ICS 35.040
L 80

中华人民共和国国家标准化指导性技术文件

GB/Z 29830.1—2013/ISO/IEC TR 15443-1:2005

信息技术　安全技术
信息技术安全保障框架
第1部分:综述和框架

Information technology—Security technology—A framework for IT security assurance—Part 1:Overview and framework

(ISO/IEC TR 15443-1:2005,IDT)

2013-11-12 发布　　2014-02-01 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

中 华 人 民 共 和 国
国家标准化指导性技术文件
信息技术　安全技术
信息技术安全保障框架
第 1 部分：综述和框架
GB/Z 29830.1—2013/ISO/IEC TR 15443-1：2005
*
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.spc.net.cn
总编室：(010)64275323　发行中心：(010)51780235
读者服务部：(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230　1/16　印张 1.5　字数 38 千字
2014 年 4 月第一版　2014 年 4 月第一次印刷
*
书号：155066·1-48740　定价　24 00 元

目　　次

前　言

GB/Z 29830《信息技术　安全技术　信息技术安全保障框架》分为以下3个部分：

——第1部分：综述和框架；

——第2部分：保障方法；

——第3部分：保障方法分析。

本部分为GB/Z 29830的第1部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分采用翻译法等同采用ISO/IEC TR 15443-1:2005《信息技术　安全技术　信息技术安全保障框架　第1部分：综述和框架》。

本部分做了如下编辑性修改：

——国际标准2.9与2.16为重复性内容，转标时删除2.16。

本部分由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本部分主要起草单位：中国电子技术标准化研究院。

本部分主要起草人：罗锋盈、张明天、王延鸣、陈星、杨建军。

引　言

本指导性技术文件的目的是，为了获得一个给定交付件满足其所指出的信息安全保障需求的信心，给出各种保障方法，并指导信息安全专业人员如何选择一个合适的保障方法（或组合一些方法）。这一报告审视了不同类型组织所提出的保障方法和途径，包括已批准的标准和事实标准。

为了达到这一目的，本指导性技术文件由以下 7 个方面内容组成：

a) 一个框架模型，用于定位现有的保障方法并给出它们之间的关系；

b) 一组保障方法以及对它们的描述和引用；

c) 特定保障方法的共性和个性的表达；

d) 现有保障方法的定性比较，其中尽可能进行定量比较；

e) 与当前保障方法关联的保障模式的标识；

f) 不同保障方法之间关系的描述；以及

g) 有关保障方法的应用、组合和认知的指导。

本指导性技术文件由 3 部分组成，对保障途径、分析和相互间的关系处理如下：

第 1 部分：综述和框架。概述了一些基础性概念，例如保障、保障框架等，并给出了安全保障方法的一般性描述。其目的是帮助理解本指导性技术文件的第 2 部分和第 3 部分内容。第 1 部分针对信息安全管理人员和其他人员，其中包括负责开发安全保障程序、确定他们的交付件的安全保障、参加安全评估审计或参加其他保障活动的人员。

第 2 部分：保障方法。描述由不同类型的组织提出和使用的各种 IT 安全保障方法和途径，不论它们是被一般公认的、事实上被认可的或标准的；并把这些保障方法与第 1 部分的保障模型关联起来。重点是识别对保障有影响的保障方法的定性特征，在可能的地方，还将定义保障级别。该材料面向 IT 安全专业人员，帮助理解如何在产品或服务的特定的生存周期阶段中获得保障。

GB/Z 29830.2—2013 使用定义在 GB/Z 29830.1—2013 中的术语和定义。

该部分应与 GB/Z 29830.1—2013 一并使用。

第 3 部分：保障方法分析。分析了各种保障方法的保障特征。这个分析有助于保障机构在确定每一种保障途径的相对值并确定保障途径，使这些途径提供最适合于运行环境的具体上下文的需求的保障结果。而且，这个分析还有助于保障机构运用保障方法的结果，实现交付件所预想的确信度。这部分材料面向的对象是那些必须选择保障方法和保障途径的 IT 安全专业人员。

GB/Z 29830.3—2013 使用定义在 GB/Z 29830.1—2013 中的术语和定义。

该部分应与 GB/Z 29830.1—2013 一并使用。

本指导性技术文件分析了一些可能不为 IT 安全所专有的保障方法；然而，在指导性技术文件中所给出的指导将限于 IT 安全需求。只对 IT 安全领域提供相应的指导，并不期望这一指导对一般的质量管理、评估或 IT 符合性具有指导意义。

信息技术　安全技术
信息技术安全保障框架
第1部分：综述和框架

1　范围

1.1　意图

GB/Z 29830的本部分的意图是，以一种能使递增地获得交付件安全功能确信度的方式，按照一般生存周期模型，介绍交付件的安全保障方法、联系及其分类。

1.2　途径

本部分通篇采用的途径是，通过标识各种不同保障途径和保障阶段的框架，概述了一些所需要的基本概念和术语，以便理解并应用其中所涉及的保障方法。

1.3　应用

本指导性技术文件的第2部分和第3部分通过运用本部分有关保障方法的分类，指导读者针对一个给定的交付件，选择合适的保障方法以及可能的组合。

1.4　适用领域

本部分给出保障方法的分类指导，其中包括一些不是信息安全领域所特有的保障方法。在必要时，该标准可用于IT安全之外的一些领域。

1.5　限制性

本部分仅适用于交付件(参考4.3)及其相关组织信息安全问题。

2　术语和定义

下列术语和定义适用于本文件。

注：为支持本部分中的安全保障模型，给出的术语和定义尽可能具有一般性。保障模型要适用于范围宽泛的保障途径，这就要求不能把特定的术语应用于范围宽泛的保障途径。

为了满足一些可用的保障途径，已存在大量的保障术语，因此，为一个通用的保障模型定义术语是一项困难的任务。另外在现有的术语中，相似的术语具有不同的定义，并且许多术语是专为一些特定保障途径而定义的，因此为保障模型构建一个一般化的语言十分困难。面对这些困难，为了确保保障框架的固有特性，并为了适用于大量、广泛的保障方法，本指导性技术文件精心给出了术语和定义。特别地，为了保持与ISO/IEC 15408第1～3部分和ISO 9000系列标准的一致性，尽可能地采用相关的ISO标准。

接下来的一个困难是如何处理同一术语有多个定义，以及如何处理那些由于其一般性含义对保障模型不够充分而没有使用的定义。这些术语是否应予忽略或保留以便引用。如果忽略这些定义的话，在讨论中出现这些定义的保障途径时，会使读者产生困惑。如果保留特定于一种保障途径的术语，就会增加本指导性技术文件编排的复杂性；因此，本指导性技术文件在正确的上下文下来使用术语的适当定义。针对同一术语存在多个定义的情况，本指导性技术文件首先列出主要定义。可替代的定义，用半括号和斜体标出，它们仅适用于引用源的上下文。

