定义的开发工具(如程序语言或计算机辅助设计(CAD)系统)来产生一致且可预测的结果。

13.8.3.2 输入

本子活动的评估证据是:

a) 开发工具文档;

b) 实现表示的子集。

13.8.3.3 应用注释

本次工作可以与子活动 ADV_IMP.1“TSF 实现的子集”同时进行,特别是在确定那些会影响目标代码的工具的特征时(如编译选项)。

13.8.3.4 行为 ALC_TAT.1.1E

13.8.3.4.1 工作单元 4:ALC_TAT.1-1

ISO/IEC 15408-3 ALC_TAT.1.1C 所有用于实现的开发工具应是明确定义的。

评估者***应检查***所提供的开发工具文档,以确定所有开发工具都是明确定义的。

例如,认为明确定义的编程语言、编译器或 CAD 系统,就是遵循一种公认标准,如 ISO 标准的那些编程语言、编译器或 CAD 系统。明确定义的编程语言是指语法有清晰完备的描述,且每一种结构的语义也都有详细描述的那种编程语言。

13.8.3.4.2 工作单元 4:ALC_TAT.1-2

ISO/IEC 15408-3 ALC_TAT.1.2C 开发工具文档应无歧义地定义实现中每个语句的含义。

评估者***应检查***开发工具文档,以确定它是否无歧义地定义了用于实现的所有陈述的含义。

开发工具文档(如,程序语言规范和用户手册)应覆盖 TOE 实现表示中的所有陈述,并对每一项陈述定义了一个清晰且无歧义的目的和作用。这部分工作可以与评估者在子活动 ADV_IMP.1“TSF 实现的子集”中执行的实现表示检查同时进行。测试的关键是确定文档是否足够清晰,以致评估者能够理解实现表示。例如,文档不应假定读者是所用程序语言的专家。

倘若评估者可以获得一些文献标准,那么引用这些文献标准就是一种满足该要求的可接受的方法,开发工具文档中任何与标准之间的差异都应记录下来。

关键是测试在对子活动 ADV_IMP“实现表示”涵盖的源代码进行分析时,评估者能否理解源代码。另外,下述要点可用于发现问题域:

a) 在语言定义方面,诸如“此结构的作用未定义”、“实现依赖的”以及“错误的”等句子或术语都可能表明那些定义不是十分明确的区域;

b) 别称(允许以不同方式引用同一内存)是引发歧义的普遍来源;

c) 异常处理(如,内存用尽或堆栈溢出后的处理)常常都定义得不是很好。

通常使用的多数语言,尽管设计得很好,也会有一些有问题的结构。如果实现语言大部分都是明确定义的,只是有些有问题的结构,就应赋予一种不确定的裁定,暂缓对源代码的检查。

评估者应核实在源代码的检查过程中,问题结构的使用不会引入脆弱性,也应确保通过文档化标准

排除掉的结构不会被使用。

13.8.3.4.3 工作单元 4:ALC_TAT.1-3

ISO/IEC 15408-3 ALC_TAT.1.3C 开发工具文档应无歧义地定义所有实现依赖选项的含义。

评估者***应检查***开发工具文档,以确定它是否无歧义地定义了所有实现依赖选项的含义。

软件开发工具文档应定义哪些可能影响可执行代码含义的实现依赖选项,以及与文档化标准语言的差异之处。给评估者提供源代码时,也应提供所用的编译和链接选项的信息。

硬件设计和开发工具的文档应描述所有影响工具输出(如详细的硬件规范或真实硬件)的选项用法。

13.9 测试活动

本活动的目的是通过独立测试 TSF 的一个子集来确定在设计文档中规定的 TSF 行为是否与在 ST 中规定的 TOE 安全功能要求一致。本活动是通过确定开发者已经根据 TSF 的功能规范及其高层设计测试了 TSF 来完成的,可以通过对开发者的测试进行抽样验证和独立测试 TSF 的一个子集而获得对开发者测试结果的信任。

13.9.1 应用注释

评估者测试子集的构成和大小依赖于独立测试子活动(ATE_IND.2“独立测试——抽样”)中所讨论的几个因素。已知的公开弱点便是这类因素之一,评估者需访问这些信息(例如,从评估体制获取)。

ISO/IEC 15408 已经将覆盖和深度从功能测试中分离出来,以便增强使用族中组件的灵活性。但希望这些族的要求被一起应用,以确认 TSF 是根据规范进行运行的。这些族的紧密结合已经导致评估工作的子活动有一些重复,以下的这些应用注释将使相同活动的子活动和 EAL 之间的文本重复减到最少。

13.9.1.1 理解 TOE 的预期行为

在正确评估测试文档是否充分之前,或在新的测试创建之前,评估者应理解安全功能在满足要求的情况下所期望的预期行为。

评估者可以选择每一次只关注 TSF 的一个安全功能。对于每个安全功能,评估者检查 ST 要求和功能规范、高层设计与指导性文档的相关部分,以获得对 TOE 预期行为方式的理解。

在理解预期行为之后,评估者要检查测试计划,以获得对测试方法的理解。在大多数情况下,测试方法要通过在外部或内部接口处激发安全功能并观察其反应来进行。但,有些情况下安全功能不能在一个接口处被充分测试(比如对于残余信息的保护功能而言),此时需要使用其他的方法。

13.9.1.2 测试与验证安全功能预期行为的替代方法

如果在接口处不能进行测试或者没有充分测试,测试计划应确定其他替代方法验证预期行为。评估者有责任确定替代方法的适用性。但是,在评估替代方法的适用性时应考虑以下几个方面:

a) 对实现表示进行分析,确定 TOE 应该执行的必要行为就是一个可接受的替代方法。这意味着可以检查一个软件 TOE 的代码,或者可以对一个硬件 TOE 进行芯片掩膜检查。

b) 即使 EAL 与低层设计或实现的评估不匹配时,使用开发者集成或模块化测试的证据也是可接受的。如果在检验一个安全功能的预期行为时使用了开发者集成或模块化测试的证据,应注意确认测试证据是否反映了 TOE 的当前实现。如果因为测试导致子系统或者模块发生了改变,那么通常需要通过分析或进一步测试来跟踪和处理证据的变化。

应该强调的是,只有在开发者和评估者都确认不存在其他实际手段对某一安全功能的预期行为进行测试时,方可用替代方法进行补充测试。这种替代使开发者可以把在上述环境下测试的开销(时间或金钱)减少到最小;这并不是为赋予评估者更多自由,索要不必要的 TOE 附加信息而设计的,也不会取代原有测试计划。

13.9.1.3 确认测试的充分性

测试前应建立测试所需的初始条件,可用应设置的参数形式表示,也可用测试顺序表示即以一个测试的完成作为另一个测试的必备条件。为了使观察测试结果不偏向预期测试结果,评估者应确定初始条件是完备的、适当的。

测试步骤和预期结果描述用于接口的行为和参数,就像预期结果应该是什么样的以及怎样被验证。评估者应确定测试步骤和预期结果与功能规范和高层设计是一致的。测试应验证规范中确定的行为。这意味着在功能规范和高层设计中明确描述的每个安全功能行为特征都应具有可测性和预期结果,以验证其行为。

虽然开发者应测试所有 TSF,但不要求对接口的所有规范进行测试。本活动的总体目的是确定已经依据功能规范和高层设计中的行为声明,对每个安全功能进行了充分测试。测试程序将提供了解开发者在测试中是如何检验安全功能的方法。当评估者开发附加测试进行 TOE 独立测试时,可以使用这种信息。

13.9.2 覆盖评估(ATE_COV.2)

13.9.2.1 目的

本子活动的目的是确定测试(像文件说明的那样)是否充分保证已经依据功能规范系统地测试过 TSF。

13.9.2.2 输入

本子活动的评估证据是:

a) ST;
b) 功能规范;
c) 测试文档;
d) 测试覆盖分析。

13.9.2.3 行为 ATE_COV.2.1E

13.9.2.3.1 工作单元 4:ATE_COV.2-1

ISO/IEC 15408-3 ATE_COV.2.1C 测试覆盖的分析应证实测试文档中的测试项与功能规范中所描述的 TSF 之间的对应性。

评估者***应检查***测试覆盖分析,以确定测试文档中所标识的测试与功能规范之间的对应是准确的。

对应性可采用表格或矩阵的形式来表示。有时映射关系足以表明测试的对应关系;但有时,开发者提供的基本原理(一般性描述)应补充对应关系的分析。

图 13 示意了功能规范中所描述的安全功能与测试文档中概括的测试之间对应关系的概念框架。测试中可能包括一项或几项安全功能,这取决于测试依赖性或实施测试的总体目标。

测试覆盖分析中列出的测试和安全功能的标识应是明确无误的。测试覆盖分析可使评估者把所标识的测试追溯到测试文档,并把被测试的特殊安全功能追溯到功能规范。

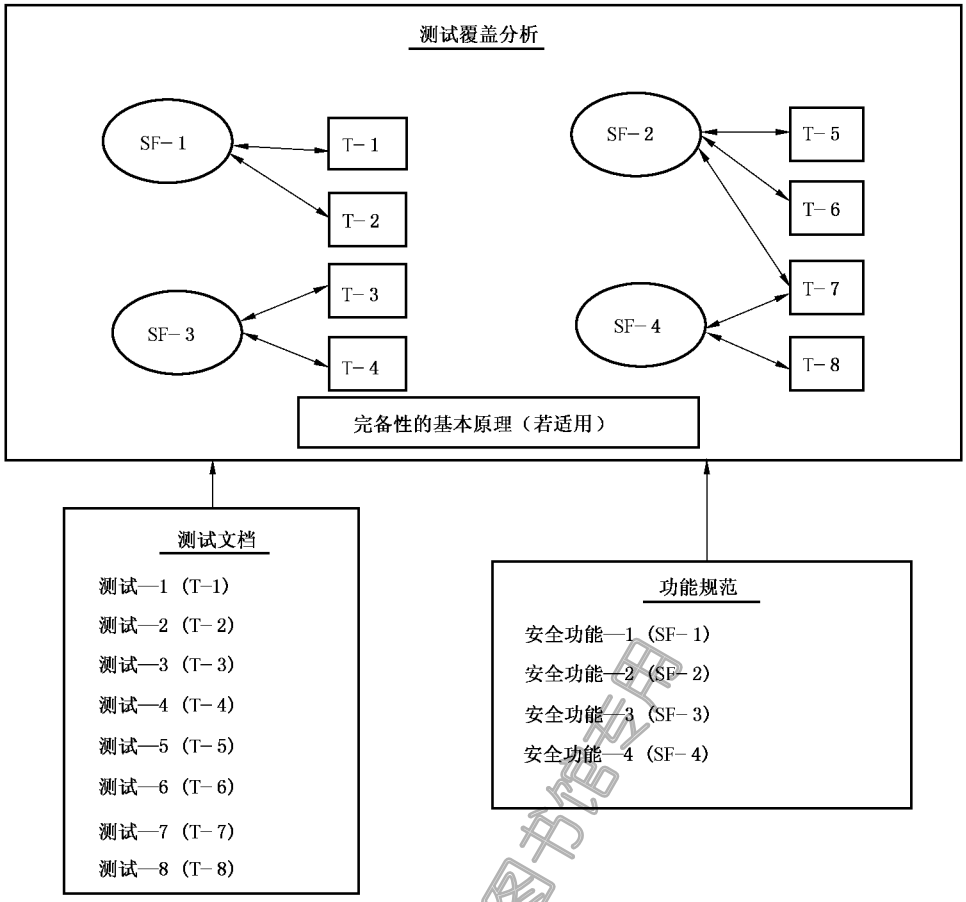

图 13　测试覆盖分析的概念框架

13.9.2.3.2　工作单元 4:ATE_COV.2-2

评估者***应检查***测试计划,以确定关于 TSF 每个安全功能的测试方法适于证实预期行为。

本工作单元的指南参见:

a)　13.9.1.1 应用注释“理解 TOE 的预期行为”;

b)　13.9.1.2 应用注释“测试与验证安全功能预期行为的替代方法”。

13.9.2.3.3　工作单元 4:ATE_COV.2-3

评估者***应检查***测试程序,以确定测试的初始条件、测试步骤和预期结果足以测试每个安全功能。

本工作单元的指南与功能规范相关,可参见:

a)　13.9.1.3 应用注释“确认测试的充分性”。

13.9.2.3.4　工作单元 4:ATE_COV.2-4

ISO/IEC 15408-3 ATE_COV.2.2C 测试覆盖的分析应证实功能规范中所描述的 TSF 与测试文档所标识的测试之间的对应性是完备的。

评估者***应检查***测试覆盖的分析,以确定功能规范中所描述的 TSF 与测试文档中标识的测试之间的对应性是完备的。

尽管不要求详尽的接口规范测试,但所有在功能规范中描述的安全功能和接口应在测试覆盖的分

析中说明,并映射到测试中,以满足完备性的要求。如图 13 所示,所有的安全功能具有相应的测试,因此在这个例子中描述了完整的测试覆盖。如果测试覆盖分析中标识的安全功能没有属于它的测试,那么说明覆盖不是完备的。

13.9.3 深度评估(ATE_DPT.1)

13.9.3.1 目的

本子活动的目的是要确定开发者是否已经对照高层设计测试了 TSF。

13.9.3.2 输入

本子活动的评估证据是:

a) ST;
b) 功能规范;
c) 高层设计;
d) 测试文档;
e) 测试深度分析。

13.9.3.3 行为 ATE_DPT.1.1E

13.9.3.3.1 工作单元 4:ATE_DPT.1-1

ISO/IEC 15408-3 ATE_DPT.1.1C 深度分析应证实测试文档中所标识的测试足以证实该 TSF 是依照其高层设计运行的。

评估者***应检查***测试深度分析,是否在测试文档中的测试项和高层设计之间建立了映射关系。

测试深度分析标识了在高层设计中描述的所有子系统,并提供了测试到这些子系统的一个映射关系。对应性可以采用表格或矩阵形式来表示。在有些情况下,映射关系可以充分说明测试的对应性。在其他情况下,开发者有必要用一个基本原理(一般的描述)来补充映射关系的证据。

在高层设计中可映射到并满足 TOE 安全要求的设计细节都应该经过测试,从而应映射到测试文档。图 14 展示了在高层设计中描述的子系统和用于测试这些子系统的 TOE 测试文档中所描述测试之间映射关系的一个概念框架。测试项可能涉及一个或多个安全功能,这依赖于测试依赖性或执行测试的总体目标。

13.9.3.3.2 工作单元 4:ATE_DPT.1-2

评估者***应检查***开发者的测试计划,以确定 TSF 的每个安全功能的测试方法适用于证实预期的行为。

本工作单元的指南参见:

a) 13.9.1.1 应用注释“理解 TOE 的预期行为”;
b) 13.9.1.2 应用注释“测试与验证安全功能预期行为的替代方法”。

TSF 的测试可以在外部接口、内部接口或两处同时执行。无论何种情况,评估者都应考虑其对充分测试安全功能的适当性,特别要确定对某个安全功能内部接口的测试是否有必要,或者能否通过操纵外部接口的方式来充分地测试这些内部接口(虽然是隐含的)。出于公正的目的,这个决定留给评估者。

13.9.3.3.3 工作单元 4:ATE_DPT.1-3

评估者***应检查***测试程序,以确定测试的初始条件、测试步骤和期望结果足以测试每个安全功能。

本工作单元的指南与高层设计相关,可参见:

a) 13.9.1.3 应用注释“确认测试的充分性”。

13.9.3.3.4 工作单元 4:ATE_DPT.1-4

评估者***应检查***测试深度分析,以确保高层设计中定义的 TSF 完全映射到测试文档中的测试项。

测试深度分析提供了高层设计和测试计划与程序之间对应性的一个完备陈述。在高层设计中描述的所有子系统和内部接口应在测试深度分析中说明。所有在测试深度分析中说明的子系统和内部接口应有对应的测试,从而满足完备性的要求。如图 14 所示,所有的子系统和内部接口都有属于它们的测试,因此这个例子描述了完整的测试深度。如果测试深度分析中标识的子系统或内部接口没有属于它们的测试,那么说明覆盖不是完备的。

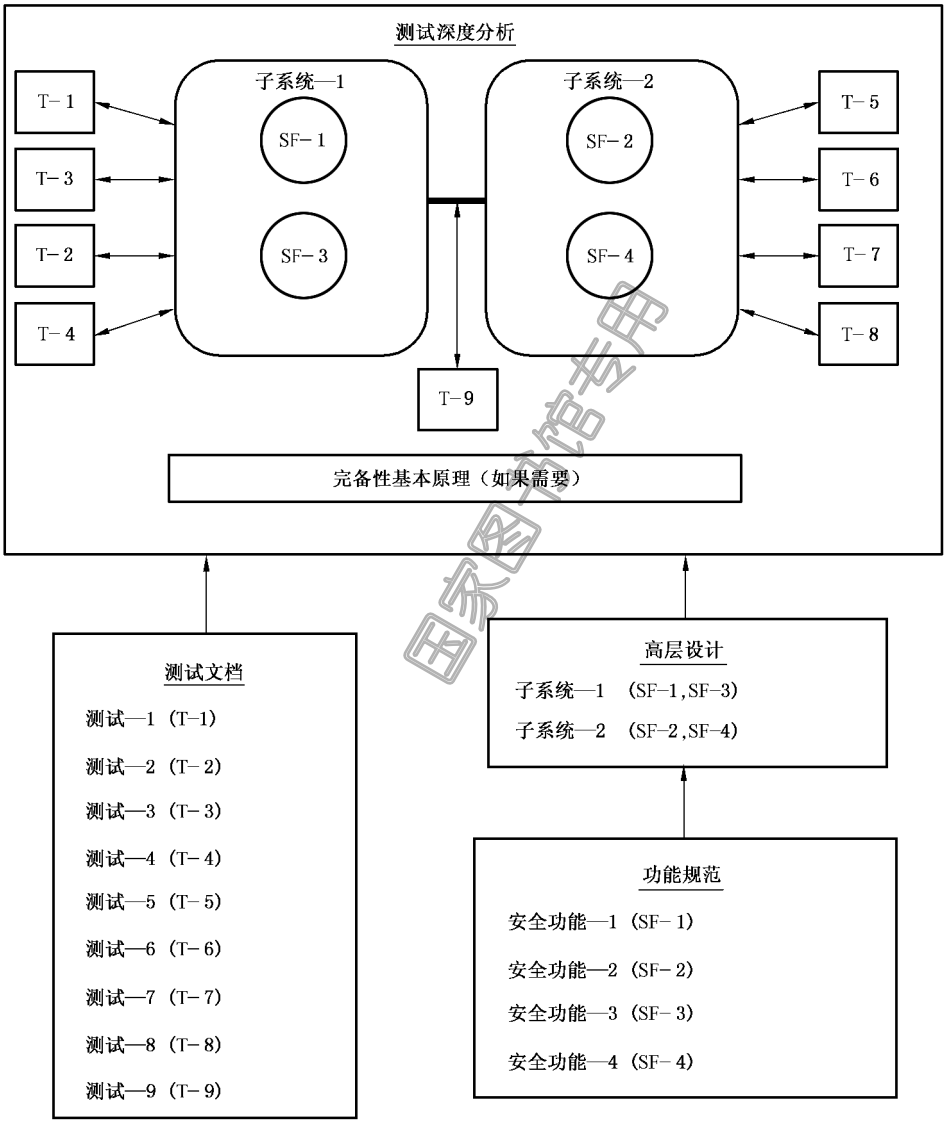

图 14 测试深度分析的概念框架

13.9.4 功能测试评估(ATE_FUN.1)

