GA

中华人民共和国公共安全行业标准

GA/T 388 --2002

计算机信息系统安全等级保护操作系统技术要求

Operating system technology requirement

in computer information system security protection

2002-07-18 发布　　2002-07-18 实施

中华人民共和国公安部　发布

目　　次

前　　言

GB17859-1999《计算机信息系统安全保护等级划分准则》作为我国计算机信息系统安全等级管理的重要标准，已于1999年9月13日发布。为促进安全等级管理的工作的正常有序开展，特制定一系列相关的标准，包括：

——计算机信息系统安全等级保护技术要求系列标准；

——计算机信息系统安全等级保护管理要求；

——计算机信息系统安全等级保护工程实施要求；

——计算机信息系统安全等级保护实施管理办法；

——计算机信息系统安全保护等级评测系列标准。

其中，计算机信息系统安全等级保护技术要求系列标准主要包括以下五个标准：

——GA ××1 — ×××× 计算机信息系统安全等级保护通用技术要求；

——GA ××2 — ×××× 计算机信息系统安全等级保护网络技术要求；

——GA ××3 — ×××× 计算机信息系统安全等级保护操作系统技术要求；

——GA ××4 — ×××× 计算机信息系统安全等级保护数据库管理系统技术要求；

——GA ××5 — ×××× 计算机信息系统安全等级保护应用系统技术要求。

《计算机信息系统安全等级保护操作系统技术要求》作为计算机信息系统安全等级保护技术要求系列标准之一，详细说明了计算机信息系统为实现GB17859所提出的安全等级保护要求对操作系统的安全技术要求,以及为确保这些安全技术所实现的安全功能达到其应具有的安全性而采取的保证措施，并将GB17859对计算机信息系统五个安全保护等级每一级的要求，从技术要求方面进行详细描述。

本标准分由公安部公共信息网络安全监察局提出。

本标准起草单位：江南计算技术研究所。

本标准主要起草人：汪晓茵 、吉增瑞、徐良华、袁志平

引　　言

《计算机信息系统安全等级保护操作系统技术要求》是计算机信息系统安全等级保护技术要求系列标准的重要组成部分，用以指导设计者如何设计和实现具有所需要的安全等级的操作系统，主要从对操作系统的安全保护等级进行划分的角度来说明其技术要求，即主要说明为实现《计算机信息系统安全保护等级划分准则》中每一个保护等级的安全要求对操作系统应采取的安全技术措施，以及各安全技术要求在不同安全级中具体实现上的差异。

本标准按照 GB17859 五个安全等级的划分，对每一个安全等级的安全功能技术要求和安全保证技术要求做了详细描述。本标准参考的主要文件是：

——GB17859-1999 计算机信息系统安全保护等级划分准则；

——ISO/IEC 15408：1999 Information technology—Security techniques— Evaluation Criteria for IT Security ，Version 2.0。

计算机信息系统安全等级保护操作系统技术要求

1 范围

本标准规定了对操作系统进行安全保护等级划分所需要的详细技术要求，并给出了每一个安全保护等级的不同技术要求。

本标准适用于按照《计算机信息系统安全保护等级划分准则》（以下简称《准则》）的安全等级保护要求所进行的操作系统的设计和实现，按照《准则》安全等级保护的要求对操作系统进行的测试、管理也可参照使用。

如不做特殊说明，本部分中的安全技术要求，适用于各种类型的操作系统，包括单处理机操作系统和多处理机操作系统（并行操作系统、分布式操作系统、网络操作系统等）。

2 引用文件

下列文件中的有关条款通过引用而成为本标准的条款。凡注日期或版次的引用文件，其后的任何修改单（不包括勘误的内容）或修订版本都不适用于本标准，但提倡使用本标准的各方探讨使用其最新版本的可能性。凡不注日期或版次的引用文件，其最新版本适用于本标准。

GB17859-1999 计算机信息系统安全等级划分准则

GA ××1 — ×××× 计算机信息系统安全等级保护通用技术要求

3 定义

GB17859—1999 和 GA ××1 — ××××确立的术语和定义适用于本标准。

4 安全保护等级划分技术要求

4.1 第一级：用户自主保护级

4.1.1 安全功能

4.1.1.1 自主访问控制

应按照《通用技术要求》6.1.3.3 条自主访问控制的要求，设计和实现操作系统的自主访问控制功能。

在本安全级中，应允许命名用户以用户和/或用户组的身份规定并控制对客体的共享，并阻止非授权用户读取敏感信息。按照主体与客体的关系，即主体为客体的拥有者/同组/其它，常用的自主访问控制策略为访问控制表（ACL），包括：

——目录表访问控制；

——存取控制表访问控制；

——访问控制矩阵访问控制等。

自主访问控制应设置缺省功能。当一个主体生成一个客体时，在该客体的访问控制表中相应地应具有生成者的主体设置的缺省值。

实现操作系统自主访问控制的具体方法有：

a) 基于目录表访问的自主访问控制，应为每个实施访问的主体建立一张可以被该主体访问的“客体目录表”。每个用户在其文件目录表中依次列出文件名，并逐一标明对这些文件的访问权限。权限一般分为四种：读、写、执行和属主。每个客体应有唯一的属主。属主具有访问权和分配、回收其他用户的访问权的权限。文件目录表的修改只有文件的属主才能实施，其他任何用户不允许在文件目录表中写，因此，操作系统应在文件的拥有者控制下维护所有的文件目录。

b） 基于存取控制表的自主访问控制，应决定任何一个确定的主体是否可对某一客体进行访问，并识别存取文件的单个用户或用户组。对系统中每一个需要保护的客体，都应为其附加一个主体明细表，表中的每一项包括主体的身份以及对该客体的访问权。这些信息应贮存在某个地方，清楚地与客体相连，高效地标识可存取文件的用户。

c） 访问控制矩阵模型，应用状态和状态转换进行访问关系定义。访问控制矩阵可是一张表格，每行代表一个用户（主体），每列代表一个存取目标（客体），表中的每个元素是该主体对客体的访问权集合。访问的权限应包括读、写、执行和删除。访问控制矩阵一般是稀疏的，矩阵内多数的项为空，即多数主体无权访问多数客体。访问控制矩阵根据不同类型的客体被允许实施的操作规定存取的种类。矩阵状态的转换通过命令集合将命令规定成一系列基本操作实现，主要包括：

——在 A[S,O]中增加权力 R；

——在 A[S,O]中删除权力 R；

——生成主体 S；

——生成客体 O；

——删除主体 S；

——删除客体 O。

4.1.1.2 身份鉴别

应按照《通用技术要求》6.1.3.1 条用户标识和《通用技术要求》6.1.3.2 条用户鉴别的要求，设计和实现操作系统的身份鉴别功能。本安全级要求：

a） 采用口令进行鉴别，并在每次用户登录系统时进行鉴别。口令应是不可见的，并在存储时按《通用技术要求》4.3.13 条密码支持第一级的要求进行保护。

4.1.1.3 数据完整性

应按照《通用技术要求》6.1.3.4 条数据完整性的要求，设计和实现操作系统的数据完整性功能。本安全级要求：

a） 应通过对系统中的信息采取有效措施，防止其遭受非授权用户的修改、破坏或删除。

b） 进程应具有高完整性，确保系统能正确运行，不致混乱或崩溃。为此，需要设计相应的 TCB 来实现有关功能。

c） 对在操作系统中经网络传输信息的完整性保护，应提供监视用户数据完整性的功能，即能检测出被传输的用户数据被篡改、删除、插入和重用等情况发生，并进行报警。

4.1.2 TCB 自身安全保护

4.1.2.1 TSF 保护

应按照《通用技术要求》6.1.4.1 条 TSF 保护的要求，设计和实现操作系统的 TSF 保护。本安全级中，操作系统 TSF 保护的具体要求为：

a） 系统在设计时不应留有“后门”。即不应以维护、支持或操作需要为借口，设计有违反或绕过安全规则的任何类型的入口和文档中未说明的任何模式的入口。

b） 安全结构应是一个独立的、严格定义的系统软件的一个子集，并应防止外部干扰和破坏，如修改其代码或数据结构。

c） 操作系统应进行分层设计，对操作系统程序和用户程序要进行隔离。

d） 一个进程的虚地址空间至少应被分为两个段：用户空间和系统空间，两者的隔离应是静态的。驻留在内存中的操作系统应由所有进程共享。用户进程之间应是彼此隔离的。应禁止在用户

模式下运行的进程对系统段进行写操作，而在系统模式下运行时，应允许进程对所有的虚存空间进行读、写操作。用户模式到系统模式的转换应由一个特殊的指令完成，该指令将限制进程只能对部分系统空间进程访问，这些访问限制应由硬件根据该进程的特权模式实施。

e） TCB 应提供一个设置和升级配置参数的安装机制。在初始化和对与安全有关的数据结构进行保护之前，应对用户和管理员的安全策略属性应进行定义。

f） TCB 应区分普通操作模式和系统维护模式，TCB 的恢复、全系统操作恢复的启动、配置 TCB 内部的数据库和表等动作应在维护模式中执行。

g） 在 TCB 失败或中断后，进程应保证保护文本以最小的损害得到恢复。大多数情况下，重新启动或安装是唯一可行的途径。

4.1.2.2 资源利用

应按照《通用技术要求》**6.1.4.2** 条资源利用的要求，设计和实现操作系统的资源利用。在本安全级中，资源利用设计的具体要求为：

a） 应通过一定措施确保当系统出现某些确定的故障情况时，TSF 也能维持正常运行。

b） 应采取适当的策略，有限服务优先级提供主体使用 TSC 内某个资源子集的优先级，进行 TCB 资源的管理和分配；

c） 应按资源分配中最大限额的要求，进行 TCB 资源的管理和分配，要求配额机制确保用户和主体将不会独占某种受控的资源。

4.1.2.3 TCB 访问控制

应按照《通用技术要求》**6.1.4.3** 条 **TCB** 访问控制的要求，设计和实现操作系统的 **TCB** 访问控制。本安全级中，操作系统 TCB 访问控制设计的具体要求为：

a） 应按照可选属性范围限定最小级的要求，选择某种会话安全属性的所有失败的尝试 ，对用来建立会话的安全属性的范围进行限制；

b） 应按照多重并发会话限定中基本限定的要求，进行会话管理的设计。基于同步标识的基础上，TSF 应限制系统的并发会话的最大数量，并应利用缺省值作为会话次数的限定数；

c） 应按照最小级会话建立机制，对会话建立的管理进行设计。

4.1.3 TCB 设计和实现

4.1.3.1 配置管理

应按照《通用技术要求》**6.1.5.1** 条配置管理的要求，设计和实现操作系统 **TCB** 的配置管理。本安全级的具体要求为：

a) 应具有基本的配置管理能力，即要求开发者所使用的版本号与所应表示的 TCB 样本完全对应。

4.1.3.2 分发和操作

应按照《通用技术要求》**6.1.5.2** 条分发和操作的要求，设计和实现操作系统的 **TCB** 分发和操作。本安全级的具体要求为：

a) 应以文档形式提供对 TCB 安全地进行分发的过程，以及安装、生成和启动的过程进行说明，并最终生成安全的配置。文档中所描述的内容应包括：

——提供分发的过程；

——安全启动和操作的过程。

b) 对系统的未授权修改的风险，应在交付时控制到最低限度。在包装及安全分送和安装过程中，这种控制应采取软件控制系统的方式，确认安全性会由末端用户考虑，所有安全机制都应以

