

# 中华人民共和国国家标准

GB/T 18336.5—2024/ISO/IEC 15408-5:2022

部分代替 GB/T 18336.3—2015

## 网络安全技术 信息技术安全评估准则 第5部分：预定义的安全要求包

Cybersecurity technology—Evaluation criteria for IT security—  
Part 5: Pre-defined packages of security requirements

(ISO/IEC 15408-5:2022, Information security, cybersecurity and privacy  
protection—Evaluation criteria for IT security—Part 5: Pre-defined packages  
of security requirements, IDT)

2024-04-25 发布

2024-11-01 实施

国家市场监督管理总局 发布  
国家标准化管理委员会



目 次

前言 ..... III

引言 ..... V

1 范围 ..... 1

2 规范性引用文件 ..... 1

3 术语和定义 ..... 1

4 评估保障级 ..... 2

    4.1 族名 ..... 2

    4.2 评估保障级概述 ..... 2

    4.3 评估保障级的目的 ..... 4

    4.4 评估保障级 ..... 4

5 组合保障包 ..... 14

    5.1 族名 ..... 14

    5.2 组合保障包概述 ..... 14

    5.3 组合保障包的目的 ..... 15

    5.4 CAP 族中的包 ..... 16

6 复合产品包 ..... 20

    6.1 包名 ..... 20

    6.2 包类型 ..... 20

    6.3 包概述 ..... 20

    6.4 目的 ..... 20

    6.5 安全保障组件 ..... 20

7 保护轮廓保障 ..... 21

    7.1 族名 ..... 21

    7.2 PPA 族概述 ..... 21

    7.3 PPA 族目的 ..... 21

    7.4 PPA 包 ..... 21

8 安全目标保障 ..... 23

    8.1 族名 ..... 23

    8.2 STA 族概述 ..... 23

    8.3 STA 族目的 ..... 23

    8.4 STA 包 ..... 23

附录 NA (资料性) 缩略语 ..... 25

参考文献 ..... 26



## 前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件是 GB/T 18336《网络安全技术 信息技术安全评估准则》的第5部分。GB/T 18336 已经发布以下部分：

- 第1部分：简介和一般模型；
- 第2部分：安全功能组件；
- 第3部分：安全保障组件；
- 第4部分：评估方法和活动的规范框架；
- 第5部分：预定义的安全要求包。

本文件和 GB/T 18336.3—2024《网络安全技术 信息技术安全评估准则 第3部分：安全保障组件》、GB/T 18336.4—2024《网络安全技术 信息技术安全评估准则 第4部分：评估方法和活动的规范框架》共同代替 GB/T 18336.3—2015《信息技术 安全技术 信息技术安全评估准则 第3部分：安全保障组件》。

本文件部分代替 GB/T 18336.3—2015《信息技术 安全技术 信息技术安全评估准则 第3部分：安全保障组件》。与 GB/T 18336.3—2015 相比，除结构调整和编辑性改动外，主要技术变化如下：

- 删除了保障范型(见 GB/T 18336.3—2015 年版的第5章)；
- 删除了安全保障组件(见 GB/T 18336.3—2015 年版的第6章)；
- 增加了复合产品包(COMP)(见第6章)；
- 增加了保护轮廓保障(PPA)(见第7章)；
- 增加了安全目标保障(STA)(见第8章)；
- 删除了 APE 类：保障轮廓评估(见 GB/T 18336.3—2015 年版的第9章)；
- 删除了 ASE 类：安全目标评估(见 GB/T 18336.3—2015 年版的第10章)；
- 删除了 ADV 类：开发(见 GB/T 18336.3—2015 年版的第11章)；
- 删除了 AGD 类：指导性文档(见 GB/T 18336.3—2015 年版的第12章)；
- 删除了 ALC 类：生命周期支持(见 GB/T 18336.3—2015 年版的第13章)；
- 删除了 ATE 类：测试(见 GB/T 18336.3—2015 年版的第14章)；
- 删除了 AVA 类：脆弱性评定(见 GB/T 18336.3—2015 年版的第15章)。

本文件等同采用 ISO/IEC 15408-5:2022《信息安全、网络安全和隐私保护 信息技术安全评估准则 第5部分：预定义的安全要求包》。

本文件做了下列最小限度的编辑性改动：

- 为与现有标准协调，将标准名称改为《网络安全技术 信息技术安全评估准则 第5部分：预定义的安全要求包》；
- 增加资料性附录 NA“缩略语”。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：中国信息安全测评中心、中国电子科技集团公司第十五研究所、中贸促信息技术有限责任公司、维沃移动通信有限公司、工业信息安全(四川)创新中心有限公司、吉林信息安全测评中心、国家广播电视总局广播电视科学研究院、北京神州绿盟科技有限公司、国民技术股份有限公司、广东

美的制冷设备有限公司、广东省农村信用社联合社、联想(北京)有限公司、中通服咨询设计研究院有限公司、成都虚谷伟业科技有限公司、北京东方金信科技股份有限公司、北京蓝象标准咨询服务有限公司。

本文件主要起草人：张宝峰、许源、杨永生、李凤娟、石竑松、高金萍、刘晖、霍珊珊、刘健、徐曼、李宾、刘尚麟、赵良福、赵珮含、肖丰佳、明玉琢、刘娟、戚进业、姚俊先、李汝鑫、王伟哲、乔华阳、张德保、毕海英、邓辉、贾炜、陈锋、王书毅。

本文件于 2001 年首次发布为 GB/T 18336.3—2001,2008 年第一次修订,2015 年第二次修订,本次为第三次修订,部分代替 GB/T 18336.3—2015,编号为 GB/T 18336.5。

# 引 言

本文件提供了预定义的安全要求包。安全要求包能有助于标准使用者在评估时保持一致,也能有助于减少开发保护轮廓(PP)和安全目标(ST)的工作量。

GB/T 18336 拟由五部分构成。

- 第 1 部分:简介和一般模型。旨在对 GB/T 18336 进行整体概述,定义信息技术安全评估的一般概念和原则,并给出了评估的一般模型。
- 第 2 部分:安全功能组件。旨在建立一套可用于描述安全功能要求的功能组件标准化模板。这些功能组件按类和族的方式进行结构化组织,通过组件选择、细化、裁剪等方式构造出具体的安全功能要求。
- 第 3 部分:安全保障组件。旨在建立一套可用于描述安全保障要求的保障组件标准化模板。这些安全保障组件按类和族的方式进行结构化组织,定义了针对 PP、ST 和 TOE 进行评估的准则,通过组件选择、细化、裁剪等方式构造出具体的安全保障要求。
- 第 4 部分:评估方法和活动的规范框架。旨在为规范评估方法和活动提供一个标准化框架。这些评估方法和活动包含在 PP、ST 及任意支持这些方法和活动的文档中,供评估者基于 GB/T 18336 的其他部分中描述的模型开展评估工作。
- 第 5 部分:预定义的安全要求包。旨在提供利益相关者通常使用的安全保障要求和安全功能要求的包,提供的包示例包括评估保障级(EAL)和组合保障包(CAP)。

GB/T 18336.1—2024 定义了术语“包”并描述了基本概念。

注:本文件在某些情况下使用粗体字和斜体字来区分术语和其余部分的文本。族内组件之间的关系约定使用粗体突出显示,对所有新的要求也约定使用粗体字。对于分层的组件,当要求被增强或修改,且超出了前一个组件的要求时,以粗体显示。此外,除了前面的组件之外,任何新的或增强的允许的操作也会使用粗体突出显示。约定使用斜体来表示具有精确含义的文本。对于安全保障要求,该约定也适用于与评估相关的特殊动词。





# 网络安全技术 信息技术安全评估准则

## 第 5 部分：预定义的安全要求包

### 1 范围

本文件给使用者提供了通用的安全保障要求包和安全功能要求包。

示例：

提供了评估保障级(EAL)和组合保障包(CAP)。

本文件描述了：

- 评估保障级包(EAL)，明确规定了可在 PP 和 ST 中引用的预先定义的一系列安全保障组件集，这些组件也用于为 TOE 评估提供适当的安全保障；
- 组合保障包(CAP)，明确规定了组合 TOE 评估所需的一系列安全保障组件集；
- 复合产品包(COMP)，明确规定了复合产品 TOE 评估所需的一系列安全保障组件集；
- 保护轮廓保障包(PPA)，明确规定了保护轮廓评估所需的一系列安全保障组件集；
- 安全目标保障包(STA)，明确规定了安全目标评估所需的一系列安全保障组件集。