13.9.4.1 目的

本子活动的目的是确定开发者的功能测试文档是否可充分地证实安全功能都以按规定实现。

13.9.4.2 输入

本子活动的评估证据是：

a) ST；

b) 功能规范；

c) 测试文档；

d) 测试流程。

13.9.4.3 应用注释

测试文档应覆盖 TSF 的程度依赖于覆盖保证组件。

对于开发者提供的测试，评估者确定测试是否是可复验的，并确定开发者的测试在多大程度上可用于评估者的独立测试工作。开发者测试结果中表明可能有未按照规定执行的安全功能，评估者应对其进行独立测试，以确定情况是否属实。

测试文档应标识为测试建立测试条件或为后续测试清除相关条件而使用特权模式的情况。测试文档要描述为什么必需使用特权模式以获得必要的条件（例如：测试套件的效率、产生测试所需的非特权用户不能创建的特殊对象），以及在执行 TOE 安全功能测试步骤前如何退出特权模式。因此，虽然在建立测试条件时，测试配置可能与 ST 中描述的 TOE 不一致，但是测试文档应描述如何使配置返回到与 ST 所描述配置相一致的状态，以便执行测试步骤。

13.9.4.4 行为 ATE_FUN.1.1E

13.9.4.4.1 工作单元 4：ATE_FUN.1-1

ISO/IEC 15408-3 ATE_FUN.1.1C 测试文档应包括测试计划、测试流程描述、预期测试结果和实际测试结果。

评估者***应检查***测试文档是否包括测试计划、测试流程描述、预期测试结果和实际测试结果。

13.9.4.4.2 工作单元 4：ATE_FUN.1-2

ISO/IEC 15408-3 ATE_FUN.1.2C 测试计划应标识要测试的安全功能，并应描述测试的目标。

评估者***应核查***测试计划是否标识了待测安全功能。

用于标识待测安全功能的一种方法是可参考规定特定安全功能的功能规范中所描述的相应部分。

在执行本工作单元时，评估者可能希望采用抽样的策略。

关于抽样的指南参见 A.2“抽样”。

13.9.4.4.3 工作单元 4：ATE_FUN.1-3

评估者***应检查***测试计划，以确定它描述了测试的目标。

测试计划提供了关于安全功能如何测试的信息以及测试过程中的测试配置信息。

在执行本工作单元时，评估者可能希望采用抽样的策略。

关于抽样的指南参见 A.2“抽样”。

13.9.4.4.4 工作单元 4：ATE_FUN.1-4

评估者***应检查***测试计划，以确定 TOE 测试配置是否与在 ST 中列出的评估配置一致。

开发者测试计划中所提到的 TOE，其唯一参照号应与 CM 能力（ACM-CAP.*）子活动建立的唯一参照号相同。

ST 有可能指定不止一个评估配置，TOE 可能由多个不同的硬件和软件实现组成，应根据 ST 对它们进行测试。评估者要核实在开发者测试文档中所标识的测试配置是否与 ST 中描述的每个评估配置相一致。

评估者应考虑 ST 中描述的可适用于测试环境的关于 TOE 环境安全方面的假设。ST 中的某些假设可能不适用于测试环境。例如，关于用户许可方面的假设就可能不适用，但关于网络单点接入的假设就适用。

13.9.4.4.5 工作单元 4：ATE_FUN.1-5

评估者***应检查***测试计划，以确定它是否与测试流程描述一致。

在执行本工作单元时，评估者可能希望采用抽样的策略。

关于抽样的指南参见 A.2“抽样”，关于一致性分析的指南参见 A.3“一致性分析”。

13.9.4.4.6 工作单元 4：ATE_FUN.1-6

ISO/IEC 15408-3 ATE_FUN.1.3C 测试流程描述应标识要执行的测试和描述每个安全功能的测试情景。这些情景应包括对于其他测试结果的任何顺序依赖性。

评估者***应核查***测试流程描述是否标识了每一个待测安全功能行为。

用于标识待测安全功能行为的一种方法是引用设计规范中规定特定待测行为的相应部分。

在执行本工作单元时，评估者可能希望采用抽样的策略。

关于抽样的指南参见 A.2“抽样”。

13.9.4.4.7 工作单元 4：ATE_FUN.1-7

评估者***应检查***测试流程描述，以确定是否提供了足够的命令以建立可重复的测试初始条件，有时也包括顺序依赖关系。

为建立初始条件可能要采取一些步骤。例如，用户帐号应在其能被删除前添加。对于与其他测试结果有顺序依赖关系的一个例子是，在依靠审计功能对其他安全机制如访问控制产生审计记录之前，需要测试审计功能。另一个顺序依赖关系的例子是，某个测试用例所产生的数据文件被用作其他测试用例的输入。

在执行本工作单元时，评估者可能希望采用抽样的策略。

关于抽样的指南参见 A.2“抽样”。

13.9.4.4.8 工作单元 4：ATE_FUN.1-8

评估者***应检查***测试流程描述，以确定是否提供了足够的命令，以便拥有可重复的手段来激发安全功能和观察安全功能行为。

激励通常通过 TSFI 从外部提供给安全功能。一旦输入（激励）传给了 TSFI，安全功能行为就可以在 TSFI 观察到。除非测试流程包含足够的细节以明确无误地描述激励和期望作为该激励结果的行为，否则不能保证测试是可重复执行的。

在执行本工作单元时，评估者可能希望采用抽样的策略。

关于抽样的指南参见 A.2“抽样”。

13.9.4.4.9 工作单元 4：ATE_FUN.1-9

评估者***应检查***测试流程描述，以确定它们与实际测试流程是一致的。

如果两者一致，那么本工作单元就不适用，并认为已经满足要求。

在执行本工作单元时，评估者可能希望采用抽样的策略。

关于抽样的指南参见 A.2“抽样”,关于一致性分析的指南参见 A.3“一致性分析”。

13.9.4.4.10 工作单元 4:ATE_FUN.1-10

ISO/IEC 15408-3 ATE_FUN.1.4C 预期测试结果应指出测试成功执行后的预期输出。

评估者***应检查***测试文档,以确定其包括了足够的预期测试结果。

预期的测试结果用以确定测试是否成功执行。如果预期测试结果是明确无误的并且与给定测试方法的预期行为是一致的,那么该预期结果就足够了。

在执行本工作单元时,评估者可能希望采用抽样的策略。

关于抽样的指南参见 A.2“抽样”。

13.9.4.4.11 工作单元 4:ATE_FUN.1-11

ISO/IEC 15408-3 ATE_FUN.1.5C 开发者执行测试所得到的测试结果应证实每个被测试的安全性功能都按照规定执行。

评估者***应检查***测试文档中的预期测试结果,是否与给出的实际测试结果一致。

由开发者提供的实际测试结果和预期测试结果的比较将揭示出二者间的任何不一致。

只有当对某些数据进行约减或综合后,方可进行实际结果的直接比较。在这种情况下,开发者的测试文档应描述约减或综合真实数据的过程。

例如,开发者可能需要在网络连接建立后测试消息缓冲区以确定缓冲区中的内容。消息缓冲区将包含一个二进制数。这个二进制数应被转换为其他的数据表现形式以使测试更有意义。开发者应足够详细地描述从数据的二进制表示到更高级表示的转换,以便评估者能够实施转换过程(例如:同步或异步传输、停止位位数、奇偶校验位数等)。

应当注意,评估者使用约减或综合真实数据过程的描述,不是实际执行必要的修改,而是评定这一过程是否正确。开发者负责把预期测试结果转换为容易与实际测试结果相比较的格式。

在执行本工作单元时,评估者可能希望采用抽样的策略。

关于抽样的指南参见 A.2“抽样”。

如果任何测试的预期结果和实际结果不相同,那么表明安全功能没有正确执行。这种情况将会影响评估者的独立测试工作,包括隐含安全功能的测试。评估者要考虑增加本工作单元执行的证据样本。

13.9.4.4.12 工作单元 4:ATE_FUN.1-12

评估者***应报告***开发者测试工作,概述测试方法、配置、深度和结果。

对于在 ETR 中报告的开发者测试信息,可以允许评估者转述开发者测试 TOE 时的方法和成果。提供这种信息的目的是为了对开发者的测试工作给出一个有意义的概述,在 ETR 中关于开发者测试的信息不是为了精确再现特定的测试步骤或个别测试结果。其目的是要提供足够的细节,以便允许其他评估者和监督者了解开发者的测试方法、执行的测试数量、TOE 测试配置和开发者测试的总体结果。

一般可在 ETR 中找到关于开发者测试工作的信息有:

a) TOE 测试配置,被测 TOE 的特殊配置;

b) 测试方法,开发者全部测试策略的账目;

c) 开发者执行的测试数量,开发者测试覆盖和深度的描述;

d) 测试结果,开发者测试结果的整体描述。

以上列出的信息并不全面,只是为应呈现在 ETR 中的关于开发者所做测试的信息类型提供借鉴。

13.9.5 独立测试评估(ATE_IND.2)

13.9.5.1 目的

本子活动的目的是通过对 TSF 的一个子集进行独立测试,确定 TOE 是否按规定执行。同时,通过抽样执行开发者的测试,以获得对开发者测试结果的信任。

13.9.5.2 输入

本子活动的评估证据是:

a) ST;
b) 功能规范;
c) 用户指南;
d) 管理员指南;
e) 安全安装、生成和启动程序;
f) 测试文档;
g) 测试覆盖分析;
h) 测试深度分析;
i) 适于测试的 TOE。

13.9.5.3 行为 ATE_IND.2.1E

13.9.5.3.1 工作单元 4:ATE_IND.2-1

ISO/IEC 15408-3 ATE_IND.2.1C TOE 应适合测试。

评估者***应检查***TOE,以确定测试配置与所评估的 ST 中规定的配置是一致的。

用于评估者测试的 TOE,其唯一参照号应与 CM 能力(ACM-CAP.*)子活动建立的唯一参照号相同。

ST 有可能指定不止一个评估配置,TOE 可能由多个不同的硬件和软件实现组成,应根据 ST 对它们进行测试。评估者的 TOE 测试配置应与 ST 中所描述的每个评估配置相一致。

评估者应考虑 ST 中所描述的可用于测试环境的关于 TOE 环境安全方面的假设。ST 中可能有一些假设不适用于测试环境。例如,关于用户许可方面的假设可能就不适用,但关于网络单点接入的假设就适用。

如果使用了任何测试资源(例如仪表、分析仪),评估者有责任保证这些资源是校准正确的。

13.9.5.3.2 工作单元 4:ATE_IND.2-2

评估者***应检查***TOE,以确定它已被正确安装并处于一个已知状态。

评估者可能以多种方式来确定 TOE 的状态。例如,只要评估者仍然相信正在用于测试的 TOE 是正确安装的并且处于一个已知状态,先前的 ADO_IGS.1“安装、生成和启动程序”子活动的成功完成将满足本工作单元。如果情况不是这样,那么评估者只需根据提供的指南按照开发者的规程来安装、生成和启动 TOE。

如果由于 TOE 处于未知状态,评估者不得不执行安装过程,在成功完成后即可满足工作单元 ADO_IGS.1-2 的要求。

13.9.5.3.3 工作单元 4:ATE_IND.2-3

ISO/IEC 15408-3 ATE_IND.2.2C 开发者应提供一组相当的资源,该资源曾被用于开发者的 TSF 功

能测试。

评估者***应检查***开发者提供的资源集，以确认它们与开发者做 TSF 功能测试时使用的资源集等同。

资源集可能包括实验室和专用测试设备等。这里的资源与开发者所使用的资源不一定完全相同，但在对测试结果的影响方面上，两者应是等同的。

13.9.5.4 行为 ATE_IND.2.2E

13.9.5.4.1 工作单元 4：ATE_IND.2-4

评估者***应设计***一个测试子集。

评估者选择一个适合于 TOE 的测试子集和测试策略。一个极端的测试策略是让测试子集包含尽可能多的安全功能，但不是很严格地测试它们。另一个极端的测试策略是根据觉察到的相关性，让测试子集包含少数几个安全功能，并严格地测试这些安全功能。

评估者采用的测试方法一般会处于这两种极端情况之间。评估者应至少使用一项测试来试验 ST 中标明的大部分安全功能要求，但不必进行所有的规范测试。

评估者在选择被测 TSF 子集时应该考虑以下因素：

a) 开发者测试证据。开发者测试证据包括：测试覆盖分析、测试深度分析和测试文档。开发者测试证据将使评估者了解有关安全功能是如何被开发者测试的。当评估者在开发新的测试来对 TOE 进行独立性测试时会用到这一信息。评估者应特别考虑：
   1) 针对特定安全功能，增加开发者测试。评估者或许希望通过修改参数进行多个同类测试，以便更严格地测试安全功能；
   2) 针对特定安全功能，补充开发者测试策略。评估者或许希望通过使用另外一个测试策略测试某个特定的安全功能，以改变对该安全功能的测试方法。

b) 测试子集中包括的安全功能个数。如果 TOE 只包含少量安全功能，就要对所有安全功能进行严格测试。如果 TOE 包含很多安全功能，执行全班测试将是不合算的，此时可执行抽样测试。

c) 维持评估活动的平衡。评估者花费在测试活动上的工作应与花费在其他评估活动上的工作相称。

评估者选择安全功能组成测试子集。这种选择依赖于很多因素，对这些因素的考虑也可能影响测试子集大小的选择：

a) 开发者对安全功能测试的严格性。根据 ATE_COV.2“覆盖分析”的要求，在功能规范中所标识的所有安全功能应具有开发者测试证据。评估者决定需要补充测试的那些安全功能应包括在测试子集中。

b) 开发者测试结果。如果开发者的测试结果导致评估者对某个安全功能或某个方面产生怀疑，那么评估者应该将这些安全功能包括在测试子集中。

c) 与 TOE 的类型(例如，操作系统、防火墙)相关的已知公共域中的弱点。这些弱点将影响测试子集的选择过程。评估者应将涉及这些弱点的安全功能包含在子集中(这里的已知公共域中的弱点并不是指脆弱性，而是该类 TOE 所带有的不充分的情况或问题区)。如果不知道这样的弱点，那么采用选择更宽范围安全功能的这一通用方法可能更合适。

d) 安全功能的重要性。根据 TOE 的安全目的，那些较重要的安全功能应包含在测试子集中。

e) ST 中给出的 SOF 声明。所有有 SOF 声明的安全功能应包括在测试子集中。

f) 安全功能的复杂性。复杂的安全功能可能需要复杂的测试，这些测试对开发者或评估者施以更繁重的要求，这将不利用提高评估效率。相反，从更易找出错误的角度，复杂的安全功能又是子集的一个理想候选对象。因此，评估者需要在这些考虑因素之间寻求一种平衡。

g) 隐含的测试。某些安全功能的测试可能往往隐含着需要测试其他安全功能，把它们包括在子集中可以使被测安全功能数最大化(虽然是隐含的)。典型地，某些特定接口被用于提供多种安全功能特性，这是一种有效的测试方法。

h) TOE 的接口类型(例如，编程的、命令行的、协议的)。评估者应考虑在子集中包括 TOE 支持的所有不同接口类型的测试。

i) 创新的或不寻常的功能。当 TOE 包含有创新的或不寻常的安全功能时，这些功能在市场宣传中可能颇具分量，应该成为测试的重点候选对象。

这一部分指南清楚地说明了在选择合适的测试子集过程中应考虑的因素，但不代表已详述了所有因素。

关于抽样的指南参见 A.2“抽样”。

13.9.5.4.2 工作单元 4：ATE_IND.2-5

评估者***应***为测试子集生成足够详细的测试文档，以便测试情况是可再现的。

参照 ST 和功能规范，在对一个安全功能的预期行为有了一定了解后，评估者应确定测试该功能的最可行的方法。

评估者应特别考虑以下几点：

a) 将采用的方法，例如，是否在外部接口上测试安全功能，是否使用测试设备在内部接口上测试安全功能，或者使用其他测试方法(例如在异常情况下，代码检查)；

b) 用于激发安全功能并观察响应的安全功能接口；

c) 测试所需的初始条件(例如：任何需要具备的特殊客体或主体以及它们需要拥有的安全属性)；

d) 激发安全功能或观察安全功能所需的专用测试设备(例如，包发生器、网络分析仪)。

评估者可能发现，使用一系列测试用例测试每个安全功能是切实可行的，而每个测试用例将测试预期行为的某个特定的方面。

评估者的测试文档应指明每个测试的出处，如有必要，将其追溯到相关的设计规范和 ST。

13.9.5.4.3 工作单元 4：ATE_IND.2-6

评估者***应实施***测试。

评估者使用测试文档作为对 TOE 进行测试的基础。测试文档用作测试的基础，但是这并不排除评估者执行附加的特别测试。基于测试中发现的 TOE 行为，评估者可以设计新的测试，这些新的测试应记录在测试文档中。

13.9.5.4.4 工作单元 4：ATE_IND.2-7

评估者***应记录***包含在测试子集中的如下测试信息：

a) 待测试的安全功能行为的标识；

b) 测试设备的连接说明与设置说明；

c) 测试所需初始条件的说明；

d) 激发安全功能的说明；

e) 观察安全功能行为的说明；

f) 所有预期结果的描述，以及用以比较预期结果的必要分析；

g) 总结测试和为 TOE 建立必要的测试后状态的说明；

h) 实际测试结果。

测试文档中的细节描述应达到这样的程度：使其他评估者能重复测试并获得相同的结果，尽管测试结果的某些特定细节可能不同(例如，审计记录中的时间和日期字段)，但整体结果应该是相同的。

有些情况可以不必提供本工作单元中出现的全部信息(例如,在可以与预期结果做比较前,可能不需要对实际测试结果进行任何分析)。这些信息的省略由评估者决定,这样才合理。

13.9.5.4.5 工作单元 4:ATE_IND.2-8

评估者***应核查***所有的实际测试结果,是否与预期测试结果一致。

实际测试结果和预期测试结果间的任何差别可能表明 TOE 与其规定不一致,或者评估者的测试文档是错误的。出现意料之外的实际测试结果,可能需要对 TOE 或测试文档进行纠正维护,也许需要重新运行受到影响的测试,并且修改测试样本的数量和组成。该决定由评估者作出,这样才合理。

13.9.5.5 行为 ATE_IND.2.3E

13.9.5.5.1 工作单元 4:ATE_IND.2-9

评估者***应***使用在开发者测试计划和测试流程中抽取的测试样本***实施***测试。

本工作单元的总体目的是要实施足够数量的开发者测试,以确认开发者的测试结果的有效性。评估者必须确定样本量和构成样本的开发者测试。

考虑到整个测试活动的评估工作,通常应该完成 20%的开发者测试,当然这可以根据 TOE 的特性和所提交的测试证据而改变。

所有的开发者测试都能被追溯到特定的安全功能。因此,在选择构成样本的测试时,所需考虑的因素要相似于在工作单元 ATE_IND.2-4 中为子集选择列出的那些因素。此外,评估者可以使用一个随机抽样的方法来选择构成样本的开发者测试。

关于抽样的指南参见 A.2“抽样”。

13.9.5.5.2 工作单元 4:ATE_IND.2-10

评估者***应核查***所有的实际测试结果,是否与预期测试结果一致。

开发者的预期测试结果和实际测试结果之间的不一致将迫使评估者解决这个差异。评估者最初遇到的不一致性可由开发者提供的合理解释和不一致性解决办法予以解决。

如果没有一个满意的解释或解决办法,评估者可能会降低对开发者测试结果的信任,并且有必要增加试样量,以便重新获取对开发者测试的信任。如果增加试样量还不能满足评估者的要求,就有必要重复整个开发者测试集。最后,就充分测试在工作单元 ATE_IND.2-4 中所标识的 TSF 子集而言,开发者测试的不足将导致要么需要对开发者测试进行纠正,要么由评估者产生新的测试。