功能状态交付。

c) 所有软件应提供安全安装默认值，在客户不做选择时，默认值应使安全机制有效地发挥安全功能。

d) 随同系统交付的全部默认用户标识码，应在交付时处于非激活状态，并在使用前由管理员激活。

e) 用户文档应同交付的软件一起包装，并应有一套规程确保当前送给用户的系统软件是严格按照最新的系统版本来制作的。

4.1.3.3 开发

应按照《通用技术要求》**6.1.5.3** 条开发的要求，进行操作系统 **TCB** 的开发。本安全级的具体要求为：

a) 按非形式化功能说明、描述性高层设计、TSF 子集实现、TSF 内部结构模块化、描述性低层设计和非形式化对应性说明的要求，进行 TCB 的开发。

b) 系统的设计和开发应保护数据的完整性，例如，检查数据更新的规则，二重/多重输入的正确处理，返回状态的检查，中间结果的检查，合理值输入检查，事务处理更新的正确性检查等。

c) 在内部代码检查时，应解决潜在的安全缺陷，关闭或取消所有的后门。

d) 所有交付的软件和文档，应进行关于安全缺陷的定期的和书面的检查，并将检查结果告知用户。

e) 系统控制数据，如口令和密钥，不应在未受保护的程序或文档中以明文形式存储，并以书面形式提供给用户关于软件所有权法律保护的指南。

4.1.3.4 指导性文档

应按照《通用技术要求》**6.1.5.4** 条指导性文档的要求，编制 **TCB** 的指导性文档。本安全级的具体要求为：

a) 用户文档应提供关于不同用户的可见的安全机制以及如何利用它们的信息，描述没有明示用户的保护结构，并解释它们的用途和提供有关它们使用的指南，不应包括那些如果公开将会危及系统安全的任何信息。

b) 系统管理员文档应提供关于系统的安全开机、操作和重新启动的信息，包括启动系统的过程（如引导系统进入安全方式）、在系统操作失误时恢复安全系统操作的过程、运行软件和数据备份及转储的方法和过程，还应提供一个单独的安装指南，详细说明设置系统的配置和初始化过程，提供一个新系统版本的安全设置和安装文档，包括对所有用户可见的安全相关过程、软件和数据文档的描述。

c) 安全管理员文档应提供有关如何设置、维护和分析系统安全的详细指导，包括当运行一个安全设备时，需要控制的有关功能和特权的警告，以及与安全有关的管理员功能的详细描述，包括增加和删除一个用户、改变用户的安全特征等。

d) 文档中不应提供任何一旦泄露将会危及系统安全的信息。有关安全的指令和文档应划分等级分别提供给用户、系统管理员和系统安全员。这些文档应为独立的文档，或作为独立的章节插入到管理员指南和用户指南中。文档也可为硬拷贝、电子文档或联机文档。如果是联机文档应控制对其的访问。

4.1.3.5 生命周期支持

应按照《通用技术要求》**6.1.5.5** 条生命周期支持的要求，设计和实现操作系统的 **TCB**。本安全级的具体要求为：

a) 应按开发者定义生命周期模型进行开发。

b) 应提供安全安装默认值。在未做特殊选择时,应按默认值安装安全机制。

c) 随同系统交付的全部默认用户标识号，在刚安装完时应处于非激活状态，并由系统管理员加以激活。

d) 文档应详细阐述安全启动和操作的过程，详细说明安全功能在启动、正常操作维护时是否能被撤消或修改，说明在故障或系统出错时如何恢复系统至安全状态。

4.1.3.6 测试

应按照《通用技术要求》6.1.5.6 条测试的要求，对操作系统的 TCB 进行测试。本安全级的具体要求为：

a) 应通过一般功能测试和相符性独立测试，确认 TCB 的功能与所要求的功能相一致。

b) 所有系统的安全特性，应被全面测试。所有发现的漏洞应被改正、消除或使其无效，并在消除漏洞后重新测试，以证实它们已被消除，且没有引出新的漏洞。

c) 应提供测试文档，详细描述测试计划、测试过程、测试结果。

4.1.4 TCB 安全管理

应按照《通用技术要求》6.1.6 条 TCB 安全管理所描述的要求，实现 TCB 的安全管理。本安全级的具体要求为：

a) 对相应的 TCB 的访问控制、鉴别控制、审计和安全属性管理等相关的功能，以及与一般的安装、配置等有关的功能，制定相应的操作、运行规程和行为规章制度。

b) 根据本级中安全功能技术要求所涉及的自主访问控制、身份鉴别、数据完整性、和安全保证技术要求所涉及的配置管理、分发和操作、开发、指导性文档、生命周期支持、测试等所涉及的有关内容设计 TCB 安全管理。

4.2 第二级：系统审计保护级

4.2.1 安全功能

4.2.1.1 自主访问控制

应按照《通用技术要求》6.2.3.3 条的要求，设计和实现操作系统的自主访问控制功能。

在本安全级中，要求有更细粒度的自主访问控制。对系统中的每一个客体，都应能够实现由客体的创建者（用户）以用户指定方式或默认方式确定其对该客体的访问权限，而别的同组用户或非同组的用户和用户组对该客体的访问权则应由创建者用户授予，并将访问控制的粒度控制在单个用户，做到只有授权用户才能对该客体实施所授权的访问，而阻止那些非授权的用户对该客体进行任何访问，也阻止授权用户以非授权的操作形式对该客体进行访问。本级还要求自主访问控制能与身份鉴别和审计相结合，通过确认用户身份的真实性和记录用户的各种成功的或不成功的访问，使用户对自己的行为承担明确的责任。

本级中，对自主访问控制的要求应包括：

——定义访问控制属性，并保护这些属性。主体的访问控制属性至少应有：读、写、运行等；客体的访问控制属性应包含可分配给主体的读、写和执行的权限。

——定义分配和修改主体和客体的访问控制属性的规则，并执行对主体和客体的访问控制属性的分配和修改，规则的结果应达到只有被授权的用户才允许访问一个客体。

——定义主体对客体的访问授权规则。该规则应基于主体对客体的访问控制属性，授权的范围应包括主体和客体及相关的访问控制属性，同时应指出主体和客体对这些规则应用的类型。

——所有主体和客体的创建和删除应由系统来进行。主体可请求系统创建和删除主体和客体，但不允许它自己去做这些，从而保证主体和客体不能以危害由系统包含的信息的方式来创建。无论何时一个主体或客体被创建，系统应保证被用于创建该主体或客体的资源不能包含以前使用的任何信息，这些资源主要有：存储器、文件、目录、符号连接、管道、消息队列、信号灯、共享主存等。

实现操作系统自主访问控制的具体方法有：

a) 基于目录表访问的自主访问控制，应为每个实施访问的主体建立一张可以被该主体访问的“客体目录表”。每个用户在其文件目录表中依次列出文件名，并逐一标明对这些文件的访问权限。权限一般分为四种：读、写、执行和属主。每个客体应有唯一的属主。属主具有访问权和分配、回收其他用户的访问权的权限。文件目录表的修改只有文件的属主才能实施，其他任何用户不允许在文件目录表中写，因此，操作系统应在文件的拥有者控制下维护所有的文件目录。

b) 基于存取控制表的自主访问控制，应决定任何一个确定的主体是否可对某一客体进行访问，并识别存取文件的单个用户或用户组。对系统中每一个需要保护的客体，都应为其附加一个主体明细表，表中的每一项包括主体的身份以及对该客体的访问权。这些信息应贮存在某个地方，清楚地与客体相连，高效地标识可存取文件的用户。

c) 访问控制矩阵模型，应用状态和状态转换进行访问关系定义。访问控制矩阵可是一张表格，每行代表一个用户（主体），每列代表一个存取目标（客体），表中的每个元素是该主体对客体的访问权集合。访问的权限应包括读、写、执行和删除。访问控制矩阵一般是稀疏的，矩阵内多数的项为空，即多数主体无权访问多数客体。访问控制矩阵根据不同类型的客体被允许实施的操作规定存取的种类。矩阵状态的转换通过命令集合将命令规定成一系列基本操作实现，主要包括：

   ——在 A[S,O]中增加权力 R；
   ——在 A[S,O]中删除权力 R；
   ——生成主体 S；
   ——生成客体 O；
   ——删除主体 S；
   ——删除客体 O。

d) 能力表是存取矩阵的另一种改进类型。能力表与主体相关，每个用户应有一个能力表，决定用户是否可以对客体进行访问以及进行何种模式的访问（读、写、执行）。一个拥有一定能力的主体允许依照一定的模式访问客体，在进程运行期间，可删除或添加某些能力。一个用户的能力可以转让，也可以回收，还可以包含在程序、数据文件、硬件、软件中，并采用一定措施进行保护。

e) 拥有者/同组/其他访问控制机制，是在每个文件上附加一段有关存取控制信息的二进制位，这些位应反映不同类型用户的存取方式，一般不超过四类：文件的拥有者、与文件拥有者同组的用户、特定的系统用户和其他用户。每一类用户都应有一组权限，每组权限有三个权限标志位来控制以下权限：

   ——可读（r）：如果被设置，则文件或目录可读。
   ——可写（w）：如果被设置，文件或目录可以被写入或修改。
   ——可执行（x）：如果被设置，文件或目录可以被执行和搜索。

f) **客体的拥有者应是唯一有权修改客体访问权限的主体，拥有者对其拥有的客体应具有全部控制权，但是，不允许客体拥有者把该客体的控制权分配给其他主体。因此，客体拥有者在任何时候都可以改变其所属客体的访问控制表，并可对其他主体授予或撤消对该客体的任何一种访问模式。另外，可设立系统管理员（也称为超级用户），有权修改系统中所有客体的访问控制表，并可对所有客体进行所有模式的访问。**

4.2.1.2 身份鉴别

应按照**《通用技术要求》6.2.3.1 条用户标识和《通用技术要求》6.2.3.2 条用户鉴别**的要求，设计和实现操作系统的身份鉴别功能。**本安全级的具体要求为：**

a) 采用口令进行鉴别，并要求在每次用户登录系统时进行鉴别即可。口令应是不可见的，并在存储和传输时按**《通用技术要求》4.3.13 条密码支持第二级**的要求进行保护。

4.2.1.3 客体重用

应按照《通用技术要求》6.2.3.4 条客体重用的要求设计操作系统的客体重用功能。本安全级的具体要求为：

a) **应确保动态分配与管理的资源，在保持信息安全的情况下被再利用，主要包括：**

——确保非授权用户不能查找在使用后返还系统的记录介质中的信息内容；

——确保非授权用户不能查找系统现已分配给他的记录介质中以前的信息内容。

b) **在单用户系统中，存储器保护应防止用户进程不影响系统的运行.**

c) **在一个多用户系统中，存储器保护应保证系统内各个用户之间互不干扰。**

d) **存储器保护应包括:**

——对存储单元的地址的保护，使非法用户不能访问那些受到保护的存储单元；

——对被保护的存储单元的操作提供各种类型的保护。最基本的保护类型是“读/写”和“只读”。不能读/写的存储单元，若被用户读/写时，系统应及时发出警报或中断程序执行。

——可采用逻辑隔离的方法进行存储器保护，具体有：界限地址寄存器保护法、内存标志法、锁保护法和特征位保护法等。

4.2.1.4 审计

应按照《通用技术要求》6.2.2.3 条审计的要求设计操作系统的审计功能。本安全级的具体要求为：

a) **审计功能应与用户标识与鉴别、自主访问控制等安全功能的设计紧密结合。**

b) **应能够生成、维护及保护审计过程，使其免遭修改、非法访问及破坏，特别要保护审计数据，要严格限制未经授权的用户访问。**

c) **应记录以下类型的事件：**

——使用识别与鉴别机制（如注册过程）；

——将某个客体引入某个用户的地址空间（如打开文件）；

——删除客体及计算机操作员、系统管理员与系统安全管理员进程的操作。

d) **每个审计记录应记录事件发生的日期与时间、产生这一事件的用户、事件的类型以及该事件成功与否。对于识别与鉴别事件，审计记录应记录事件发生的源地点；对于将一个客体信息引入某个用户地址空间中的事件以及删除客体的事件，审计记录应包括客体名及客体的安全级别。**

e) **本安全级要求基本的审计功能主要包括：**

——授权控制和审计跟踪，应能够创建并维护一个对受保护客体访问的审计跟踪，保护审计记录不被未授权的访问、修改和破坏。

——可记录的安全相关事件，应能指出可记录的审计事件的最少类型，包括建立会话登录成功和失败，使用的系统接口，系统数据库管理的改变（改变用户账户属性、审计跟踪设置和分析、为程序分配设置用户 ID、附加或改变系统程序或进程、改变日期和时间等），超级用户命令改变用户身份等。当审计激活时应确保审计跟踪事件的完整性；应提供一个机制来显示当前选择的审计事件，这个机制的使用者应是有限的授权用户。