2.1

认可　accreditation

权威机构针对以下三方面所关联的残余风险，给出正式的认知、批准和接受所采用的规程：

a) *有关一个自动化系统使用特定的一组安全措施，以特定安全模式的运行[引自 AGCA]；*

b) *有关一个安全团体或个人胜任执行特定的任务[引自 ISO/IEC 指南 2]，以及*

c) *有关一个安全服务适合于目标环境。*

2.2

途径　approach

处置一项任务或一个问题所使用的方法或采取的步骤。

2.3

评估　assessment

遵循一个标准，使用相应的方法，对交付件所进行的验证，以建立与标准的符合性并确定其保障。

2.4

保障　assurance

适当活动或过程的执行，以建立交付件满足其安全目标的信心。

a) *确信一个实体满足其安全目标的基本依据[ISO/IEC 15408-1]。*

2.5

保障途径　assurance approach

依据所检查的方面，对保障方法的一个分组。

2.6

保障论据　assurance argument

一个由证据和推理支持的、结构化的保障断言集合，该集合清晰地表明保障需求如何得以满足。

2.7

保障评估　assurance assessment

验证并记录与交付件关联的全部保障类型和保障值(是保障论据的一部分)。

2.8

保障机构　assurance authority

有权对交付件有关保障(例如，选择、规格说明、接受、增强)作出决策的组织或个人。其中，该保障最终导致该交付件信心的建立。

注：在特定的方案和组织中，保障机构的术语可能是不同的，例如评价机构。

2.9

保障证据　assurance evidence

由交付件(包括综合报告和其他理由)的保障分析而产生的、支持保障断言的工作产品。

2.10

保障等级　assurance level

依据特定尺度，保障方法所获得的保障值。

注 1：以定量术语，保障等级可能是不可测量的。

注 2：所取得的保障值一般与执行活动所付出的工作量有关。

2.11

保障方法　assurance method

关于获得可重复保障结果的、被认可的规格说明。

2.12

保障特性　assurance property

对保障结果起作用的保障方法的一个特征。

2.13

保障结果　assurance result

关于一个交付件的、文档化的定量或定性的保障陈述。

2.14

保障模式　assurance scheme

行政管理和规章制度的框架，在该框架内，特定团体或组织内的保障机构应用保障方法。

a）　*行政管理和规章制度的框架，特定团体内的评价机构在该框架下应用通用准则[ISO/IEC 15408 - 1]。*

2.15

保障阶段　assurance stage

一个给定的保障方法所关注的交付件生存周期阶段。交付件的整体保障要考虑该交付件整个生存周期所应用的所有保障方法的结果。

2.16

认证　certification

证实交付件与指定要求一致并给出正式保障声明的规程。认证可由第三方执行或自认证[引自ISO/IEC 指南 2:1996]。

a）　*发布正式声明——证实评价结果并证实正确应用了评价准则[ITSEC]。*

b）　*认证过程是对评估结果的独立审查，导致产生最终的认证或批准[ISO/IEC 15408-1]。*

c）　*对一个信息技术系统所做的技术和非技术的安全特征综合评价，支持建立系统满足指定安全政策程度的认可[AGCA]。*

2.17

信心　confidence

有把握认为交付件将以预期的或所声称的那样执行（即正确、值得信任、执行安全政策、可靠、有效）。

2.18

交付件　deliverable

IT 安全产品、系统、服务、过程、或环境因素（如，职员、组织）、或保障评价的对象。对象可以为 ISO/IEC 15408-1 所定义的保护轮廓（PP）或者安全目标（ST）。

注：ISO 9000:2000 认为服务是一类产品。而且，在 ISO 9000 系列标准中，采用“产品和/或服务”。

2.19

评价　evaluation

按已定义的标准对交付件的评估[ISO/IEC 15408-1]。

a）　*对一个实体能够满足指定要求程度的系统化检查（质量评价）[ISO/IEC 14598-1]。*

2.20

保证　guarantee

参考 2.35 条款有关担保的定义。

2.21

IT 安全产品　IT security product

提供一定安全功能的一组 IT 软件、固件和/或硬件，其设计是为了使用或为了组合到不同系统中[ISO/IEC 15408-1]。

2.22

生存周期阶段　life cycle stage

与交付件状态有关的生存周期的一个时段。

a) *与系统描述的状态和/或系统本身相关的系统生存周期中的一个时段[ISO/IEC 15288]。*

2.23

良源 pedigree

对供应商一种非正式的认知，即它们所提供的交付件，可重复地一贯满足其安全策略或如其所声称的那样执行。（良源是一个与供应商或交付件相关联的环境因素。）

2.24

过程 process

有序的活动集合，该集合使用一些资源，把输入转换为输出[ISO 9000:2000]。

2.25

过程保障 process assurance

对一个过程中的活动进行评价而导出的保障。

2.26

产品 product

参见交付件的定义。

2.27

模式 scheme

定义环境的一组规则，其中包括进行一次评估所要求的准则和方法学[ISO/IEC 18045(共同评价方法)]。

2.28

安全 security

与定义、实现和维护保密性、完整性、可用性、可核查性、真实性和可靠性等相关的所有方面[ISO/IEC 13335-1]。

注：产品、系统、或服务会被认为是安全的，其用户一定程度上就信赖它们会(或将会)按预期的方式运行。这通常在对一个实际的或可察觉的威胁进行评价中要予考虑的。

a) *软件产品保护信息和数据的能力，致使未经授权的个人或系统不能读取或修改信息和数据，而不拒绝授权个人或系统对信息和数据的访问[ISO/IEC 9126-1]。*

2.29

安全评估 security assessment

依据一个安全标准，采用相对应的安全方法，对安全交付件的验证，以建立与标准的符合性并确定安全保障。

a) *产品评价过程的最后一个阶段[ISO/IEC 14598-1]。*

2.30

安全元素 security element

一个不可分割的安全需求。

2.31

服务 service

由交付件、组织、或个人所执行的安全过程或任务。

2.32

利益攸关方 stakeholder

在交付件风险或在其特征的拥有方面，具有权利(共担风险或拥有资产)的一个团体，该权利满足该团体的需要和期望。

a) *在系统或它的特征拥有方面，具有权利(共担风险或拥有资产)的一个团体，该权利满足该团体的需要和期望[ISO/IEC 15288]。*

2.33

系统 system

具有特定的目的和运行环境的特定 IT 装置 [ISO/IEC 15408-1] 。

a) *为实现一个或多个所指出目的，有关交互元素的组合 [ISO/IEC 15288]* 。

注 1：系统可以看成是一个产品和/或产品所提供的服务 [ISO/IEC 15288] 。

注 2：在实践中，对系统含义的解释，经常通过使用一个关联的名词予以阐明，例如飞机系统(注：用名词“飞机”来阐明“系统”)。另一个途径是，词“系统”可以简单地通过一个上下文依赖的同义词来替代，例如飞行器，尽管这样做可能会隐晦系统原理的视角 [ISO/IEC 15288] 。