13.9.5.5.3 工作单元 4:ATE_IND.2-11

评估者***应***在 ETR 中***报告***评估者的测试成果、测试大纲、配置、深度和结果。

在 ETR 中报告的评估者测试信息允许评估者告知总体测试方法和在评估过程中测试活动所付出的效果。提供这种信息的目的是对测试工作给出一个有意义的概述,这并不是为了精确再现特定的测试说明或个别测试结果。其目的是要提供足够的细节,以便允许其他评估者和监督者了解评估者所选择的测试方法、执行的评估者测试数量、执行的开发者测试数量、TOE 测试配置和测试活动的总体结果。

一般可在 ETR 中找到关于评估者测试工作的信息有:

a) TOE 测试配置。被测 TOE 的特殊配置;

b) 所选子集的大小。在评估中要被测试的安全功能的数量和确定子集大小的理由;

c) 构成子集的安全功能选择标准。简要说明在选择组成子集的安全功能时考虑的因素;

d) 被测的安全功能。包含在子集中的安全功能的简表;

e) 所执行的开发者测试。所执行的开发者测试的数量和对用于选择测试标准的一个简要描述；

f) 活动的裁定。对测试结果的总体判断。

以上列出的信息并不全面，只是为应呈现在 ETR 中的关于评估期间评估者所做测试的信息类型提供借鉴。

13.10 脆弱性评定活动

脆弱性评定活动的目的是确定 TOE 在预期使用环境下的缺陷或弱点的存在性和可利用性。这种确定是基于开发者和评估者所进行的分析，并由评估者的测试予以支持。

13.10.1 误用评估(AVA_MSU.2)

13.10.1.1 目的

本子活动的目的是确定指南是否是令人误解的、不合理的或是自相矛盾的，是否已经提出了关于所有操作方式的安全流程，以及指南的使用是否便于防止和检测到不安全的 TOE 状态。

13.10.1.2 输入

本子活动的评估证据是：

a) ST；

b) 功能规范；

c) 高层设计；

d) 低层设计；

e) 实现表示的子集；

f) TOE 安全策略模型；

g) 用户指南；

h) 管理员指南；

i) 安全安装，生成与启动程序；

g) 指南的误用分析；

k) 测试文档；

l) 适于测试的 TOE。

13.10.1.3 应用注释

术语“指南”在本子活动中指用户指南、管理员指南和安全安装、生成和启动程序。安装、生成和启动程序指管理员负责执行的使 TOE 从交付状态进入运行状态的全部流程。

本组件包括了未在 AVA_MSU.1“指南检查”中呈现的关于开发者分析的要求。开发者分析的确认不应用来代替评估者对指南文档的检查，而应用来提供开发者已明确地表述了误用问题的证据。

13.10.1.4 行为 AVA_MSU.2.1E

13.10.1.4.1 工作单元 4：AVA_MSU.2-1

ISO/IEC 15408-3 AVA_MSU.2.1C 指导性文档应标识所有可能的 TOE 操作模式(包括失败或操作失误后的操作)、它们的后果以及对于保持安全运行的意义。

评估者***应检查***指南和其他评估证据，以确定指南标识了所有可能的 TOE 操作模式(例如：失败或操作失误后的操作)、它们的后果以及对于保持安全运行的意义。

其他评估证据，特别是功能规范和测试文档，为评估者提供了信息源。评估使用这些信息确认指南

是否包含了足够的指导信息。

评估者应每次只关注单个安全功能，并将其他评估证据与指南中有关安全地使用安全功能的部分相比较，从而确定指南中有关安全功能的部分足以保证安全功能的安全使用(即与 TSP 一致)。评估者也应考虑安全功能之间的关系，并寻找潜在的冲突。

13.10.1.4.2 工作单元 4:AVA_MSU.2-2

ISO/IEC 15408-3 AVA_MSU.2.2C 指导性文档应是完备的、清晰的、一致的、合理的。

评估者***应检查***指南，以确定它是清晰的和内在一致的。

如果指南可能能被管理员或用户曲解，并且以有害于 TOE 或 TOE 安全的方式使用，那么这个指南就是不清晰的。

关于一致性的指南参见 A.3“一致性分析”。

13.10.1.4.3 工作单元 4:AVA_MSU.2-3

评估者***应检查***指南和其他评估证据，以确认指南是完备的和合理的。

评估者应利用从其他评估活动中所获得的对 TOE 的熟悉程度来确认指南是完备的。

评估者特别要考虑功能规范和 TOE 概要规范。所有这些文档中描述的安全功能应在指南中加以描述，以便安全地管理和使用。评估者也可以在指南和这些文件之间找出非形式化的映射关系。在这个映射关系中任何省略都意味着不全面。

如果指南对 TOE 的使用或运行环境要求与 ST 不一致，或者维持安全的负担过于繁重，那么这个指南就是不合理的。

评估者应注意到，执行 AGD_ADM 子活动的工作单元所得到的结果将对此检查提供有用的输入。

13.10.1.4.4 工作单元 4:AVA_MSU.2-4

ISO/IEC 15408-3 AVA_MSU.2.3C 指导性文档应列出关于预期使用环境的所有假设。

评估者***应检查***指南，以确定其列出了关于预期使用环境的所有假设。

评估者分析 ST 中预期 TOE 安全环境的假设，并且与指南相比较，以确保在指南中适当地描述了所有与管理员和用户有关的 ST 预期 TOE 安全环境的假设。

13.10.1.4.5 工作单元 4:AVA_MSU.2-5

ISO/IEC 15408-3 AVA_MSU.2.4C 指导性文档应列出对外部安全措施(包括外部程序的、物理的或人员的控制)的所有要求。

评估者***应检查***指南，以确定其列出了所有外部安全措施要求。

评估者分析指南，以确保其列出了所有的外部程序的、物理的、人员的和连接控制。ST 中非 IT 环境的安全目的将指出什么是必需的。

13.10.1.4.6 工作单元 4:AVA_MSU.2-6

ISO/IEC 15408-3 AVA_MSU.2.5C 分析文档应证实指导性文档是完备的。

评估者***应检查***开发者的分析，以确定开发者已采取足够的措施确保指南是完备的。

开发者的分析可以由从 ST 或功能规范到指南的映射组成，以证明指南是完备的。开发者无论提供什么证据来表明指南是完备的，评估者都应评定开发者的分析，这种分析要对照在执行工作单元 AVA_MSU.2-1 至 AVA_MSU.2-5，AVA_MSU.2-7 时发现的缺陷来进行。

13.10.1.5 行为 AVA_MSU.2.2E

13.10.1.5.1 工作单元 4:AVA_MSU.2-7

评估者***应执行***所有管理员和用户(可用的话)流程,这些流程对于 TOE 的配置和安装是必要的,从而确定只要利用所提供的指南就能配置并安全地使用 TOE。

配置和安装要求评估者将 TOE 从一个可交付状态,推进到 TOE 运行的状态,并促使 TSP 与 ST 中规定的安全目的一致。

评估者应仅遵循正式提交给 TOE 使用者的用户和管理员指南中给出的开发者制定的流程。在操作中遇到任何困难都说明指南是不完备的、不清晰的、不一致的或者不合理的。

注意,满足本工作单元的工作,同时也满足评估者行为 ADO_IGS.1-2E 的要求。

13.10.1.5.2 工作单元 4:AVA_MSU.2-8

评估者***应执行***指南中规定的其他安全相关流程,以确定只需使用所提供的指南就能够安全地配置和使用 TOE。

评估者应仅遵循正式提交给 TOE 使用者的用户和管理员指南中给出的开发者制定的流程。

评估者应采用抽样的办法实施本工作单元。当选择样本时,评估者应考虑:

a) 指南的清晰程度:指南中任何潜在不清晰的部分应包含在样本中;

b) 最常使用的指南部分:指南中不常使用的部分通常不应包含在样本中;

c) 指南的复杂性:指南中的复杂部分应包含在样本中;

d) 错误的严重程度:那些因错误可严重损害安全的程序应包含在样本中;

e) TOE 特性:指南中有关 TOE 正式或最可能使用的部分应包含在样本中。

关于抽样方法的指南,参照 A.2“抽样”。

13.10.1.6 行为 AVA_MSU.2.3E

13.10.1.6.1 工作单元 4:AVA_MSU.2-9

评估者***应检查***指南,以确定其给用户提供了足够的指导信息,使得他们能有效地管理和使用 TOE 的安全功能,并能检测不安全的状态。

TOE 可能使用多种方法来帮助用户安全地使用 TOE。在 TOE 处于不安全的状态时,TOE 可以使用某种功能(特性)来警告用户。同时 TOE 可以在带有增强型指南的情况下被交付,其中增强型指南包括建议、提示、流程等内容,以更有效使用现有安全特性。例如,关于使用审计特性的指南就有助于检测不安全的状态。

为作出对本工作单元的裁定,评估者考虑 TOE 的功能性、目的、预期使用环境,以及关于使用方法或用户的假设。如果 TOE 可能会转变到不安全状态,但使用指南可以一种及时的方式检测到不安全状态,对此情况,评估者应给出结论。可使用诸如 ST、TSF 的功能规范和高层设计这样的评估交付件来确定 TOE 转换到不安全状态的可能性。

13.10.1.7 行为 AVA_MSU.2.4E

13.10.1.7.1 工作单元 4:AVA_MSU.2-10

评估者***应检查***开发者对指南的分析,以确定为 TOE 所有操作模式中的安全操作提供了指南。

评估活动 AVA_MSU.2.1E 的结果应为评估开发者的分析提供基础。当完成指南的潜在误用评估后,评估者应能够确定开发者所进行的误用分析是否满足本子活动的目的。

13.10.2 TOE 安全功能强度评估(AVA_SOF.1)

13.10.2.1 目的

本子活动的目的是确定,在 ST 中是否为所有概率或置换机制作出了 SOF 声明,以及开发者在 ST 中所作的 SOF 声明是否都是有正确的分析予以支持。

13.10.2.2 输入

本子活动的评估证据是:

a) ST;
b) 功能规范;
c) 高层设计;
d) 低层设计;
e) 实现表示的子集;
f) 用户指南;
g) 管理员指南;
h) TOE 安全功能强度分析。

13.10.2.3 应用注释

对 SOF 进行的分析在本质上是针对概率或置换的机制(例如:口令机制或生物识别)而实施的。尽管密码机制在本质上也是概率性的并且经常用“强度”来描述,但是 AVA_SOF.1“TOE 安全功能强度评估”却不适用于密码机制。对这种情况,评估者应遵循评估体制的规定来执行。

尽管 SOF 分析是在单个机制的基础上进行的,但是对 SOF 的总体判断却是基于功能的。当采用多个概率或置换机制来实现一个安全功能时,应分析每个不同的机制。提供安全功能的这些机制的组合方式将决定这个功能的总体 SOF 级别。评估者需要设计信息以理解这些机制如何协同工作才能实现一个功能,并且依据 ADV_HLD.1“描述性高层设计”给出这些信息的最小级别。评估者可获得由 EAL 确定的实际的设计信息,并且在必要时这些信息应能被用于支持评估者的分析。

对于涉及多个 TOE 域的 SOF 的讨论参见 ASE_REQ.1“IT 安全要求评估”。

13.10.2.4 行为 AVA_SOF.1.1E

13.10.2.4.1 工作单元 4:AVA_SOF.1-1

ISO/IEC 15408-3 AVA_SOF.1.1C 对于每个具有 TOE 安全功能强度声明的安全机制,TOE 安全功能强度分析应说明该机制达到或超过 PP/ST 中定义的最低强度级别。

评估者***应核查***开发者是否已为每个具有 SOF 声明的安全机制提供了 SOF 分析,该声明在 ST 中是以 SOF 级别的方式予以表示的。

如果仅以 SOF 度量标准的方式来声明 SOF,那么本工作单元是不适用的,视为已满足要求。

SOF 级别分为基本级功能强度、中级功能强度或高级功能强度,这些级别是根据攻击潜力来定义的,参见 ISO/IEC 15408-1 第 2 章。表示成一个级别的最小整体 SOF 要求适用于所有非密码的概率或置换安全机制。但个别机制可能具有一个被表示成超出整体 SOF 要求级别的 SOF 声明。

确定实现一个攻击所必需的攻击潜力,从而确定出 SOF 级别的指南参见 A.8“功能强度和脆弱性分析”。

SOF 分析中要包含基本原理以证明 ST 中所作的 SOF 声明。

13.10.2.4.2 工作单元 4:AVA_SOF.1-2

ISO/IEC 15408-3 AVA_SOF.1.2C 对于每个具有特定 TOE 安全功能强度声明的安全机制,TOE 安全功能强度分析应说明该机制达到或超过 PP/ST 中定义的特定功能强度度量标准。

评估者***应核查***开发者是否已为每个具有 SOF 声明的安全机制提供了 SOF 分析,该声明在 ST 中是以度量标准的方式予以表示的。

如果仅以 SOF 级别的方式来声明 SOF,那么本工作单元是不适用的,视为已满足要求。

表示成一个级别的最小整体 SOF 要求适用于所有非密码的概率或置换机制。但个别机制可能具有一个被表示成满足或超出整体 SOF 要求度量的 SOF 声明。

SOF 分析中要包含基本原理以证明 ST 中所作的 SOF 声明。

13.10.2.4.3 工作单元 4:AVA_SOF.1-3

评估者***应核查***SOF 分析,以确定支持分析的任何主张或假设都是有效的。

例如,认为伪随机数发生器的特定实现将拥有必要的熵,该熵是产生与 SOF 分析相关的安全机制所必需的,那么该假设就是有缺陷的。

支持 SOF 分析的假设应该反映“最差情形”,除非“最差情形”被 ST 确定是无效的。当许多不同的情形存在时,并且这些情形都是依赖于人类用户或攻击者行为时,代表最低强度的情形应被假设,除非如以上所述该情况无效。

例如,基于最大理论口令空间(例如,所有可打印的 ASCII 码)的强度声明,就不是“最差情形”,因为人类习惯于使用自然语言口令,但这样的行为却大大地减少了口令空间和相关强度。然而,如果在 ST 中列出了 TOE 使用的 IT 措施,例如用口令过滤器将自然语言口令的使用降至最少,那么这样的假设就是适当的。

13.10.2.4.4 工作单元 4:AVA_SOF.1-4

评估者***应检查***SOF 分析,以确定用以支持分析的任何算法、原理、性质和计算都是正确的。

本工作单元高度依赖于所考虑的机制类型。A.8“功能强度和脆弱性分析”提供了一个使用口令机制实现标识和鉴别功能的 SOF 分析实例;该分析考虑用最大口令空间以最终达到一个 SOF 级别。对于生物测量学,该分析应考虑解决方法和其他影响机制的欺骗敏感性的因素。

SOF 表示成一个级别,该级别是基于可击败安全机制所必需的最小攻击潜力。SOF 级别是在 ISO/IEC 15408-1 第 2 章中以攻击潜力进行定义的。

关于攻击潜力的指南参见 A.8“功能强度和脆弱性分析”。

13.10.2.4.5 工作单元 4:AVA_SOF.1-5

评估者***应检查***SOF 分析,以确定每个 SOF 声明被满足或超过。

关于 SOF 声明级别的指南参见 A.8“功能强度和脆弱性分析”。

13.10.2.4.6 工作单元 4:AVA_SOF.1-6

评估者***应检查***SOF 分析,以确定所有带有 SOF 声明的功能都达到了 ST 中所定义的最低强度级别。

13.10.2.5 行为 AVA_SOF.1.2E

13.10.2.5.1 工作单元 4:AVA_SOF.1-7

评估者***应检查***功能规范、高层设计、低层设计、用户指南和管理员指南,以确定所有的概率或置换

机制都具有相应的 SOF 声明。

通过概率或置换机制实现的安全功能应由开发者予以标识,该标识应在 ST 评估活动期间予以验证。但是,由于 TOE 概要规范可能是执行此项活动的唯一有效证据,因此这种机制的识别可能是不完备的。作为本子活动输入的附加评估证据,可能识别出未在 ST 中列出的额外的概率或置换机制。如果是这样的话,那么应适当地更新 ST 以反映附加的 SOF 声明,而且开发者需提供额外的分析以证明该声明合理的,其可以作为评估者行为 AVA_SOF.1.1E 的输入。

13.10.2.5.2 工作单元 4:AVA_SOF.1-8

评估者**应检查**SOF 声明,以确定它们是正确的。

当 SOF 分析包括断言或假设时(例如,每分钟可能有多少次鉴别尝试),评估者应独立地确认它们是正确的。这可通过测试或独立的分析来完成。

13.10.3 脆弱性分析评估(AVA_VLA.2)

13.10.3.1 目的

本子活动的目的是确定在其预期使用环境中的 TOE 是否有可被具备低攻击潜力的攻击者利用的脆弱性。

13.10.3.2 输入

本子活动的评估证据是:

a) ST;
b) 功能规范;
c) 高层设计;
d) 低层设计;
e) 实现表示的子集;
f) TOE 安全策略模型;
g) 用户指南;
h) 管理员指南;
i) 安全安装、生成和启动程序;
j) 脆弱性分析;
k) 功能强度声明分析;
l) 适于测试的 TOE。

本子活动的其他输入有:

a) 关于明显脆弱性的当前信息(例如:来自监督者)。

13.10.3.3 应用注释

术语“指南”在本子活动中指用户指南、管理员指南和安全安装、生成和启动程序。

对可利用脆弱性的考虑是由 ST 中安全目的和功能要求确定的。例如,如果 ST 中不要求描述防止安全功能被旁路的措施(不选 FPT_PHP“TSF 物理保护”、FPT_RVM“参照仲裁”和 FPT_SEP“域分离”),那么基于旁路的脆弱性就无需考虑。

脆弱性可能存在于公共域中,也可能不在,并且利用它可能需要技巧,也可能不要。这两方面是相关的,但是有区别的。不应仅仅因为脆弱性存在于公共域中而认为其容易被利用。

指南中的以下术语具有特定含义:

a) 脆弱性:在一定条件下能被利用来违反安全策略的 TOE 的弱点;
b) 脆弱性分析:系统地搜寻 TOE 中的脆弱性并且对所寻找到的脆弱性进行评判,以确定它们与 TOE 预期使用环境的关系;
c) 明显脆弱性:只要求对 TOE 有最低程度的了解、最小的技术复杂性和最少的资源就可公开利用的脆弱性;
d) 潜在脆弱性:怀疑在 TOE 中存在(根据假定的攻击途径)但并未被证实的脆弱性;
e) 可利用的脆弱性:在 TOE 预期使用环境下可被利用的脆弱性;
f) 不可利用的脆弱性:在 TOE 预期使用环境下不能被利用的脆弱性;
g) 残余脆弱性:一种几乎无法利用的脆弱性,但是在 TOE 预期使用环境下却能够被那些在预计之外的具备更大攻击潜力的攻击者所利用;
h) 穿透性测试:在 TOE 的预期使用环境下进行的测试,以确定已标识的 TOE 潜在脆弱性的可利用程度。