——每个事件的数据记录，应包括的信息有：事件发生的日期和时间、触发事件的用户、事件的类型、事件成功或失败等。对于身份识别和认证事件，应记录请求的源（如终端号或网络地址）；对于创建和删除客体的事件，应记录客体的名字和属性。

——审计跟踪控制、管理和检查，应提供一个受保护的打开和关闭审计的机制。该机制能选择和改变审计事件，并在系统工作时处于默认状态；该机制的使用应受到系统管理员的授权限制，系统管理员应能够选择一个或多个基于身份识别或客体属性的用户的审计活动；审计工具应能够授权个人监察和浏览审计数据，同时数据应得到授权的使用、修改和删除；应提供对审计跟踪管理功能的保护，使之可以完成审计跟踪的创建、破坏、腾空和存档；系统管理员应能够定义超过审计跟踪极限的阈值；当存储空间被耗尽时，应能按管理员的指定决定采取的措施，包括：报警并丢弃未记录的审计信息、暂停审计、覆盖以前的审计记录等。

4.2.1.5 数据完整性

应按照**《通用技术要求》6.2.3.5 条数据完整性**的要求，设计和实现操作系统的数据完整性功能。**本安全级的具体要求为：**

a) 应通过对系统中的信息采取有效措施，防止其遭受非授权用户的修改、破坏或删除。

b) 进程应具有高完整性，确保系统能正确运行，不致混乱或崩溃。为此，需要设计相应的 TCB 来实现有关功能。

c) 对在操作系统中经网络传输信息的完整性保护，要求 TCB 提供监视用户数据完整性的功能，即能检测出被传输的用户数据被篡改、删除、插入和重用等情况发生，并进行报警。

d) 对存储在 TCB 安全控制范围内的用户数据应进行完整性保护，实现存储数据的完整性监视，并进行报警。

e) 对磁盘设备中存储的数据，可通过增加磁盘扫描程序实现以下功能：

——自动检查文件与磁盘表面是否完好；

——修复扇区交错和扇区流失；

——将磁盘表面的问题自动记录下来；

——将数据移到好的扇区；

——随时检查、诊断和修复磁盘上的错误。

——可在系统中增加计算机病毒检测、诊断和预防程序；

——也可增加硬盘数据备份和修复程序，将硬盘中的数据压缩、备份，并在必要时恢复。

g) 对在操作系统中进行处理的信息的完整性保护，应通过对各种异常情况事务的回退，以事务的完整性确保数据的完整性。

4.2.2 TCB 自身安全保护

4.2.2.1 TSF 保护

应按照**《通用技术要求》6.2.4.1 条 TSF 保护**的要求，设计和实现操作系统的 TSF 保护。本安全级中，操作系统 TSF 保护的具体要求为：

a) 系统在设计时不应留有“后门”。即不应以维护、支持或操作需要为借口，设计有违反或绕过安全规则的任何类型的入口和文档中未说明的任何模式的入口。

b) 安全结构应是一个独立的、严格定义的系统软件的一个子集，并应防止外部干扰和破坏，如修改其代码或数据结构。

c) 操作系统应进行分层设计，对操作系统程序和用户程序要进行隔离。

d) 一个进程的虚地址空间至少应被分为两个段：用户空间和系统空间，两者的隔离应是静态的。驻留在内存中的操作系统应由所有进程共享。用户进程之间应是彼此隔离的。应禁止在用户模式下运行的进程对系统段进行写操作，而在系统模式下运行时，应允许进程对所有的虚存空间进行读、写操作。用户模式到系统模式的转换应由一个特殊的指令完成，该指令将限制进程只能对部分系统空间进程访问，这些访问限制应由硬件根据该进程的特权模式实施。

e) TCB 应提供一个设置和升级配置参数的安装机制。在初始化和对与安全有关的数据结构进行保护之前，应对用户和管理员的安全策略属性应进行定义。

f) TCB 应区分普通操作模式和系统维护模式，TCB 的恢复、全系统操作恢复的启动、配置 TCB 内部的数据库和表等动作应在维护模式中执行。

g) TCB 应防止一个普通用户从未经允许的系统进入维护模式，并应防止一个普通用户与系统内维护模式交互。从而保证在普通用户访问系统之前，系统能以一个安全的方式进行安装和配置。安全机制应在维护模式中保护普通用户的入口。

h) 对备份或不影响 TCB 的常规的系统维护，不要求所有的系统维护都在维护模式中执行。

i) 当操作系统安装完成后，在普通用户访问之前，系统应配置好初始用户和管理员职责、根目录、审计参数、系统审计跟踪设置以及对文件和目录的合适的访问控制。

j) 执行系统所提供的实用程序，应（默认地）限定于对系统的有效使用，只允许系统管理员修改或替换系统提供的实用程序。

k) 操作环境应为用户提供一个机制，来控制命令的目录/路径的查找顺序。

l) 在 TCB 失败或中断后，进程应保证保护文本以最小的损害得到恢复。并按照失败保护中所描述的内容，实现对 TSF 出现失败时的处理。

m) 操作系统环境应控制和审计系统控制台的使用情况。

n) 系统应能识别由通信渠道接收的信息的来源者，所有待确认的数据应能从进入点被安全地传送到确认系统，如口令不应由公共的或共享的网络以明文发送，可使用数据加密设备或通过加密信道用加密模式传送。

4.2.2.2 资源利用

应按照**《通用技术要求》6.2.4.2 条资源利用**的要求，设计和实现操作系统的资源利用。在本安全级中，资源利用设计的具体要求为：

a) 应通过一定措施确保当系统出现某些确定的故障情况时，TSF 也能维持正常运行，**如系统应检测和报告系统的服务水平已降低到预先规定的最小值；**

b) 应采取适当的策略，有限服务优先级提供主体使用 TSC 内某个资源子集的优先级，进行 TCB

资源的管理和分配；

c） 应按资源分配中最大限额的要求，进行 TCB 资源的管理和分配，要求配额机制确保用户和主体将不会独占某种受控的资源。

d） 系统应确保在被授权的主体发出请求时，资源能被访问和利用。

e） 当系统的服务水平降低到预先规定的最小值时，应能检测和发出报告。

f） 系统应提供管理维护状态中运行的能力，在管理维护状态下各种安全性能全部失效，系统只允许由系统管理员使用。

g） 系统应以每个用户或每个用户组为基础，提供一种机制，控制他们对磁盘的消耗和对 CPU 的使用。

4.2.2.3 TCB 访问控制

应按照**《通用技术要求》6.2.4.3 条 TCB 访问控制**的要求，设计和实现操作系统的 TCB 访问控制。本安全级中，操作系统 TCB 访问控制设计的具体要求为：

a） 应按照可选属性范围限定最小级的要求，选择某种会话安全属性的所有失败的尝试 ，对用来建立会话的安全属性的范围进行限制；

b） 应按照多重并发会话限定中基本限定的要求，**提供适用于 TSF 内所有用户的限制实现对会话管理的设计，允许用户会话建立的所有尝试；**

c） 应按照 TCB 访问历史所描述的要求，实现对会话管理的设计，在会话成功建立的基础上，TSF 应显示用户上一次成功/不成功的会话建立的日期，时间，方法，位置，以及从上一次成功的会话建立以来的不成功的尝试的次数。

d） 应按照 TCB 会话建立所描述的要求，实现对会话管理的设计，TSF 应根据属性允许或拒绝该次会话的建立，这些属性包括：访问地址或端口，用户安全属性（如用户身份、许可证等级、完整性等级、角色中的成员资格），时间范围（如一天中的某些时间、一周的某些天、某些特定日期），或上述属性的组合。

按照以上要求，本级要求在操作系统中应采取的措施主要有：

a） 在建立 TCB 会话之前，认证机制应用这个用户的认证数据由 TCB 校验用户的身份。登录机制不允许认证机制本身被旁路。

b） 为给用户提供系统登录活动的有关信息，让用户识别入侵的企图，采取行动防止可能的未授权使用， 成功登录系统后，TCB 应向用户显示以下数据：

——日期、时间、来源和上次成功登录系统的情况；

——上次成功访问系统以来身份识别失败的情况；

——应显示口令到期的天数；

——成功或不成功的事件次数的显示可以用整数计数、时间戳列表等表述方法。

4.2.3 TCB 设计和实现

4.2.3.1 配置管理

应按照**《通用技术要求》6.2.5.1 条配置管理**所描述的要求进行设计。**本安全级的具体要求为：**

a） 在配置管理能力方面应实现对版本号、**配置项、授权控制**等方面的要求。

b） 在 TCB 的配置管理范围方面，应将 TCB 的实现表示、设计文档、测试文档、用户文档、管理员文档以及配置管理文档等置于配置管理之下。

c） 在系统的整个生存期，即在它的开发、测试和维护期间，应有一个软件配置管理系统处于保持对改变源码和文件的控制状态。只有被授权的代码和代码修改才允许被加进已交付的源码

的基本部分。所有改变应被记载和检查，以确保未危及系统的安全。在软件配置管理系统中，应包含从源码产生出系统新版本、鉴定新生成的系统版本和保护源码免遭未授权修改的工具和规程。通过技术、物理和保安规章三方面的结合，可充分保护生成系统所用到的源码免遭未授权的修改和毁坏。

4.2.3.2 分发和操作

应按照**《通用技术要求》6.2.5.2 条分发和操作**的要求，设计和实现操作系统的 TCB 分发和操作。**本安全级的具体要求为：**

a) 应以文档形式提供对 TCB 安全地进行分发的过程，以及安装、生成和启动的过程进行说明，并最终生成安全的配置，

b) 应以文档形式提供对 TCB 安全地进行分发的过程，以及安装、生成和启动的过程进行说明，并最终生成安全的配置。文档中所描述的内容应包括：

——提供分发的过程；

——安全启动和操作的过程；

——建立日志的过程。

c) 对系统的未授权修改的风险，应在交付时控制到最低限度。在包装及安全分送和安装过程中，这种控制应采取软件控制系统的方式，确认安全性会由末端用户考虑，所有安全机制都应以功能状态交付。

d) 所有软件应提供安全安装默认值，在客户不做选择时，默认值应使安全机制有效地发挥安全功能。

e) 随同系统交付的全部默认用户标识码，应在交付时处于非激活状态，并在使用前由管理员激活。

f) 用户文档应同交付的软件一起包装，并应有一套规程确保当前送给用户的系统软件是严格按照最新的系统版本来制作的。

4.2.3.3 开发

应按照**《通用技术要求》6.2.5.3 条**开发的要求，进行操作系统 TCB 的开发。**本安全级的具体要求为：**

a) 要求按非形式化功能说明、**完全定义的外部接口、**描述性高层设计、TSF 子集实现、TSF 内部结构模块化和**复杂性降低**、描述性低层设计、非形式化对应性说明以及**非形式化安全策略模型**的要求，进行 TCB 的开发。

b) 系统的设计和开发应保护数据的完整性，例如，检查数据更新的规则，二重/多重输入的正确处理，返回状态的检查，中间结果的检查，合理值输入检查，事务处理更新的正确性检查等。

c) 在内部代码检查时，应解决潜在的安全缺陷，关闭或取消所有的后门。

d) 所有交付的软件和文档，应进行关于安全缺陷的定期的和书面的检查，并将检查结果告知用户。

e) 系统控制数据，如口令和密钥，不应在未受保护的程序或文档中以明文形式存储，并以书面形式提供给用户关于软件所有权法律保护的指南。

4.2.3.4 指导性文档

应按照**《通用技术要求》6.2.5.4 条指导性文档**的要求，编制 TCB 的指导性文档。本安全级的具体要求为：

a) 用户文档应提供关于不同用户的可见的安全机制以及如何利用它们的信息，描述没有明示用户的保护结构，并解释它们的用途和提供有关它们使用的指南，不应包括那些如果公开将会危及系统安全的任何信息。

b) 系统管理员文档应提供：

——关于系统的安全开机、操作和重新启动的信息，包括启动系统的过程（如引导系统进入安全方式）、在系统操作失误时恢复安全系统操作的过程、运行软件和数据备份及转储的方法和过程；