本文件的读者包括安全信息技术产品的消费者、开发者和评估者。

### 2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 18336.1—2024 网络安全技术 信息技术安全评估准则 第 1 部分：简介和一般模型 (ISO/IEC 15408-1:2022, IDT)

ISO/IEC 15408-1 信息安全、网络安全和隐私保护 信息技术安全评估准则 第 1 部分：简介和一般模型 (Information security, cybersecurity and privacy protection—Evaluation criteria for IT security—Part 1: Introduction and general model)

注：GB/T 18336.1—2024 网络安全技术 信息技术安全评估准则 第 1 部分：简介和一般模型 (ISO/IEC 15408-1:2022, IDT)

ISO/IEC 15408-3 信息安全、网络安全和隐私保护 信息技术安全评估准则 第 3 部分：安全保障组件 (Information security, cybersecurity and privacy protection—Evaluation criteria for IT security—Part 3: Security assurance components)

注：GB/T 18336.3—2024 网络安全技术 信息技术安全评估准则 第 3 部分：安全保障组件 (ISO/IEC 15408-3:2022, IDT)

### 3 术语和定义

ISO/IEC 15408-1、ISO/IEC 15408-3 界定的术语和定义适用于本文件。

注：附录 NA 给出了本文件使用的缩略语。

4 评估保障级

4.1 族名

本族包的名称为评估保障级(EAL)。

4.2 评估保障级概述

4.2.1 概述

评估保障级(EAL)提供了一种递增的尺度,以保障程度的获取成本和可行性来权衡保障级别。ISO/IEC 15408-1 中的方法确定了 TOE 评估结束时不同级别的保障概念,以及 TOE 运行使用时维护该保障的概念。

注:并非所有 ISO/IEC 15408-3 中的族和组件都包含在 EAL 中。这并不意味着这些族和组件不提供有意义的和所需要的保障。相反,期望能把这些族和组件作为 PP 和 ST 中 EAL 的增强。另外,ISO/IEC 15408-3 中的一些类和 EAL 无关,如 APE 和 ACO 类。

每个 EAL 由一系列保障组件组成。

通过以下方式能获得比给定的 EAL 更高的保障级别:

- a) 增加来自其他保障族的额外的保障组件;
- b) 替换某个保障组件为相同保障族更高级别的保障组件。

4.2.2 保障和保障级之间的关系

图 1 表明了 ISO/IEC 15408-3 中的安全保障要求(SAR)和本文件定义的评估保障级之间的关系。当保障组件进一步分解为保障元素时,保障元素不能被保障级单独引用。

注:图 1 中的箭头表示 EAL 与保障类组件的引用关系。

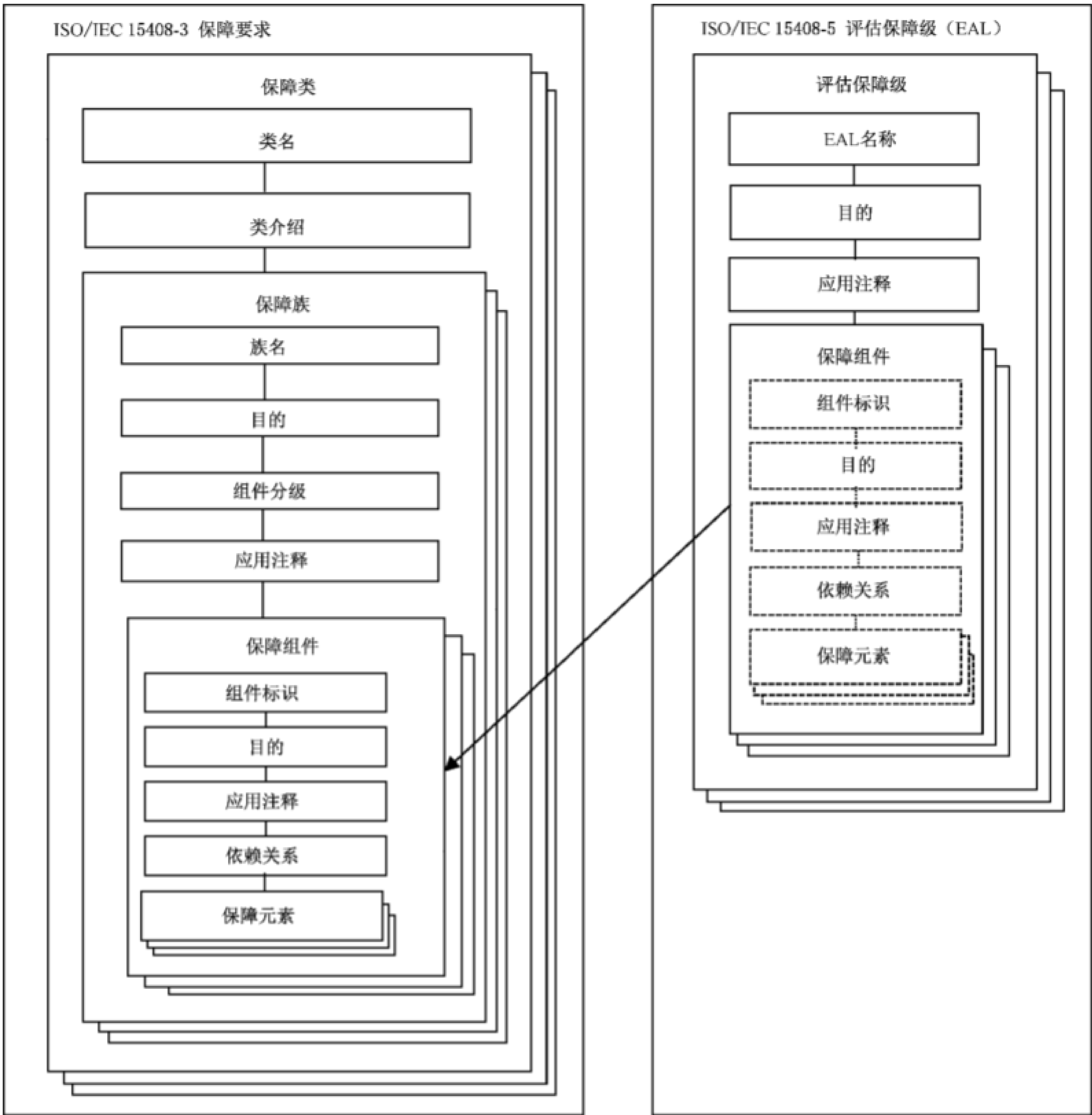


图 1 保障和保障级的关系

表 1 是对 EAL 的汇总。其中列表示一组按层级排序的 EAL,行表示保障族。表格矩阵中的每一个数字标识出了此处适宜的特定保障组件。

表 1 中涂灰的项目代表不适用该 EAL,但能作为该 EAL 包的增强。

注：虽然 ALC\_FLR 族和 ALC\_TDA 族未在表 1 中显示,但它们通常用作 EAL 的增强。

表 1 评估保障级汇总

保障类	保障族		评估保障级依据的保障组件						
			EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
开发	ADV_ARC	安全架构		1	1	1	1	1	1
	ADV_FSP	功能规范	1	2	3	4	5	5	6
	ADV_IMP	实现表示				1	1	2	2
	ADV_INT	TSF 内部					2	3	3

表 1 评估保障级汇总（续）

保障类	保障族		评估保障级依据的保障组件						
			EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
开发	ADV_SPM	安全策略模型						1	1
	ADV_TDS	TOE 设计		1	2	3	4	5	6
指导性文档	AGD_OPE	操作用户指南	1	1	1	1	1	1	1
	AGD_PRE	准备程序	1	1	1	1	1	1	1
生命周期支持	ALC_CMC	CM 能力	1	2	3	4	4	5	5
	ALC_CMS	CM 范围	1	2	3	4	5	5	5
	ALC_DEL	交付		1	1	1	1	1	1
	ALC_DVS	开发者环境安全			1	1	1	2	2
	ALC_LCD	开发生命周期定义			1	1	1	1	2
	ALC_TAT	工具和技术				1	2	3	3
ST 评估	ASE_CCL	符合性声明	1	1	1	1	1	1	1
	ASE_ECD	扩展组件定义	1	1	1	1	1	1	1
	ASE_INT	ST 引言	1	1	1	1	1	1	1
	ASE_OBJ	安全目的	1	2	2	2	2	2	2
	ASE_REQ	安全要求	1	2	2	2	2	2	2
	ASE_SPD	安全问题定义		1	1	1	1	1	1
	ASE_TSS	TOE 概要规范	1	1	1	1	1	1	1
测试	ATE_COV	覆盖		1	2	2	2	3	3
	ATE_DPT	深度			1	1	3	3	4
	ATE_FUN	功能测试		1	1	1	1	2	2
	ATE_IND	独立测试	1	2	2	2	2	2	3
脆弱性评定	AVA_VAN	脆弱性分析	1	2	2	3	4	5	5