13.10.3.4 行为 AVA_VLA.2.1E

13.10.3.4.1 工作单元 4:AVA_VLA.2-1

ISO/IEC 15408-3 AVA_VLA.2.1C 脆弱性分析文档应描述对 TOE 交付件的分析,以寻找用户能够违反 TSP 的途径。

ISO/IEC 15408-3 AVA_VLA.2.2C 脆弱性分析文档应描述如何处理已标识的脆弱性。

ISO/IEC 15408-3 AVA_VLA.2.3C 脆弱性分析文档应针对所有已标识的脆弱性,说明该脆弱性不能在 TOE 的预期使用环境中被利用。

ISO/IEC 15408-3 AVA_VLA.2.4C 脆弱性分析文档应证明带有已标识脆弱性的 TOE 可以抵御明显的穿透性攻击。

评估者***应检查***开发者的脆弱性分析,以确定对脆弱性的搜索已经考虑了所有相关的信息。

开发者的脆弱性分析应涵盖开发者在所有评估交付件和公共域信息源中搜索到的脆弱性。

公共域中的信息是高度动态的。因此,在开发者执行脆弱性分析和评估完成之间的这一段时间内可能在公共域中有新的脆弱性报告。具体在那一个点停止对公共域信息的监测是评估授权机构的问题,因此相应的指南和协议应从评估授权机构得到。

13.10.3.4.2 工作单元 4:AVA_VLA.2-2

评估者***应检查***开发者的脆弱性分析,以确定每个已标识的脆弱性都已被描述,并就它在 TOE 的预期使用环境中为什么是不可利用的给出合理的解释。

如果存在下列条件中的一个或多个,那么脆弱性就是不可利用的:

a) (IT 或非 IT)环境中的安全功能或措施防止了在预期使用环境中脆弱性的利用。例如,限定只有授权用户可对 TOE 进行物理访问,可以有效地致使一个 TOE 脆弱性成为不可利用的脆弱性。
b) 脆弱性只能被拥有中级或高级攻击潜力的攻击者利用。例如,对于分布式 TOE 的会话劫持攻击的脆弱性来说,就需要一个高于低攻击潜力的攻击者才能利用该脆弱性。然而,这样的脆弱性在 ETR 中被报告为残余脆弱性。
c) 在 ST 中既没有声明要抵抗的威胁,也没有声明要满足的组织安全策略。例如,一个防火墙,其 ST 中没有作有效性策略声明并易受到 TCP SYN 攻击(一种基于通用 Internet 协议的攻击,使得主机无法为连接请求提供服务),不应仅基于这种脆弱性认为该评估活动失败。

关于确定利用某个脆弱性所应具备的攻击潜力的指南,请参见 A.8“功能强度和脆弱性分析”。

13.10.3.4.3 工作单元 4:AVA_VLA.2-3

评估者*应检查*开发者的脆弱性分析,以确定其与 ST 和指南都是一致的。

开发者的脆弱性分析可通过建议对 TOE 功能进行特殊配置或设置来处理一个脆弱性。如果认为这样的操作限制是有效的并与 ST 是一致的,那么所有这样的配置/设置都应该在指南中得到充分描述,这样才可能被用户使用。

13.10.3.5 行动 AVA_VLA.2.2E

13.10.3.5.1 工作单元 4:AVA_VLA.2-4

评估者*应*基于开发者的脆弱性分析*设计*穿透性测试。

评估者准备穿透性测试:

a) 当需尝试驳斥开发者的分析,质疑开发者关于脆弱性为什么不可利用的解释时;

b) 当需确定 TOE 在其预期使用环境中对未被开发者考虑到的脆弱性的敏感程度时。评估者应有权使用关于公共域中开发者尚未考虑到的脆弱性的最新信息(例如,来自监督者的信息),也可拥有一些作为执行其他评估活动的结果而识别出的潜在脆弱性。

不能期望评估者对具备低攻击潜力的攻击者无法利用的脆弱性进行测试(包括那些在公共域中的)。然而,许多情况下,在确定攻击所需潜力之前,应先进行测试。如果作为评估专家意见,评估者发现一个脆弱性超出了低攻击潜力,则这样的脆弱性在 ETR 报告中被报告为残余脆弱性。

在理解可疑脆弱性的基础上,评估者决定出最合理的方法测试 TOE 是否存在这样的脆弱性。评估者应特别考虑:

a) 用于激发 TSF 和观察反应的安全功能接口;

b) 测试所需的初始条件(例如:任何需要存在的特殊客体或主体及它们需要拥有的安全属性);

c) 激发安全功能或观察安全功能所需的专用测试设备。

评估者可能会将发现采用一系列测试用例来进行穿透性测试是可行的,其中每个测试用例将测试一个特定的脆弱性。

13.10.3.5.2 工作单元 4:AVA_VLA.2-5

评估者*应*基于开发者的脆弱性分析*编制*穿透性测试文档,并且应足够详尽使得测试可重复。测试文档应包括:

a) 标识被测 TOE 的脆弱性;

b) 进行穿透性测试所需的所有测试设备连接和设置的说明;

c) 建立所有穿透性测试的必备条件的说明;

d) 激发 TSF 的说明;

e) 观察 TSF 行为的说明;

f) 所有预期结果的描述,并对用于比较预期结果的观察行为进行必要的分析;

g) 总结测试和为 TOE 建立必要的测试后状态的说明。

测试文档中的细节描述应达到这种程度:其他的评估者能再现测试并获得相同的结果。

13.10.3.5.3 工作单元 4:AVA_VLA.2-6

评估者*应*基于开发者的脆弱性分析*实施*穿透性测试。

评估者使用工作单元 4:AVA_VLA.2-4 产生的穿透性测试文档作为对 TOE 进行穿透性测试的基础,但这并不排除评估者执行其他特别的穿透性测试。如果有必要的话,评估者可根据在穿透性测试期

间(如果由评估者执行)所获得的信息设计特别的测试,这些测试应记录在穿透性测试文档中。这些测试有必要深入研究意外的结果或观察结果,或在预先测试计划阶段评估者所要研究的潜在脆弱性。

13.10.3.5.4 工作单元 4:AVA_VLA.2-7

评估者***应记录***穿透性测试的实际结果。

尽管实际测试结果的某些特定细节可能与预期的不同(例如:审计记录中的时间和日期字段),但整体结果应该是相同的。任何差异都应被证明是合理的。

13.10.3.5.5 工作单元 4:AVA_VLA.2-8

评估者***应***在 ETR 中***报告***穿透性测试工作、测试方法大纲、配置、深度和结果。

在 ETR 中报告的穿透性测试信息允许评估者描述全部穿透性测试方法和本子活动所做的工作。提供该信息的目的是对评估者的穿透性测试工作给出一个有意义的概述。这不意味着 ETR 中关于穿透性测试的信息完全复制于单个穿透性测试的具体测试步骤或测试结果。其目的是提供足够的细节,以便其他评估者和监督者了解所选择的穿透性测试方法、执行穿透性测试的数量、TOE 测试配置和穿透性测试活动的总体结果。

在 ETR 中,在有关评估者穿透性测试工作的章节中通常应包括以下信息:

a) TOE 测试配置。进行穿透性测试的 TOE 的特殊配置;

b) 进行穿透性测试的安全功能。穿透性测试所关注的安全功能简单列表;

c) 子活动的裁定。穿透性测试结果的总体判断。

以上列出的并不全面,只是为应在 ETR 中出现的,在评估期间评估者所做穿透性测试的信息的类型提供一些借鉴。

13.10.3.6 行为 AVA-VLA.2.3E

13.10.3.6.1 工作单元 4:AVA_VLA.2-9

评估者***应检查***本子活动的所有输入,以确定开发者的脆弱性分析未提及一些可能的安全脆弱性。

应当使用缺陷假设方法借以分析 TOE 的规范和文档,于是 TOE 中的脆弱性都成为了假设或推测。假设的脆弱性列表基于以下几个方面进行优先级排序:估计脆弱性存在的可能性;假设脆弱性存在时,利用该脆弱性所需的攻击潜能;该脆弱性的可控范围或危害程度。潜在脆弱性的优先级列表通常用于指导对 TOE 的穿透性测试。

关于确定利用某个脆弱性所应具备的攻击潜力的指南,参见 A.8“功能强度和脆弱性分析”。

假设只能由拥有中级或高级攻击潜力的攻击者利用的脆弱性,不会导致本评估者行为失败。这里所做的分析用以支持该假设,不必将其作为穿透性测试的输入而进一步加以考虑。但是,这些脆弱性应在 ETR 中报告为残余脆弱性。

假设可被具有低攻击潜力的攻击者利用的脆弱性,不会违背 ST 中规定的安全目的,也不会导致本评估者行为失败。这里所做的分析用以支持该假设,不必将其作为穿透性测试的输入而进一步加以考虑。

假设可被具有低攻击潜力的攻击者潜在利用,并导致违反安全目的的脆弱性,这些脆弱性组成具有最高优先级的潜在脆弱性列表,该列表用于指导对 TOE 进行的穿透性测试。

依据在预期使用环境中面临的威胁,评估者的独立脆弱性分析应考虑以下几种一般脆弱性:

a) 与被评估 TOE 的类型相关的一般脆弱性(可能由监督者提供);

b) 旁路;

c) 篡改;

d) 直接攻击；

e) 误用。

下文给出 b)～d)项的详细解释。

13.10.3.6.1.1 旁路

旁路包括攻击者能够避开安全强制措施所采取的以下任何手段：

a) 对 TOE 接口的利用，或者对能与 TOE 交互的实用程序的利用；

b) 对特权或其他能力的继承，否则应被拒绝；

c) (如果涉及保密性的话)对存储或复制到未被充分保护区域的敏感数据的读取。

在评估者独立脆弱性分析中，应考虑以下方面(如相关的话)：

a) 基于利用接口或实用程序的攻击，通常可以借助接口缺乏必要的安全强制措施来达到目的。例如，在较低级别而不是在加强的访问控制措施上获取对功能的访问。包括以下几方面：

   1) 改变功能调用的预定义序列；

   2) 执行附加的功能；

   3) 在意想不到的情况或目的下使用部件；

   4) 对较抽象的陈述中引入的实现细节的利用；

   5) 访问核查和使用之间的时间延时的利用。

b) 应该考虑改变部件调用的预定义序列，其中存在一个预期顺序：调用 TOE 的接口(例如：用户命令)是为了执行某些安全功能(例如，为访问打开文件，并从中读取数据)。如果一个安全功能是在一个 TOE 接口被调用的(例如访问控制核查)，评估者应该考虑是否可以通过调用序列中稍后的某一点或不执行该调用的方式旁路安全功能。

c) 类似于前面描述的攻击形式，执行附加部件(在预定义序列中)，但是牵涉到在序列中某些点上对其他 TOE 接口的调用。这种攻击涉及到通过使用网络通信分析工具对网络上传输的敏感数据进行侦听截获(这里的附加部件是指网络通信分析工具)。

d) 在意想不到的情况或目的下使用部件，包括使用一个 TOE 接口绕过安全功能，通过使用这个接口以达到设计或预期之外的目的。隐蔽信道就是这类攻击的例子。使用未在文档中描述的接口(这可能是不安全的)的也属于此类攻击(包括未在文档中描述的支持或帮助工具)。

e) 再次利用在较低级别表示中引入的实施细节，包括隐蔽信道的使用，攻击者利用隐蔽信道向 TOE 中引入附加功能、资源或属性(例如：使一个锁变量作为隐蔽信道)。附加功能可能还包括软件模块中的测试代码。

f) 核查和使用之间的延时的利用，包括以下情形：如果实施访问控制核查并且该访问是被允许的，同时攻击者随后可利用访问核查的时间来创造条件导致核查失败。例如，用户创建一个后台进程来读取和发送高敏感性的数据到用户终端，随后退出登录并回到较低敏感级别的登录状态。如果该后台进程在用户退出登录时没有被终止，那么 MAC 核查将被旁路。

g) 基于权限继承的攻击一般是基于对某些特权部件的特权或能力的非法获得，通常是以非受控或非预期的方式从某些特权的部件中退出时获得的。相关项目包括：

   1) 执行不期望运行的数据，或使之可执行；

   2) 使部件产生意外的输入；

   3) 使低级别部件所依赖的假设和属性失效。

h) 执行不期望运行的数据或使之可运行，包括与病毒有关的攻击(例如：当文件被编辑或访问时，在该文件中植入可以自动运行的代码或命令，从而继承该文件所有者的全部特权)。

i) 使部件产生意外的输入，能够造成被攻击者利用的结果。例如，如果 TOE 是一个实现安全功能的应用程序，如果用户获得了对底层操作系统的访问权限，那么就有可能通过探测登录顺序

得到不同控制权限,或者通过鉴别口令时的换码顺序获得访问权限,那么 TOE 的安全功能就会被旁路。

j) 使低级别部件所依赖的假设和属性失效,包括基于摆脱应用程序的约束,以得到底层操作系统访问权限的攻击,其目的是旁路由应用程序实现的安全功能。在这种情况下,失效的假设是指应用程序用户不可能得到该访问权限。如果安全功能是由底层数据库管理系统上的应用程序实现的,那么可以设想的类似攻击:如果攻击者能够摆脱应用程序的约束,那么安全功能就能再次被旁路。

k) 基于读取存储在未被充分保护区域中(当涉及机密性时)的敏感数据的攻击,作为获得敏感数据访问权限的可能的方式,应考虑以下几方面的问题:

1) 磁盘清理;

2) 访问未受保护的内存;

3) 利用对共享可写文件或其他共享资源(例如,交换文件)的访问。

l) 启动错误恢复以确定用户能够获得哪些访问权限。例如,当系统崩溃后,自动文件恢复系统可为磁盘上没有标签的无头文件启用一个丢失和找到目录。如果 TOE 实现了强制访问控制,则审查该目录处于什么安全级别(例如,处于系统级)并且谁有访问权就显得重要了。

13.10.3.6.1.2 篡改

篡改包括基于攻击者试图影响安全功能或机制的行为(例如:破坏或使失效)的任何攻击,例如通过:

a) 访问某些数据,而安全功能或机制依赖这些数据的机密性或完整性;

b) 迫使 TOE 处理异常或意外情况;

c) 禁止或延迟安全实施。

在评估者的独立脆弱性分析中,应考虑下列的每一种情况:

a) 某些攻击基于对某些数据的访问,而安全功能或机制依赖这些数据的机密性或完整性。这样的攻击包括:

1) 直接或间接地读、写或修改内部数据;

2) 在意想不到的情况或目的下使用某个部件;

3) 利用在更高抽象层中不可见的部件之间的干扰。

b) 对于直接或间接地读、写或修改内部数据的攻击类型应考虑下列情况:

1) 读取内部存储的秘密信息,例如用户口令;

2) 骗取安全执行机制所依赖的内部数据;

3) 修改环境变量(例如,逻辑名称),或者修改配置文件或临时文件中的数据。

c) 可能欺骗一个可信进程以修改某个受保护的文件,而该文件通常是不可访问的。

d) 评估者也应考虑下列“危险要素”:

1) 源代码连同编译器驻留在 TOE 中(比如,可能修改登录源代码);

2) 一个交互式的调试和补丁工具(比如,可能修改可执行映像);

3) 改变设备控制器级别的可能性,在这里不存在文件保护;

4) 源代码中的诊断用代码,它可以选择性地包括在源代码内;

5) 开发者的工具遗留在 TOE 中。

e) 在意想不到的情况或目的下使用某个部件,包括(例如)当 TOE 是构建在某操作系统上的一个应用,用户利用某个文字处理工具或其他编辑器的知识,修改自己的命令文件(例如试图获得更高的权限)。

f) 利用在更高抽象层中不可见的部件之间的干扰,包括利用对资源的共享访问进行攻击,在这种

情况下,通过一个部件修改某个资源可能影响到其他(可信)部件的行为。例如,在源代码级,可以通过使用全局数据或间接机制如共享内存或信号机。

g) 总是应考虑迫使 TOE 处理异常或意外情况的攻击。相关的事项包括:
   1) 为某个部件产生意外的输入;
   2) 使得较低级别部件所依赖的假设和属性失效。

h) 某个部件产生意外的输入,当下列情况发生时检查 TOE 的行为:
   1) 命令输入中的缓冲区溢出(攻击者可以利用"堆栈崩溃"来覆盖其他存储空间,或者强制崩溃置转储如明文口令之类包含的敏感信息);
   2) 输入无效的命令或参数(包括向接口提供一个只读参数,期望通过该参数返回数据);
   3) 在某个审计迹中插入文件结束标记(例如 CTRL/Z 或 CTRL/D)或空字符。

i) 使较低级别部件所依赖的假设和属性失效的攻击,这类攻击包括利用源代码中的错误,假定这些代码中(明确地或隐含地)与安全有关的数据具有特定的格式或特定的数值范围。在这种情况下,评估者应确定攻击者是否通过修改数据格式或数值范围就能够使得这部分源代码失效,并且如果他能够这样做的话,攻击者是否可从中受益。

j) 安全功能的正确行为可能依赖这样的假设:在诸如资源达到极限 或者参数达到最大数值等极端情况下将失效。评估者应考虑(如果可行)TOE 在这些极端情况下的行为。例如:
   1) 改变日期(例如当超过一个关键日期阈值时,检查 TOE 的行为);
   2) 磁盘的存储空间满时;
   3) 超过最大用户数;
   4) 审计日志的存储空间满时;
   5) 控制台的安全警告队列饱和时;
   6) 过于依赖通信部件的多用户 TOE 的各个部分过载;
   7) 使用流量淹没网络或单个主机;
   8) 缓冲区或字段的存储空间满时。

k) 基于禁止或延迟安全实施的攻击包括以下方面:
   1) 使用中断或调度功能来扰乱先后顺序;
   2) 扰乱并发;
   3) 利用在更高抽象层中不可见的部件之间的干扰。

l) 使用中断或调度功能来扰乱先后顺序,当在下列情况发生时需检查 TOE 的行为:
   1) 某个命令被中断(使用 CTRL/C、CTRL/Y 等);
   2) 在第一个中断未响应前就发出第二个中断。

m) 应探测终止安全关键进程(例如审计守护程序)的影响。与此类似,还可延迟审计日志的记录或延迟告警的发出和接收,以至于这些信息对管理员来说是无用的(因为攻击可能已经成功)。

n) 扰乱并发包括当两个或更多的主体试图同时访问时,检查 TOE 的行为。当两个主体试图同时访问时,TOE 也许能够处理所需的交替操作,但是出现更多的主体时,其行为可能将变得很难确定。例如,如果两个其他的进程正在访问一个安全关键进程所需要的资源时,那么这个安全进程就可能只好进入资源等待状态。

o) 利用在更高抽象层中不可见的部件之间的干扰,可能会提供一种延迟与时间有关的可信进程的手段。

13.10.3.6.1.3 直接攻击

直接攻击包括证实或否定所声称的最小功能强度时所必需的任何穿透性测试的鉴定结果。当在此前提下鉴定穿透性测试时,评估者还应该注意到脆弱性存在的可能性,因为脆弱性的存在可导致安全机

制直接受到攻击。

13.10.3.6.1.4 误用

误用包括证实或否定误用分析时所必需的任何穿透性测试的鉴定结果。要考虑的问题包括：

a) 当进行启动、关闭或错误恢复时的 TOE 行为；

b) 在极端情况下(比如过载或渐近行为)的 TOE 行为，特别是在可能会导致激活或禁用安全执行的功能或机制的情况下的行为；

c) 在前面“篡改”条款中提到的，任何可能因无意的错误配置或不安全的使用所带来的攻击。

13.10.3.7 行动 AVA_VLA.2.4E

13.10.3.7.1 工作单元 4：AVA_VLA.2-10

评估者***应***基于独立的脆弱性分析***设计***穿透性测试。

评估者应基于在评估者活动 AVA_VLA.2.3E 中所假设的脆弱性优先级列表准备穿透性测试。

不能期望评估者测试那些高于低攻击潜力的攻击者所能利用的脆弱性。但作为评估专家意见，评估者可能发现了可被高于低攻击潜力的攻击者所利用的脆弱性，这样的脆弱性在 ETR 中报告为残余脆弱性。