——一个单独的安装指南，详细说明设置系统的配置和初始化过程，提供一个新系统版本的安全设置和安装文档，包括对所有用户可见的安全相关过程、软件和数据文档的描述。

c) 安全管理员文档应提供：

——有关如何设置、维护和分析系统安全的详细指导，包括当运行一个安全设备时，需要控制的有关功能和特权的警告；

——与安全有关的管理员功能的详细描述，包括增加和删除一个用户、改变用户的安全特征等；

——**提供关于所有审计工具的文档，包括为检查和保持审计文件所推荐的过程、针对每种审计事件的详细审计记录文件、为周期性备份和删除审计记录所推荐的过程、为检查能被目录文件所利用的磁盘剩余空间所推荐的过程；**

——**关于设置所有文件和目录的最低访问许可的建议；**

——**运行文件系统或磁盘完整性检测所做的建议；**

——**如何进行系统自我评估的章节（带有网络管理、口令要求、拨号访问控制、意外事故计划的安全报告），为灾害恢复计划所做的建议；**

——**描述普通侵入技术和其它威胁，并查出和阻止它们的内容。**

d) 文档中不应提供任何一旦泄露将会危及系统安全的信息。有关安全的指令和文档应划分等级分别提供给用户、系统管理员和系统安全员。这些文档应为独立的文档，或作为独立的章节插入到管理员指南和用户指南中。文档也可为硬拷贝、电子文档或联机文档。如果是联机文档应控制对其的访问。

4.2.3.5 生命周期支持

应按照**《通用技术要求》6.2.5.5 条生命周期支持**的要求，设计和实现操作系统的 TCB。本安全级的具体要求为：

a) 应按开发者定义生命周期模型进行开发，并提供**开发过程中的安全措施说明。**

b) 所有安全软件应提供安全安装默认值。在未做特殊选择时,应按默认值安装安全机制。

c) 随同系统交付的全部默认用户标识号，在安装完时应处于非激活状态，并由系统管理员加以激活。

d) 文档应详细阐述安全启动和操作的过程，详细说明安全功能在启动、正常操作维护时是否能被撤消或修改，说明在故障或系统出错时如何恢复系统至安全状态。

e) **如果系统含有加强安全性的硬件，那么管理员、终端用户或自动的诊断测试，应能在各自的操作环境中运行它并详细说明操作过程。**

4.2.3.6 测试

应按照**《通用技术要求》6.2.5.6 条测试**的要求，对操作系统的 TCB 进行测试。本安全级的具体要求为：

a) 应通过一般功能测试和相符性独立测试、**测试的范围分析、高层设计的测试**，确认 TCB 的功能与所要求的功能相一致。

b) 所有系统的安全特性，应被全面测试，**包括查找漏洞，如允许违反系统访问控制要求、允许违反资源访问控制要求、允许拒绝服务、允许多审计或验证数据进行未授权访问等。**所有被发现的漏洞应被改正、消除或使其无效，并在消除漏洞后重新测试，以证实它们已被消除，且没有引出新的漏洞。

c) 应提供测试文档，详细描述测试计划、测试过程、测试结果。

4.2.3.7 脆弱性评定

应按照《通用技术要求》6.2.5.7 条脆弱性评定所描述的要求对所开发的 TCB 进行脆弱性评定。本安全级的具体要求为：

a) 从指南检查、TCB 安全功能强度评估和开发者脆弱性分析等方面进行脆弱性评定。

4.2.4 TCB 安全管理

应按照**《通用技术要求》6.2.6 条 TCB 安全管理**所描述的要求，实现 TCB 的安全管理。本安全级的具体要求为：

a) 对相应的 TCB 的访问控制、鉴别控制、审计和安全属性管理等相关的功能，以及与一般的安装、配置**和维护**有关的功能，制定相应的操作、运行规程和行为规章制度。

b) 根据本级中安全功能技术要求所涉及的自主访问控制、身份鉴别、**客体重用、审计、**数据完整性、和安全保证技术要求所涉及的配置管理、分发和操作、开发、指导性文档、生命周期支持、测试、**脆弱性评定**等所涉及的有关内容设计 TCB 安全管理。

4.3 第三级：安全标记保护级

4.3.1 安全功能

4.3.1.1 自主访问控制

应按照**《通用技术要求》6.3.3.3 条**的要求，设计和实现操作系统的自主访问控制功能。

在本安全级中，要求有更细粒度的自主访问控制。对系统中的每一个客体，都应能够实现由客体的创建者（用户）以用户指定方式或默认方式确定其对该客体的访问权限，而别的同组用户或非同组的用户和用户组对该客体的访问权则应由创建者用户授予，并将访问控制的粒度控制在单个用户，做到只有授权用户才能对该客体实施所授权的访问，而阻止那些非授权的用户对该客体进行任何访问，也阻止授权用户以非授权的操作形式对该客体进行访问。本级还要求自主访问控制能与身份鉴别和审计相结合，通过确认用户身份的真实性和记录用户的各种成功的或不成功的访问，使用户对自己的行为承担明确的责任。

本级中，对自主访问控制的要求应包括：

——定义访问控制属性，并保护这些属性。主体的访问控制属性至少应有：读、写、运行等；客体的访问控制属性应包含可分配给主体的读、写和执行的权限。

——定义分配和修改主体和客体的访问控制属性的规则，并执行对主体和客体的访问控制属性的分配和修改，规则的结果应达到只有被授权的用户才允许访问一个客体。

——定义主体对客体的访问授权规则。该规则应基于主体对客体的访问控制属性，授权的范围应包括主体和客体及相关的访问控制属性，同时应指出主体和客体对这些规则应用的类型。

——所有主体和客体的创建和删除应由系统来进行。主体可请求系统创建和删除主体和客体，但不允许它自己去做这些，从而保证主体和客体不能以危害由系统包含的信息的方式来创建。

无论何时一个主体或客体被创建，系统应保证被用于创建该主体或客体的资源不能包含以前使用的任何信息，这些资源主要有：存储器、文件、目录、符号连接、管道、消息队列、信号灯、共享主存等。

实现操作系统自主访问控制的具体方法有：

a) 基于目录表访问的自主访问控制，应为每个实施访问的主体建立一张可以被该主体访问的“客体目录表”。每个用户在其文件目录表中依次列出文件名，并逐一标明对这些文件的访问权限。权限一般分为四种：读、写、执行和属主。每个客体应有唯一的属主。属主具有访问权和分配、回收其他用户的访问权的权限。文件目录表的修改只有文件的属主才能实施，其他任何用户不允许在文件目录表中写，因此，操作系统应在文件的拥有者控制下维护所有的文件目录。

b) 基于存取控制表的自主访问控制，应决定任何一个确定的主体是否可对某一客体进行访问，并识别存取文件的单个用户或用户组。对系统中每一个需要保护的客体，都应为其附加一个主体明细表，表中的每一项包括主体的身份以及对该客体的访问权。这些信息应贮存在某个地方，清楚地与客体相连，高效地标识可存取文件的用户。

c) 访问控制矩阵模型，应用状态和状态转换进行访问关系定义。访问控制矩阵可是一张表格，每行代表一个用户（主体），每列代表一个存取目标（客体），表中的每个元素是该主体对客体的访问权集合。访问的权限应包括读、写、执行和删除。访问控制矩阵一般是稀疏的，矩阵内多数的项为空，即多数主体无权访问多数客体。访问控制矩阵根据不同类型的客体被允许实施的操作规定存取的种类。矩阵状态的转换通过命令集合将命令规定成一系列基本操作实现，主要包括：

——在 A[S,O]中增加权力 R；

——在 A[S,O]中删除权力 R；

——生成主体 S；

——生成客体 O；

——删除主体 S；

——删除客体 O。

d) 能力表是存取矩阵的另一种改进类型。能力表与主体相关，每个用户应有一个能力表，决定用户是否可以对客体进行访问以及进行何种模式的访问（读、写、执行）。一个拥有一定能力的主体允许依照一定的模式访问客体，在进程运行期间，可删除或添加某些能力。一个用户的能力可以转让，也可以回收，还可以包含在程序、数据文件、硬件、软件中，并采用一定措施进行保护。

e) 拥有者/同组/其他访问控制机制，是在每个文件上附加一段有关存取控制信息的二进制位，这些位应反映不同类型用户的存取方式，一般不超过四类：文件的拥有者、与文件拥有者同组的用户、特定的系统用户和其他用户。每一类用户都应有一组权限，每组权限有三个权限标志位来控制以下权限：

——可读（r）：如果被设置，则文件或目录可读。

——可写（w）：如果被设置，文件或目录可以被写入或修改。

——可执行（x）：如果被设置，文件或目录可以被执行和搜索。

f) 客体的拥有者应是唯一有权修改客体访问权限的主体，拥有者对其拥有的客体应具有全部控制权，但是，不允许客体拥有者把该客体的控制权分配给其他主体。因此，客体拥有者在任

何时候都可以改变其所属客体的访问控制表，并可对其他主体授予或撤消对该客体的任何一种访问模式。另外，可设立系统管理员（也称为超级用户），有权修改系统中所有客体的访问控制表，并可对所有客体进行所有模式的访问。

4.3.1.2 强制访问控制

应按照《通用技术要求》6.3.3.5 条强制访问控制的要求，设计和实现所需要的强制访问控制功能。本安全级的具体要求为：

a) **应由专门设置的系统安全员统一管理计算机信息系统中与强制访问控制有关的事件和信息，并将系统的常规管理、与安全有关的管理以及审计管理，分别由系统管理员、系统安全员和系统审计员来承担，按最小授权原则分别授予它们各自为完成自己所承担任务所需的最小权限，在三者之间形成相互制约的关系。**

b) **强制访问控制应与用户身份鉴别、标记等安全功能密切配合，使系统对用户的安全控制包含从用户进入系统到退出系统的全过程。本安全级，要求对客体的控制范围仅涉及信息系统内部的存储、处理和传输过程，可不包括将信息进行输入、输出操作的过程。**

c) **对运行于网络环境的分布式操作系统，应设计统一的 TCB，考虑到跨网络的情况，应在分布式控制中心设置 TCB 安全功能模块，统一实现强制访问控制功能。**

d) **对运行于网络环境的多台计算机系统上的操作系统，应在每一台计算机操作系统内设计一个完整的 TCB，实现强制访问控制功能，并在需要时实现跨网络的 TCB 间用户数据保密性和完整性保护，还应统一考虑各台计算机系统的主、客体安全属性设置的一致性。**

4.3.1.3 标记

应按照《通用技术要求》6.3.3.4 条标记的要求，设计和实现标记功能。本安全级的具体要求为：

a) **应采用标记的方法为操作系统 TCB 安全功能控制范围内的主体和客体设置安全属性。这些安全属性构成采用多级安全模型的强制访问控制机制的属性库——强制访问控制的基础数据。操作系统用户的安全属性应在用户建立注册帐户后由系统安全员通过 TCB 所提供的安全员界面进行标记；客体的安全属性应在数据输入到由 TCB 安全功能所控制的范围内时以缺省方式生成或由安全员进行标记。**

b) **当信息从 TCB 控制范围之内向 TCB 控制范围之外输出时，可不带有安全属性；当信息从 TCB 控制范围之外向 TCB 控制范围之内输入时，应通过标记标明其安全属性。**