4.3 评估保障级的目的

如 4.4 所述,本文件定义了七个层级的评估保障等级,用于对 TOE 的保障进行分级。它们按层级排序,每一个 EAL 比其较低级别的 EAL 体现了更多的保障。相对较高级别 EAL 保障的增强,是通过替换相同保障族中更高层次的保障组件(即增加严格性、范围和/或深度)来实现的,以及增加其他保障族中的保障组件(即加入新的要求)来实现的。

这些 EAL 由 ISO/IEC 15408-3 所描述的保障组件以适当的组合构成。更确切地说,每个 EAL 可包含每个保障族中的最多一个组件,并满足每个组件的所有保障依赖关系。

“增强”的概念是允许向一个 EAL 增加保障组件(来自尚未包含在 EAL 中的保障族)或替换保障组件(相同保障族中其他更高层次的保障组件)。在 ISO/IEC 15408-1 定义的保障结构中,只有 EAL 可增强。ISO/IEC 15408-1 认为,EAL 去除任一构成的保障组件是无效的。“增强者”有义务论证对 EAL 增加保障组件的实际意义和额外价值。一个 EAL 也可用扩展的保障要求来增强。

注：在声称精确符合 PP 的 ST 中的 EAL 是不能被增强的。

4.4 评估保障级

4.4.1 概述

4.4 提供了 EAL 的定义,用粗体字强调了各级特定要求和这些要求一般特征之间的差异。

4.4.2 评估保障级 1(EAL1)——功能测试

4.4.2.1 包名

本包的名称为评估保障级 1(EAL1)——功能测试。

4.4.2.2 包类型

本包为保障包。

4.4.2.3 包概述

EAL1 适用于需要对 TOE 正确运行有一定信心,但安全威胁又并不严重的情况。对于需要独立保障来支持个人信息或类似信息已得到应有保护的情况,EAL1 具有一定的价值。

EAL1 仅要求一个简化的 ST。该 ST 只要简单地说明 TOE 所需的安全功能要求(SFR),而不用通过从假设、威胁和组织安全策略(OSP),进而从安全目的来推导 SFR。

EAL1 提供了一个对客户可用的 TOE 的评估,包括根据规范进行的独立测试和对所提供的指导性文档的检查。其目的是,无需 TOE 开发者的帮助,即能成功进行 EAL1 评估,而且支出最少。

EAL1 评估提供了 TOE 功能与其文档一致的证据。

4.4.2.4 包目的

EAL1 通过简化的 ST 提供了基本级别的保障,并使用功能和接口规范以及指导性文档来分析该 ST 中的 SFR,以理解安全行为。

通过搜索公开域的潜在脆弱性和对 TOE 安全功能的独立测试(功能测试和穿透性测试)来支持该分析。

EAL1 还通过 TOE 和相关评估文档的唯一标识来提供保障。

与未经评估的 IT 产品相比,EAL1 在保障方面提供了有意义的增强。

4.4.2.5 保障组件

表 2 给出了 EAL1 包括的保障组件。

表 2 EAL1

保障类	保障组件
ADV:开发	ADV_FSP.1 基本功能规范
AGD:指导性文档	AGD_OPE.1 操作用户指南
	AGD_PRE.1 准备程序
ALC:生命周期支持	ALC_CMC.1 TOE 标识
	ALC_CMS.1 TOE CM 覆盖
ASE:ST 评估	ASE_CCL.1 符合性声明
	ASE_ECD.1 扩展组件定义
	ASE_INT.1 ST 引言
	ASE_OBJ.1 运行环境安全目的
	ASE_REQ.1 直接基本原理安全要求
	ASE_TSS.1 TOE 概要规范
ATE:测试	ATE_IND.1 独立测试——符合性
AVA:脆弱性评定	AVA_VAN.1 脆弱性调查



4.4.3 评估保障级 2(EAL2)——结构测试

4.4.3.1 包名

本包的名称为评估保障级 2(EAL2)——结构测试。

4.4.3.2 包类型

本包为保障包。

4.4.3.3 包概述

EAL2 需要开发者在交付设计信息和测试结果方面提供配合,但不应要求开发者付出超出良好商业惯例的努力。这样,就不需要增加过多的成本或时间投入。

EAL2 适用于这样的情况,即开发者或用户在没有完整开发记录的情况下需要取得低级到中级的独立安全保障。在加固遗留系统或开发者配合程度可能受限时会出现这种情况。

4.4.3.4 包目的

EAL2 在利用功能和接口规范、指导性文档和 TOE 结构的基本描述的基础上,通过分析一个完整的 ST 中的安全功能要求来提供保障,以理解安全行为。

EAL2 通过完备的 ST 和对该 ST 中的 SFR 分析来提供保障。使用功能和接口规范、指导性文档和 TOE 结构的基本描述,以理解安全行为。

通过对 TSF 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独立确认、证实可抵御具有基本攻击潜力穿透攻击者的脆弱性分析(基于功能规范、TOE 设计、安全架构描述和提供的指导性证据)等来支持 SFR 分析。

EAL2 还通过使用配置管理系统和安全交付程序证据来提供保障。

与 EAL1 相比,EAL2 通过要求进行开发者测试、脆弱性分析(除了公开域的搜索外)和基于更详细的 TOE 规范进行独立测试等内容,体现了对保障的有意义增强。

4.4.3.5 保障组件

表 3 给出了 EAL2 包括的保障组件。

表 3 EAL2

保障类	保障组件
ADV:开发	ADV_ARC.1 安全架构描述
	ADV_FSP.2 安全执行功能规范
	ADV_TDS.1 基础设计
AGD:指导性文档	AGD_OPE.1 操作用户指南
	AGD_PRE.1 准备程序
ALC:生命周期支持	ALC_CMC.2 CM 系统的使用
	ALC_CMS.2 部分 TOE CM 覆盖
	ALC_DEL.1 交付程序
ASE:ST 评估	ASE_CCL.1 符合性声明
	ASE_ECD.1 扩展组件定义
	ASE_INT.1 ST 引言

表 3 EAL2（续）

保障类	保障组件
ASE;ST 评估	ASE_OBJ.2 安全目的
	ASE_REQ.2 推导出的安全要求
	ASE_SPD.1 安全问题定义
	ASE_TSS.1 TOE 概要规范
ATE:测试	ATE_COV.1 覆盖证据
	ATE_FUN.1 功能测试
	ATE_IND.2 独立测试——抽样
AVA:脆弱性评定	AVA_VAN.2 脆弱性分析

4.4.4 评估保障级 3(EAL3)——系统地测试和检查

4.4.4.1 包名

本包的名称为评估保障级 3(EAL3)——系统地测试和检查。

4.4.4.2 包类型

本包为保障包。

4.4.4.3 包概述

EAL3 允许尽责的开发者在设计阶段不需要对现有合理的开发实践作实质性变更,就能从积极安全工程中获得最大限度的保障。

EAL3 适用于这样的情况,即开发者或用户需要中级的独立安全保障,同时要求在不进行实质性重新设计的情况下,对 TOE 及其开发过程进行彻底调查。

4.4.4.4 包目的

EAL3 通过完备的 ST 和对该 ST 中的 SFR 分析来提供保障,使用功能和接口规范、指导性文档和 TOE 设计的架构描述,以理解安全行为。

通过对 TSF 的独立测试、开发者基于功能规范和 TOE 设计进行测试的证据、对开发者测试结果的选择性独立确认、证实可抵御具有基本攻击潜力穿透攻击者的脆弱性分析(基于功能规范、TOE 设计、安全架构描述和提供的指导性证据)等来支持 SFR 分析。