在理解可疑脆弱性的基础上，由评估者确定出最合理的方法测试 TOE 受脆弱性的影响。评估者应特别考虑：

a) 用于激发 TSF 并观察反应的安全功能接口；

b) 测试所需的初始条件(例如：任何需要存在的特殊客体或主体及它们需要拥有的安全属性)；

c) 激发安全功能或观察安全功能所需的专用测试设备。

评估者很可能发现采用一系列测试用例来进行穿透性测试是可行的，每个测试用例测试一个特定的脆弱性。

13.10.3.7.2 工作单元 4：AVA_VLA.2-11

评估者***应***基于独立的脆弱性分析***编制***穿透性测试文档，并且文档应足够详尽使得测试可重复。测试文档应包括：

a) 被测 TOE 的明显脆弱性的标识；

b) 进行穿透性测试所需的所有测试设备连接和设置的说明；

c) 建立所有穿透性测试必备的初始条件的说明；

d) 激活 TSF 的说明；

e) 观察 TSF 行为的说明；

f) 所有预期结果的描述，并对用于比较预期结果的观察行为进行必要的分析；

g) 总结测试和为 TOE 建立必要的测试后状态的说明。

在测试文档中进行详细描述的目的是使其他的评估者能够重复测试并获得相同的结果。

13.10.3.7.3 工作单元 4：AVA_VLA.2-12

评估者***应***基于独立的脆弱性分析***实施***穿透性测试。

评估者使用工作单元 AVA_VLA.2-10 产生的穿透性测试文档，作为对 TOE 进行穿透性测试的基础，但这并不妨碍评估者执行额外特别的穿透性测试。如果有必要的话，评估者可设计新的测试，作为在穿透性测试期间(如果由评估者执行)了解到的信息的结果，如果评估者执行了这样的测试，那么这些

测试应记录在穿透性测试文档中。这样的测试可能需要跟进意想不到的结果或意见,或建议评估者在测试前期计划阶段研究潜在脆弱性。

如果穿透性测试结果显示某个假设的脆弱性不存在,那么评估者应确定评估者本人的分析是否正确,或者是否评估交付件是不正确或不完备的。

13.10.3.7.4 工作单元 4:AVA_VLA.2-13

评估者***应记录***穿透性测试的实际结果。

尽管实际测试结果的某些特定细节可能与预期的不同(例如,审计记录中的时间和日期字段),但整体结果应该是相同的。任何差异都应被证明是合理的。

13.10.3.7.5 工作单元 4:AVA_VLA.2-14

评估者***应***在 ETR 中***报告***评估者的穿透性测试工作、测试方法大纲、配置、深度和结果。

在 ETR 中报告的穿透性测试信息允许评估者描述全部穿透性测试方法和本子活动所做的工作。提供该信息的目的是对评估者的穿透性测试工作给出一个有意义的概述。这不意味着 ETR 中关于穿透性测试的信息完全复制于单个穿透性测试的具体测试步骤或测试结果。其目的是提供足够的细节,以便其他评估者和监督者了解所选择的穿透性测试方法、执行穿透性测试的数量、TOE 测试配置和穿透性测试活动的总体结果。

在 ETR 中,在有关评估者穿透性测试工作的章节中通常应包括以下信息:

a) TOE 测试配置。进行穿透性测试的 TOE 的特殊配置;

b) 进行穿透性测试的安全功能。穿透性测试所关注的安全功能简单列表;

c) 子活动的裁定。穿透性测试结果的总体判断。

以上列出的并不全面,只是为应在 ETR 中出现的,在评估期间评估者所做穿透性测试的信息的类型提供一些借鉴。

13.10.3.8 行动 AVA_VLA.2.5E

13.10.3.8.1 工作单元 4:AVA_VLA.2-15

评估者***应检查***所有穿透性测试结果和所有脆弱性分析的结论,以确定 TOE 在其预期使用环境中可以抵御拥有低攻击潜力的攻击者的攻击。

如果结果表明,TOE 在其预期使用环境中具有的脆弱性可以被拥有低于中等攻击潜力的攻击者所利用,那么本评估者行为就是失败的。

13.10.3.8.2 工作单元 4:AVA_VLA.2-16

评估者***应***在 ETR 中***报告***所有可利用的脆弱性和残余脆弱性,每种脆弱性应包括以下细节:

a) 来源(例如,在进行评估方法活动时构想到的、评估者知晓的、出版物上读到的);

b) 牵涉到哪些或哪个安全功能,哪些或哪个目的没有满足,违反了哪些或哪个组织安全策略和实现了哪些或哪个威胁;

c) 描述;

d) 在其预期环境中是否可被利用(例如,可利用的,还是残余的);

e) 识别出该脆弱性的评估方(例如开发者、评估者)的标识。

14 缺陷纠正子活动

14.1 缺陷纠正评估(ALC_FLR.1)

14.1.1 目的

本子活动的目的是确定开发者是否已建立了缺陷纠正程序,该程序用以描述安全缺陷跟踪、纠正行为标识,以及如何分发纠正行为信息到 TOE 用户。

14.1.2 输入

本子活动的评估证据是:

a) 缺陷纠正程序文档。

14.1.3 行为 ALC_FLR.1.1E

14.1.3.1 工作单元 ALC_FLR.1-1

ISO/IEC 15408-3 ALC_FLR.1.1C 缺陷纠正程序文档应描述用于跟踪每个在 TOE 发布版本中已报告的所有安全缺陷的程序。

评估者***应检查***缺陷纠正程序文档以确定它描述了用于跟踪每个 TOE 发布版本中已报告所有安全缺陷的程序。

程序描述了从每个可疑的安全缺陷被报告起到它被解决完毕为止,开发者所采取的行为。这包括缺陷的整个生存期,从最初的发现,到确定其为安全缺陷,直到安全缺陷被解决。

如果发现一个缺陷不是和安全相关的,则(根据 ALC_FLR"缺陷纠正"要求的目的)不需继续实施缺陷纠正程序予以跟踪,只需要阐述为何该缺陷不是和安全相关的。

虽然这些要求都不是强制的,TOE 用户可以通过公开方式报告安全缺陷,但是所有已报告的安全缺陷应被跟踪却是强制的。也就是,不能因为一个已报告的安全缺陷来自于开发组织外部,就简单地忽略它。

14.1.3.2 工作单元 ALC_FLR.1-2

ISO/IEC 15408-3 ALC_FLR.1.2C 缺陷纠正程序应要求描述所提供的每个安全缺陷的性质和影响,以及缺陷修正的情况。

评估者***应检查***缺陷纠正程序以确定这些程序的应用可产生一种按照性质和影响对每个安全缺陷的描述。

程序应确定开发者行为并详细地描述每个安全缺陷的性质和影响,以便能够重现它。安全缺陷性质的描述指出它是否为一个文档性错误,是否为一个 TSF 设计缺陷,是否为一个 TSF 实现缺陷等。安全缺陷影响的描述则标明 TSF 受影响的部分和它们是如何被影响的。例如,一个实现方面的安全缺陷可能通过允许使用带口令"BACKDOOR"的鉴别,而影响了 TSF 实施的标识和鉴别被发现。

14.1.3.3 工作单元 ALC_FLR.1-3

评估者***应检查***缺陷纠正程序以确定这些程序的应用可标识出每个安全缺陷修正发现的状态。

缺陷纠正程序需标识出安全缺陷的不同阶段,至少包括如下阶段:可疑安全缺陷已被报告、可疑安全缺陷已被确认为安全缺陷和安全缺陷的解决方案已被实现。还可以包括其他阶段(例如,缺陷已被报告但尚未调查、缺陷正在被调查中、安全缺陷的解决方案已被发现但尚未实施)。

14.1.3.4 工作单元 ALC_FLR.1-4

ISO/IEC 15408-3 ALC_FLR.1.3C 缺陷纠正程序应要求标识对每个安全缺陷所采取的修正行为。

评估者***应检查***缺陷纠正程序以确认程序的应用可标识对每个安全缺陷的修正行为。

“修正行为”可能包括对 TOE 硬件、固件和软件部分的修补，TOE 指南的修改，或者两者都有。构成 TOE 指南修改的修正行为(例如，用来消除安全缺陷的详细程序性措施)包括只作为过渡性方案(直至补丁发布)的那些措施和作为最终方案(即程序措施已被认定为最佳方案)的那些措施。

如果安全缺陷的来源是一个文档性错误，则修正行为包括更新受影响的 TOE 指南。如果修正行为是一个程序性措施，那么此措施应包括对受影响 TOE 指南所作的更新，以反映这些修正程序。

14.1.3.5 工作单元 ALC_FLR.1-5

ISO/IEC 15408-3 ALC_FLR.1.4C 缺陷纠正程序文档应描述用于向 TOE 用户提供缺陷信息、修正行为和修正行为指南给的方法。

评估者***应检查***缺陷纠正程序文档，以确定它描述了向 TOE 用户提供每个安全缺陷必需信息的方法。

关于每个安全缺陷的“必要信息”包括安全缺陷描述(在详细程度上可以不必和工作单元 ALC_FLR.1-2 所提供的一样)、规定的修正行为和关于实现修正的任何相关指南。

可通过几种途径为 TOE 用户提供信息、修正和文档更新，比如通过网站发布、邮件发送和安排由开发者安装修正等。当提供这些信息的方式要求由用户来发起时，评估者应检查 TOE 指南以确保它包含获取相关信息的规程。

评定用于提供信息、修正和指南的方法是否充分的唯一度量是存在一个合理的期望：TOE 用户能够获取或接收到。例如，考虑将必要的数据在网站发布一个月的分发方法时，要确保 TOE 用户知道这一情况将要发生并知道何时将要发生。这种方法可能不是非常合理或有效的(与在网站上永久发布相比)，但是切实可行的，因为 TOE 用户能够获取这些必要的信息。另一方面，如果信息仅在网站发布一个小时，再加上 TOE 用户无法得知这些或它何时将被发布，那么这对 TOE 用户总能得到这些必要的信息而言，就是不切实际的。

14.2 缺陷纠正评估(ALC_FLR.2)

14.2.1 目的

本子活动的目的是确定开发者是否建立了描述安全缺陷跟踪、修正行为标识、分发修正行为信息到 TOE 用户的缺陷纠正程序。此外，这一子活动还确定开发者的程序是否提供了安全缺陷的修正、来自 TOE 用户的缺陷报告的接受以及修正不会引入新安全缺陷的保证。

为了开发者能够正确处理来自 TOE 用户的安全缺陷报告，TOE 用户需要了解如何提交安全缺陷报告给开发者，开发者需要知道如何接收这些报告。缺陷纠正指南应针对 TOE 用户，以确保 TOE 用户知道如何与开发者进行沟通；缺陷纠正程序应描述开发者在沟通中的角色。

14.2.2 输入

本子活动的评估证据是：

a) 缺陷纠正程序文档；

b) 缺陷纠正指南文档。

14.2.3 行为 ALC_FLR.2.1E

14.2.3.1 工作单元 ALC_FLR.2-1

ISO/IEC 15408-3 ALC_FLR.2.1C 缺陷纠正程序文档应描述用于跟踪每一个 TOE 发布版本中所有已报告安全缺陷的程序。

评估者***应检查***缺陷纠正程序文档以确定它描述了用来跟踪每个 TOE 发布版本中所有已报告安全缺陷的程序。

程序描述从每个可疑的安全缺陷被报告起到它被解决完毕为止,开发者所采取的行为。这包括缺陷的整个生存期,从最初的发现,到确定其为安全缺陷,直到安全缺陷被解决。

如果发现一个缺陷不是和安全相关的,则(根据 ALC_FLR“缺陷纠正”要求的目的)不需继续实施缺陷纠正程序予以跟踪,只需要阐述为何该缺陷不是和安全相关的。

14.2.3.2 工作单元 ALC_FLR.2-2

ISO/IEC 15408-3 ALC_FLR.2.2C 缺陷纠正程序应要求描述所提供的每个安全缺陷的性质和影响,以及缺陷修正的情况。

评估者***应检查***缺陷纠正程序以确定这些程序的应用可产生一种按照性质和影响对每个安全缺陷的描述。

程序应确定开发者行为并详细地描述每个安全缺陷的性质和影响,以便能够重现它。安全缺陷性质的描述指出它是否为一个文档性错误,是否为一个 TSF 设计缺陷,是否为一个 TSF 实现缺陷等。安全缺陷影响的描述则标明 TSF 受影响的部分和它们是如何被影响的。例如,一个实现方面的安全缺陷可能通过允许使用带口令“BACKDOOR”的鉴别,而影响了 TSF 实施的标识和鉴别被发现。

14.2.3.3 工作单元 ALC_FLR.2-3

评估者***应检查***缺陷纠正程序以确定这些程序的应用可标识出对每个安全缺陷发现修正的状态。

缺陷纠正程序需标识出安全缺陷的不同阶段,至少包括如下阶段:可疑安全缺陷已被报告、可疑安全缺陷已被确认为安全缺陷和安全缺陷的解决方案已被实现。还可以包括其他阶段(例如,缺陷已被报告但尚未调查、缺陷正在被调查中、安全缺陷的解决方案已被发现但尚未实施)。

14.2.3.4 工作单元 ALC_FLR.2-4

ISO/IEC 15408-3 ALC_FLR.2.3C 缺陷纠正程序应要求标识对每个安全缺陷所采取的修正行为。

评估者***应检查***缺陷纠正程序以确认程序的应用可标识对每个安全缺陷的修正行为。

“修正行为”可能包括对 TOE 硬件、固件和软件部分的修补,TOE 指南的修改,或者两者都有。构成 TOE 指南修改的修正行为(例如,用来消除安全缺陷的详细程序性措施)包括只作为过渡性方案(直至补丁发布)的那些措施和作为最终方案(即程序措施已被认定为最佳方案)的那些措施。

如果安全缺陷的来源是一个文档性错误,则修正行为包括更新受影响的 TOE 指南。如果修正行为是一个程序性措施,那么此措施应包括对受影响 TOE 指南所作的更新,以反映这些修正程序。

14.2.3.5 工作单元 ALC_FLR.2-5

ISO/IEC 15408-3 ALC_FLR.2.4C 缺陷纠正程序文档应描述用于提供缺陷信息、修正行为和修正行为指南给 TOE 用户的方法。

评估者***应检查***缺陷纠正程序文档,以确定它描述了向 TOE 用户提供每个安全缺陷必需信息的

方法。

关于每个安全缺陷的“必要信息”包括安全缺陷描述(在详细程度上可以不必和工作单元 ALC_FLR.2-2 所提供的一样)、规定的修正行为和关于实现修正的任何相关指南。

可通过几种途径为 TOE 用户提供信息、修正和文档更新,比如通过网站发布、邮件发送和安排由开发者安装修正等。当提供这些信息的方式要求由用户来发起时,评估者应检查 TOE 指南以确保它包含获取相关信息的规程。

评定用于提供信息、修正和指南的方法是否足够的唯一度量是存在一个合理的期望:TOE 用户能够获取或接收到。例如,考虑将必要的数据在网站发布一个月的分发方法时,要确保 TOE 用户知道这一情况将要发生并知道何时将要发生。这种方法可能不是非常合理或有效的(与在网站上永久发布相比),但是切实可行的,因为 TOE 用户能够获取这些必要的信息。另一方面,如果信息仅在网站发布一个小时,再加上 TOE 用户无法得知这些或它何时将被发布,那么这对 TOE 用户总能得到这些必要的信息而言,就是不切实际的。

14.2.3.6 工作单元 ALC_FLR.2-6

ISO/IEC 15408-3 ALC_FLR.2.5C 缺陷纠正程序应描述开发者接收 TOE 用户报告并询问 TOE 中可疑安全缺陷的手段。

评估者***应检查***缺陷纠正程序,以确定其描述了开发者接受安全缺陷报告或缺陷修正请求的程序。

程序要确保 TOE 用户拥有与 TOE 开发者沟通的手段。通过拥有开发者的联系方式,用户能够报告安全缺陷、询问安全缺陷的现状和请求修正缺陷。这种联系方式对报告非安全相关问题来说是更通用的联系方法的组成部分。

这些程序的使用不限于 TOE 用户,但是,仅向 TOE 用户主动提供这些程序的详细内容。其他可访问 TOE 或熟悉 TOE 的人员也可以采用同样的程序,向开发者提交报告,以便开发者处理。除了开发者标明的方式之外,向开发者提交报告的任何其他方式都超出了本工作单元的范围,通过其他产生方式产生的报告无需处理。

14.2.3.7 工作单元 ALC_FLR.2-7

ISO/IEC 15408-3 ALC_FLR.2.6C 处理所报告安全缺陷的程序应确保任何已报告的缺陷都已被修正,并且该修正已发布给 TOE 用户。

评估者***应检查***缺陷纠正程序,以确定这些程序的应用可帮助确保修正了被报告的每个安全缺陷。

缺陷纠正程序不仅涵盖开发人员所发现和报告的安全缺陷,还包括 TOE 用户报告的安全缺陷。程序应足够详细,以便描述如何确保每个被报告的安全缺陷都被修正。程序包含合理的步骤,展示提出最终的、必然的解决办法的进程。

程序描述从一个可疑的缺陷被确定为安全缺陷到其被解决,所采取的处理过程。

14.2.3.8 工作单元 ALC_FLR.2-8

评估者***应检查***缺陷纠正程序以确定这些程序的应用可帮助确保向 TOE 用户发布了每个安全缺陷的修正行为。

程序描述从安全缺陷被确定到修正行为被提供出来,所采取的处理过程。修正行为交付程序应与安全目的一致;如果这些程序包含在保证要求内,它们不需与用于交付 TOE 的程序完全相同,即不需要书面说明满足 ALC_DEL 要求。例如,如果 TOE 的硬件部分最初是通过速递的方式交付的,那么由于缺陷纠正导致的硬件升级同样也可采用速递的方式来分发。与缺陷纠正无关的更新宜遵循满足 ALC_DEL“交付”要求的程序。

14.2.3.9 工作单元 ALC_FLR.2-9

ISO/IEC 15408-3 ALC_FLR.2.7C 处理所报告安全缺陷的程序应提供预防措施，确保对这些安全缺陷的任何修正不会引入任何新的缺陷。

评估者***应检查***缺陷纠正程序，以确定这些程序的应用可保证潜在的修正不会带来不良影响。

通过分析、测试或者两者的结合，开发者可以降低在修正安全缺陷时引入不良影响的可能性。评估者评估该程序是否详细提供了针对给定修正，如何确定分析和测试行为的必要联合。

评估者还需确定当安全缺陷来源于文档问题时，纠正程序是否包含了防止引入与其他文档矛盾之处的保障手段。

14.2.3.10 工作单元 ALC_FLR.2-10

ISO/IEC 15408-3 ALC_FLR.2.8C 缺陷纠正指南应描述 TOE 用户将 TOE 中任何可疑安全缺陷报告给开发者的手段。

评估者***应检查***缺陷纠正指南，以确定这些程序的应用可为 TOE 用户提供报告可疑安全缺陷或请求对该缺陷进行修正的手段。

指南要确保 TOE 用户拥有能够与 TOE 开发者进行沟通的方式。通过拥有与开发者的联系方式，TOE 用户能够报告安全缺陷、询问安全缺陷的现状和请求对缺陷进行修正。