4.3.1.4 身份鉴别

应按照**《通用技术要求》6.3.3.1 条用户标识和《通用技术要求》6.3.3.2 条用户鉴别**的要求，设计和实现操作系统的身份鉴别功能。本安全级的具体要求为：

a) 在以请求访问方式引起信息流动时，除可采用口令进行鉴别，并在每次用户登录系统时对请求者的身份进行鉴别外，**还应有更加严格的身份鉴别，如采用智能 IC 卡、指纹、视网膜等特殊信息进行身份鉴别，并应在每次用户登录系统之前进行鉴别。智能 IC 卡身份鉴别应以密码技术为基础，并符合 X .509 协议。**

b) 在以交换方式引起信息流动时，**应进行通行双方身份的真实性和双方对对信交换行为的不可抵赖性鉴别。**

4.3.1.5 客体重用

应按照**《通用技术要求》6.3.3.6 条客体重用**的要求设计操作系统的客体重用功能。本安全级的具体要求为：

a) 应确保动态分配与管理的资源，在保持信息安全的情况下被再利用，主要包括：

——确保非授权用户不能查找在使用后返还系统的记录介质中的信息内容；

——确保非授权用户不能查找系统现已分配给他的记录介质中以前的信息内容。

b) 在单用户系统中，存储器保护应防止用户进程不影响系统的运行.

c) 在一个多用户系统中，存储器保护应保证系统内各个用户之间互不干扰。

d) 存储器保护应包括:

——对存储单元的地址的保护，使非法用户不能访问那些受到保护的存储单元；

——对被保护的存储单元的操作提供各种类型的保护。最基本的保护类型是“读/写”和“只读”。不能读/写的存储单元，若被用户读/写时，系统应及时发出警报或中断程序执行。

——可采用逻辑隔离的方法进行存储器保护，具体有：界限地址寄存器保护法、内存标志法、锁保护法和特征位保护法等。

4.3.1.6 审计

应按照**《通用技术要求》6.3.2.4 条审计**的要求设计操作系统的审计功能。本安全级的具体要求为：

a) 审计功能应与用户标识与鉴别、自主访问控制、**标记及强制访问控制**等安全功能的设计紧密结合。

b) 应能够生成、维护及保护审计过程，使其免遭修改、非法访问及破坏，特别要保护审计数据，要严格限制未经授权的用户访问。

c) 应记录以下类型的事件：

——使用识别与鉴别机制（如注册过程）；

——将某个客体引入某个用户的地址空间（如打开文件）；

——删除客体及计算机操作员、系统管理员与系统安全管理员进程的操作。

d) 每个审计记录应记录事件发生的日期与时间、产生这一事件的用户、事件的类型以及该事件成功与否。对于识别与鉴别事件，审计记录应记录事件发生的源地点；对于将一个客体信息引入某个用户地址空间中的事件以及删除客体的事件，审计记录应包括客体名及客体的安全级别。

e) 本安全级要求基本的审计功能主要包括：

——授权控制和审计跟踪，应能够创建并维护一个对受保护客体访问的审计跟踪，保护审计记录不被未授权的访问、修改和破坏。

——可记录的安全相关事件，应能指出可记录的审计事件的最少类型，包括建立会话登录成功和失败，使用的系统接口，系统数据库管理的改变（改变用户账户属性、审计跟踪设置和分析、为程序分配设置用户 ID、附加或改变系统程序或进程、改变日期和时间等），超级用户命令改变用户身份等。当审计激活时应确保审计跟踪事件的完整性；应提供一个机制来显示当前选择的审计事件，这个机制的使用者应是有限的授权用户。

——每个事件的数据记录，应包括的信息有：事件发生的日期和时间、触发事件的用户、事件的类型、事件成功或失败等。对于身份识别和认证事件，应记录请求的源（如终端号或网络地址）；对于创建和删除客体的事件，应记录客体的名字和属性。

——审计跟踪控制、管理和检查，应提供一个受保护的打开和关闭审计的机制。该机制能选择和改变审计事件，并在系统工作时处于默认状态；该机制的使用应受到系统管理员的授权限制，系统管理员应能够选择一个或多个基于身份识别或客体属性的用户的审计活

动；审计工具应能够授权个人监察和浏览审计数据，同时数据应得到授权的使用、修改和删除；应提供对审计跟踪管理功能的保护，使之可以完成审计跟踪的创建、破坏、腾空和存档；系统管理员应能够定义超过审计跟踪极限的阈值；当存储空间被耗尽时，应能按管理员的指定决定采取的措施，包括：报警并丢弃未记录的审计信息、暂停审计、覆盖以前的审计记录等。

4.3.1.7 数据完整性

应按照**《通用技术要求》6.3.3.7 条数据完整性**的要求，设计和实现操作系统的数据完整性功能。本安全级的具体要求为：

a) 应通过对系统中的信息采取有效措施，防止其遭受非授权用户的修改、破坏或删除。

b) 进程应具有高完整性，确保系统能正确运行，不致混乱或崩溃。为此，需要设计相应的 TCB 来实现有关功能。

c) 对在操作系统中经网络传输信息的完整性保护，要求 TCB 提供监视用户数据完整性的功能，即能检测出被传输的用户数据被篡改、删除、插入和重用等情况发生，并进行报警。

d) 对存储在 TCB 安全控制范围内的用户数据应进行完整性保护，实现存储数据的完整性监视，并进行报警。

e) 对磁盘设备中存储的数据，可通过增加磁盘扫描程序实现以下功能：

——自动检查文件与磁盘表面是否完好；

——修复扇区交错和扇区流失；

——将磁盘表面的问题自动记录下来；

——将数据移到好的扇区；

——随时检查、诊断和修复磁盘上的错误。

——可在系统中增加计算机病毒检测、诊断和预防程序；

——也可增加硬盘数据备份和修复程序，将硬盘中的数据压缩、备份，并在必要时恢复。

g) 对在操作系统中进行处理的信息的完整性保护，应通过对各种异常情况事务的回退，以事务的完整性确保数据的完整性。

4.3.2 TCB 自身安全保护

4.3.2.1 TSF 保护

应按照**《通用技术要求》6.3.4.1 条 TSF 保护**的要求，设计和实现操作系统的 TSF 保护。本安全级中，操作系统 TSF 保护的具体要求为：

a) 系统在设计时不应留有“后门”。即不应以维护、支持或操作需要为借口，设计有违反或绕过安全规则的任何类型的入口和文档中未说明的任何模式的入口。

b) 安全结构应是一个独立的、严格定义的系统软件的一个子集，并应防止外部干扰和破坏，如修改其代码或数据结构。

c) 操作系统应进行分层设计，对操作系统程序和用户程序要进行隔离。

d) 一个进程的虚地址空间至少应被分为两个段：用户空间和系统空间，两者的隔离应是静态的。驻留在内存中的操作系统应由所有进程共享。用户进程之间应是彼此隔离的。应禁止在用户模式下运行的进程对系统段进行写操作，而在系统模式下运行时，应允许进程对所有的虚存空间进行读、写操作。用户模式到系统模式的转换应由一个特殊的指令完成，该指令将限制进程只能对部分系统空间进程访问，这些访问限制应由硬件根据该进程的特权模式实施。

e) TCB 应提供一个设置和升级配置参数的安装机制。在初始化和对与安全有关的数据结构进行保护之前，应对用户和管理员的安全策略属性应进行定义。

f) TCB 应区分普通操作模式和系统维护模式，TCB 的恢复、全系统操作恢复的启动、配置 TCB 内部的数据库和表等动作应在维护模式中执行。

g) TCB 应防止一个普通用户从未经允许的系统进入维护模式，并应防止一个普通用户与系统内维护模式交互。从而保证在普通用户访问系统之前，系统能以一个安全的方式进行安装和配置。安全机制应在维护模式中保护普通用户的入口。

h) 对备份或不影响 TCB 的常规的系统维护，不要求所有的系统维护都在维护模式中执行。

i) 当操作系统安装完成后，在普通用户访问之前，系统应配置好初始用户和管理员职责、根目录、审计参数、系统审计跟踪设置以及对文件和目录的合适的访问控制。

j) 执行系统所提供的实用程序，应（默认地）限定于对系统的有效使用，只允许系统管理员修改或替换系统提供的实用程序。

k) 操作环境应为用户提供一个机制，来控制命令的目录/路径的查找顺序。

l) 系统应提供一个实用程序来校验文件系统和磁盘的完整性。此实用程序应由操作系统自动执行。

m) 系统应为系统管理员提供一种机制，来产生安全参数值的详细报告。

n) 在 TCB 失败或中断后，进程应保证保护文本以最小的损害得到恢复。并按照失败保护中所描述的内容，实现对 TSF 出现失败时的处理。**系统因故障或其它原因中断后，应有一种机制去恢复系统。系统应提供在管理维护状态中运行的能力，管理维护状态只能被系统管理员使用，各种安全功能全部失效。**

o) 操作系统环境应控制和审计系统控制台的使用情况。

p) 系统应能识别由通信渠道接收的信息的来源者，所有待确认的数据应能从进入点被安全地传送到确认系统，如口令不应由公共的或共享的网络以明文发送，可使用数据加密设备或通过加密信道用加密模式传送。

4.3.2.2 资源利用

应按照**《通用技术要求》6.3.4.2 条资源利用**的要求，设计和实现操作系统的资源利用。在本安全级中，资源利用设计的具体要求为：

a) 应通过一定措施确保当系统出现某些确定的故障情况时，TSF 也能维持正常运行，如系统应检测和报告系统的服务水平已降低到预先规定的最小值；

b) 应采取适当的策略，有限服务优先级提供主体使用 TSC 内某个资源子集的优先级，进行 TCB 资源的管理和分配；

c) 应按资源分配中最大限额的要求，进行 TCB 资源的管理和分配，要求配额机制确保用户和主体将不会独占某种受控的资源。

d) 系统应确保在被授权的主体发出请求时，资源能被访问和利用。

e) 当系统的服务水平降低到预先规定的最小值时，应能检测和发出报告。

f) 系统应提供管理维护状态中运行的能力，在管理维护状态下各种安全性能全部失效，系统只允许由系统管理员使用。

g) 系统应以每个用户或每个用户组为基础，提供一种机制，控制他们对磁盘的消耗和对 CPU 的使用。

h) 系统应提供软件及数据备份和复原的过程，在系统中应加入再启动的同步点，以便于系统的

复原。

i） **操作系统应能提供任一命名的或用户可访问的系统资源的修改历史记录。**

j） **系统应提供能用于定期确认系统正确操作的机制和过程，这些机制或过程应涉及系统资源的监督、硬件和固件单元的正确操作、对可能在全系统内传播的错误状态的检测以及超过用户规定的门限的通讯差错的检测等内容。**

4.3.2.3 TCB 访问控制

应按照**《通用技术要求》6.3.4.3 条 TCB 访问控制**的要求，设计和实现操作系统的 TCB 访问控制。本安全级中，操作系统 TCB 访问控制设计的具体要求为：

a） 应按照可选属性范围限定最小级的要求，选择某种会话安全属性的所有失败的尝试 ，对用来建立会话的安全属性的范围进行限制；

b） 应按照多重并发会话限定中基本限定的要求，提供适用于 TSF 内所有用户的限制实现对会话管理的设计，允许用户会话建立的所有尝试；

c） 应按照 TCB 访问历史所描述的要求，实现对会话管理的设计，在会话成功建立的基础上，TSF 应显示用户上一次成功/不成功的会话建立的日期，时间，方法，位置，以及从上一次成功的会话建立以来的不成功的尝试的次数。

d） 应按照 TCB 会话建立所描述的要求，实现对会话管理的设计，TSF 应根据属性允许或拒绝该次会话的建立，这些属性包括：访问地址或端口，用户安全属性（如用户身份、许可证等级、完整性等级、角色中的成员资格），时间范围（如一天中的某些时间、一周的某些天、某些特定日期），或上述属性的组合。