EAL3 还通过使用开发环境控制、TOE 配置管理和安全交付程序证据来提供保障。

与 EAL2 相比,EAL3 通过要求对安全功能和机制和/或程序进行更完备的测试覆盖,以增加 TOE 在开发过程中不会被篡改的信心,体现了对保障的有意义增强。

4.4.4.5 保障组件

表 4 给出了 EAL3 包括的保障组件。

表 4 EAL3

保障类	保障组件
ADV:开发	ADV_ARC.1 安全架构描述
	ADV_FSP.3 带完整摘要的功能规范
	ADV_TDS.2 结构化设计
AGD:指导性文档	AGD_OPE.1 操作用户指南
	AGD_PRE.1 准备程序
ALC:生命周期支持	ALC_CMC.3 授权控制
	ALC_CMS.3 实现表示 CM 覆盖
	ALC_DEL.1 交付程序
	ALC_DVS.1 安全控制标识
	ALC_LCD.1 开发者定义的生命周期过程
ASE:ST 评估	ASE_CCL.1 符合性声明
	ASE_ECD.1 扩展组件定义
	ASE_INT.1 ST 引言
	ASE_OBJ.2 安全目的
	ASE_REQ.2 推导的安全要求
	ASE_SPD.1 安全问题定义
	ASE_TSS.1 TOE 概要规范
ATE:测试	ATE_COV.2 覆盖分析
	ATE_DPT.1 测试:基本设计
	ATE_FUN.1 功能测试
	ATE_IND.2 独立测试——抽样
AVA:脆弱性评定	AVA_VAN.2 脆弱性分析

4.4.5 评估保障级 4(EAL4)——系统地设计、测试和复查

4.4.5.1 包名

本包的名称为评估保障级 4(EAL4)——系统地设计、测试和复查。

4.4.5.2 包类型

本包为保障包。

4.4.5.3 包概述

EAL4 允许开发者基于良好的商业开发实践,从积极安全工程中获得最大限度的保障,虽然这些开发实践很严格,但并不需要大量的专业知识、技能和其他资源。EAL4 是改造现有产品线且可能在经济上可行的最高级别。

EAL4 适用于这样的情况,即开发者或用户在传统商品化的 TOE 中需要一个中级到高级的独立安全保障,并准备负担额外的安全专用的工程成本。

4.4.5.4 包目的

EAL4 通过完备的 ST 和对该 ST 中的 SFR 分析来提供保障,使用功能和完备的接口规范、指导性



文档、TOE 基本模块设计的描述和实现的子集,以理解安全行为。

通过对 TSF 的独立测试、开发者基于功能规范和 TOE 设计进行测试的证据、对开发者测试结果的选择性独立确认、证实可抵御具有**增强型基本**攻击潜力穿透攻击者的脆弱性分析(基于功能规范、TOE 设计、实现表示、结构性设计和提供的指导性证据)等来支持 SFR 分析。

EAL4 还通过使用开发环境控制,包括自动化在内的额外的 TOE 配置管理和安全交付程序证据来提供保障。

与 EAL3 相比,EAL4 通过要求更多的设计描述、所有 TSF 的实现表示和改进机制和/或程序,以增加 TOE 在开发过程中不会被篡改的信心,体现了对保障的有意义增强。

4.4.5.5 保障组件

表 5 给出了 EAL4 包括的保障组件。

表 5 EAL4

保障类	保障组件
ADV:开发	ADV_ARC.1 安全架构描述
	ADV_FSP.4 完备的功能规范
	ADV_IMP.1 TSF 实现表示
	ADV_TDS.3 基础模块设计
AGD:指导性文档	AGD_OPE.1 操作用户指南
	AGD_PRE.1 准备程序
ALC:生命周期支持	ALC_CMC.4 生产支持、接受程序和自动化
	ALC_CMS.4 问题跟踪 CM 覆盖
	ALC_DEL.1 交付程序
	ALC_DVS.1 安全控制标识
	ALC_LCD.1 开发者定义的生命周期过程
	ALC_TAT.1 明确定义的开发工具
ASE:ST 评估	ASE_CCL.1 符合性声明
	ASE_ECD.1 扩展组件定义
	ASE_INT.1 ST 引言
	ASE_OBJ.2 安全目的
	ASE_REQ.2 推导出的安全要求
	ASE_SPD.1 安全问题定义
	ASE_TSS.1 TOE 概要规范
ATE:测试	ATE_COV.2 覆盖分析
	ATE_DPT.1 测试:基本设计
	ATE_FUN.1 功能测试
	ATE_IND.2 独立测试——抽样
AVA:脆弱性评定	AVA_VAN.3 聚焦的脆弱性分析

4.4.6 评估保障级 5(EAL5)——半形式化设计和测试

4.4.6.1 包名

本包的名称为评估保障级 5(EAL5)——半形式化设计和测试。

4.4.6.2 包类型

本包为保障包。

4.4.6.3 包概述

EAL5 允许开发者以严格的商业开发实践为基础,适度应用专业安全工程技术,从安全工程中获得最大限度的保障。这样的 TOE 可能是以实现 EAL5 的保障为目的而设计和开发的。相对于没有应用专业技术的严格开发而言,由 EAL5 要求所带来的额外成本也许并不高。

EAL5 适用于这样的情况,即开发者或用户在计划的开发中需要高级别的独立安全保障,以及需要有严格的开发方法,以避免因专业安全工程技术而产生不合理的成本。

4.4.6.4 包目的

EAL5 通过完备的 ST 和对该 ST 中的 SFR 分析来提供保障,使用功能和完备的接口规范、指导性文档、TOE 的设计描述和实现,以理解安全行为。此外还需要模块化的 TSF 设计。

通过对 TSF 的独立测试,开发者基于功能规范、TOE 设计进行测试的证据,对开发者测试结果的选择性独立确认,证实可抵御具有中等攻击潜力穿透攻击者的独立的脆弱性分析等来支持 SFR 分析。

EAL5 还通过使用开发环境控制,包括自动化在内的全面的 TOE 配置管理和安全交付程序证据来提供保障。

与 EAL4 相比,EAL5 通过要求半形式化的设计描述、可分析的更结构化的体系架构和改进机制和/或程序,以增加 TOE 在开发过程中不会被篡改的信心,体现了对保障的有意义增强。

4.4.6.5 保障组件

表 6 给出了 EAL5 包括的保障组件。

表 6 EAL5

保障类	保障组件
ADV;开发	ADV_ARC.1 安全架构描述
	ADV_FSP.5 附加错误信息的完备的半形式化功能规范
	ADV_IMP.1 TSF 实现表示
	ADV_INT.2 内部结构合理
	ADV_TDS.4 半形式化模块设计
AGD;指导性文档	AGD_OPE.1 操作用户指南
	AGD_PRE.1 准备程序
ALC;生命周期支持	ALC_CMC.4 生产支持、接受程序和自动化
	ALC_CMS.5 开发工具 CM 覆盖
	ALC_DEL.1 交付程序
	ALC_DVS.1 安全控制标识
	ALC_LCD.1 开发者定义的生命周期过程
	ALC_TAT.2 遵从实现标准
ASE;ST 评估	ASE_CCL.1 符合性声明
	ASE_ECD.1 扩展组件定义
	ASE_INT.1 ST 引言

表 6 EAL5（续）

保障类	保障组件
ASE;ST 评估	ASE_OBJ.2 安全目的
	ASE_REQ.2 推导的安全要求
	ASE_SPD.1 安全问题定义
	ASE_TSS.1 TOE 概要规范
ATE;测试	ATE_COV.2 覆盖分析
	ATE_DPT.3 测试;模块设计
	ATE_FUN.1 功能测试
	ATE_IND.2 独立测试——抽样
AVA;脆弱性评定	AVA_VAN.4 系统的脆弱性分析

4.4.7 评估保障级 6(EAL6)——半形式化验证的设计和测试

4.4.7.1 包名

本包的名称为评估保障级 6(EAL6)——半形式化验证的设计和测试。

4.4.7.2 包类型

本包为保障包。

4.4.7.3 包概述

EAL6 允许开发者通过将安全工程技术应用于严格的开发环境中来获得高级别保障,以产生优质的 TOE 来保护高价值的资产免受重大风险。

EAL6 适用于开发在高风险环境下使用的安全 TOE,受保护资产的价值可证明额外成本的合理性。

4.4.7.4 包目的

EAL6 通过完备的 ST 和对该 ST 中的 SFR 分析来提供保障,使用功能和完备的接口规范、指导性文档、TOE 设计和实现,以理解安全行为。通过所选 TOE 安全策略的形式化模型,功能规范和 TOE 设计的半形式化描述,可进一步获得保障。此外还需要模块化、层次化和简单化的 TSF 设计。

通过对 TSF 的独立测试,开发者基于功能规范、TOE 设计进行测试的证据,对开发者测试结果的选择性独立确认,以及证实可抵御具有高等攻击潜力穿透攻击者的独立的脆弱性分析等来支持 SFR 分析。