2.34

系统生存周期 system life cycle

系统从概念到消亡，随着时间的演进[ISO/IEC 15288]。

2.35

担保 warranty

当交付件不满足其安全策略时，对其操作(部署、执行或交付)进行纠正或缓解的一种安全服务。

2.36

工作产品 work product

为了开发并支持一个交付件，在执行任一过程期间所产生的所有项(即文档、报告、文件、数据等) [SSE-CMM (ISO/IEC 21827)] 。

a) *使用资源将输入转变为输出的系统活动的结果 [ISO 9001]* 。

3 缩略语

下列缩略术语适用于本文件。

AST	抽象安全目标(Abstract Security Target)
BSI	德国联邦情报局[Bundesamt fur Sicherheit in der Informationstechnik(German Information Security Agency)]
CASCO	ISO 合格评定委员会(ISO Committee on conformity assessment)
CEM	通用评价方法学(先于并等同于 NP N2729r1 IT 安全评价方法)Common Evaluation Methodology)
CMM	能力成熟度模型(Capability Maturity Model)
CSE	通信安全机构(加拿大 IT 安全机构)(Communications Security Establishment)
CTCPEC	加拿大可信计算机产品评估准则(由 CSE 编辑)(Canadian Trusted Computer Product Evaluation Criteria)
HCD	以人为中心的设计(Human Centered Design)
IEC	国际电工委员会(International Electrotechnical Commission)
IT	信息技术(Information Technology)
ISO	国际标准化组织(International Organization for Standardisation)
ITSEC	信息技术安全评估准则(欧洲共同体委员会官方文件发布办公室)(Information Technology Security Evaluation Criteria)
ITSEM	信息技术安全评估方法学 (欧洲共同体委员会官方文件发布办公室)(Information Technology Security Evaluation Methodology)
NSA	国家安全局(美国政府机构)(National Security Agency)
PP	保护轮廓(ISO/IEC 15408-1 定义)(Protection Profile)

RAMP	评定和维护阶段(根据 TCSEC 进行评估的 NSA 过程)(Ratings And Maintenance Phase)
RM	评定和维护阶段(根据 CTCPEC 进行评估的 NSA 过程)(Ratings and Maintenance phase)
SCT	严格(安全)一致性测试[Strict (Security) Conformance Testing]
SE-CMM	系统工程能力成熟度模型(能力成熟度模型是卡耐基-梅农大学的商标)(System Engineering Capability Maturity Model)
ST	安全目标(ISO/IEC 15408-1 中定义)(Security Target)
SSAM®	SSE-CMM 估值方法学(由支持组织提出),国际系统安全工程协会(ISSEA)里的一个实体(SSE-CMM Appraisal Methodology)
SSE-CMM®	系统安全工程-能力成熟度模型,ISO/IEC 21827(由国际系统安全工程协会的支持组织提交给 ISO 的公开标准)(System Security Engineering - Capability Maturity Model ISO/IEC 21827)
TCSEC	可信计算机系统评价准则(NSA 编辑)(Trusted Computer System Evaluation Criteria)
TOE	评估对象(ISO/IEC 的具体术语,定义在 ISO/IEC 15408-1)(Target of Evaluation)
TPEP	可信产品评价程序(TCSEC 和 CTCPEC)(Trusted Product Evaluation Program)
TRA	威胁和风险评估(Threat and Risk Assessment)

4 概念

本章介绍有关保障的概念,其目的是给出这些概念在一般 IT 保障和 IT 安全保障应用中的区别。有关保障的概念是宽泛的,不应特定化地应用于 IT 安全或应用于符合性评价。

4.1 为什么需要保障

由于错误和脆弱性,IT 系统易于失效和受到安全侵害。引起这些错误和脆弱性的主要原因是,快速变化的技术、人为错误以及不良的需求规约和不良的开发过程或低估威胁的结果。此外,由于系统的经常修改,新的缺陷和遭受新的攻击,导致脆弱性、失效和安全侵害在整个 IT 系统生存周期中不断增长。

由于人为错误或疏忽,由于部件或设备失效,以及由于相对的安全机制不完美,在可接受的成本和在 IT 系统生存周期的该交付件的时间限制内,无错误、无失效和无风险的运行通常是不可达到的。这一情况就使得几乎不可能保证一个 IT 系统是无错误的、无风险的安全系统。

由上可见,错误、脆弱性和风险可能始终存在,并可能在交付件的生存周期内发生变化。因此,在交付件的生存周期中,在可接受的参数范围内,必须对错误、脆弱性和风险进行管理,否则该可交付的保障就将发生变化。IT 安全工程和管理的任务就是管理风险,即采用技术上和组织上的安全措施,减少脆弱性和威胁,以使一个交付件具有可接受的保障。IT 安全管理还有一个另外的任务,即建立可接受的保障和风险目标。以这一方式,IT 系统的利益攸关方就有理由相信,该交付件在可接受的风险和预算内,将以预期的或所声称方式执行。从安全的观点上来看,这就形成该交付件实施了适用安全策略的信心。

4.2 保障与信心的区别

重要的一点是,保障和信心是不同的,并且是不可互换使用的。由于这两个术语关系紧密,因而经

常不能正确使用。对读者而言，重要的是要理解这两个术语之间的区别。从个体的角度来看，信心与人们对交付件的保障的信任程度相关，而保障则与交付件执行其安全目标的已予证实的能力相关。因此，信心不是一种确定性的心理属性，而是通过保障所创建的可信和相信来表达的。

保障是由交付件的评估过程所产生的证据来确定的。证据通常由保障论据、文档以及其他相关的工作产品组成，基于安全工程和评价活动，列举事实以支持所声称的保障。

信心受限于个体对交付件的特定安全要求的理解，并受限于在评价过程中所获得的有关交付件将以预期的或声称的方式运行的理解，还包括有关评价准则、评价方法、评价方案以及所使用的评价过程的理解。进一步，评估人员和操作人员的声誉，在建立交付件的信心上是重要的因素，因为他们的资历和经验是认可的或是不认可的。结果，由特定个人或机构所执行的给定保障方法之后，依据个体的理解，利益攸关方可能具有不同的信心程度。

4.3 什么是交付件

传统上，保障仅关联由硬件和软件组成的 IT 产品和系统，并称为产品或系统的保障。现已认识到，保障关注较大范围的风险，因此，对其他安全目标的保障，例如安全服务、过程、人员、组织以及环境因素，均存在一定的要求。为了强调这一新的需求，术语“交付件”用来专指安全评价的对象。

“交付件”的定义是宽泛的，根据具体情况，包含了列在合同中要交付给客户或为客户执行的安全项(如，服务)。合同条款可以包括购买的(可以是一类的或大批量生产的)、租赁的、用于培训的 IT 安全产品、服务以及其他有形或无形的安全项。进一步，还包括作为服务而提供的任何交付件——共享软件、免费软件、样本等，以及通过其他途径，或直接供给的，或间接(授权、抵押、良种等)供给的任何交付件，或由客户假定的任何交付件(良种、担保等)。交付件具有可度量的安全属性，以便可以验证是否满足其安全策略。比如，交付件可以特指一个由组织执行的威胁和风险评估服务，或特指一个有关评估个人是否具备运用 ISO/IEC 15408 标准资格的认证。执行安全服务或任务的人员，也被认为是交付件。例如，经培训已成为评估人员的那些人员，与培训组织有合同，为了获得知识和执行特定的活动，按照他们的能力进行度量和分级。类似地，在合同的范围内，执行一项服务或任务安全咨询人员也看作是交付件。

一些保障交付件，尽管它们已向保障机构提供不同的确信度，但并不总是以线性方式出现，因此它们必须被作为安全评估因素。例如，由供应商提供的担保或保证，就是一种以独立的或者是与交付件绑定在一起的形式提供的特定服务。如果交付件不满足安全策略，担保服务用于纠正或缓和交付件的操作(部署、执行或交付)。良源是一个与供应商或交付件关联的环境因素，尽管有些含糊，也不应当被忽略，因为它有被承认的特定执行的历史，例如，一贯地满足交付件的安全政策或满足供应商所声称的。