按照以上要求，本级要求在操作系统中应采取的措施主要有：

a） 在建立 TCB 会话之前，认证机制应用这个用户的认证数据由 TCB 校验用户的身份。登录机制不允许认证机制本身被旁路。

b） 为给用户提供系统登录活动的有关信息，让用户识别入侵的企图，采取行动防止可能的未授权使用，成功登录系统后，TCB 应向用户显示以下数据：

——日期、时间、来源和上次成功登录系统的情况；

——上次成功访问系统以来身份识别失败的情况；

——应显示口令到期的天数；

——成功或不成功的事件次数的显示可以用整数计数、时间戳列表等表述方法。

c) 在规定的未使用时限后，系统应断开会话或重新认证用户，系统应提供期限的默认值。

d) 系统应提供锁定用户键盘的机制，键盘开锁过程应要求验证用户。

e) 当用户认证过程不正确的次数达到系统规定的次数时，系统应退出登录过程并终止与用户的交互。系统应提供门限默认值。当门限值被超过时，系统应立即通知系统管理员，同时系统可以指定一段停顿时间，在这段时间之后，才允许重新开始登录程序。系统应具有在连续的侵入尝试下，增加时间间隔的能力，从而延长系统被攻破的时间。

f) 系统应保证即使输入的用户标识是无效的，也应进行完整的用户验证过程，出错的反馈信息不应暴露是哪一部分的验证信息是错误的。

g) 系统应提供一种机制，能按钟点、周日、年月日等条件规定哪些用户能进入系统，哪些用户不能进入系统。

h) 系统应提供一种机制，能按照进入方式或地点拒绝或接受用户。系统应提供限制被授权的用

户通过拨号设备或网络设备访问系统的机制。

i) 系统应提供一种机制，能限制用户在指定的网络地址或端口访问系统。例如，限制系统管理员只能通过系统控制台访问系统。

j) 系统应提供一种机制，限制指定的用户或用户组只能进行不修改的访问。

4.3.3 TCB 设计和实现

4.3.3.1 配置管理

应按照**《通用技术要求》6.3.5.1 条配置管理**所描述的要求进行设计。本安全级的具体要求为：

a) 在配置管理自动化方面要求部分的配置管理自动化。

b) 在配置管理能力方面应实现对版本号、配置项、授权控制等方面的要求。

c) 在 TCB 的配置管理范围方面，应将 TCB 的实现表示、设计文档、测试文档、用户文档、管理员文档以及配置管理文档等置于配置管理之下，**要求实现对配置管理范围内的问题，特别是安全缺陷问题进行跟踪。**

d) 在系统的整个生存期，即在它的开发、测试和维护期间，应有一个软件配置管理系统处于保持对改变源码和文件的控制状态。只有被授权的代码和代码修改才允许被加进已交付的源码的基本部分。所有改变应被记载和检查，以确保未危及系统的安全。在软件配置管理系统中，应包含从源码产生出系统新版本、鉴定新生成的系统版本和保护源码免遭未授权修改的工具和规程。通过技术、物理和保安规章三方面的结合，可充分保护生成系统所用到的源码免遭未授权的修改和毁坏。

4.3.3.2 分发和操作

应按照**《通用技术要求》6.3.5.2 条分发和操作**的要求，设计和实现操作系统的 TCB 分发和操作。本安全级的具体要求为：

a) 应以文档形式提供对 TCB 安全地进行分发的过程，以及安装、生成和启动的过程进行说明，并最终生成安全的配置。文档中所描述的内容应包括：

——提供分发的过程；

——安全启动和操作的过程；

——建立日志的过程；

——修改检测的内容；

——对任何安全加强功能在启动、正常操作维护时能被撤消或修改的阐述；

——在故障或硬件、软件出错后恢复系统至安全状态的规程；

——对含有加强安全性的硬件部件，应说明用户或自动的诊断测试的操作环境和使用方法；

——所有诊断测试过程中，为加强安全性的硬件部件所提供例证的结果；

——在启动和操作时产生审计踪迹输出的例证。

b) 对系统的未授权修改的风险，应在交付时控制到最低限度。在包装及安全分送和安装过程中，这种控制应采取软件控制系统的方式，确认安全性会由末端用户考虑，所有安全机制都应以功能状态交付。

c) 所有软件应提供安全安装默认值，在客户不做选择时，默认值应使安全机制有效地发挥安全功能。

d) 随同系统交付的全部默认用户标识码，应在交付时处于非激活状态，并在使用前由管理员激活。

e) 用户文档应同交付的软件一起包装，并应有一套规程确保当前送给用户的系统软件是严格按

照最新的系统版本来制作的。

f) **以安全方式开发并交付系统后，仍应提供对产品的长期维护和评估的支持，包括产品中的安全漏洞和现场问题的解决。**

g) **向客户通告新的全问题应用书面说明。**

h) **可能受到威胁的所有的安全问题，均描述其特点，并被作为主要的问题对待，直到它被解决或在用户同意下降级使用。**

i) **为了支持已交付的软件的每个版本，对所有已有的安全漏洞都应有文档书面说明，并且该文档能在限制的基础上被用户得到。**

j) **对安全漏洞的修改不必等到系统升级到下一个版本。安全功能的增加和改进应独立于系统版本的升级，也就是说，应存在适应性独立于系统其它功能的改进。**

k) **没有客户授权，不允许在客户正在生产性运行的系统上进行新特性和简易原型的开发、测试和安装。**

l) **新的版本应避免违反最初的安全策略和设想，也应避免在维护、增加或功能升级中引入安全漏洞，所有功能的改变和安全结构设置的缺省默认值都应被记录。在新版本交付给用户使用前，用户应能得到该相应的文档。**

4.3.3.3 开发

应按照**《通用技术要求》6.3.5.3 条**开发的要求，进行操作系统 TCB 的开发。本安全级的具体要求为：

a) 应按非形式化功能说明、完全定义的外部接口、**安全加强的高层设计、TSF 完全实现、**TSF 内部结构模块化和复杂性降低、描述性低层设计、非形式化对应性说明以及非形式化安全策略模型的要求，进行 TCB 的开发。

b) 系统的设计和开发应保护数据的完整性，例如，检查数据更新的规则，二重/多重输入的正确处理，返回状态的检查，中间结果的检查，合理值输入检查，事务处理更新的正确性检查等。

c) 在内部代码检查时，应解决潜在的安全缺陷，关闭或取消所有的后门。

d) 所有交付的软件和文档，应进行关于安全缺陷的定期的和书面的检查，并将检查结果告知用户。

e) 系统控制数据，如口令和密钥，不应在未受保护的程序或文档中以明文形式存储，并以书面形式提供给用户关于软件所有权法律保护的指南。

f) **在操作系统开发的敏感阶段，应保持一个安全环境，该安全环境要求：**

——**描述操作系统开发所使用的计算机系统的安全使用和维护情况的安全策略和措施应有书面记载，并可供检查；**

——**系统开发过程中使用的所有计算机系统应接受定期的和有书面记载的内部安全审计，描述审计过程的文件和真实的审计报告应可供检查；**

——**除授权的分发机构外，不应在开发环境外部复制或分发内部文档；**

——**开发环境的计算机系统使用的所有软件应当合法地从确定的渠道获得；**

——**开发者个人独自开发的软件，应在被开发管理者审核后才能用于开发的系统。**

4.3.3.4 指导性文档

应按照**《通用技术要求》6.3.5.4 条指导性文档**的要求，编制 TCB 的指导性文档。本安全级的具体要求为：

a) **应为最终用户提供简单概要、分章节或手册形式的文档，保证用户拥有进行安全操作所需要的所有信息。与安全有关的信息应包含在一个特别的手册中或许多标准的文本集中，提供用户查阅所有的安全功能。这些信息可随系统发送，也可明确指出它包含在哪个文本当中。**

b) **通过提供指导性文档，应把如何安全使用和维护操作系统的信息交付给系统的用户、系统管理员和系统安全员。对文档的总体要求是：**

——应对所有的安全访问和相关过程、特权、功能等适当的管理加以阐述；

——应阐述安全管理和安全服务的交互，并提供新的 TCB 安全生成的指导；

——应详细给出每种审计事件的审计记录的结构，以便考察和维护审计文件和进程；

——应提供一个准则集用于保证附加的说明的一致性不受破坏。

c) 用户文档应提供关于不同用户的可见的安全机制以及如何利用它们的信息，描述没有明示用户的保护结构，并解释它们的用途和提供有关它们使用的指南，不应包括那些如果公开将会危及系统安全的任何信息。

d) 系统管理员文档应提供：

——关于系统的安全开机、操作和重新启动的信息，包括启动系统的过程（如引导系统进入安全方式）、在系统操作失误时恢复安全系统操作的过程、运行软件和数据备份及转储的方法和过程；

——一个单独的安装指南，详细说明设置系统的配置和初始化过程，提供一个新系统版本的安全设置和安装文档，包括对所有用户可见的安全相关过程、软件和数据文档的描述。

e) 安全管理员文档应提供：

——有关如何设置、维护和分析系统安全的详细指导，包括当运行一个安全设备时，需要控制的有关功能和特权的警告；

——与安全有关的管理员功能的详细描述，包括增加和删除一个用户、改变用户的安全特征等；

——提供关于所有审计工具的文档，包括为检查和保持审计文件所推荐的过程、针对每种审计事件的详细审计记录文件、为周期性备份和删除审计记录所推荐的过程、为检查能被目录文件所利用的磁盘剩余空间所推荐的过程；

——关于设置所有文件和目录的最低访问许可的建议；

——运行文件系统或磁盘完整性检测所做的建议；

——如何进行系统自我评估的章节（带有网络管理、口令要求、拨号访问控制、意外事故计划的安全报告），为灾害恢复计划所做的建议；

——描述普通侵入技术和其它威胁，并查出和阻止它们的内容。

f) **安全管理员文档应提供安全管理员了解如何用安全的方式管理系统，除了给出一般的安全忠告，还要明确：**

——在系统用安全的方法设置时，围绕用户、用户帐号、用户组成员关系、主体和客体的属性等，应如何安装或终止安装；

——在系统的生命周期内如何用安全的方法维护系统，包括为了防止系统被破坏而进行的每天、每周、每月的安全常规备份等；

——如何用安全的方法重建部分 TCB（如内核）的方法（如果允许在系统上重建 TCB）；

——说明审计跟踪机制，使授权用户可以有效地使用审计跟踪来执行本地的安全策略；

——必要时，如何调整系统的安全默认配置。

g) 文档中不应提供任何一旦泄露将会危及系统安全的信息。有关安全的指令和文档应划分等级分别提供给用户、系统管理员和系统安全员。这些文档应为独立的文档，或作为独立的章节插入到管理员指南和用户指南中。文档也可为硬拷贝、电子文档或联机文档。如果是联机文档应控制对其的访问。

4.3.3.5 生命周期支持

应按照**《通用技术要求》6.3.5.5 条生命周期支持**的要求，设计和实现操作系统的 TCB。本安全级的具体要求为：

a) **应按标准的生命周期模型进行开发，**提供安全措施说明，**并明确定义开发工具。**

b) 所有安全软件应提供安全安装默认值。在未做特殊选择时,应按默认值安装安全机制。

c) 随同系统交付的全部默认用户标识号，在安装完时应处于非激活状态，并由系统管理员加以激活。

d) 文档应详细阐述安全启动和操作的过程，详细说明安全功能在启动、正常操作维护时是否能被撤消或修改，说明在故障或系统出错时如何恢复系统至安全状态。

e) 如果系统含有加强安全性的硬件，那么管理员、终端用户或自动的诊断测试，应能在各自的操作环境中运行它并详细说明操作过程。

4.3.3.6 测试

a) 应按照**《通用技术要求》6.3.5.6 条测试**的要求，对操作系统的 TCB 进行测试。

b) 应通过一般功能测试和**抽样性独立测试**，测试的范围分析，高层设计测试、**低层设计测试，顺序的功能测试等**，确认 TCB 的功能与所要求的功能相一致。

c) 所有系统的安全特性，应被全面测试，包括查找漏洞，如允许违反系统访问控制要求、允许违反资源访问控制要求、允许拒绝服务、允许多审计或验证数据进行未授权访问等。所有被发现的漏洞应被改正、消除或使其无效，并在消除漏洞后重新测试，以证实它们已被消除，且没有引出新的漏洞。