EAL6 还通过使用结构化的开发过程、开发环境控制,包括完全自动化在内的全面的 TOE 配置管理和安全交付程序证据等来提供保障。

与 EAL5 相比,EAL6 通过要求更全面的分析、结构化的实现表示、更体系化的结构(如分层)、更全面的独立脆弱性分析,以及改进的配置管理和开发环境控制,体现了对保障的有意义增强。

4.4.7.5 保障组件

表 7 给出了 EAL6 包括的保障组件。

表 7 EAL6

保障类	保障组件
ADV:开发	ADV_ARC.1 安全架构描述
	ADV_FSP.5 附加错误信息的完备的半形式化功能规范
	ADV_IMP.2 TSF 实现表示的完全映射
	ADV_INT.3 内部复杂度最小化
	ADV_SPM.1 形式化 TOE 安全策略模型
	ADV_TDS.5 完全半形式化模块设计
AGD:指导性文档	AGD_OPE.1 操作用户指南
	AGD_PRE.1 准备程序
ALC:生命周期支持	ALC_CMC.5 高级支持
	ALC_CMS.5 开发工具 CM 覆盖
	ALC_DEL.1 交付程序
	ALC_DVS.2 充分的安全控制
	ALC_LCD.1 开发者定义的生命周期过程
	ALC_TAT.3 遵从实现标准——所有部分
ASE:ST 评估	ASE_CCL.1 符合性声明
	ASE_ECD.1 扩展组件定义
	ASE_INT.1 ST 引言
	ASE_OBJ.2 安全目的
	ASE_REQ.2 推导的安全要求
	ASE_SPD.1 安全问题定义
	ASE_TSS.1 TOE 概要规范
ATE:测试	ATE_COV.3 严格的覆盖分析
	ATE_DPT.3 测试:模块设计
	ATE_FUN.2 顺序的功能测试
	ATE_IND.2 独立测试——抽样
AVA:脆弱性评定	AVA_VAN.5 高级的系统的脆弱性分析

4.4.8 评估保障级 7(EAL7)——形式化验证的设计和测试

4.4.8.1 包名

本包的名称为评估保障级 7(EAL7)——形式化验证的设计和测试。

4.4.8.2 包类型

本包为保障包。

4.4.8.3 包概述

EAL7 适用于开发在极高风险环境中使用的安全 TOE,和/或资产的高价值可证明较高的成本。EAL7 的实际应用目前仅限于一些具有严密安全功能的 TOE,且这些功能适合进行广泛的形式化分析。



4.4.8.4 包目的

EAL7 通过完备的 ST 和对该 ST 中的 SFR 分析来提供保障,使用功能和完整的接口规范、指导性文档、TOE 设计和**结构化的实现表示**,以理解安全行为。通过所选 TOE 安全策略的形式化模型,功能规范和 TOE 设计的半形式化描述,可进一步获得保障。此外还需要模块化、层次化和简单化的 TSF 设计。

通过对 TSF 的独立测试,开发者基于功能规范、TOE 设计和**实现表示**进行测试的证据,对开发者测试结果的**完备的**独立确认,以及证实可抵御具有高等攻击潜力穿透攻击者的独立脆弱性分析等来支持 SFR 分析。

EAL7 还通过使用结构化的开发过程、开发环境控制,包括完全自动化在内的全面的 TOE 配置管理和安全交付程序证据等来提供保障。

与 EAL6 相比,EAL7 通过要求使用**形式化表示、形式化对应**来进行更全面的分析,以及要求**全面的测试**,体现了对保障的有意义增强。

4.4.8.5 保障组件

表 8 给出了 EAL7 包括的保障组件。

表 8 评估保障级 7

保障类	保障组件
ADV:开发	ADV_ARC.1 安全架构描述
	ADV_FSP.6 附加形式化描述的完备的半形式化功能规范
	ADV_IMP.2 TSF 实现表示的完全映射
	ADV_INT.3 内部复杂度最小化
	ADV_SPM.1 形式化 TOE 安全策略模型
	ADV_TDS.6 带形式化高层设计表示的完全半形式化模块设计
AGD:指导性文档	AGD_OPE.1 操作用户指南
	AGD_PRE.1 准备程序
ALC:生命周期支持	ALC_CMC.5 高级支持
	ALC_CMS.5 开发工具 CM 覆盖
	ALC_DEL.1 交付程序
	ALC_DVS.2 充分的安全控制
	ALC_LCD.2 可测量的生命周期模型
	ALC_TAT.3 遵从实现标准——所有部分
ASE:ST 评估	ASE_CCL.1 符合性声明
	ASE_ECD.1 扩展组件定义
	ASE_INT.1 ST 引言
	ASE_OBJ.2 安全目的
	ASE_REQ.2 推导的安全要求
	ASE_SPD.1 安全问题定义
	ASE_TSS.1 TOE 概要规范

表 8 评估保障级 7（续）

保障类	保障组件
ATE:测试	ATE_COV.3 严格覆盖分析
	ATE_DPT.4 测试:实现表示
	ATE_FUN.2 顺序的功能测试
	ATE_IND.3 独立测试——完全
AVA:脆弱性评定	AVA_VAN.5 高级的系统的脆弱性分析