注：除了交付件的应用更广泛之外，这里的交付件的定义与 ISO/IEC 15408-1 定义的 TOE 相似。

4.4 利益攸关方

由于交付件为其资产带来风险的利益攸关方可能寻求保障，因此，确定可接受的保障方法和保障等级，可能是利益攸关方的要求或受其影响，具体如下所列：

a) 标准团体；
b) 国家的或者国际法律或规定；
c) 特定团体(比如政府和银行界)；
d) 一个组织内的授权单位；
e) 策略(安全、人事、供应、市场、认证政策，等)所有者；
f) 系统所有者；
g) 系统认可者；
h) 最终用户；以及

1) 一般公众。

4.5 保障需求

在 IT 技术安全术语中，准确的保障意味着：按规定的那样，通过选择的评估方法，执行合适的保障过程和活动，满足预先定义的特定安全保障需求。保障需求是由安全需求及其所导出的其他因素来确定的。

通过对交付件、影响因素、安全需求(策略)、业务驱动方以及该交付件目标环境的安全需求分析，确定安全保障需求。影响因素是那些需要予以关注的、可能影响交付件保障需求的方方面面。影响因素可以来自于任何方面，甚至可以是无形的，例如政治、文化、地方法律以及强制性要求。执行风险评估，是为了对资产敏感性、脆弱性和风险提供深入的了解，以便确定残余风险，并对现有的和已提出的安全措施给出建议。被采纳的建议就成为原安全需求中的要素，以便修正安全保障需求。

在 ISO/IEC 13335 和 ISO/IEC 17799 中，给出了有关安全管理和进行风险分析的一般性指导。ISO/IEC 15408 中包括了有关 IT 产品和系统的安全功能和保障需求的信息，这些信息是针对传统 IT 安全评估的。

由于业务是大量的，并且每一环境的安全需求也是大量的，因此保障需求往往是针对每一环境的，即环境不同，保障需求也不同。因此，同样交付件如果不修改的话，要满足不同的保障需求，可能就不适宜其他环境。

4.6 保障方法对 IT 安全的适用性

本节对 2.4 中的保障定义进行扩展，讨论保障的不同方面，为了证实保障的不同方面如何能应用于 IT 安全。

根据 2.4 中的保障定义可以看出，合适保障活动的应用，建立了该交付件满足其安全目标的信心。信心是通过对保障证据的评审来实现的，其中评估证据是通过开发、部署和运行期间的评估过程和活动而获得的，以及通过实际使用交付件的经验而获得的。任何能够减少不确定性的活动，由于产生可证实该交付件属性正确性、有效性以及质量的证据，因此在确定安全保障中这样的活动才是有用的。应认识到，一些类型的证据与其他类型证据相比，更清晰地建立了声明，但关键的是创建一个综合的保障论据，该论据坚实地建立了从所应用的保障方法中所获得的保障类型和保障值。在现有的许多保障方法中，仅有少量方法是针对 IT 安全的。然而，非 IT 技术安全保障方法也可能包含一些与 IT 安全保障有关的保障特性。由于只有少量可用的保障方法，因此重要的是要意识到所有保障方法的价值，因为许多非安全保障方法已应用于整个 IT 产业。保障证据经常是文档的形式，而这样的文档通常是在 IT 工程活动的过程中开发的。为了构造保障论据，只要能减少与特定交付件相关联的不确定性(风险)的任何东西均可使用，这是一项重要的考虑。

在这里，期望的是交流有关非信息技术安全保障方法的价值，而不是忽视 IT 安全保障方法的价值。显然后者是更优先的，然而一些保障只可能从许多源中获得，因此不能简单地因为该保障不是来自于已认可的安全保障方法而受到忽视。说到这，非常重要的是，当开发保障论据时，要了解证据源并考虑之。此外，必须熟知安全和保障需求，理解证据的价值及其证据源，以便确保证据满足它们的需要。

例如，虽然 ISO 9000 最初是为制造业组织制定的质量保障标准，但它还包括一些适用于软件的过程保障特性，并同样适用于 IT 安全软件产品和系统。与之相比，SSE-CMM(ISO/IEC 21827)是一个安全保障方法，尽管它不是传统的保障方法。这一方法通过评价组织的安全工程过程而不是直接评价交付件来产生保障。

一些保障方法特别关注定义一致并完整的安全特征集合，该集合经常反映一个标准威胁场景或好的实践。不同的保障方法可能有一些共同的部件或保障方面。

所有这些因素将对保障框架是有影响的，尤其是对度量的定义。保障方法之间的关系应考虑这些

因素。

4.7 保障模式

一个特定保障方法，可以以一种方式实施，其中强调了该方法予以执行的上下文，该上下文称为一个保障模式。认可的设施和评估人员，通过使用相应的保障方法，可以确保高水平的保障。如此的保障模式，还可为保障方法所获取的结果或结论被广泛的接受，提供一个基础。

4.8 保障风险量化与机制增强

保障并不“增加”交付件的任何安全装置或服务。因此，对于非安全的人员来说，有时理解投资保障可以使他们得到什么收益，这是困难的。例如，对于一个 IT 安全产品，往往争议保障是否有助于“增强”安全机制；然而，由于保障可以减少导致安全损害的威胁发生的不确定性(或可能性)，因此实际上保障有助于确信机制得以增强。例如，与单一口令相比，双因素认证经常被错误地认为它有更强的保障，实际上它仅是一种更强的认证机制。双因素认证是更强的机制是因为它验证两个用户属性，而口令机制验证一个属性。双因素认证本身并不提供保障，因为它是开发机制中的保障活动，有助于该机制的保障。

重要的是要理解保障并不自然地意味着好的安全，保障仅满足它的安全目的(安全策略)。换言之，保障提供了有关交付件执行其安全目的的信心，而没有检查安全目的是否合适地关注了风险和威胁。例如，尽管一个高保障的 IT 产品可以信任其满足它的安全目的，但该产品是否以一种安全方式行为，这依赖于这些目的的内涵。相反地，具有更合适目的的低保障产品，实际上可能更加安全。

4.9 保障减少安全风险

保障有助于减少风险，保障越多，减少与交付件的脆弱性所关联的不确定性就越多；因此，减少了潜在的脆弱性，就一定会降低与交付件关联的整体风险。如前一条款所讨论的，在对抗安全相关的风险方面，保障并不增加任何额外的安全控制，保障活动仅是试图证实交付件满足它的安全目的。这涉及与保障相关证据的产生和推理，以便为已实施的控制将会减少预期风险这一点提供信心。

4.10 量化保障

保障机构是在交付件生存周期的特定阶段做出有关决定的个人(或团体)。假定在交付件的生存周期中存在多个阶段和多个利益攸关方，那么就可能存在多个保障机构，每一个机构具有所授予的关注和明确的责任。例如，在开发阶段，保障机构可能是供应商组织中的安全工程师，其责任是确保为交付件构造合适的保障。同时，客户组织可以有他们自己的保障机构，这个保障机构则责任确保供应商组织关注了客户组织的保障需求。甚至在评价组织中，也可存在另一个保障机构，负责确保交付件满足保障模式。这里我们看到三个保障机构，每一个机构从不同的视角负责交付件的特定阶段。另外，一个保障机构可以负责多个阶段。在以上三个例子中存在这样的情况，即客户的保障机构是否还应负责接受认证机构所提呈的认证报告。