14.3 缺陷纠正评估(ALC_FLR.3)

14.3.1 目的

本子活动的目的是确定开发者是否建立了描述安全缺陷跟踪、修正行为标识、分发修正行为信息到 TOE 用户的缺陷纠正程序。此外，这一子活动还确定开发者的程序是否描述了安全缺陷的修正、来自 TOE 用户的缺陷报告的接受、修正不会引入新安全缺陷的保证、每个 TOE 用户联系点的建立、给 TOE 用户的修正行为的及时发布。

为了开发者能够正确处理来自 TOE 用户的安全缺陷报告，TOE 用户需要了解如何提交安全缺陷报告给开发者，开发者需要知道如何接收这些报告。缺陷纠正指南针对 TOE 用户，保证 TOE 用户知道如何与开发者进行沟通；缺陷纠正程序描述了开发者在沟通中的角色。

14.3.2 输入

本子活动的评估证据是：

a) 缺陷纠正程序文档；

b) 缺陷纠正指南文档。

14.3.3 行为 ALC_FLR.3.1E

14.3.3.1 工作单元 ALC_FLR.3-1

ISO/IEC 15408-3 ALC_FLR.3.1C 缺陷纠正程序文档应描述用于跟踪每一个 TOE 发布版本中所有已报告安全缺陷的程序。

评估者***应检查***缺陷纠正程序文档以确定它描述了用来跟踪每个 TOE 发布版本中所有已报告安全缺陷的程序。

程序描述从每个可疑的安全缺陷被报告起到它被解决完毕为止，开发者所采取的行为。这包括缺陷的整个生存期，从最初的发现，到确定其为安全缺陷，到安全缺陷被解决。

如果发现一个缺陷不是和安全相关的，则(根据 ALC_FLR“缺陷纠正”要求的目的)不需继续实施

缺陷纠正程序跟踪它，只需要阐述为何该缺陷不是和安全相关的。

14.3.3.2 工作单元 ALC_FLR.3-2

ISO/IEC 15408-3 ALC_FLR.3.2C 缺陷纠正程序应要求描述所提供的每个安全缺陷的性质和影响，以及缺陷修正的情况。

评估者***应检查***缺陷纠正程序以确定这些程序的应用可产生一种按照性质和影响对每个安全缺陷的描述。

程序应确定开发者行为并详细地描述每个安全缺陷的性质和影响，以便能够重现它。安全缺陷性质的描述指出它是否为一个文档性错误，是否为一个 TSF 设计缺陷，是否为一个 TSF 实现缺陷等。安全缺陷影响的描述则标明 TSF 受影响的部分和它们是如何被影响的。例如，一个实现方面的安全缺陷可能通过允许使用带口令“BACKDOOR”的鉴别，而影响了 TSF 实施的标识和鉴别被发现。

14.3.3.3 工作单元 ALC_FLR.3-3

评估者***应检查***缺陷纠正程序以确定这些程序的应用可标识出对每个安全缺陷发现修正的状态。

缺陷纠正程序需标识出安全缺陷的不同阶段，至少包括如下阶段：可疑安全缺陷已被报告、可疑安全缺陷已被确认为安全缺陷和安全缺陷的解决方案已被实现。还可以包括其他阶段（例如缺陷已被报告但尚未调查、缺陷正在被调查中、安全缺陷的解决方案已被发现但尚未实施）。

14.3.3.4 工作单元 ALC_FLR.3-4

ISO/IEC 15408-3 ALC_FLR.3.3C 缺陷纠正程序应要求标识对每个安全缺陷所采取的修正行为。

评估者***应检查***缺陷纠正程序以确认程序的应用可标识对每个安全缺陷的修正行为。

“修正行为”可能包括对 TOE 硬件、固件和软件部分的修补，TOE 指南的修改，或者两者都有。构成 TOE 指南修改的修正行为（例如，用来消除安全缺陷的详细程序性措施）包括只作为过渡性方案（直至补丁发布）的那些措施和作为最终方案（即程序措施已被认定为最佳方案）的那些措施。

如果安全缺陷的来源是一个文档性错误，则修正行为包括更新受影响的 TOE 指南。如果修正行为是一个程序性措施，那么此措施应包括对受影响 TOE 指南所作的更新，以反映这些修正程序。

14.3.3.5 工作单元 ALC_FLR.3-5

ISO/IEC 15408-3 ALC_FLR.3.4C 缺陷纠正程序文档应描述用于提供缺陷信息、修正行为和修正行为指南给 TOE 用户的方法。

评估者***应检查***缺陷纠正程序文档，以确定它描述了向 TOE 用户提供每个安全缺陷必需信息的方法。

关于每个安全缺陷的“必要信息”包括安全缺陷描述（在详细程度上可以不必和工作单元 ALC_FLR.3-2 所提供的一样）、规定的修正行为和关于实现修正的任何相关指南。

可通过几种途径为 TOE 用户提供信息、修正和文档更新，比如通过网站发布、邮件发送和安排由开发者安装修正等。当提供这些信息的方式要求由用户来发起时，评估者检查 TOE 指南以确信它包含获取相关信息的规程。

评定用于提供信息、修正和指南的方法是否足够的唯一度量是存在一个合理的期望：TOE 用户能够获取或接收到。例如，考虑将必要的数据在网站发布一个月的分发方法时，要确保 TOE 用户知道这一情况将要发生并知道何时将要发生。这种方法可能不是非常合理或有效的（与在网站上永久发布相比），但是切实可行的，因为 TOE 用户能够获取这些必要的信息。另一方面，如果信息仅在网站发布一个小时，再加上 TOE 用户无法得知这些或它何时将被发布，那么这对 TOE 用户总能得到这些必要的

信息而言,就是不切实际的。

对于已向开发者注册的TOE用户(参见工作单元ALC_FLR.3-12)而言,仅仅被动地获得该信息是不够的。开发者应主动地向已注册的TOE用户发送该信息(或该信息可用的提示)。

14.3.3.6 工作单元 ALC_FLR.3-6

ISO/IEC 15408-3 ALC_FLR.3.5C 缺陷纠正程序应描述开发者接收TOE用户报告并询问TOE中可疑安全缺陷的手段。

评估者***应检查***缺陷纠正程序,以确定其描述了开发者接收安全缺陷报告或缺陷修正请求的程序。

程序要确保TOE用户拥有与TOE开发者沟通的手段。通过拥有开发者的联系方式,用户能够报告安全缺陷、询问安全缺陷的现状和请求修正缺陷。这种联系方式对报告非安全相关问题来说是更通用的联系方法的组成部分。

这些程序的使用不限于TOE用户,但是,仅向TOE用户主动提供这些程序的详细内容。其他可访问TOE或熟悉TOE的人员也可以采用同样的程序,向开发者提交报告,以便开发者处理。除了开发者标明的方式之外,向开发者提交报告的任何其他方式都超出了本工作单元的范围,通过其他产生方式产生的报告无需处理。

14.3.3.7 工作单元 ALC_FLR.3-7

ISO/IEC 15408-3 ALC_FLR.3.6C处理所报告安全缺陷的程序应确保任何已报告的缺陷都已被修正,并且该修正已发布给TOE用户。

评估者***应检查***缺陷纠正程序,以确定这些程序的应用可帮助确保修正了被报告的每个安全缺陷。

缺陷纠正程序不仅涵盖开发人员所发现和报告的安全缺陷,还包括TOE用户报告的安全缺陷。程序应足够详细,以便描述如何确保每个被报告的安全缺陷都被修正。程序包含合理的步骤,展示提出最终的、必然的解决办法的进程。

程序描述从一个可疑的缺陷被确定为安全缺陷到其被解决,所采取的处理过程。

14.3.3.8 工作单元 ALC_FLR.3-8

评估者***应检查***缺陷纠正程序以确定这些程序的应用可帮助确保向TOE用户发布了每个安全缺陷的修正行为。

程序描述从安全缺陷被确定到修正行为被提供出来,所采取的处理过程。修正行为交付程序应与安全目的一致;如果这些程序包含在保证要求内,它们不需与用于交付TOE的程序完全相同,即不需要书面说明满足ALC_DEL要求。例如,如果TOE的硬件部分最初是通过速递的方式交付的,那么由于缺陷纠正导致的硬件升级同样也可采用速递的方式来分发。与缺陷纠正无关的更新宜遵循满足ALC_DEL“交付”要求的程序。

14.3.3.9 工作单元 ALC_FLR.3-9

ISO/IEC 15408-3 ALC_FLR.3.7C处理所报告安全缺陷的程序应提供预防措施,确保对这些安全缺陷的任何修正不会引入任何新的缺陷。

评估者***应检查***缺陷纠正程序,以确定这些程序的应用可保证潜在的修正不会带来不良影响。

通过分析、测试或者两者的结合,开发者可以降低在修正安全缺陷时引入不良影响的可能性。评估者评估该程序是否详细提供了针对给定修正,如何确定分析和测试行为的必要联合。

评估者还需确定当安全缺陷来源于文档问题时,纠正程序是否包含了防止引入与其他文档矛盾之处的保障手段。

14.3.3.10 工作单元 ALC_FLR.3-10

ISO/IEC 15408-3 ALC_FLR.3.8C 缺陷纠正指南应描述 TOE 用户将 TOE 中任何可疑安全缺陷报告给开发者的手段。

评估者***应检查***缺陷纠正指南,以确定这些程序的应用可为 TOE 用户提供报告可疑安全缺陷或请求对该缺陷进行修正的手段。

指南要确保 TOE 用户拥有能够与 TOE 开发者进行沟通的方式。通过拥有与开发者的联系方式,TOE 用户能够报告安全缺陷、询问安全缺陷的现状和请求对缺陷进行修正。

14.3.3.11 工作单元 ALC_FLR.3-11

ISO/IEC 15408-3 ALC_FLR.3.9C 缺陷纠正程序应包含一个程序,要求及时对安全缺陷报告和相关修正的自动分发做出响应,将其分发给可能受到安全缺陷影响的注册用户。

评估者***应检查***缺陷纠正程序,以确定这些程序的应用可以带来一种及时向可能受影响的 TOE 注册用户提供每个安全缺陷报告和相关修正的方法。

及时发布适用于安全缺陷报告和相关修正的发布。但是它们不必在同一时间被发布。下面的做法是得到认可的:一旦过渡性解决方案被提出,即使该解决方案是和关掉 TOE 一样极端,缺陷报告就应立即被产生和发布。同样的,当一个更持久(且不过激)的修正方案被提出时,则该修正不应该被拖延发布。

不必把安全缺陷报告和相关修正的接受者仅限于可能受此安全缺陷影响的 TOE 用户,把所有安全缺陷的此类报告和修正都提供给全部 TOE 用户是允许的,且应及时提供此类信息。

14.3.3.12 工作单元 ALC_FLR.3-12

评估者***应检查***缺陷纠正程序,以确定这些程序的应用可实现向可能受安全缺陷影响的 TOE 注册用户自动发布安全缺陷报告和相关修正。

"自动发布"并不意味着禁止采用人工参与发布方式。实际上,发布方式可能全部由手工处理程序组成,可通过一个带自动调整手段的严密的监控程序监测报告或修正发布的不足之处。

把安全缺陷报告和相关修正的接受者仅限于可能受此安全缺陷影响的 TOE 用户是不必要的,提供所有安全缺陷的此类报告和修正给全部 TOE 用户是允许的,应自动提供此类信息。

14.3.3.13 工作单元 ALC_FLR.3-13

ISO/IEC 15408-3 ALC_FLR.3.10C 缺陷纠正指南应描述 TOE 用户向开发者注册以便有资格接收安全缺陷报告和修正的手段。

评估者***应检查***缺陷纠正指南,以确定它描述了使 TOE 用户能向开发者注册的方法。

*"使 TOE 用户能向开发者注册"*仅仅指对每个 TOE 用户都有一个途径向开发者提供联系方式;此联系方式可被用来向 TOE 用户提供与可能影响 TOE 用户的安全缺陷相关的信息,连同对安全缺陷的所有修正。TOE 用户注册可以作为 TOE 用户为了向开发者标识自己而需要执行的标准程序的一部分来完成,不管该过程是为了注册软件许可证,还是为了获得更新和其他有用的信息。

无需为每个 TOE 的安装注册一个 TOE 用户;通常一个组织注册一个 TOE 用户就足够了。例如,一个公司性质的 TOE 用户可能有一个面向它的全部场所的集中采购办公室。在这种情况下,采购办公室可能是一个对于所有 TOE 用户场所都满足要求的联系点,这样 TOE 的所有 TOE 用户安装只需使用一个注册的联系点。

另一方面,为了确保每一个 TOE 都有一个注册用户,将每一个 TOE 同它被交付给的组织进行关联应是可行的。对于拥有多个办公地址的组织,这种方法可以确保不存在某个用户被错误的假设为已

被一个 TOE 注册用户涵盖。

注意,TOE 用户不是必须注册,仅需要给他们提供注册的方法。但对于选择注册的用户必须直接发送这些信息(或其可用的提示)。

14.3.3.14 工作单元 ALC_FLR.3-14

ISO/IEC 15408-3 ALC_FLR.3.11C 缺陷纠正指南应标识特定的联系点,以便完全地报告和询问涉及 TOE 的安全问题。

评估者***应检查***缺陷纠正指南,以确定它标识了特定的联系点,便于用户报告和询问涉及 TOE 的安全问题。

指南包含一种手段,据此 TOE 注册用户可以同开发者交互,向其报告所发现的 TOE 安全缺陷或询问关于已发现的 TOE 安全缺陷方面的问题。

附 录 A
（规范性附录）
通用评估指南

A.1 目的

本章的目的是要涵盖提供评估结果技术性证据的基本评估技术。这些技术的使用有助于评估者所完成的工作满足客观性、可重复性和可再现性。

A.2 抽样

本条为抽样提供通用的技术指导。具体和详细的信息在那些与包含抽样的特定评估者行为元素相关的工作单元中给出。

抽样是评估者的一个既定程序，据此检查某个能代表整个评估证据规定集合的子集，以允许评估者不用对全部证据进行分析，就能足够信任特定评估证据的正确性。抽样的目的是在保证足够保证级别的前提下节约资源。对证据进行抽样可能出现两个结果：

a） 子集没有揭示错误，因此评估者对整个集合的正确性产生一定的信任；

b） 子集揭示了错误，因此整个集合正确性值得怀疑。即使找到了针对所有错误的解决办法，评估者也不能对此产生足够的信任，因此评估者可能会增加子集的大小，或者对该特定的证据不再采取抽样的办法。

抽样是一种从一组本质特征相似的证据中获得可靠结论的技术，例如，通过一个明确定义的过程产生的证据。

ISO/IEC 15408 指出在以下评估者行为元素中，抽样是明确接受的：

a） ADV_RCR.3.2E“评估者应选择性地验证形式化分析过程来决定对应性证明的准确性”。

b） ATE_IND.*.2E“评估者应适当地测试 TSF 的一个子集，以确认 TOE 按照规定运行”。

c） ATE_IND.2.3E“评估者应执行测试文档中的一个测试样本，以验证开发者的测试结果”。

d） AVA_CCA.*.3E“评估者应通过测试，有选择地验证隐蔽信道分析”。

e） AVA_MSU.2.2E 和 AVA_MSU.3.2E“评估者应重复所有的配置和安装程序，并有选择地重复其他的程序，以确认只使用所提供的指导性文档就能安全配置和使用 TOE”。

此外，ADV_IMP.1.1D 要求开发者提供一个 TSF 子集的实现表示，子集样本的选取应该得到评估者的同意。通过所提供的实现表示样本，评估者可以评估实现表示本身的陈述，并通过对可追溯性证据进行抽样，得到低层设计和实现表示之间相对应的保证。

除 ISO/IEC 15408 认可的抽样外，在本标准的下列行为中抽样也是可接受的：

a） 行为 ACM_CAP.*.1E：“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”。其中对 EAL3 和 EAL4 中的 ACM_CAP.*.8C 和 ACM_CAP.*.9C 的证据的内容和形式元素进行抽样是可接受的。

b） 行为 ATE_FUN.1.1E：“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”。其中对 EAL2、EAL3 和 EAL4 中的 ATE_FUN.1.3C、ATE_FUN.1.4C 和 ATE_FUN.1.5C 的证据的内容和形式元素进行抽样是可接受的。

c） 行为 ALC_DVS.1.1E：“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”。其中对 EAL3 和 EAL4 中的 ALC_DVS.1.2C 的证据的内容和形式元素进行抽样是可接受的。

在执行评估者行为时，实施 ISO/IEC 15408 中标识的抽样和在通用评估方法工作项中所作的特定抽样，是一种比较合算的方法。其他的抽样只在一些特殊情况下才被允许，例如，某项特殊评估活动的开销整体上与其他活动不成比例，且付出这种开销又无法相应地提高保证性时。在这种情况下，应制定在这些领域实施抽样的基本原理。TOE 本身的庞大、复杂，或内在的众多安全功能要求，都不能成为使用抽样的充分理由，因为对于庞大复杂的 TOE 的评估只是需要付出更多的努力。更确切些，例外办法只是针对以下特殊情况考虑的：TOE 开发方法产生了大量的关于特定 ISO/IEC 15408 要求的素材，这些素材通常都需要被核查或检查，但这些行为又不指望能够相应地提高保证性。

论证抽样的合理性也是必要的。这可通过分析抽样对安全目的以及 TOE 的威胁可能产生的影响来实现。这种影响依赖于因抽样而被遗漏的东西。另外，还需要考虑抽样证据的性质，不能因抽样而降低或忽略任何安全功能要求等。

应该认识到，与 TOE 实现直接相关的证据的抽样（例如，开发者测试结果）方法，和确定一个过程是否被遵循相关的证据抽样方法存在差异。在很多情况下，评估者需要确定某个过程是否被遵循了，这有一个推荐的抽样策略。此时的抽样方法与对开发者测试结果进行抽样时所采用的方法不一样。这是因为前者关心的是确保过程是合理的，而后者却是考虑 TOE 是否被正确实现了。通常，在和 TOE 正确实现有关的情况下，应当分析的样本比需要确保过程合理的情况下的样本多。

抽样应遵守下列原则：

a) 样本量应该与评估的成本效率相称，同时还应考虑许多与 TOE 相关的因素（例如，TOE 的大小和复杂程度、文档的数量等）。作为一个基准，对与 TOE 实现相关的材料进行抽样时，应当抽取至少 20%的样本量。但是，当抽取与某个过程（例如访问者控制或设计审查过程）正被遵循的证据相关的样本时，样本大小为一个百分数就不再恰当了。评估者应当抽取足够的信息样本以确信该过程正在被遵循，并证明样本量是合适的。

b) 样本应该能代表被抽样素材相关的各个方面。特别是，应当选择覆盖多种组件、安全功能、开发和运行场所（如果包括不止一个）以及硬件平台类型（如果包括不止一个）。

c) 在确保样本和支持性交付件及时交付的条件下（例如，依照评估计划，将测试套件和设备交付给评估者），不应事先告知评估发起者和开发者样本的确切组成。

d) 样本的选择应当尽可能的公正（评估者不应总是选择第一项或最后一项）。理想情况下，样本应当由评估者之外的人员选择。

在样本中找到的错误可以按系统性或者偶然性进行分类。如果是系统性错误，则应该纠正问题并且采用一个全新的样本。如果是偶然性错误，只要解释恰当，不需要新样本就可能解决问题，当然这些解释需要得到确认。在此情况下，评估者应决定是扩大样本量，还是使用不同的样本。