5 组合保障包

5.1 族名

本族包的名称为组合保障包(CAP)。

5.2 组合保障包概述

5.2.1 规则

CAP 的结构与 EAL 的结构类似。这两种类型包的主要区别是其所适用的 TOE 类型不同。EAL 适用于部件 TOE,CAP 适用于组合 TOE。

一些依赖关系标识了对组合 TOE 活动所依赖部件进行评估期间所完成的活动。如果没有明确标识与依赖部件活动存在依赖关系,则依赖于组合 TOE 的其他评估活动。

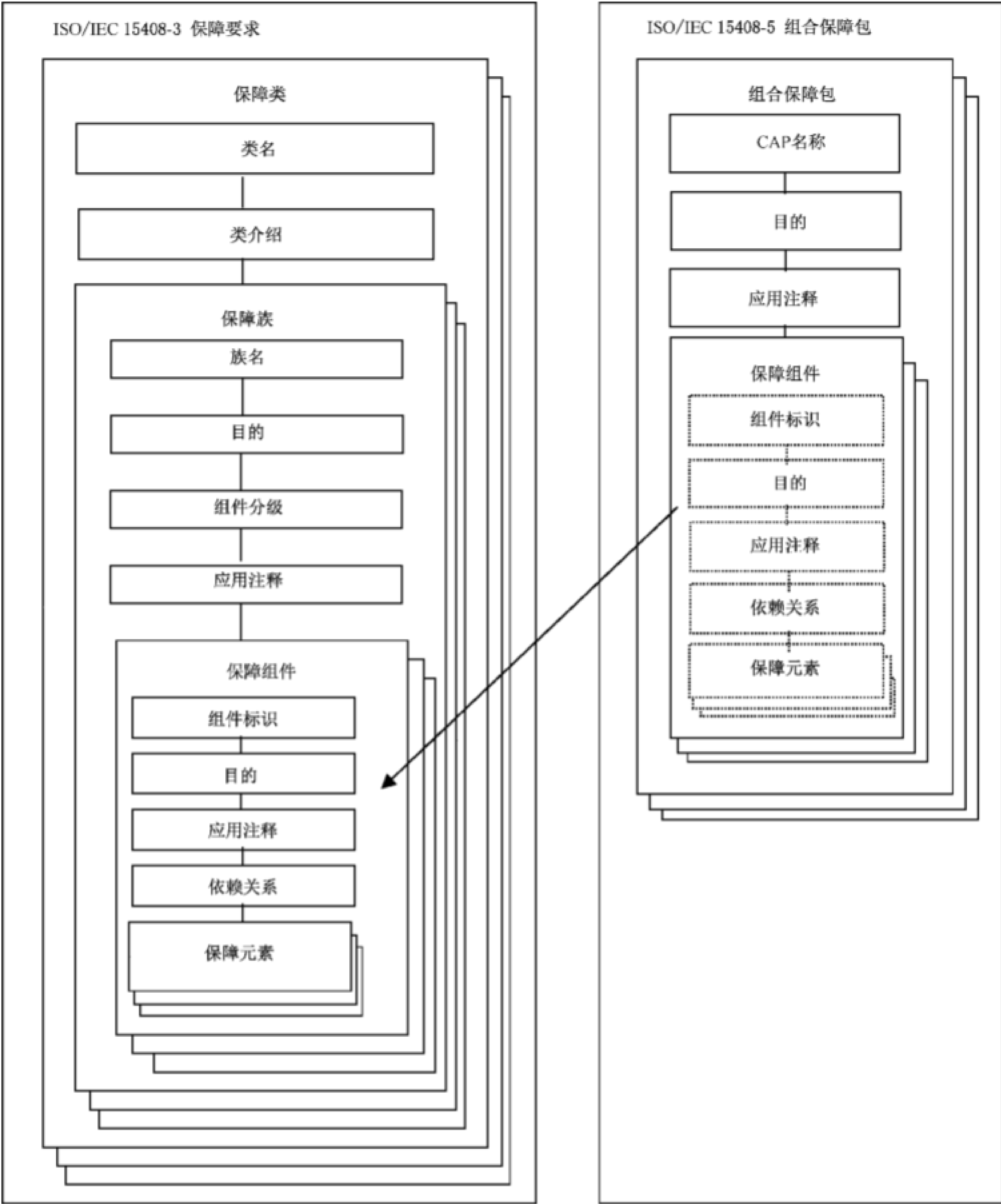
通过以下方式能获得比给定的 CAP 更高的保障级别：

- a) 增加来自其他保障族的额外的保障组件；
- b) 替换某个保障组件为相同保障族更高级别的保障组件。

ACO:CAP 保障包中包含的组合组件不应用于部件 TOE 评估的增强,因为它无法为部件提供任何有意义的保障。

5.2.2 保障和保障包之间的关系

图 2 表明了本文件中的 SAR 和本文件定义的 CAP 之间的关系。当保障组件进一步分解为保障元素时,保障元素不能被保障包单独引用。



注：图 2 中的箭头表示 CAP 与保障类组件的引用关系。

图 2 保障和组合保障包的关系

5.3 组合保障包的目的

CAP 提供了一个递增的尺度,来权衡所获得的保障级与达到该组合 TOE 保障程度所需的代价和可行性。

注：ISO/IEC 15408-3 中的族和组件仅有少部分被包括在 CAP 中。这是由于组合保障包是建立在先前已评估的实体(基础部件和依赖部件)之上,并不是说这些未被选择的族和组件不能提供有意义的和期望的保障。

CAP 应适用于组合 TOE,它由已经通过或正在进行部件 TOE 评估的部件组成(参见 GB/T 18336.3—2024 的附录 B)。各个部件通过 EAL 或在 ST 中指定的其他保障包进行认证。通过应用 EAL1,预计组合 TOE 可获得基本水平的保障,这能通过公共域中通常可获得的部件信息来实现。(部件和组合 TOE 都能应用 EAL1。)与应用 EAL1 以上的 EAL 相比,CAP 为组合 TOE 提供了一种替代方法来获

得更高水平的保障。

一个依赖部件能用一个先前已评估或认证过的基础部件来满足环境中的 IT 平台要求,但这种方式不提供任何关于部件之间的交互或组合是否会引入脆弱性的正式保障。组合保障包会考虑这些交互,并在更高的保障级别中确保部件之间的接口被纳入测试范围。同时,通过对组合 TOE 进行脆弱性分析来考虑部件组合引入脆弱性的问题。

表 9 是对 CAP 的汇总。其中列表示一组按层级排序的 CAP,行表示保障族。表格矩阵中的每一个数字标识出了此处适宜的具体保障组件。

如 5.4 所述,在本文件中为评定组合 TOE 的保障等级定义了三个层级的 CAP。它们按层级排序,每一个 CAP 比其较低等级的 CAP 体现更多的保障。相对较高级别 CAP 的保障增加,是通过替换同一保障族中的一个更高层次的保障组件(即增加严格性、范围和/或深度)和添加其他保障族的保障组件(即增加新的要求)来实现的。这些增加导致了对组合的更多分析,来确定对单个 TOE 获得的评估结果的影响。

这些 CAP 由 GB/T 18336.3—2024 的第 6 章所描述的保障组件以适当的组合构成。更确切地说,每个 CAP 包含每个保障族中的最多一个组件,并满足每个组件的所有保障依赖关系。

CAP 仅考虑能够抵御增强型基本攻击潜力的攻击者。这是由于通过 ACO\_DEV 能提供的设计信息级别限制了一些与攻击潜力有关的因素(组合 TOE 的知识),也影响了评估者能执行脆弱性分析的严格程度。因此,组合 TOE 的保障级别是有限的,尽管组合 TOE 中的单个部件的保障可以较高。

表 9 是对 CAP 的汇总。

表 9 组合保障包汇总

保障类	保障族	组合保障包依据的保障组件		
		CAP-A	CAP-B	CAP-C
组合	ACO_COR	1	1	1
	ACO_CTT	1	2	2
	ACO_DEV	1	2	3
	ACO_REL	1	1	2
	ACO_VUL	1	2	3
指导性文档	AGD_OPE	1	1	1
	AGD_PRE	1	1	1
生命周期支持	ALC_CMC	1	1	1
	ALC_CMS	2	2	2
ST 评估	ASE_CCL	1	1	1
	ASE_ECD	1	1	1
	ASE_INT	1	1	1
	ASE_OBJ	1	2	2
	ASE_REQ	1	2	2
	ASE_SPD		1	1
	ASE_TSS	1	1	1

5.4 CAP 族中的包

5.4.1 组合保障包 A(CAP-A)——结构组合

5.4.1.1 包名

本包的名称为组合保障包 A(CAP-A)——结构组合。



5.4.1.2 包类型

本包为保障包。

5.4.1.3 包概述

CAP-A 适于组合 TOE 是完整一体的,且需要对产生组合的正确安全操作具有信心。这要求依赖部件的开发者在交付设计信息和依赖部件认证的测试结果方面提供配合,但无需基础部件开发者的参与。

因此,CPA-A 适用于在缺乏现成可用的完整开发记录时,开发者或用户需要一种低到中等级别的独立保障的安全性的情况。

5.4.1.4 包目的

CAP-A 通过分析组合 TOE 的 ST 来提供保障。利用 TOE 组成部件的评估输出(如 ST、指导性文档等)和 TOE 组成部件之间的接口规范对组合 TOE 的 ST 中的 SFR 进行分析,以理解安全行为。

以下内容可为该分析提供支持:对依赖部件所依赖的基础部件接口(描述在依赖信息中)的独立测试,开发者基于依赖信息、开发信息和组合基本原理进行测试的证据,以及对开发者测试结果的选择性独立确认。由评估者进行的组合 TOE 的脆弱性审查也提供支持。

CAP-A 还通过组合 TOE 的唯一标识(即 IT TOE 和指导性文档)提供保障。

5.4.1.5 保障组件

表 10 给出了 CAP-A 包含的保障组件。

表 10 CAP-A

保障类	保障组件
ACO:组合	ACO_COR.1 组合基本原理
	ACO_CTT.1 接口测试
	ACO_DEV.1 功能描述
	ACO_REL.1 基本依赖信息
	ACO_VUL.1 组合脆弱性审查
AGD:指导性文档	AGD_OPE.1 操作用户指南
	AGD_PRE.1 准备程序
ALC:生命周期支持	ALC_CMC.1 TOE 标识
	ALC_CMS.2 部分 TOE CM 覆盖
ASE:ST 评估	ASE_CCL.1 符合性声明
	ASE_ECD.1 扩展组件定义
	ASE_INT.1 ST 引言
	ASE_OBJ.1 运行环境安全目的
	ASE_REQ.1 直接基本原理安全要求
	ASE_TSS.1 TOE 概要规范

5.4.2 组合保障包 B(CAP-B)——系统组合

5.4.2.1 包名

本包的名称为组合保障包 B(CAP-B)——系统组合。

5.4.2.2 包类型

本包为保障包。

5.4.2.3 包概述

CAP-B 可使尽责的开发者通过在子系统层面上,理解组合 TOE 各组成部件之间的交互影响,以获得最大程度的保障,同时最大限度地减少基础部件开发者的参与需求。

CAP-B 适用于开发者或用户需要一个中等级别的独立保障的安全性,以及无需进行大量的重新设计来对组合 TOE 及其开发过程进行彻底地调查的情况。

5.4.2.4 包目的

**CAP-B** 通过分析组合 TOE 的**完备** ST 来提供保障。利用 TOE 组成部件的评估输出(如 ST、指导性文档等),TOE 组成部件之间的接口规范,以及**包含**在组合开发过程中的**TOE 设计信息**(描述 TSF 子系统),对组合 TOE 的 ST 中的 SFR 进行分析,以理解安全行为。