保障机构可针对所有类型的安全交付件，包括产品、系统、服务、过程或人员等。保障机构围绕交付件及其相关的组织目的，负责做出保障决定。

依据一个组织及其责任，保障机构可拥有任意多的职责。它们的某些任务可包括，选择合适的保障方法，标识为了满足它们的特定需求所要求的保障类型和保障值。保障机构还负责与其他组织的联络，例如与保障评价组织联络并讨论 IT 安全评价模式问题，如是否正在使用 ISO/IEC 15408 以及相对应的模式。

在某些组织中，尤其是在政府和军事组织中，保障可能是有规定的，限制选择保障值，并同时限制针对组织的风险。组织可以为保障机构指派不同的角色，并且根据组织特定的运行模型保障机构的职责

可能是有区别的;然而,保障机构一定总要负起所要求的职责。在规模不大的组织里,一个雇员除了承担保障机构责任之外,通常可能还有其他的职责;而在规模较大的组织里,可能指定一个雇员来承担保障机构的角色。在更大一点的组织里,通常指定一个高级雇员作为保障机构,负责保障方法的实施和保障结果。

依据组织具体情况,负责最终接受保障结果的人,还可能负责交付件的运行(即把交付件放入系统中并使之运行,或接受所交付的服务)。因此,保障机构经常必须在所执行保障的广度和深度之间,确定一个合适的程度,并确定与此相关的评价活动的成本和时间框架。

5 选择安全保障

选择一个安全保障方法和相对合适的保障值,这是一个决策问题,该决策应基于组织的安全保障策略、业务需求以及交付件的类型(即产品、过程、环境、系统、服务或人员)。例如,一些保障方法仅适用于过程[即 SSE-CMM (ISO/IEC 21827)],而一些其他方法适用于产品(即 ISO/IEC 15408)。

所选择的保障方法应与组织的环境相一致,并且能够检查交付件所期望的属性和生存周期阶段。保障方法的选择必须考虑可用的资源(时间、人员、预算等),以便确保耗费的资源对于所获得保障的类型和值是合理的。例如,为一个低保障的交付件,增加 50 000 美元的安全设施,这就是不合理的。类似地,当一种较低的保障方法是可接受的(假定没有强制一种评估方法),并可节省数月进度的话,那么就没有必要选择像 TCSEC、ITSEC、CTCPEC,ISO/IEC 15408 等评估保障方法。对于要求选择开发过 IT 安全产品并为了获得保障而使用已经 IT 安全评价产品的组织(即政府部门)而言,为了做出有关保障方法选择的决策,几乎没有多少需求,从而可省去考虑选择所花费的大部分甚至全部的资源。

例如,一个私营组织可以采用 SSE-CMM (ISO/IEC 21827)保障方法,建立他们公司网站的保障,防止未经授权的人访问他们的私有部分。这将围绕网站的开发、部署以及运行,要求一个过程评估,包括实现安全策略和运行安全策略的过程。基于评估的发现,可产生一个保障论据以及该组织的成熟度等级[SSE-CMM (ISO/IEC 21827)]。当只需要保障机构关注他们内部的安全保障策略时,采用这个保障方法也就足够了。第二个例子是一个政府部门使用 ISO/IEC 15408 保障方法来建立高的保障,因为要求该部门使用这一特定的保障方法和途径来满足特定的政府安全需求。这个例子说明,保障机构和组织及其安全保障策略必须是相互依赖的。关于哪一种保障方法更好或哪一种保障方法能够提供更大的保障,对此是无法描述的。在现有政策或规章制度并没有规定特定保障方法和保障等级的地方,作为安全目的的功能而选择的保障方法和保障等级,必须要能够达到相应安全需求的保障需求。然而,有可能安全风险管理指出一些情况,其中要求像什么一样大的保障,如果安全风险管理已强调高水平的不确定性,那么增强的保障就有益于减少整体的不确定性,因而也就降低了安全风险。在这些情形中,要指明增强的保障。

注意,即使保障方法是强制的时候,也存在一些可用的选择,例如:

a) 保障什么;

b) 保障值;

c) 要使用哪一个评价实验室;以及

d) 要采用哪一种认证认可服务。

存在许多不同的保障途径和方法,可用于几种被广泛接受或规约的保障方法中。因此,需要给出相应的指导,以支持利益攸关方来选择并应用一种保障方法。

5.1 保障需求描述

在选择和/或执行保障方法之前,必须规约保障需求。已有一些方法可用于产生保障需求规格说明。一般地,TRA 和组织上的安全保障需求可支持选择保障方法。保障需求还可包括区域上的和业务

上的一些方面，例如，当客户需要一个特定的保障途径（如 ISO/IEC 15408）来满足内部需求或采购需求时。

为了强调组织需求或市场需求，保障需求规格说明可包括对保障方法或保障模式的认知和接受，以及对相互认可和最低保障等级的认知和接受。

例如，保障需求包括对开发过程严格程度的限制，以及（或）探索有关潜在安全脆弱性影响分析的需求。

当交付件包括诸如口令和杂凑函数等安全机制时，保障需求可以依据所声称的安全目的，规定一个最小的强度等级约束。

保障需求规格说明应强调组织上的所有需求，并包含所有相互支持的保障成分，例如正确性保障和有效性保障。另外，需要详细地表述可接受的保障途径和方法，并要指明保障机构、它们的职责以及沟通渠道等。

5.2 经济方面

保障通常是需要密集资源的，因而带来成本和延时等问题。另外，保障往往是防止损失而不是提供收益或获利。因此对其投资回报是不可测量的，但可假设类似于保险损失。即使供应者在大量 IT 安全产品之上摊还保障的时候，还要依据保障方法和所期望的保障水平，可能需要几年的时间才能收回投资。有关组织能在保障的资源投资得到收益方面，对于不熟悉安全问题的人而言是不明显的，因此需要大量的解释，并必须予以很好地表达，以获得管理层的批准。

不同形式的保障是针对不同对象的。例如，由担保所提供的保障，当系统宕机时，对于用户而言其价值是很小的；但对管理者而言，担保在支付延时的成本中是有价值的。类似地，由技术支持措施所提供的保障，如果系统运行功能时失败，则其价值是很小的，而对系统的操作故障，就是有价值的。

所有形式的保障为组织的不同部门带来不同的收益；不对这些不同的收益进行评价将会贬值所获得的保障。

实际上所做的保障减少了不确定性，至少减少了与 IT 安全产品或服务所关联的脆弱性。不确定性是与评价安全风险评价中所使用的所有因素相关联的。因此，减少不确定性，就可集中关注对组织的真正最大风险。这表明了组织的可测量收益以及有益的资源投入。

5.3 组织方面

重要的是要认识安全环境，尤其是要理解保障需求反映了组织文化和业务需求。必需理解组织的需求，以便决定一个特定的保障方法是否是可接受的，以及（或）多少保障才是充分的。组织策略应描述以下内容：

a) 如何确定保障需求；
b) 依据特定标准认证交付件的情况；
c) 认证交付件所依据的标准；
d) 在指定情况中，认证过程所要求的保障等级；
e) 保障机构的责任；以及
f) 交付件必须进行认证的情况。