A.3 一致性分析

本条提供一致性分析的通用指南。具体和详细的信息在特定评估者行为元素中的那些工作单元给出，这些元素应进行一致性分析。

一致性分析是评估者的一个既定程序，此过程或者要对评估交付件的特定部分进行分析（内在一致），或者将其与一个或多个其他评估交付件进行比较。

ISO/IEC 15408 区分了不同种类的一致性分析：

a) 评估者应分析评估交付件的内在一致性。例如：

——ADV_FSP.1.2C：“功能规范应是内在一致的”。

——ADV_HLD.1.2C：“高层设计应是内在一致的”。

——ADV_IMP.1.2C：“实现表示应是内在一致的”。

——ADV_LLD.1.2C：“低层设计应是内在一致的”。

当进行内在一致性分析时，评估者应确信所提供的交付件不包括模棱两可的内容。评估交付件不应包含交付件不同部分相互矛盾的陈述。例如，对同一个证据采用的非形式化、半形式化和形式化描述都应相互一致。

评估者应该考虑一个评估交付件的各个部分可能存在于不同文档中的情况（例如，安全安装、生成和启动程序可能存在于三个不同的文件中）。

b) 评估者应分析评估交付件是与另外一个或多个交付件一致的。例如：

——AGD_ADM.1.7C：“管理者指南应与供评估的所有其他文档保持一致”。

——AGD_USR.1.5C：“用户指南应与供评估的所有其他文档保持一致”。

一致性分析要求评估者证实，在一个文档中描述的功能、安全参数、程序和安全相关事件与供评估的其他文档所描述的相关内容是一致的。这意味着评估者应该考虑可能会出现与其他信息来源不一致的地方。例如：

——与其他安全功能使用指南不一致。

——与 ST 不一致（例如威胁、安全使用假设、非 IT 安全目的或者 IT 安全功能等）。

——与功能规范或低层设计中对安全参数使用的描述不一致。

——与高层设计或低层设计文档中对安全相关事件的描述不一致。

——安全强制功能与非形式化 TSP 模型的冲突。

c) 评估者应分析两方面的情况，即评估交付件是内在一致的以及评估交付件与其他交付件也是一致的。例如：

——AVA_MSU.1.2C：“指导性文档应是完备的、清晰的、一致的和合理的”。

此处说明指南整体上应满足一致性的要求。假设该指导性材料包含在一个单独的文档中，或者分散到多个不同的文档中，则不管是在文档内部还是文档之间，一致性要求都应覆盖所有指南。

d) 评估者应核查开发者为论证一致性所提供的分析，例如：

——ADV_SPM.1.3C：“TSP 模型应包含一个基本原理，以证实该模型与所有可被模型化的 TSP 策略是一致的和完备的”。

——ADV_SPM.1.4C：“TSP 模型和功能规范之间对应性的证明应说明功能规范中的所有安全功能在 TSP 模型下是一致的和完备的”。

在这些情况下，开发者应提交一致性证据。然而，评估者应理解并确认这种分析，必要时甚至还要进行独立分析。

一致性分析可以通过检查评估交付件来完成。评估者应该采用合理的结构化方法分析文件的一致性，并且可以把它与其他活动结合起来，例如，映射或者可追溯性，以作为其他工作单元的一部分来开展。评估者也许能够解决任何借助形式化描述发现的不一致问题（如果存在的话）。类似地，在交付件中使用半形式化符号，虽不象形式化符号那样准确，也可用于减少交付件的模糊性。

歧义产生于相互冲突的陈述，也可隐含在不够准确的陈述中。应该注意到，繁琐本身不足以作为裁定一致性为“不通过”的依据。

对交付件的一致性核查可省略那些要求重做已执行的工作单元的活动。例如，安全目的一致性核查可以指定省略一个或者多个安全要求，在这种情况下评估者应该检查安全目的与 TSF 之间的对应性。

A.4 依赖性

一般来讲，可以任何次序，也可以并行方式执行需要的评估活动、子活动和行为。但是，存在多种不同的依赖性需要评估者考虑。本条提供不同活动、子活动和行为之间依赖性分析的通用指南。

A.4.1 活动之间的依赖性

由于某些原因，不同的保证类可以推荐甚至要求一个关于相关活动的执行顺序。一个特定的实例是 ST 评估活动。因为 ST 提供了 TOE 评估活动的基础和背景，所以 ST 评估活动应先于这些评估活动启动。但是直到 TOE 评估完成后，对 ST 的评估才能得出最终裁定，这是因为 TOE 评估活动中的发现可能会用于修改 ST。

A.4.2 子活动之间的依赖性

评估者需要考虑在 ISO/IEC 15408-3 中标识出的组件之间的依赖性。这种依赖性的一个例子是 AVA_VLA.1 “开发者脆弱性分析”组件，该组件声明依赖于 ADV_FSP.1“非形式化功能规范”、ADV_HLD.1“描述性高层设计”、AGD_ADM.1 “管理员指南”和 AGD_USR.1“用户指南”。

通常一个子活动只有在所有和它有依赖关系的其他子活动都成功完成后才能被裁定为“通过”。例如，通常只有在与 ADV_FSP.1“非形式化功能规范”、ADV_HLD.1“描述性高层设计”、AGD_ADM.1“管理员指南”和 AGD_USR.1“用户指南”相关的子活动都被裁定为“通过”时，AVA_VLA.1 才能够被正式裁定为“通过”。

因此，当需要确定一个子活动是否会影响另一个子活动时，评估者需要考虑这个活动是否依赖于来自其他相关子活动的潜在评估结果。事实上，可能是这样的情况，即一个相关的子活动会影响该子活动，这时需要重新执行先前已完成的评估者行为。

在评估者探测到缺陷时，一种重要的依赖性影响将发生。如果在某个子活动中发现了一个缺陷，那么只有当所有和该子活动相关的缺陷都被解决后，该依赖性子活动才有可能被赋予“通过”的裁定。

注意 ISO/IEC 15408-3 中的某些组件是相互依赖的，例如 ASE_INT 和 ASE_DES，因此上述依赖性问题将可能出现在每个相关子活动的评估序列中。

A.4.3 行为之间的依赖性

可能的情况是，评估者在一个行为中产生的结果，被用来执行另一个行为。例如，只有对内容和形式的检查完成以后，关于完备性和一致性的行为才能完成。这意味着，只有当评估者对 PP/ST 的要素部分评估完成以后，才推荐评估者评估 PP/ST 的基本原理。

A.5 现场核查

本条提供了关于现场核查的通用指南。具体和详细的信息在下列需要执行现场核查活动的工作单元中给出：

a) ACM_AUT“CM 自动化”；
b) ACM_CAP.n（其中 n>2）“CM 能力”；
c) ADO_DEL“交付”；
d) ALC_DVS“开发安全”。

进行现场核查是，评估者借以确定程序执行的方式是否与文档描述的方式一致的有效手段。

现场核查的动机主要有：

a) 观察 CM 规划中所描述的 CM 系统的使用；
b) 观察交付程序的实际应用；
c) 观察在开发中安全措施的应用。

在评估过程中，评估者经常需要与开发者反复会谈，如何很好地将现场核查与其他的会谈相结合以降低成本是一个问题。例如，评估者可以将针对配置管理、开发安全及交付的现场核查组合在一起，一

次完成。为了核查所有的开发阶段,对同一场所进行多次访问也是有必要的。同时,还应该考虑开发活动是在一幢建筑内的多个设备上、在同一个场所多个建筑内或者在多个场所内进行的情形。

在评估过程初期,应计划好第一次现场核查。如果评估是在 TOE 开发阶段开始的,在必要的情况下,可以允许采取纠正行为。如果评估是 TOE 开发后才开始,及早的现场核查能够在程序使用过程中出现严重缺陷时,及时采取纠正措施,这可避免不必要的评估开销。

会谈也是确定所编写的程序是否反映了其功能的一种有效手段。在进行会谈时,评估者应有意识获得开发现场程序分析的更深层理解,进一步了解这些程序在实践中是如何应用的,以及它们是否像所提供的评估证据中所描述的那样被使用。这样的会谈可作为补充但不能取代对评估证据的检查。

为了准备一个现场核查,评估者应根据所提供的评估证据形成一个相关事项清单。现场核查的结果应该被记录。

如果开发场所最近被另外一个 TOE 评估调查过或确认符合特定的 ISO9000 程序,那么可以认为现场核查不是必需的。应当考虑其他获得信任的方法,提供同等级别的保证(例如分析评估证据)。任何不做调查的决定应当和监督者商量后决定。

A.6 TOE 边界

被评估对象的标识将会出现在 ETR、证书、ST 和评估产品列表中。尽管产品通常是用于买卖的,但评估活动关心的是 TOE。下列各部分连同其内在关系以及对评估和认证的影响一起将作为本标准中所采用的定义的基础。

A.6.1 产品和系统

产品是可使用的硬件和软件的集合。一些销售商可能将某些产品(例如文字处理器、制表软件、图像应用)绑定到另外一个产品(例如办公自动化系统)。但是,假定该产品可以被大众、其他生产商、有限的客户使用,那么该绑定后的软件、硬件集合可认为是一个产品。

在已知的运行环境中,一个系统由一个或多个产品组成。产品评估和系统评估的主要区别是,评估者在系统评估中需要考虑实际的环境,但在产品评估中考虑的则是理论上的假想环境。

A.6.2 TOE

TOE 是通过 ST 定义的被评估的实体。虽然有时 TOE 代表了一个完整的产品,但这并不是必然的情形。TOE 可以是在某个特定配置或一组配置下的一个产品、产品的一部分或一组产品,也可以是某项从未被制成产品的独特技术,或者是这些东西的组合。这个特定配置或配置集被称作'评估配置'。ST 清楚地描述了 TOE 与任何关联产品的关系。

评估配置非常清楚地标识了其所包含的硬件,而未被包含的硬件部分也可能从 TOE 所在的产品中获得。这种标识有助于潜在客户明确地选择购买哪些产品及使用何种配置选项,以便 TOE 能安全运行。

A.6.3 TSF

TSF 是 TOE 中实施 ST 所定义的 TOE 安全性的那些功能的集合。TOE 中的一些功能可能并没有对 ST 所定义的 TOE 安全性起多大作用,因此不是 TSF 的组成部分。

TSF 硬件部分的描述细节与保证要求相称,这些保证要求与相应的开发文档(功能规范、高层设计和低层设计)及测试文档有关。硬件标识的细节程度由硬件特征对已声称的安全功能和保证要求产生的影响来决定。

A.6.4 评估

所有评估的一个隐含假设是 TOE(根据定义)是在其评估配置下的产品和系统。这个假设不需要显性的出现在评估假设列表中。TOE 经过评估的仔细审查:分析只在评估配置内进行,测试是在评估配置上执行,可利用的脆弱性在该评估配置中被标识,假设只有在评估配置中才是相关的。TOE 脱离该配置的情形是很重要的,应该在 AVA_MSU"误用"发生时进行考虑。这需要考虑 TOE 配置的健壮性以及任何无法检测到的偶然或有意的偏差带来的影响。

下面的例子给出了三个 TOE,它们都是基于相同虚拟专网(VPN)的防火墙产品,但是由于 ST 的差异得出了不同的评估结果。

1) **VPN 防火墙被配置为关闭 VPN 功能。ST 中的所有威胁都和从不安全网络访问安全网络相关。**

该 TOE 是被配置为关闭 VPN 功能的 VPN 防火墙。如果管理员将全部或部分 VPN 功能激活,产品将不在评估配置下的。因此,将不考虑对其进行评估,也不会对它的安全性作任何声明。

2) **VPN 防火墙,ST 中的所有威胁都和从不安全网络访问安全网络相关。**

该 TOE 是整个 VPN 防火墙。VPN 功能是这个 TOE 的一部分,因此在评估期间需要确定的一件事情是:是否存在通过 VPN 功能从不安全网络获得安全网络访问权的手段。

3) **VPN 防火墙,ST 中的所有威胁都和从不安全网络访问安全网络相关,或者与不安全网络中通信的保密性相关。**

该 TOE 是整个 VPN 防火墙。VPN 功能是这个 TOE 的一部分,因此在评估期间需要确定的一件事情是:VPN 功能是否允许 ST 中描述的任何威胁变为现实。

A.6.5 认证

上面几段清楚的表明,评估具有不同 ST 的同一件产品,将导致具有不同 TSF 的不同 TOE 。因此,证书、ETR、ST 和评估产品列表中的条目都应区分不同的评估,以便潜在的客户使用。

需要注意的是,上面三个不同的防火墙评估例子,它们之间明显的不同在证书中的表述是很微妙的,三个 VPN 防火墙都将导致在证书中如下标识 TOE:

XYZ 防火墙产品,如在 ST≠ABC 中标识的评估配置所描述的那样。

其中,每一个 ST ABC 有一个不同的标识符。

因此,评估者应根据评估范围内的 TOE 功能,确保 ST 充分描述了 TOE。一份清楚的解释是至关重要的,因为被评估产品的预期客户在考虑是否购买该产品时将要查阅产品的 ST,以便确定这些产品的哪些安全功能是通过了评估的。

A.7 威胁与 FPT 需求

PP/ST 作者标识威胁(从威胁角度看,来自恶意用户的威胁与通过 TSF 外部接口可利用的非正确实现带来的威胁并没有截然不同),并以此决定在 PP/ST 中是包含,还是排除 FPT_PHP"TSF 物理保护"、FPT_SEP"域分离"或 FPT_RVM"参照仲裁"。也就是说,所有这些要求族预先假定了一个对 TOE 物理篡改、用户干扰或旁路的威胁:

a) 关于 TSF 保护的要求直接与 TOE 环境陈述有关。当提及篡改或旁路威胁时,不管是显性的还是隐性的, TOE 或其运行环境应提供相关措施处理该威胁。

b) 通常,当 TOE 环境中出现了不可信主体(通常是人类用户),其存在攻击 TOE 意图保护的资产的动机时,篡改或旁路威胁就要被提及。

c) 在评估 PP/ST 中安全要求的陈述时,评估者确定 TSF 保护的需求以满足安全目的,并在该需

求建立处检查功能要求的存在性以满足安全目的。当保护需求被标识出，但 TOE 或其环境没有提供该保护，那么 PP/ST 评估子活动 APE/ASE_REQ 将判定为“不通过”。

如果 TOE 能够实施其安全策略，就应为 TOE 提供某些形式的保护。毕竟，如果 TSF 没有提供防止破坏的保护，那么就不能保证其策略实施功能将按所期望的执行。

这种保护可以由多种方式提供。一个操作系统，存在多个用户拥有丰富的 TOE(编程)接口，TSF 应能自我保护。然而，如果 TOE 只有一个受限接口，或接口的使用受到限制，则可能借助 TOE 之外的手段来提供必要的保护。

PP/ST 作者有责任选择 TOE 安全功能的组合、IT 环境假设和其他需要 TOE 安全功能自我保护的假设。评估者的职责是确认已经提供了必需的保护。依赖于 TOE 和假设，需要的保护可以从 FPT 类中得到功能安全要求，但在有些情况下也不必这样。

A.7.1 未必需要 FPT 类的 TOE

可以想象，有些 TOE(比如无用户接口的嵌入式 TOE)不会遇到这些威胁。一个针对提供了丰富用户接口的 TOE 的 PP/ST，若包含上述威胁但没有 FPT_PHP“TSF 物理保护”、FPT_RVM“参照仲裁”和 FPT_SEP“域分离”这些要求，则它很可能是一个无用的 PP/ST。不必包括 FPT：“TSF 保护”自我保护要求的 TOE 可分为以下三种类型。

A.7.1.1 包含受限用户接口的 TOE

向(非信任)用户提供受限接口的 TOE，由于受限接口对用户的行为能产生足够的约束，即使恶意用户也不能破坏它。例如，计算器或用户认证令牌这样的设备，仅有少数几个可输入键。非信任用户与诸如路由器、防护装置之类的通信设备的接口甚至受到更严格的限制：用户只能通过协议数据单元或消息，进行间接通信。

A.7.1.2 未实施相关安全策略的 TOE

对未实施访问控制或信息流控制策略的 TOE，不必担心一个用户访问另一用户或 TSF 的数据这样的事情。在这种情况下，几乎不需要 FPT_SEP“域分离”所暗指的用户分离。类似的，如果认为没有资产(如 IT 资源)需要保护(如对付拒绝服务攻击)，那么就不需要 FPT 要求。

A.7.1.3 由环境提供保护

TSF 的保护经常由 TOE 环境提供，而不是 TOE 自身(例如，一个运行在可信操作系统之上的应用程序，其中应用程序就是 TOE)。在这种情况下，评估将考虑环境机制是否提供了所需的保护。即使保护措施本身都是操作正确的，其用以保护 TOE 的方式也能影响到评估的范围。

例如，操作系统赋予某个应用程序中的目标文件的权限，将决定应用程序侵害底层操作系统的 TSP 的潜力。可以想象，对同一个应用程序采用两种不同操作系统保护措施的实现将意味着显著不同的 TSF。此时，即使由 TOE 环境来实现保护机制，仍然需要在判断 TSF 前，检查这些机制的使用。

A.7.2 对保证族的影响

在 PP/ST 中是否包括 FPT 自我保护要求将影响以下要求。

A.7.2.1 ADV

如果篡改或旁路威胁不存在，评估将集中在 TSF 的运行正确性上。这将包括考虑 TOE 中直接或间接作用于 TSP 实施的所有功能，不属于这些范畴的功能不需要检查(这些功能实现中的错误能够妨碍 TSF 的正确操作，这些错误可以通过 TSF 测试来找出)。

当宣称 TOE 具备了自我保护功能时，对其实现方法的描述应确定其保护机制，据此以确定 TSF 的边界。TSF 边界和接口的标识，与所宣称的 TSF 保护机制的性能一起，将限制评估的范围。这种限制将排除 TSF 以外的功能，因为这些功能不会干预正确的 TSF 运行。在很多情况下，TSF 边界将包括一些功能，这些功能不作用于 TSP 实施，但在评估过程中将被检查。那些可以断定不属于 TSF 的功能不需要评估者检查。

A.7.2.2 AVA_VLA

ISO/IEC 15408 中脆弱性分析决定了脆弱性在 TOE 预期使用环境中对 TOE 运行的影响。如果 ST 中没有标识篡改或旁路威胁，开发者和评估者（如果需要）查找脆弱性的时应不考虑此类攻击。

A.7.2.3 ATE_IND

ATE_IND“独立测试”中应用注释要求对可能适用于 TOE 的明确公开的弱点进行测试。这种基于故意篡改或旁路 TOE 的弱点，只需在威胁已经被标识的地方考虑就可以了。

A.8 功能强度和脆弱性分析

对比表明 TOE 安全功能强度分析和脆弱性分析既有明显的不同，也有显著的相似之处。

一个显著的相似之处在于它们对攻击潜力的运用上。对这两种分析，评估者确定攻击者发起一个有效攻击所需要的最小攻击潜力，并且得出某些关于 TOE 攻击抵抗力的结论。表 A.1 和表 A.2 显示并进一步描述了这些分析和攻击潜力的关系。

表 A.1 脆弱性分析和攻击潜力

脆弱性组件	TOE 抵抗具有如下攻击潜力的攻击者	只对具有如下攻击潜力的攻击者才可利用的残余脆弱性
VLA.4	高	不适用——成功攻击超过了实际范围
VLA.3	中	高
VLA.2	低	中