以下内容可为该分析提供支持:对依赖信息(**现在也包括 TOE 设计**)中描述的依赖部件所依赖的基础部件接口的独立测试,开发者基于依赖信息、开发相关信息和组合基本原理而进行测试的证据,以及对开发者测试结果的选择性独立确认。评估者为证实组合 TOE 可抵御基本攻击潜力的攻击者而进行的脆弱性分析也提供支持。

与 CAP-A 相比,通过要求对安全功能进行更完整的测试覆盖,CAP-B 在保障方面体现了有意义的增强。

5.4.2.5 保障组件

表 11 给出了 CAP-B 包含的保障组件。

表 11 CAP-B

保障类	保障组件
ACO:组合	ACO_COR.1 组合基本原理
	ACO_CTT.2 严格的接口测试
	ACO_DEV.2 基本的设计证据
	ACO_REL.1 基本依赖信息
	ACO_VUL.2 组合脆弱性分析
AGD:指导性文档	AGD_OPE.1 操作用户指南
	AGD_PRE.1 准备程序
ALC:生命周期支持	ALC_CMC.1 TOE 标识
	ALC_CMS.2 部分 TOE CM 覆盖
ASE:ST 评估	ASE_CCL.1 符合性声明
	ASE_ECD.1 扩展组件定义
	ASE_INT.1 ST 引言
	ASE_OBJ.2 安全目的
	ASE_REQ.2 推导的安全要求
	ASE_SPD.1 安全问题定义
	ASE_TSS.1 TOE 概要规范

5.4.3 组合保障包 C(CAP-C)——系统组合、测试和复查

5.4.3.1 包名

本包的名称为组合保障包 C(CAP-C)——系统组合、测试和复查。

5.4.3.2 包类型

本包为保障包。

5.4.3.3 包概述

CAP-C 可使开发者从对组合 TOE 部件之间交互的实证分析中获得最大限度的保障,这虽然很严格,但不需要完全获得基础部件的所有评估证据。

CAP-C 适用于开发者或用户在常规商品的组合 TOE 中需要一个中到高级别的独立保障的安全性,并准备负担额外的安全专用工程费用的情况。

5.4.3.4 包目的

**CAP-C** 通过分析组合 TOE 的完备 ST 来提供保障。利用 TOE 组成部件的评估输出(如 ST、指导性文档等),TOE 组成部件之间的接口规范,以及包含在组合开发过程中的 TOE 设计信息(描述 TSF 模块),对组合 TOE 的 ST 中的 SFR 进行分析,以理解安全行为。

以下内容可为该分析提供支持:对依赖信息(包括 TOE 设计)中描述的依赖部件所依赖的基础部件接口(描述在包括 TOE 设计的依赖信息中)的独立测试,开发者基于依赖信息、开发相关信息和组合基本原理而进行测试的证据,以及对开发者测试结果的选择性独立确认。评估者为证实组合 TOE 可抵御**增强型基本攻击潜力**的攻击者而进行的脆弱性分析也提供支持。

与 **CAP-B** 相比,通过要求更多的设计描述和证实对更高攻击潜力的抵御能力,CAP-C 在保障方面体现了有意义的增强。

5.4.3.5 保障组件

表 12 给出了 CAP-C 包含的保障组件。

表 12 CAP-C

保障类	保障组件
ACO:组合	ACO_COR.1 组合基本原理
	ACO_CTT.2 严格的接口测试
	ACO_DEV.3 详细的设计证据
	ACO_REL.2 依赖信息
	ACO_VUL.3 增强的基本组合脆弱性分析
AGD:指导性文档	AGD_OPE.1 操作用户指南
	AGD_PRE.1 准备程序
ALC:生命周期支持	ALC_CMC.1 TOE 标识
	ALC_CMS.2 部分 TOE CM 覆盖
ASE:ST 评估	ASE_CCL.1 符合性声明
	ASE_ECD.1 扩展组件定义
	ASE_INT.1 ST 引言

表 12 CAP-C (续)

保障类	保障组件
ASE;ST 评估	ASE_OBJ.2 安全目的
	ASE_REQ.2 推导的安全要求
	ASE_SPD.1 安全问题定义
	ASE_TSS.1 TOE 概要规范

6 复合产品包

6.1 包名

本包的名称为复合产品包(COMP)。

6.2 包类型

本包为保障包。

6.3 包概述

COMP 提供了复合产品已根据相关标准进行组装和评估的保障。

6.4 目的

根据 GB/T 18336.1—2024 的第 14 章和 14.3.3,当复合评估技术用于复合产品时,保障组件\*, COMP 是适用的。目的是:

- 考虑 ISO/IEC 15408-1 和 ISO/IEC 15408-3 给出的要求,确保 TOE 由已评估的基础部件和依赖部件组成;
- 已根据 ISO/IEC 15408-3 规定的标准,对复合产品的 ST、生命周期要求、设计、测试和脆弱性分析进行了评估。

这些目的保障了由于产品的基础部件和依赖部件的复合而产生的潜在矛盾、不一致或安全差距已被考虑且不存在。

6.5 安全保障组件

表 13 中给出了 COMP 包所包含的安全保障组件。

表 13 COMP

保障类	保障组件
ASE;安全目标评估	ASE_COMP.1 安全目标一致性
ADV;开发	ADV_COMP.1 设计符合基础部件相关用户指南、复合评估 ETR 和基础部件评估机构报告
ALC;生命周期支持	ALC_COMP.1 依赖部件与相关基础部件的集成,交付和接受程序的一致性核查
ATE;测试	ATE_COMP.1 复合产品功能测试
AVA;脆弱性评定	AVA_COMP.1 复合产品脆弱性评定



7 保护轮廓保障

7.1 族名

本族包的名称为保护轮廓保障包(PPA)。

7.2 PPA 族概述

PPA 族为 PP 评估提供两个保障包：

- a) 评估直接基本原理 PP 的保障包；
- b) 评估标准化 PP 的保障包。

这些保障包提供的组件用于评估 ISO/IEC 15408-1 中所描述的每种类型的 PP。

表 14 是对 PPA 的汇总。列表示一组 PPA,行表示保障族。表格矩阵中的每一个数字标识出了此处适宜的具体保障组件。

这些 PPA 由 GB/T 18336.3—2024 的第 7 章所描述的保障组件以适当的组合构成。更确切地说,每个 PPA 可包含每个保障族中的最多一个组件,并满足每个组件的所有保障依赖关系。

表 14 PPA 汇总

保障类	保障族	PP 保障包的保障组件	
		保护轮廓保障包-直接基本原理(PPA-DR)	保护轮廓保障包-标准化(PPA-STD)
APE: 保护轮廓评估	APE_CCL	1	1
	APE_ECD	1	1
	APE_INT	1	1
	APE_OBJ	1	2
	APE_REQ	1	2
	APE_SPD	1	1

7.3 PPA 族目的

PPA 的目的是通过评估 PP 符合 ISO/IEC 15408-1 中给出的要求来支持提供保障。

7.4 PPA 包

7.4.1 保护轮廓保障包-直接基本原理

7.4.1.1 包名

本包的名称为保护轮廓保障包-直接基本原理(PPA-DR)。

7.4.1.2 包类型

本包为保障包。

7.4.1.3 包概述

PPA-DR 通过使用 ISO/IEC 15408-3 中规定的准则评估直接基本原理 PP 来提供保障。

7.4.1.4 目的

PPA-DR 适用于直接基本原理 PP 的评估。它能被用来验证直接基本原理 PP 是否符合 ISO/IEC 15408-

1 的要求。

7.4.1.5 安全保障组件

表 15 中给出了 PPA-DR 包所包含的安全保障组件。

表 15 PPA-DR

保障类	保障组件
APE:保护轮廓评估	APE_INT.1 PP 介绍
	APE_CCL.1 符合性声明
	APE_SPD.1 安全问题定义
	APE_OBJ.1 运行环境安全目的
	APE_ECD.1 扩展组件定义
	APE_REQ.1 直接基本原理 PP 模块安全要求

7.4.2 保护轮廓保障包-标准化

7.4.2.1 包名

本包的名称为保护轮廓保障包-标准化(PPA-STD)。

7.4.2.2 包类型

本包为保障包。

7.4.2.3 包概述

PPA-STD 通过使用 ISO/IEC 15408-3 中规定的准则,通过评估标准化 PP 来提供保障。

7.4.2.4 目的

PPA-STD 适用于标准化 PP 的评估。它能被用来验证标准化 PP 是否符合 ISO/IEC 15408-1 的要求。

7.4.2.5 安全保障组件

PPA\_STD 按照 ISO/IEC 15408-1 中规定的,通过对标准化 PP 的评估提供保障。表 16 中给出了 PPA-STD 中所包含的安全保障组件。