例如，政府组织可以为其特定的环境来决定规约的保障过程以及控制的保障过程。他们可以开发这些过程的所有方面，例如保障方法、准则（标准）、使用的指导标准、执行的评价，甚至所要求的保障等级。然而，负责认证的保障机构仍需要做出接受保障的最终决定，并且考虑资源和进度。与之相比，私人组织可以选择一个为其内部而开发的事实上的保障方法，如果不要求其保障机构来满足外部影响的话。当验证安全保护措施和保障是否适合该组织时，对于描述需要什么以及对什么具有影响等而言，组织策略是至关重要的。

5.4 保障类型

针对一个特定的交付件，为了强调多种保障方法的组合，最好构建一个安全保障模型，以便显示期望一些不同的保障类型如何一起工作，以利于该交付件所关联的整体保障。因此，交付件的安全保障模型可以由一些不同的子保障模型组成，每一个子模型对应一个特定的保障途径（即评价保障、过程保障、开发保障）。通过组合多个不同保障模型的这种方式，交付件的保障模型将只关注这些保障子模型如何组合在一起，而不管交付件的阶段所对应子模型的应用。进一步，可能存在这种情况，即与该交付件关联的某个安全保障，对该交付件下一个接受者而言并不是直接期望的，但实际上是最后接受者所期望的。该模型可清晰地显示这一点，并有助于确保最后接收者接受一个相关的安全保障的清晰轮廓。

因此，每一个保障模型可以针对交付件的一个特定生存周期阶段，规约相应的保障类型和保障值，以方便进行比较。通过描述这样的交替并给出相应的理由，该交付件的保障模型就将一些不同的子模型粘合在一起，以便描述该交付件最终结果的保障。

5.5 技术方面

已有许多保障方法可供选择，并依据资源和时间框架，提供可能的优化。应根据以下列表来选择保障方法，看其是否适合交付件及其要予评价的属性：

a) 专门针对诸如 IT 安全硬件或软件产品、系统、网络、人员、服务等可用的保障方法；

b) 针对生存周期过程的保障方法；或

c) 基于经验和实际用法的保障方法。

应用一种保障方法来评价交付件，可能会产生不同类型保障或保障值，由于：

a) 交付件的特征或交付件匮乏；

b) 交付件的规模和复杂度；

c) 所应用的保障方法中的差异；

d) 应用保障方法时所具有的受限严格程度或工作量；

e) 要满足的安全目标的本意；

f) 特定环境；

g) 特定 IT 生存周期阶段；或

h) 与其他方法的组合。

增强交付件的保障可以通过下面获得：

a) 增强交付件以前存在的 IT 安全能力的知识；和/或

b) 改善交付件 IT 安全机制的能力。

依据单个安全需求，每一个保障方法都有其自己的应用以及优缺点。因此就必须了解每一个保障方法是如何建立保障的，以便决策该保障方法是否满足相应的保障需求。

例如，当部署一个系统，组成一个产品集合（依据所使用的保障方法，它们的保障等级可能了解或接受，也可能不了解或不接受）时，有关保障可认知的程度一般是由运行前的系统认证予以确定的。

技术上的考虑会影响这一决策，因为相对于复杂一点的交付件，某些保障方法可能对简单的交付件要更好一些。例如，与验证一个具有数百万行代码组成的安全功能的交付件相比，通常更容易验证一个数千行代码交付件所具有的最小安全功能，并达到一个高保障结果。

对于一种特定的保障方法而言，其可能的保障类型和保障程度是由该保障方法的特征确定的，即所评价的特定生存周期阶段以及所评价的安全元素。

5.6 优化方面的考虑

确定所需要的保障方法和保障值，不存在一门精确的科学。为了满足组织的需求，需要由保障机构来确定正确的保障方法以及相应的保障值。但最终必须考虑 IT 系统和保障方法的属性。

如果应用了多个保障方法，就给出了多个值，以便在交付件被接受之前使最后那个保障方法导出最后的保障结果。因此，最后保障方法的保障机构必须定量地给出当前保障结果，并必须做出判断，先前的任意保障结果是否令人满意。另外，作为最后保障活动的机构，它们将最终负责交付件的运行。

通过 IT 安全产品的供应商、系统集成者或服务提供者，就该产品和服务的性能，以某种形式的保证和担保，可以递增地导出保障。

对于具有准确保障的交付件，应当特别注意，把一个或多个交付件集成到它们最后目标环境中，一般对产生的安全保障等级具有负面影响，因此可能需要额外的保障。

6 框架

6.1 保障途径

在高层次上，保障方法可分为三类保障途径：

a) 交付件评价，即历经评估和测试；

b) 过程评价，用于开发或生产交付件；以及

c) 环境评价，例如人员和设备的评价。

交付件评价包括对交付件（产品、系统、服务等）的检查。在这种情况里，这些保障方法独立于开发过程，检查交付件及其所关联的安全设计文档。

过程评估包括对整个交付件生存周期（开发、部署、交付、测试、维护、处置等）的生产和运行中所采用的组织过程的检查。通过对人们已执行的、影响交付件开发质量和实现质量的过程的推断，来获得保障，因此当把这一检查应用于 IT 安全交付件时，就产生该交付件的安全保障。

环境评价包括对环境因素的检查，其中，这些环境因素应有助于过程质量和交付件的生产（环境评价并不直接检查交付件或过程）。这些因素包括人员和物理设备（开发设备、生产设备、交付设备和运行设备等）。

注：相比较，一些保障途径，例如通过应用评估准则（如 ISO/IEC 15408）所获得的评估保障，直接在 TOE 的生存周期的一个子集上评价 TOE，并提供唯一一种组合保障。

例如，ISO/IEC 15408 直接检查 TOE，并产生评价保障，就开发保障、评价保障和测试保障这一集合而言，该评价保障是得到共识的，而 ISO 9001 关注于制造过程的检查。

6.2 保障方法

本指导性技术文件涵括了宽泛的、现有的用于获取保障的方法。这包括国内的或国际的正式标准、事实上的标准，以及其他已被认可的方法，它们具有或利用规范化的和系统的方法。

事实标准的一个例子是 SSE-CMM 评估方法（SSE-CMM Appraisal Method），它是一种良好文档化的保障方法；然而，它不是一个国内的或国际的标准。事实标准的另外一个例子是可信产品评价过程（Trusted Product Evaluation Process，TPEP）保障方法。尽管 TPEP 是一个被一些政府成功应用于 IT 安全产品评估的可接受标准，它却是一个无合适文档化的评估方法。

保障方法依据其技术和关注的生存周期，产生相应类型的保障，通过保障途径，支持对保障类型进行分类。根据保障方法的关注和途径，表 1 列出了一些广为人知的保障方法。在这一标准的最后部分，包含了有关保障方法的的更全面的列表，并强调了技术细节和比较。