表 A.2 TOE 安全功能强度和潜在攻击

SOF 级别	足以防范具有如下攻击能力的攻击者	不足以防范具有如下攻击能力的攻击者
高级 SOF	高	不适用——成功攻击超过了实际范围
中级 SOF	中	高
基本级 SOF	低	中

这些分析的显著不同根源于 TOE 安全功能及攻击的本质。TOE 安全功能强度分析只针对概率或置换功能执行，不包括那些基于密码的功能。进一步说，这种分析假定概率或置换安全功能能正确地执行，并且假定在受到攻击时这些安全功能正运行于其设计和实现的限制要求内。正如表 A.2 所示，SOF 级别用攻击潜力反映了概率或置换安全功能针对的攻击。

脆弱性分析适用于所有的非密码 TOE 安全功能，包括那些在本质上是概率或置换的功能。与

SOF 分析不同，这里没有关于安全功能设计和实现正确性的任何假设，也没有对攻击方法或者攻击者与 TOE 的交互方式进行限制——如果攻击可行，脆弱分析期间将考虑该攻击。正如表 A.1 所示，对脆弱性保证组件的成功评估反映了威胁的程度，该程度用攻击潜力来描述，所有 TOE 安全功能都是根据这些威胁的程度来设计的。

对攻击潜力概念的共用，在 SOF 声明与脆弱性评估之间建立了一种联系，但这种联系不应被看作是 SOF 声明级别与从 AVA_VLA“脆弱性分析”中所选保证组件之间的一种强制绑定。例如，AVA_VLA.2“独立脆弱性分析”需要对抗具有低攻击潜力的攻击者，但并没有把 SOF 级别的选择限制为基本级 SOF。假设一个脆弱性是任何概率或置换功能固有的，并且这些功能通常是实现公开接口的主导方式（例如口令），为抵御对这些方面的攻击，PP/ST 作者可要求较高级别的抵抗力，以及一个较高的 SOF 级别。只要有声明 AVA_SOF“TOE 安全功能强度”的地方，就至少需要声明一个基本级 SOF。所声明的 AVA_VLA“脆弱性分析”组件建立在 SOF 声明之上，基本级 SOF 的声明应当被看作是与 AVA_VLA.3“中级抵抗力”的选择不一致的。

A.8.1 攻击潜力

A.8.1.1 攻击潜力的应用

攻击潜力是专业技能、资源和动机的一个函数，下面将分别讨论这些因素。在 ST 评估和脆弱性评定活动期间，评估者尤其需要用两种截然不同的方式来考虑攻击潜力。在 ST 评估期间，评估者确定对保证要求组件的选择，特别是 AVA“脆弱性评定”类的组件，是否与威胁攻击潜力相匹配（见 ASE_REQ.1.4C）。如果保证是不相称的，则可能意味着评估不会提供充足的保证，或者表明评估需要一些不必要的开销。在脆弱性评估期间，评估者使用攻击潜力来确定已标识脆弱性在预期使用环境中的可利用性。

A.8.1.2 动机的处理

动机是表达攻击潜力的一个因素，可用来描述与攻击者及攻击者想得到的资产相关的多个方面的情况。首先，动机能暗示攻击的可能性——我们能够从一个被描述为高动机性的威胁推测出一个攻击即将发生，或者从没有动机的威胁中推测出没有攻击。然而，除了这两种极端情况外，很难从动机中推测出攻击发生的可能性。

其次，动机能暗示资产对攻击者和资产所有者的价值，以金钱价值或其他方式来衡量。与低价值的资产相比，高价值的资产更容易引发攻击。然而，除此之外，很难把资产价值同动机联系起来，因为资产的价值具有主观性，它在很大程度上依赖于资产所有者赋予它的价值。

其三，动机能暗示攻击者发动攻击所拥有的专业技能和愿意付出的资源。我们可以得出高动机的攻击者可能会获得足够的专业技能和并付出足够的资源来挫败资产的保护措施。相反，如果攻击者的动机是低的，拥有大量专业技能和资源的攻击者就不愿意利用这些技能和资源来发动一个攻击。

在评估工作准备及开展期间，对上述关于动机的三个方面都应该在某种程度上加以考虑。第一方面，攻击的可能性是引起开发者执行评估的主要原因。如果开发者认为攻击者有发动攻击的足够动机，那么评估就能提供 TOE 能够阻止攻击者企图的保证。如果预期使用环境是明确定义的，例如在系统评估时，攻击动机的高低可能是已知道的，并将影响对抗措施的选择。

考虑到第二方面，资产的所有者可能会认为资产的价值（不论怎样估量）足以诱发攻击。评估一旦被认为是必要的，就要考虑攻击者的动机，以便确定攻击者可能采用的攻击方法以及这些攻击所使用的专业技能和资源。一旦完成了检查，开发者就能选定适当的保证级别，特别是 AVA 要求组件，以便与威胁的攻击潜力相匹配。在评估过程中，特别是作为脆弱性评定活动完成的结果时，评估者确定在预期使用环境中运行的 TOE 是否足以挫败拥有专业技能和资源的攻击者。

A.8.2 攻击潜力的计算

本条详细论述攻击潜力的几个决定因素，并提供一些指导性意见，以帮助评估者摒弃评估过程中的一些主观性。除非评估者认为这个方法是不适当的，否则就应该采纳它。要是评估者认为不适当，就需要提供一个原理来证明可选方法的有效性。

A.8.2.1 标识和利用

对攻击者而言，要想利用一个脆弱性，应首先将这个脆弱性标识出来。划分脆弱性标识和利用这两个过程看起来无关紧要，但实际上却是一个很重要的工作。为了说明这一点，首先考虑那些经过专家几个月的分析后仍然没有发现的脆弱性，以及发布在因特网上的一个简单的攻击方法。与某个已经认知的脆弱性相比，未知脆弱性的利用则需要大量时间和资源。很明显，在这些情况下，诸如时间之类的因素需要被区别对待。

对于 SOF 分析而言，脆弱性利用问题常常是最重要的，因为概率或置换机制方面的脆弱性通常是不证自明的。然而，应该注意情况并不总是这样。以密码机制为例，很少的脆弱性知识也可能会极大地影响强力攻击的效率。而系统用户倾向于选择名字作为口令这样的知识，也将处于类似的境况。对于比 AVA_VLA.1“开发者脆弱性分析”更高的脆弱性评估，从头开始的脆弱性标识工作将成为更加重要的考虑因素，因为发掘脆弱性的难度可能是众人皆知的，而其利用往往显得非常简单。

A.8.2.2 值得考虑的因素

在分析那些利用脆弱性所需的攻击潜力时，应该考虑下列因素：

a) 标识
   1) 标识所需的时间；
   2) 专家的技术专长；
   3) TOE 的设计和操作知识；
   4) TOE 的访问；
   5) 分析所需的 IT 硬件/软件或者其他设备。
b) 利用
   1) 利用所需的时间；
   2) 专家的技术专长；
   3) TOE 的设计和操作知识；
   4) TOE 的访问；
   5) 利用所需的 IT 硬件/软件或者其他设备。

在很多情况下这些因素都不是相互独立的，但在不同的程度上又是可以相互替代的。例如，技术专长或者硬件/软件可以替代时间。下面将讨论这些因素。

时间指的是攻击者用于标识或利用一次攻击的连续时间。针对本讨论的目的而言，“在几分钟内”意味着一次攻击可以在不到半个小时内被标识或者利用，“在几小时内”意味着一次攻击可以在不到一天内就能成功进行，“在几天内”意味着一次攻击可以在不到一个月内就能成功进行，“在几个月内”意味着一次成功的攻击至少需要一个月。

专家技术专长指的是掌握应用领域或者产品类型(例如 Unix 操作系统、因特网协议)的通用知识的水平。确定的级别如下：

a) 专家，熟悉产品或系统类中实现的底层算法、协议、硬件和结构等，以及所采用的安全原理和概念；
b) 精通者，知识渊博，对产品或系统类的安全行为很熟悉；

c) 外行,相对于专家或者精通者,知识不够渊博,并没有专门技能。

TOE 知识指的是与 TOE 有关的专门技能。TOE 知识与通用的技能截然不同,但也并不是毫不相关的。确定的级别如下:

a) 除了 TOE 的通用用途外,没有关于 TOE 的信息;

b) 关于 TOE 的公共信息(例如从用户手册获得);

c) 关于 TOE 的敏感信息(例如内部设计的知识)。

应该注意区别标识脆弱性所需的信息和利用该脆弱性所需的信息,特别是在一些敏感信息方面。获取关于利用的敏感信息是不常见的。

TOE 访问同样也是一个值得重点考虑的因素,它与时间因素有关。对于脆弱性的标识或利用可能需要进行大量的 TOE 访问,这样可能会增加被探测到的可能性。某些攻击可能需要相当多的离线工作,而只对 TOE 进行短暂的访问就可以实施脆弱性利用。访问可以是连续的,也可以经由多个会话实现的。针对本讨论的目的而言,"在几分钟内"意味着一次访问需要不到半个小时时间,"在几小时内"意味着访问需要不到一天时间,"在几天内"意味着访问需要不到一个月时间,"在几个月内"意味着访问需要至少一个月时间。当访问 TOE 不会增加被探测的可能性时(例如攻击者拥有的智能卡),这个因素应该被忽略。

IT 硬件/软件或者其他设备指的是标识或者利用一个脆弱性所需的设备。

a) 标准设备指不论是标识一个脆弱性,还是标识一个攻击,攻击者都很容易得到的设备。这个设备可能是 TOE 本身的一部分(例如,操作系统中的一个调试器),或者能够很容易得到的(例如从因特网上下载,或简单的攻击脚本)。

b) 专业设备指对于攻击者来说不容易得到,但是不需要过度的代价就能获得的。这可能包括购买一定数量的设备(例如协议分析仪)或者开发更多的攻击脚本或程序。

c) 定制设备指对于公众来说是不容易得到的,它可能需要专门制造(例如非常复杂的软件),或者因为设备十分特殊以至于它的销售受到了控制,甚至可能是受限的,或者该设备可能十分昂贵。将成百上千的 PC 机通过因特网进行连接就是这种情况。

专家技能和 TOE 知识与 TOE 攻击者所需的信息有关。攻击者的专门技能和实施攻击时有效利用设备的能力之间存在一个隐含的关系。攻击者的专门技能越少,使用设备的潜力越低。同样,攻击者的专门知识越多,在攻击中使用设备的潜力越高。尽管没有明确说明,技能和设备可利用性之间的这个关系并不总是适用的,例如,当环境措施可防止专业的攻击者对设备的利用时,或者当通过其他人的努力,可有效利用且只需很少专业技能就可掌握的攻击工具将会被制造并免费发放(例如通过因特网)时。

A.8.2.3 计算方法

上一条确定了评估攻击潜力需要考虑的因素。然而,如果依据标准进行评估,还需要更进一步的指导。下面的方法将辅助这一过程。另外下面还提供了一些数据,其目的是实现与相应的评估级别一致的分级。

表 A.3 标识了上一条讨论过的因素,并为标识和利用脆弱性这两个方面列出了相关的数据值。当为某个给定的脆弱性确定攻击潜力时,应该从每个因素对应的脆弱性标识和利用列中各选一个值(这样产生了 10 个值)。在选择值时,应该先假定 TOE 的预期使用环境。这 10 个值的和将给出一个值,然后参照表 A.4,用这个值就可以确定相应的等级了。

在一个因素与一个范围的边界很接近时,评估者应该考虑使用表中所列值的中间值。例如,为了利用脆弱性,如果需要访问 TOE 1 小时,或者如果访问很快就会被探测到时,可以为该因素选择 0 和 4 之间的某个值。这个表只是起一个引导的作用。

表 A.3　攻击潜力的计算

因素	范围	标识值	利用值
消耗的时间	≤0.5 小时	0	0
	≤1 天	2	3
	≤1 月	3	5
	>1 月	5	8
	不实际	*	*
专业技能	外行	0	0
	精通者	2	2
	专家	5	4
TOE 知识	无	0	0
	公共知识	2	2
	敏感知识	5	4
TOE 访问	≤0.5 小时，或者访问无法检测到	0	0
	≤1 天	2	4
	≤1 月	3	6
	>1 月	4	9
	不实际	*	*
设备	无	0	0
	标准	1	2
	专业	3	4
	预定	5	6
“*”表示在某个时间范围内，攻击者可用的攻击途径是不可利用的。任何值“*”表示一个“高”等级。			

对于一个给定的脆弱性，可能有必要针对不同的攻击情形，利用这个表来进行好几趟计算（例如，在专业技能和时间及设备之间进行折衷考虑时）。这多次计算得到的最低值将被保留。

当脆弱性已经被标识并处于公开可知的状态时，脆弱性标识值应该体现攻击者从公开领域获取该脆弱性的难易程度，而不是反映攻击者从头开始标识该脆弱性的情况。

接下来，表 A.4 宜被用于获得脆弱性级别。

表 A.4　脆弱性级别

值的范围	抵抗具有如下攻击潜力的攻击者	SOF 级别
<10	无级别	
10-17	低	基本级
18-24	中	中级
>25	高	高级

这样的方法不可能考虑到每一种环境或者因素，但应该能更好地揭示那些要求达到标准级别的抗

攻击水平的实际情况。其他因素，例如对不太可能发生的偶然事件的依赖性，或者在攻击完成前被探测的可能性，都没有包含在基本模型中。不过除基本模型所含因素外，这些因素也可以被评估者视为评级的依据。

在某些情况下，例如在评定口令机制时，TOE 的实现只允许在攻击被阻断之前进行少量的尝试，这时强度评定就大致和在那几次尝试中正确猜中的可能性完全相关。这样的阻断措施可被看作是访问控制功能的一部分，所以口令机制本身只接收中等 SOF 级别，而访问控制功能可能被判定为 SOF 高级。

应该指出的是，尽管对大量脆弱性的单独评级可能会显示出高等级的抗攻击性，但对其他脆弱性的评级却可能会更改表的值，使得这样的脆弱性组合表现出更低的整体等级。换句话说，一个脆弱性的存在可能会使得另一个脆弱性很容易被利用。这样的评估应当构成开发者和评估者脆弱性分析的一部分。

A.8.3 功能强度分析示例

对假定的通行数机制的 SOF 分析如下。

从 ST 和设计证据中收集到的信息表明，鉴别和认证为控制从广泛分布的终端上访问网络资源提供了基础。对终端的物理访问未受任何有效手段的控制，对终端进行访问的持续时间也未受任何有效手段的控制。在初始化授权阶段，系统的授权用户可以选择自己的通行数，以后也可以应用户要求重新选择。系统对用户选择的通行数作出了如下限制：

a) 通行数至少为 4 位数字，最长不超过 6 位；

b) 不允许为连续的数字序列（如，7、6、5、4、3）；

c) 不允许有重复数字（每个数字应唯一）。

在选择通行数时，对用户的指导意见是通行数应尽可能随机并且不能以某种方式与用户关联（例如，出生日期）。

通行数空间计算如下：

a) 人的使用惯例是一个非常值得考虑的因素，它会影响搜索口令空间的方法，从而影响 SOF。考虑最糟的情况，用户选择的通行数仅有 4 位，如果每位数字应是唯一的，则通行数的排列数即为：

$$7(8)(9)(10)=5\ 040$$

b) 可能的连续递增序列数目为 7，连续递减序列数目也为 7。减去这些序列后的通行数空间为：

$$5\ 040-14=5\ 026$$

依据从设计证据得到的进一步信息，通行数机制是按照终端锁定特点设计的。规定第六次不成功的鉴别尝试后，终端“锁定”一个小时。不成功的鉴别计数在 5 min 之后重新设置，这样攻击者每 5 min 内最多能尝试 5 次通行数输入，或者每小时 60 次通行数输入。

在输入正确的通行数前，一个攻击者平均应输入通行数 2 513 次，耗时超过 2 513 min。结果是，平均成功攻击时间略小于：

$$\frac{2\ 513\ \text{min}}{60\ \text{min/h}}\approx 42\ \text{h}$$

用上条描述的方法，标识值将是每个类别的最小值（总值为 0），因为该脆弱性在该功能中是明显存在的。对于脆弱性利用，依据以上的测算，一个外行在几天之内不用任何设备，没有任何 TOE 的知识，挫败通行数字机制（获得 TOE 的访问控制权）也是可能的，因此得到的赋值为 11。给定结果值 11，则要成功发起攻击的攻击潜力测定为最少是中级。

SOF 级别可根据 ISO/IEC 15408-1 第 2 章中的术语“攻击潜力”来定义。因为该机制应抵抗具有低攻击潜力的攻击者，以声明基本级 SOF，同时因为通行数机制是用来抵抗具有低攻击潜力的攻击者

的,因此该通行数机制级别最好定义为基本级 SOF。

A.9 体制责任

本标准描述了在监督(体制)机构的监督下,评估至少应执行的技术性工作。然而,本标准也(明确或隐含地)承认有一些活动或方法是评估结果的互认所未依赖的。为了更加全面和清楚,也为了更好地描述本标准在哪里结束,单个评估体制的方法从哪里开始,列举以下的材料以供这些体制自行取舍。体制可以选择性地提供下列材料,也可保留下一些材料待定(本标准为保证此列表的完整性已经作了很多努力;当评估者遇到一个既没有在以下列表中列出、也没有在本标准中出现的问题时,应当商议其评估体制,以决定该问题由谁解决)。

体制可以选择详细说明的事项包括:

a) 在确保评估工作完成的充分性方面——要求每个体制都有核实其评估者工作的方式,不管是要求评估者提交他们的发现给监督机构,还是要求监督机构重做评估者的工作,还是通过其他方式确保该体制下所有的评估机构都是可以胜任和比较的。
b) 为完成评估而进行的评估证据处置过程。
c) 任何保密性要求(关于评估者的以及不披露在评估过程中所获信息的要求)。
d) 评估中遇到问题时采取的对策(是在问题解决后继续评估,还是立即终止并要求修补过的产品应重新提交评估)。
e) 文件编制所采用的特定(自然)语言。
f) 任何在 ETR 中应被提交的记录证据——本标准规定了在 ETR 中报告事项的最小集;然而,个别评估体制可能需要在 ETR 中包括额外的信息。
g) 需要评估者提交的任何附加报告(除 ETR 外),如测试报告。
h) 任何特定的体制需要的 OR,包括 OR 的结构、接受者等。
i) 任何特定的作为 ST 评估结果的书面报告的目录结构——体制可能有一个特定的格式,用于报告评估的详细结果,该评估可能是 TOE 评估或 ST 评估。
j) 任何必需的附加的 PP/ST 标识信息。
k) 任何确定 ST 中明确陈述要求适合性的活动。
l) 任何关于评估者证据准备的要求,以支持证据再评估和再利用。
m) 任何关于体制标识符、标志和商标等的特定处理办法。
n) 任何特定的处理密码问题的指导意见。
o) 体制的应用和管理办法、国内和国际的解释办法。
p) 在测试不可行时,适当的可选测试方法的列表或特征。
q) 监督者能够确定评估者在测试时所采用步骤的机制。
r) 首选测试途径(如果有):内部接口或外部接口。
s) 用于指导评估者脆弱性分析的可接受方式的列表或特征(如缺陷假设方法)。
t) 值得考虑的任何脆弱性和弱点的相关信息。

中华人民共和国
国家标准
信息技术 安全技术
信息技术安全性评估方法
GB/T 30270—2013/ISO/IEC 18045:2005
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址:www.gb168.cn
服务热线:400-168-0010
010-68522006
2014年6月第一版
*
书号:155066·1-49179

GB/T 30270-2013