d) 应提供测试文档，详细描述测试计划、测试过程、测试结果。

4.3.3.7 脆弱性评定

应按照《通用技术要求》6**.3.5.7 条脆弱性评定**所描述的要求对所开发的 TCB 进行脆弱性评定。本安全级的具体要求为：

a) 从指南检查、**分析确认**，TCB 安全功能强度评估，开发者脆弱性分析、**独立脆弱性分析**等方面进行脆弱性评定。

4.3.4 TCB 安全管理

应按照**《通用技术要求》6.3.6 条 TCB 安全管理**所描述的要求，实现 TCB 的安全管理。本安全级的具体要求为：

a) 对相应的 TCB 的访问控制、鉴别控制、审计和安全属性管理等相关的功能，以及与一般的安装、配置和维护有关的功能，制定相应的操作、运行规程和行为规章制度。

b) 根据本级中安全功能技术要求所涉及的自主访问控制、**标记、强制访问控制**、身份鉴别、客体重用、审计、数据完整性、和安全保证技术要求所涉及的配置管理、分发和操作、开发、指导性文档、生命周期支持、测试、脆弱性评定等所涉及的有关内容设计 TCB 安全管理。

c) 应将系统管理员、安全员和审计员等重要安全角色分别设置专人担任，并按“最小授权原则”分别授予他们各自为完成自身任务所需的最小权限，并形成相互制约的关系。

4.4 第四级：结构化保护级

4.4.1 安全功能

4.4.1.1 自主访问控制

应按照**《通用技术要求》6.4.3.3 条**的要求，设计和实现操作系统的自主访问控制功能。

在本安全级中，要求有更细粒度的自主访问控制，**并将自主访问控制扩展到计算机信息系统的所有主体与客体。**对系统中的每一个客体，都应能够实现由客体的创建者（用户）以用户指定方式或默认方式确定其对该客体的访问权限，而别的同组用户或非同组的用户和用户组对该客体的访问权则应由创建者用户授予，并将访问控制的粒度控制在单个用户，做到只有授权用户才能对该客体实施所授权的访问，而阻止那些非授权的用户对该客体进行任何访问，也阻止授权用户以非授权的操作形式对该客体进行访问。本级还要求自主访问控制能与身份鉴别和审计相结合，通过确认用户身份的真实性和记录用户的各种成功的或不成功的访问，使用户对自己的行为承担明确的责任。

本级中，对自主访问控制的要求应包括：

——定义访问控制属性，并保护这些属性。主体的访问控制属性至少应有：读、写、运行等；客体的访问控制属性应包含可分配给主体的读、写和执行的权限。

——定义分配和修改主体和客体的访问控制属性的规则，并执行对主体和客体的访问控制属性的分配和修改，规则的结果应达到只有被授权的用户才允许访问一个客体。

——定义主体对客体的访问授权规则。该规则应基于主体对客体的访问控制属性，授权的范围应包括主体和客体及相关的访问控制属性，同时应指出主体和客体对这些规则应用的类型。

——所有主体和客体的创建和删除应由系统来进行。主体可请求系统创建和删除主体和客体，但不允许它自己去做这些，从而保证主体和客体不能以危害由系统包含的信息的方式来创建。无论何时一个主体或客体被创建，系统应保证被用于创建该主体或客体的资源不能包含以前使用的任何信息，这些资源主要有：存储器、文件、目录、符号连接、管道、消息队列、信号灯、共享主存等。

实现操作系统自主访问控制的具体方法有：

a) 基于目录表访问的自主访问控制，应为每个实施访问的主体建立一张可以被该主体访问的“客体目录表”。每个用户在其文件目录表中依次列出文件名，并逐一标明对这些文件的访问权限。权限一般分为四种：读、写、执行和属主。每个客体应有唯一的属主。属主具有访问权和分配、回收其他用户的访问权的权限。文件目录表的修改只有文件的属主才能实施，其他任何用户不允许在文件目录表中写，因此，操作系统应在文件的拥有者控制下维护所有的文件目录。

b) 基于存取控制表的自主访问控制，应决定任何一个确定的主体是否可对某一客体进行访问，并识别存取文件的单个用户或用户组。对系统中每一个需要保护的客体，都应为其附加一个主体明细表，表中的每一项包括主体的身份以及对该客体的访问权。这些信息应贮存在某个地方，清楚地与客体相连，高效地标识可存取文件的用户。

c) 访问控制矩阵模型，应用状态和状态转换进行访问关系定义。访问控制矩阵可是一张表格，每行代表一个用户（主体），每列代表一个存取目标（客体），表中的每个元素是该主体对客体的访问权集合。访问的权限应包括读、写、执行和删除。访问控制矩阵一般是稀疏的，矩阵内多数的项为空，即多数主体无权访问多数客体。访问控制矩阵根据不同类型的客体被允许实施的操作规定存取的种类。矩阵状态的转换通过命令集合将命令规定成一系列基本操作实现，主要包括：

——在 A[S,O]中增加权力 R；
——在 A[S,O]中删除权力 R；
——生成主体 S；
——生成客体 O；
——删除主体 S；
——删除客体 O。

d) 能力表是存取矩阵的另一种改进类型。能力表与主体相关，每个用户应有一个能力表，决定用户是否可以对客体进行访问以及进行何种模式的访问（读、写、执行）。一个拥有一定能力的主体允许依照一定的模式访问客体，在进程运行期间，可删除或添加某些能力。一个用户的能力可以转让，也可以回收，还可以包含在程序、数据文件、硬件、软件中，并采用一定措施进行保护。

e) 拥有者/同组/其他访问控制机制，是在每个文件上附加一段有关存取控制信息的二进制位，这些位应反映不同类型用户的存取方式，一般不超过四类：文件的拥有者、与文件拥有者同组的用户、特定的系统用户和其他用户。每一类用户都应有一组权限，每组权限有三个权限标志位来控制以下权限：
——可读（r）：如果被设置，则文件或目录可读。
——可写（w）：如果被设置，文件或目录可以被写入或修改。
——可执行（x）：如果被设置，文件或目录可以被执行和搜索。

f) 客体的拥有者应是唯一有权修改客体访问权限的主体，拥有者对其拥有的客体应具有全部控制权，但是，不允许客体拥有者把该客体的控制权分配给其他主体。因此，客体拥有者在任何时候都可以改变其所属客体的访问控制表，并可对其他主体授予或撤消对该客体的任何一种访问模式。另外，可设立系统管理员（也称为超级用户），有权修改系统中所有客体的访问控制表，并可对所有客体进行所有模式的访问。

4.4.1.2 强制访问控制

应按照**《通用技术要求》6.4.3.5 条强制访问控制**的要求，设计和实现所需要的强制访问控制功能。本安全级的具体要求为：

a) 由专门设置的系统安全员统一管理计算机信息系统中与强制访问控制有关的事件和信息，并将系统的常规管理、与安全有关的管理以及审计管理，分别由系统管理员、系统安全员和系统审计员来承担，按最小授权原则分别授予它们各自为完成自己所承担任务所需的最小权限，在三者之间形成相互制约的关系。

b) 强制访问控制应与用户身份鉴别、标记等安全功能密切配合，使系统对用户的安全控制包含从用户进入系统到退出系统的全过程。本安全级，**要求将强制访问控制扩展到计算机信息系统中的所有主体与客体**；要求对客体的控制范围涉及信息系统内部的存储、处理和传输过程，**及将信息进行输入、输出操作的过程，即无论信息以何种形式存在，都应有一定的安全属性与其相关联，并按强制访问控制规则对其进行控制。**

c) 对运行于网络环境的分布式操作系统，应设计统一的 TCB，考虑到跨网络的情况，应在分布式控制中心设置 TCB 安全功能模块，统一实现强制访问控制功能。

d) 对运行于网络环境的多台计算机系统上的操作系统，应在每一台计算机操作系统内设计一个完整的 TCB，实现强制访问控制功能，并在需要时实现跨网络的 TCB 间用户数据保密性和完整

性保护，还应统一考虑各台计算机系统的主、客体安全属性设置的一致性。

4.4.1.3 标记

应按照**《通用技术要求》6.4.3.4 条标记**的要求，设计和实现标记功能。本安全级的具体要求为：

a) 应采用标记的方法为操作系统 TCB 安全功能控制范围内的主体和客体设置安全属性。这些安全属性构成采用多级安全模型的强制访问控制机制的属性库——强制访问控制的基础数据。操作系统用户的安全属性应在用户建立注册帐户后由系统安全员通过 TCB 所提供的安全员界面进行标记；客体的安全属性应在数据输入到由 TCB 安全功能所控制的范围内时以缺省方式生成或由安全员进行标记。

b) **本级要求将标记扩展到信息系统中的所有主体与客体。当信息从 TCB 控制范围之内向 TCB 控制范围之外输出时，应带有安全属性，如打印输出的数据等，应明显标示出该数据的安全标记**；当信息从 TCB 控制范围之外向 TCB 控制范围之内输入时，应通过标记标明其安全属性。

4.4.1.4 身份鉴别

应按照**《通用技术要求》6.4.3.1 条用户标识和《通用技术要求》6.4.3.2 条用户鉴别**的要求，设计和实现操作系统的身份鉴别功能。本安全级的具体要求为：

a) 在以请求访问方式引起信息流动时，除可采用口令进行鉴别，并在每次用户登录系统时对请求者的身份进行鉴别外，还应有更加严格的身份鉴别，如采用智能 IC 卡、指纹、视网膜等特殊信息进行身份鉴别，并应在每次用户登录系统之前进行鉴别。智能 IC 卡身份鉴别以密码技术为基础，并符合 X .509 协议。

b) 在以交换方式引起信息流动时，应进行通行双方身份的真实性和双方对对信交换行为的不可抵赖性鉴别。

c) **在某些情况下，除了要求确保用户身份的唯一性和真实性外，还要求对某些用户的身份进行特别保护，使其不被其他用户发现或滥用。**

4.4.1.5 客体重用

应按照**《通用技术要求》6.4.3.6 条客体重用**的要求设计操作系统的客体重用功能。本安全级的具体要求为：

a) 应确保动态分配与管理的资源，在保持信息安全的情况下被再利用，主要包括：

——确保非授权用户不能查找在使用后返还系统的记录介质中的信息内容；

——确保非授权用户不能查找系统现已分配给他的记录介质中以前的信息内容。

b) 存储器保护应包括：

——对存储单元的地址的保护，使非法用户不能访问那些受到保护的存储单元；

——对被保护的存储单元的操作提供各种类型的保护。最基本的保护类型是“读/写”和“只读”。不能读/写的存储单元，若被用户读/写时，系统应及时发出警报或中断程序执行。

——可采用逻辑隔离的方法进行存储器保护，具体有：界限地址寄存器保护法、内存标志法、锁保护法和特征位保护法等。

c) 在单用户系统中，存储器保护应防止用户进程不影响系统的运行。

d) 在一个多用户系统中，存储器保护应保证系统内各个用户之间互不干扰。

4.4.1.6 审计

应按照**《通用技术要求》6.4.2.4 条审计**的要求设计操作系统的审计功能。本安全级的具体要求为：

a) 审计功能应与用户标识与鉴别、自主访问控制、**标记及强制访问控制**等安全功能的设计紧密

结合。

b) 应能够生成、维护及保护审计过程，使其免遭修改、非法访问及破坏，特别要保护审计数据，要严格限制未经授权的用户访问。

c) 应记录以下类型的事件：

——使用识别与鉴别机制（如注册过程）；

——将某个客体引入某个用户的地址空间（如打开文件）；

——删除客体及计算机操作员、系统管理员与系统安全管理员进程的操作。

d) 每个审计记录应记录事件发生的日期与时间、产生这一事件的用户、事件的类型以及该事件成功与否。对于识别与鉴别事件，审计记录应记录事件发生的源地点；对于将一个客体信息引入某个用户地址空间中的事件以及删除客体的事件，审计记录应包括客体名及客体的安全级别。

e) 本安全级要求基本的审计功能主要包括：

——授权控制和审计跟踪，应能够创建并维护一个对受保护客体访问的审计跟踪，保护审计记录不被未授权的访问、修改和破坏。

——可记录的安全相关事件，应能指出可记录的审计事件的最少类型，包括建立会话登录成功和失败，使用的系统接口，系统数据库管理的改变（改变用户账户属性、审计跟踪设置和分析、为程序分配设置用户 ID、附加或改变系统程序或进程、改变日期和时间等），超级用户命令改变用户身份等。当审计激活时应确保审计跟踪事件的完整性；应提供一个机制来显示当前选择的审计事件，这个机制的使用者应是有限的授权用户。