表 1　保障方法示例

保障途径	保障关注点	保障方法例子(包括相应的准则或模型)
过程	质量和开发过程	ISO 9000 ISO/IEC 15504 HCD SSAM [SSE-CMM (ISO/IEC 21827)]
交付件、过程、环境	品牌-(基于历史关系或数据)承认公司会生产高质量的交付件	开发者良源
交付件	保险(由制造者承诺对交付件的错误进行纠正而得到支持)	担保保障
交付件	自我声明	供应者的声明
环境	职员的知识和技能	专业认证及许可 安全设备
交付件	交付件的直接评价	CEM (ISO/IEC 18045) ITSEM (ITSEC) TPEP (TCSEC) TPEP (CTCPEC) 等级维护[RAMP (TCSEC)] 等级维护[RM (CTCPEC)] 认证和鉴定保障 ISO/IEC 14598-1 软件产品评估
交付件、过程、环境	安全管理	信息安全管理系统　使用规范和指南(BS 7799.2) GISA/BSI 基线保护指南 ISO/IEC 13335 ISO/IEC 17799

6.3　生存周期方面

由于人为错误、设备失败、新的弱点以及威胁能在交付件的任一生存周期内发生,交付件的每一个生存周期阶段(如,概念、开发、集成、部署、运行和处置)都要求有合适的保障。因此保障方法必须适合于特定的阶段。

功能的匮乏、要求的改变、以及新的脆弱性都会影响保障,并要求再次引入更为早期的生存周期阶段。所以生存周期模型必须允许阶段之间的重复、交叠和迭代关系。

生存周期模型样例(图 1)用于证实保障方法与交付件生存周期阶段的关系。该生存周期模型样例包括了四个基本阶段,一般可映射到任意特定的生存周期模型。尽管图 1 中的每一个阶段的图示是相似的,但由于所采用的保障方法是不同的,因此这些阶段的活动和反馈将会是不同的。例如,一些保障方法采用包含于运行阶段的维护阶段方法(如 TPEP 评定维护),以强调只影响运行上保障的失效和变更需求。这个例子证实了该模型可支持特定的保障方法,该方法指示反馈是给其本身所在的阶段还是给交付件开始的设计/开发阶段。

考察 ISO 9000、ISO/IEC 15408 以及 SSE-CMM (ISO/IEC 21827)就可以看出,保障方法可针对交付件的一个特定阶段,或可适用于生存周期的多个阶段。

为达到最终的保障，每一个阶段所获得的保障必须带入下一个阶段，成为那个阶段的保障因素。这种方法持续不断地把保障增加到生存周期最后阶段，如图 1 所示样例模型中的运行阶段。

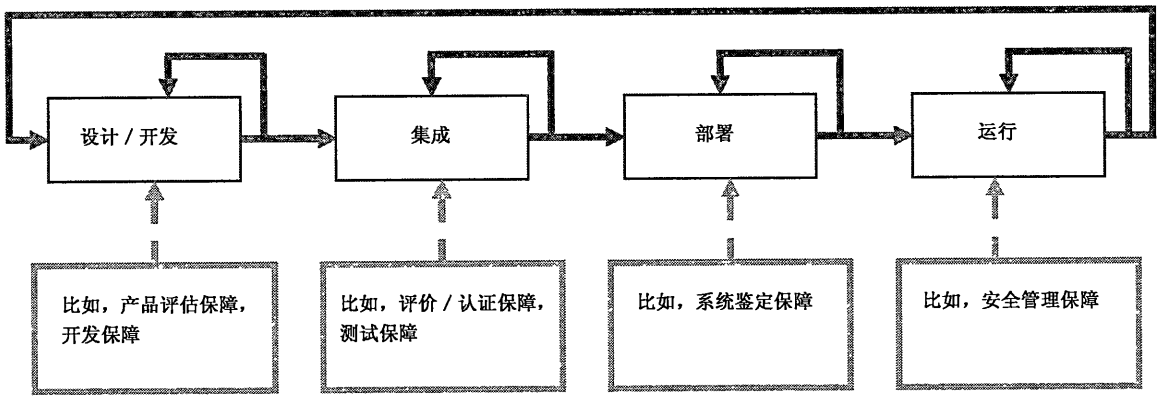

图 1　保障方法与一个简化的典型的生存周期阶段的关系

注：图 1 所示的生存周期模型是一个例子，证实一个模型与其他生存周期模型和框架是一致的，以支持本指导性技术文件中有关保障方法的分析。它不是用于指示或建议一个特定的生存周期模型。

6.4　正确性保障与有效性保障

正确性保障指的是对交付件的评价，依据设计以检验其正确的实施。与之对比，有效性指的是交付件的安全功能抵御已观察到的或已识别的风险的适宜性。下一段证实有效性保障和正确性保障是两个重要的保障特征，任一个都不是独立的，但它们每一个都强调了交付件的一些重要方面。

如果交付件的安全功能强调潜在威胁，但并未分析这个功能设计和实现的正确，那么人们就不会确信交付件能承受一个攻击。在这一例子中可以看出，由于缺少安全功能的验证，尽管建立了有效性保障，但没有建立正确性保障。类似地，如果分析发现交付件安全功能的设计和实现都是正确的，但设计却没有包括强调可能威胁的合适功能，那么人们就不会确信该交付件能对付这些威胁。在这一例子中，尽管存在正确性保障，但缺少有效性保障，因为就应对可能威胁而言，实现了一种无效的安全功能。为了达到综合全面的保障，必须对交付件进行评价，确保正确设计、实施和操作（正确要素），并且该交付件必须提供抵御已识别风险（有效性要素）的合适安全功能。

6.5　保障方法分类

按照 6.1 中描述的三个保障途径的分类，可以对保障方法进行分类。在每一个保障途径中，依赖一个保障方法的特征，该方法可能关注一个或多个特定生存周期阶段。

依赖保障方法的类型，所获得的保障是基于评价的方面和生存周期阶段的。例如，评估保障方法产生与设计、开发以及运行阶段一些相关部分的保障；开发保障方法产生与特定开发阶段相关的保障；依赖保障方法，测试保障产生与多个阶段的测试方面相关的保障。

图 2 表明，保障途径可适用于多个保障阶段。本指导性技术文件的第 2 部分和第 3 部分详细描述保障途径，其中第 2 部分给出保障方法的具体例子。

保障方法不同于保障途径类，由于保障方法具有不同的关注点，因此可产生不同的保障。虽然在同一个保障种类中，由于所检查的交付件（IT 组成部分或服务）方面，保障方法也会产生不同的保障。

依据所检查的交付件（IT 组成部分或服务）的方面，保障途径产生不同的保障。一些保障途径检查交付件生存周期的不同阶段，而另外一些途径检查生产交付件的过程（间接地检查交付件）。保障途径包括设施、开发、分析、测试、缺陷修补、操作、担保、人员等。这些保障途径可进一步划分，例如，测试保

障途径包括一般性测试保障方法和严格符合性测试保障方法。

采用这个框架，可以检测同一类中特定保障方法的冗余特性或协作特性。可以了解不同类保障方法的互补特性。一些方法可能显示涉及多个类，部分涉及或全部涉及，而其他一些方法可能只是某个类的一个部分。