表 16 PPA-STD

保障类	保障组件
APE:保护轮廓评估	APE_INT.1 PP 介绍
	APE_CCL.1 符合性声明
	APE_SPD.1 安全问题定义
	APE_OBJ.2 安全目的
	APE_ECD.1 扩展组件定义
	APE_REQ.2 推导的安全要求

8 安全目标保障

8.1 族名

本族的名称为安全目标保障(STA)。

8.2 STA 族概述

- STA 族为 ST 评估提供两个保障包：
- a) 评估直接基本原理 ST 的保障包；
  - b) 评估标准化 ST 的保障包。

这些保障包提供组件用于评估 ISO/IEC 15408-1 中所描述的每种类型的 ST。

表 17 是对 STA 的汇总。列表示一组 STA,行表示保障族。表格矩阵中的每一个数字标识出了此处适宜的具体保障组件。

这些 STA 由 GB/T 18336.3—2024 第 9 章所描述的保障组件以适当的组合构成。更确切地说,每个 STA 可包含每个保障族中的最多一个组件,并满足每个组件的所有保障依赖关系。

表 17 STA 汇总

保障类	保障族	ST 保障包的保障组件	
		安全目标保障包-直接基本原理(STA-DR)	安全目标保障包-标准化(STA-STD)
ASE; 安全目标评估	ASE_INT	1	1
	ASE_CCL	1	1
	ASE_SPD	1	1
	ASE_OBJ	1	2
	ASE_ECD	1	1
	ASE_REQ	1	2
	ASE_TSS	1	1

8.3 STA 族目的

STA 的目的是通过评估 ST 对 ISO/IEC 15408-1 所给要求的符合性,来提供保障。

8.4 STA 包

8.4.1 安全目标保障包-直接基本原理

8.4.1.1 包名

本包的名称为安全目标保障包-直接基本原理(STA-DR)。

8.4.1.2 包类型

本包为保障包。

8.4.1.3 包概述

STA-DR 通过使用 ISO/IEC 15408-3 中指定的准则评估直接基本原理 ST 来提供保障。

8.4.1.4 目的

STA-DR 适用于直接基本原理 ST 的评估。它能被用来验证直接基本原理 ST 是否符合 ISO/IEC 15408-

1 的要求。

8.4.1.5 安全保障组件

表 18 中给出 STA-DR 包中包含的安全保障组件。

表 18 STA-DR

保障类	保障组件
ASE:安全目标评估	ASE_INT.1 ST 介绍
	ASE_CCL.1 符合性声明
	ASE_SPD.1 安全问题定义
	ASE_OBJ.1 运行环境安全目的
	ASE_ECD.1 扩展组件定义
	ASE_REQ.1 直接基本原理安全要求
	ASE_TSS.1 TOE 概要规范

8.4.2 安全目标保障包-标准化

8.4.2.1 包名

本包的名称为安全目标保障包-标准化(STA-STD)。

8.4.2.2 包类型

本包为保障包。

8.4.2.3 包概述

STA-STD 通过使用 ISO/IEC 15408-3 中规定的准则评估标准化 ST 来提供保障。

8.4.2.4 目的

STA-STD 适用于标准化 ST 的评估。它可被用来验证标准化 ST 是否符合 ISO/IEC 15408-1 的要求。

8.4.2.5 安全保障组件

STA\_STD 按照 ISO/IEC 15408-1 中规定的,通过对标准化 ST 的评估提供保障。表 19 中给出 STA-STD 包中包含的安全保障组件。

表 19 STA-STD

保障类	保障组件
ASE:ST 评估	ASE_INT.1 ST 介绍
	ASE_CCL.1 符合性声明
	ASE_SPD.1 安全问题定义
	ASE_OBJ.2 安全目的
	ASE_ECD.1 扩展组件定义
	ASE_REQ.2 推导的安全要求
	ASE_TSS.1 TOE 概要规范



附 录 NA  
(资料性)  
缩略语

- CAP:组合保障包(composed assurance package)
- CM:配置管理(configuration management)
- COMP:复合产品保障(composite product assurance)
- EAL:评估保障级(evaluation assurance level)
- ETR:评估技术报告(evaluation technical report)
- PP:保护轮廓(protection profile)
- PPA:保护轮廓保障包(protection profile assurance package)
- PPA-DR:保护轮廓保障包-直接基本原理(protection profile assurance package-direct rational)
- PPA-STD:保护轮廓保障包-标准(protection profile assurance package-standard)
- SAR:安全保障要求(security assurance requirement)
- SFR:安全功能要求(security functional requirement)
- ST:安全目标(security target)
- STA:安全目标保障包(security target assurance package)
- TOE:评估对象(target of evaluation)
- TSF:评估对象安全功能(TOE security functionality)

参 考 文 献

- [1] GB/T 18336.3—2024 网络安全技术 信息技术安全评估准则 第3部分:安全保障组件
-



中 华 人 民 共 和 国  
国 家 标 准

网络安全技术 信息技术安全评估准则  
第 5 部分：预定义的安全要求包

GB/T 18336.5—2024/ISO/IEC 15408-5:2022

\*

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.spc.net.cn

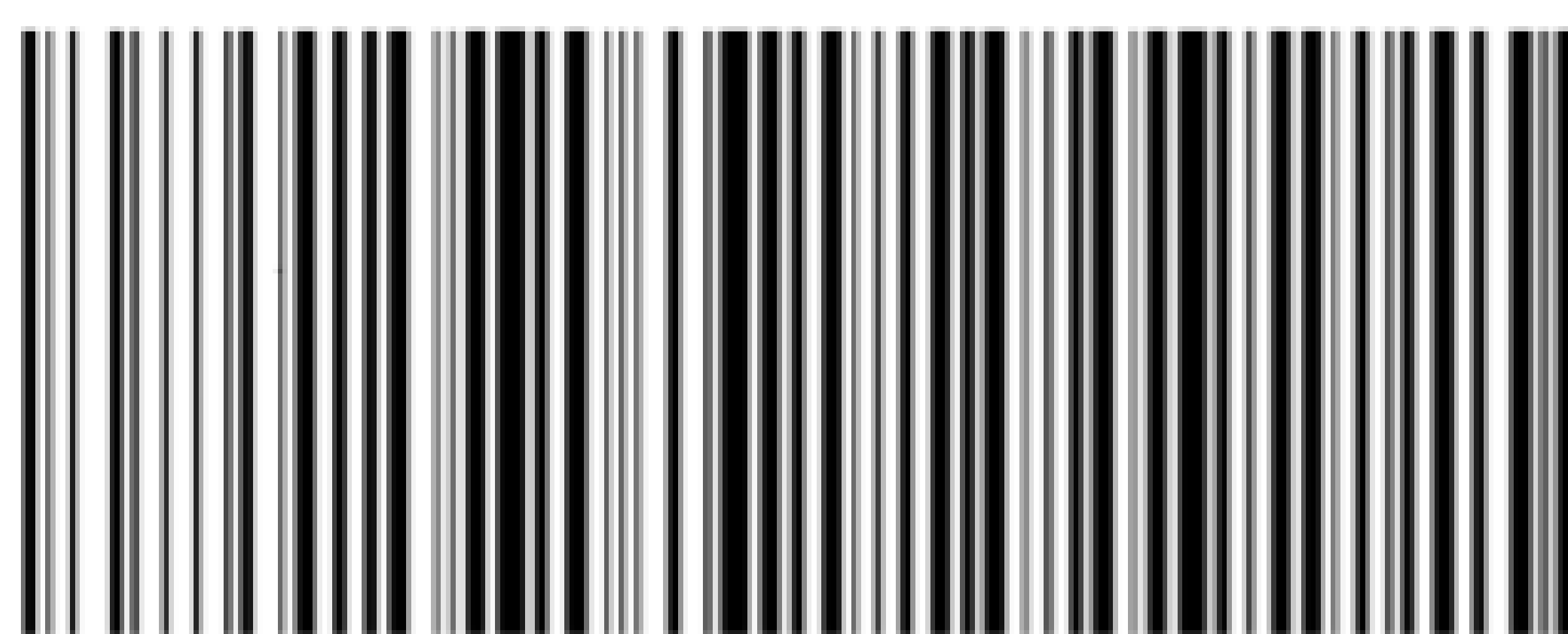
服务热线:400-168-0010

2024 年 4 月第一版

\*

书号:155066·1-75505

版权专有 侵权必究



GB/T 18336.5-2024

[www.bzxz.net](http://www.bzxz.net)

免费标准下载网