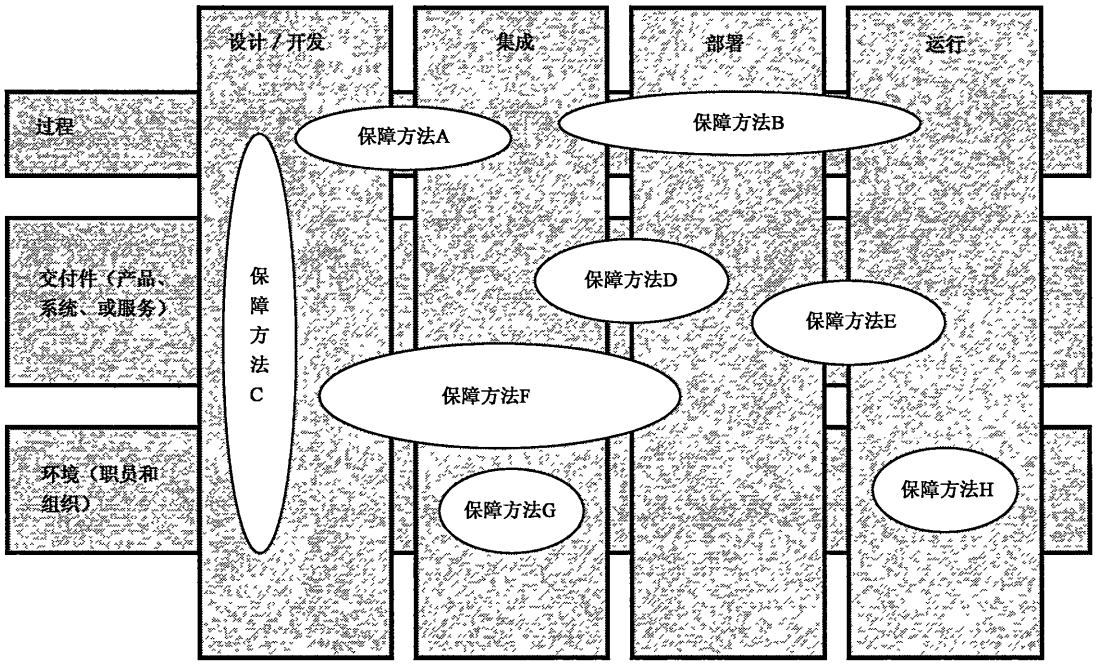

图 2　现有保障方法的分类

6.6　组合保障

交付件的最终保障通常是应用于该交付件整个生存周期不同阶段的不同保障方法的组合或合成。适当时，这一保障可以评分、类型或其他测度予以指示。

按几个不同的标准化保障方法，执行保障的组合是困难的，而且不存在穿越保障方法的保障刻度和测量。当前，保障的组合仅是可能的，即通过有经验的 IT 安全专业人员，形成保障判断和主观推断。加之，由保障机构最终确定可接受的保障。

目前，组合保障是通过在整个生存周期中应用不同的保障方法递增构建保障所产生的结果。下面的例子给出了可能的保障场景及其产生的问题：

1）　一个是检查生产交付件过程的保障方法，另一个是直接检查该交付件同一生存周期阶段不同点的保障方法；

2）　同一保障途径的两个保障方法应用于交付件的不同生存周期阶段；

3）　由大量 IT 产品和服务所组成的复杂 IT 系统（用于特定的运行环境），通过评估、担保、认证和鉴别等保障方法，具有不同的保障等级。

第一个例子显示了最简单的问题，其中组合保障是通过分别组合不同方法来确定的。

第二个例子看起来似乎是简单的，因为保障方法属于同一个保障途径，甚至如果保障方法相同的话，给出组合保障就更为直接。但如果出现有关重要性问题，即最后阶段出现的保障途径是重要的，那么组合保障就成为比较困难的。

第三个例子更为困难，因为多个不同的保障方法应用于不同生存周期阶段，并且鉴别保障方法形成了决定是否与系统一起继续存在的基础。尽管系统认证强调了早期保障证据，但在那个点上就不需要

一种特定保障途径。这建议具有更大权重的保障方法应用于后期的生存周期期阶段。

值得注意的是，许多基于标准的、处理保障的途径，现在倾向于采用持续过程改善的相同基础性模型。例如，针对质量的 ISO 9001 和针对信息安全管理的 BS 7799，均使用了 PDCA(Plan，Do，Check，Ac，即戴明环)模型。

本指导性技术文件的以后部分将强调一个问题，即应用于生存周期后期阶段的保障途径是否具有更强的相关性或更大的保障。

6.7 保障评定

本指导性技术文件第 3 部分的分析将集中关注保障度量，作为分类保障方法的一种方式，并作为测量应用一个保障方法所获得保障值(例如开发保障等级水平)的一种方式。建立保障度量还可支持描述保障方法之间的关系。

下面是本指导性技术文件第 3 部分所涉及的一些问题，因为它们与保障方法的分析和评定是有关的：

a) 比较不同的保障方法；
b) 量化保障方法；
c) 选择合适的保障方法；
d) 不同保障方法之间的关系；
e) 确定哪些保障方法可以予以组合；
f) 确定保障方法何时和如何组合；
g) 确定是否和如何定序保障方法的执行，该定序将影响整个保障；
h) 确定有关确保和增强在交付件生存周期(如运行和维护)内保障结果(和条件)确认的一些技术问题，其中使用了多个保障途径。

参 考 文 献

[1] Aaron Cohen, Review of ISO Assurance Approaches, The First Annual International Systems Security Engineering Conference, San Antonio, Texas, February 3-4, 2000.

[2] AAWG Task 1 Report, Draft Version 0.9. Common Criteria Project: Assurance Approaches Working Group (AAWG) (report: AAWG-97/037, annex A: AAWG-97/038), August 1997.

[3] Abadi, Burrows, Lampson, Plotkin: A calculus for access control in distributed systems, Digital Equipment Corporation, Palo Alto, 1991.

[4] British Standard BS 7799-2 Information Security management systems-specification and guidance for use, British Standards Institution, 2002.

[5] CMM® (model): Capability Maturity Model for Software, Version 1.1, February 1993.

[6] CMM® (method): Key Practices of the Capability Maturity Model, Version 1.1, February 1993.

[7] Gasser, Goldstein, Kaufmann, Lampson: The Digital distributed security architecture, Proc. of National Computer Security Conference, USA, 1989.

[8] Korea Information Security Evaluation Criteria, Ministry of Information and Communication, Republic of Korea, February 1998.

[9] Korea Information Security Product Evaluation Program, Ministry of Information and Communication, Republic of Korea, February 1998.

[10] The application of quality assurance procedures to security evaluation, NPL Report DITC 236/95, UK, July 1995.

[11] SCT, Strict Conformance Testing, NPL Report, UK, March 1997.

[12] SE-CMM® (model). A Systems Engineering Capability Maturity Model, Version 1.1. Carnegie Mellon University (CMU/SEI-95-MM-003), November 1995.

[13] SE-CMM® (method). A Description of the Systems Engineering Capability Maturity Model Appraisal Method, Version 1.1. Carnegie Mellon University (CMU/SEI-96-HB-004), March 1996.

[14] Strack/Lam: Context-dependent access control in distributed systems, Proc.of IFIP/SEC'93, Toronto 1993 (IFIPtransactions A-37, North-Holland, 1993). Trusted Capability Maturity Model, Version 2.0. National Security Agency (NSA), June 20, 1996. UK Certificate Maintenance Scheme, Part II Impact Analysis And Evaluation Methodology, UKSP 16, Issue 1.0, UK

[15] IT Security Evaluation & Certification Scheme Certification Body, 31 July 1996. X/Open CAE Specification Baseline Security Services (XBSS), Document Number C529, UK: X/Open Company, Ltd., December 1995.

*

书号:155066·1-48740

定价: 24 00 元