——每个事件的数据记录，应包括的信息有：事件发生的日期和时间、触发事件的用户、事件的类型、事件成功或失败等。对于身份识别和认证事件，应记录请求的源（如终端号或网络地址）；对于创建和删除客体的事件，应记录客体的名字和属性。

——审计跟踪控制、管理和检查，应提供一个受保护的打开和关闭审计的机制。该机制能选择和改变审计事件，并在系统工作时处于默认状态；该机制的使用应受到系统管理员的授权限制，系统管理员应能够选择一个或多个基于身份识别或客体属性的用户的审计活动；审计工具应能够授权个人监察和浏览审计数据，同时数据应得到授权的使用、修改和删除；应提供对审计跟踪管理功能的保护，使之可以完成审计跟踪的创建、破坏、腾空和存档；系统管理员应能够定义超过审计跟踪极限的阈值；当存储空间被耗尽时，应能按管理员的指定决定采取的措施，包括：报警并丢弃未记录的审计信息、暂停审计、覆盖以前的审计记录等。

4.4.1.7 数据完整性

应按照**《通用技术要求》6.4.3.7 条数据完整性**的要求，设计和实现操作系统的数据完整性功能。本安全级的具体要求为：

a) 应通过对系统中的信息采取有效措施，防止其遭受非授权用户的修改、破坏或删除。

b) 进程应具有高完整性，确保系统能正确运行，不致混乱或崩溃。为此，需要设计相应的 TCB 来实现有关功能。

c) 对在操作系统中经网络传输信息的完整性保护，要求 TCB 提供监视用户数据完整性的功能，即能检测出被传输的用户数据被篡改、删除、插入和重用等情况发生，并进行报警。

d) 对存储在 TCB 安全控制范围内的用户数据应进行完整性保护，实现存储数据的完整性监视，

并进行报警。

e) 对磁盘设备中存储的数据，可通过增加磁盘扫描程序实现以下功能：

——自动检查文件与磁盘表面是否完好；

——修复扇区交错和扇区流失；

——将磁盘表面的问题自动记录下来；

——将数据移到好的扇区；

——随时检查、诊断和修复磁盘上的错误。

——可在系统中增加计算机病毒检测、诊断和预防程序；

——也可增加硬盘数据备份和修复程序，将硬盘中的数据压缩、备份，并在必要时恢复。

g) 对在操作系统中进行处理的信息的完整性保护，应通过对各种异常情况事务的回退，以事务的完整性确保数据的完整性。

4.4.1.8 隐蔽通道分析

应按照《通用技术要求》6.4.3.8 条一般性隐蔽信道分析的要求进行隐蔽信道分析。本安全级的具体要求为：

a) 操作系统开发者应根据实际测量和工程估算，分析系统中存在的隐蔽信道，并采取相应措施进行防范。

4.4.1.9 可信路径

应按《通用技术要求》6.4.3.9 条用可信路径所描述的要求进行设计。本安全级的具体要求为：

a) 在对用户进行初始登录和/或鉴别时，TCB 应在它与用户之间建立一条安全的信息传输通路。

4.4.2 TCB 自身安全保护

4.4.2.1 TSF 保护

应按照**《通用技术要求》6.4.4.1 条 TSF 保护**的要求，设计和实现操作系统的 TSF 保护。本安全级中，操作系统 TSF 保护的具体要求为：

a) 系统在设计时不应留有“后门”。即不应设计有会违反或绕过安全规则的为了维护、支持或操作所需的任何类型的入口，也不应设计有系统文档中未说明的为了维护、支持或操作所需的任何模式的入口。

b) 安全结构应是一个独立的、很好定义的系统软件的一个子集，同时应防止外部干扰，如修改其代码或数据结构。

c) 操作系统应进行分层设计，对操作系统程序和用户程序要进行隔离。

d) 一个进程的虚地址空间至少应被分为两个段：用户空间和系统空间，两者的隔离应是静态的。驻留在内存中的操作系统允许由所有进程共享。用户进程之间应是彼此隔离的。应禁止在用户模式下运行的进程对系统段进行写操作，而当在系统模式下运行时，则允许进程对所有的虚存空间进行读、写操作。用户模式到系统模式的转换应由一个特殊的指令完成，该指令将限制进程只能对部分系统空间进程访问，这些访问限制一般应是由硬件根据该进程的特权模式来实施的。

e) TCB 应提供一个设置和升级配置参数的安装机制。在初始化和保护与安全有关的数据结构之前，对用户和管理员的安全策略属性应进行定义。

f) TCB 应区分普通操作模式和系统维护模式，TCB 的恢复、全系统操作恢复的启动、配置 TCB 内部的数据库和表等动作应在维护模式中执行。

g) TCB 应防止一个普通用户从未经允许的系统进入维护模式，并应防止一个普通用户与系统内

维护模式交互。从而保证在普通用户访问系统之前，系统能以一个安全的方式进行安装和配置。安全机制应在维护模式中保护普通用户的入口。

h） 不要求所有的系统维护都在维护模式中执行，如备份或常规的系统维护不影响 TCB，损坏的资源的修理不是 TCB 的一部分，并且访问对管理员应有限制，因此不需要在维护模式中执行。

i） 当操作系统安装完成后，在普通用户访问之前，系统中应配置好初始用户和管理员职责、根目录、审计参数、系统审计跟踪设置以及对文件和目录的合适的访问控制。

j） 执行系统所提供的实用程序，应（默认地）尽可能限定于对系统的有效使用，只允许系统管理员修改或替换系统提供的实用程序。

k） 操作环境应为用户提供一个机制，来控制命令的目录/路径的查找顺序。

l） 系统应提供一个实用程序来校验文件系统和磁盘的完整性。此实用程序应由操作系统自动执行。

m） 系统应为系统管理员提供一种机制，来产生安全参数值的详细报告。

n） 在 TCB 失败或中断后，进程应保证保护文本以最小的损害得到恢复。在本级中，要求按照失败保护中所描述的内容，实现对 TSF 出现失败时的处理。系统因故障或其它原因中断后，应有一种机制去恢复系统。系统应提供在管理维护状态中运行的能力，管理维护状态只能被系统管理员使用，各种安全功能全部失效。

o） 操作系统环境应控制和审计系统控制台的使用情况。

p） 系统应能识别由通信渠道接收的信息的来源者，所有待确认的数据应能从进入点被安全地传送到确认系统，如口令不应由公共的或共享的网络以明文发送，可使用数据加密设备或通过加密信道用加密模式传送。通过通信信道传送信息时，应有差错检测协议。

4.4.2.2 资源利用

应按照**《通用技术要求》6.4.4.2 条资源利用**的要求，设计和实现操作系统的资源利用。在本安全级中，资源利用设计的具体要求为：

a） 应通过一定措施确保当系统出现某些确定的故障情况时，TSF 也能维持正常运行，如系统应检测和报告系统的服务水平已降低到预先规定的最小值；

b） 应采取适当的策略，有限服务优先级提供主体使用 TSC 内某个资源子集的优先级，进行 TCB 资源的管理和分配；

c） 应按资源分配中最大限额的要求，进行 TCB 资源的管理和分配，要求配额机制确保用户和主体将　不会独占某种受控的资源。

d） 系统应确保在被授权的主体发出请求时，资源能被访问和利用。

e） 当系统的服务水平降低到预先规定的最小值时，应能检测和发出报告。

f） 系统应提供管理维护状态中运行的能力，在管理维护状态下各种安全性能全部失效，系统只允许由系统管理员使用。

g） 系统应以每个用户或每个用户组为基础，提供一种机制，控制他们对磁盘的消耗和对 CPU 的使用。

h） 系统应提供软件及数据备份和复原的过程，在系统中应加入再启动的同步点，以便于系统的复原。

i） 操作系统应能提供任一命名的或用户可访问的系统资源的修改历史记录。

j） 系统应提供能用于定期确认系统正确操作的机制和过程，这些机制或过程应涉及系统资源的

监督、硬件和固件单元的正确操作、对可能在全系统内传播的错误状态的检测以及超过用户规定的门限的通讯差错的检测等内容。

4.4.2.3 TCB 访问

应按照**《通用技术要求》6.4.4.3 条 TCB 访问控制**的要求，设计和实现操作系统的 TCB 访问控制。本安全级中，操作系统 TCB 访问控制设计的具体要求为：

a） 应按照可选属性范围限定最小级的要求，选择某种会话安全属性的所有失败的尝试 ，对用来建立会话的安全属性的范围进行限制；

b） 应按照多重并发会话限定中基本限定的要求，提供适用于 TSF 内所有用户的限制实现对会话管理的设计，允许用户会话建立的所有尝试；

c） 应按照 TCB 访问历史所描述的要求，实现对会话管理的设计，在会话成功建立的基础上，TSF 应显示用户上一次成功/不成功的会话建立的日期，时间，方法，位置，以及从上一次成功的会话建立以来的不成功的尝试的次数。

d） 应按照 TCB 会话建立所描述的要求，实现对会话管理的设计，TSF 应根据属性允许或拒绝该次会话的建立，这些属性包括：访问地址或端口，用户安全属性（如用户身份、许可证等级、完整性等级、角色中的成员资格），时间范围（如一天中的某些时间、一周的某些天、某些特定日期），或上述属性的组合。

按照以上要求，本级要求在操作系统中应采取的措施主要有：

a） 在建立 TCB 会话之前，认证机制应用这个用户的认证数据由 TCB 校验用户的身份。登录机制不允许认证机制本身被旁路。

b） 为给用户提供系统登录活动的有关信息，让用户识别入侵的企图，采取行动防止可能的未授权使用，成功登录系统后，TCB 应向用户显示以下数据：

——日期、时间、来源和上次成功登录系统的情况；

——上次成功访问系统以来身份识别失败的情况；

——应显示口令到期的天数；

——成功或不成功的事件次数的显示可以用整数计数、时间戳列表等表述方法。

c） 在规定的未使用时限后，系统应断开会话或重新认证用户，系统应提供期限的默认值。

d） 系统应提供锁定用户键盘的机制，键盘开锁过程应要求验证用户。

e） 当用户认证过程不正确的次数达到系统规定的次数时，系统应退出登录过程并终止与用户的交互。系统应提供门限默认值。当门限值被超过时，系统应立即通知系统管理员，同时系统可以指定一段停顿时间，在这段时间之后，才允许重新开始登录程序。系统应具有在连续的侵入尝试下，增加时间间隔的能力，从而延长系统被攻破的时间。

f） 系统应保证即使输入的用户标识是无效的，也应进行完整的用户验证过程，出错的反馈信息不应暴露是哪一部分的验证信息是错误的。

g） 系统应提供一种机制，能按钟点、周日、年月日等条件规定哪些用户能进入系统，哪些用户不能进入系统。

h) 系统应提供一种机制，能按照进入方式或地点拒绝或接受用户。系统应提供限制被授权的用户通过拨号设备或网络设备访问系统的机制。

i) 系统应提供一种机制，能限制用户在指定的网络地址或端口访问系统。例如，限制系统管理员只能通过系统控制台访问系统。

k) 系统应提供一种机制，限制指定的用户或用户组只能进行不修改的访问。

4.4.3 TCB 设计和实现

4.4.3.1 配置管理

应按照**《通用技术要求》6.4.5.1 条配置管理**所描述的要求进行设计。本安全级的具体要求为：

a) 在配置管理自动化方面要求部分的配置管理自动化。

b) 在配置管理能力方面应实现对版本号、配置项、授权控制、**生成支持和验收过程及进一步的支持**等方面的要求。

c) 在 TCB 的配置管理范围方面，应将 TCB 的实现表示、设计文档、测试文档、用户文档、管理员文档以及配置管理文档等置于配置管理之下，要求实现对配置管理范围内的问题，特别是安全缺陷问题进行跟踪。**还要求包括开发工具配置管理。**

d) 在系统的整个生存期，即在它的开发、测试和维护期间，应有一个软件配置管理系统处于保持对改变源码和文件的控制状态。只有被授权的代码和代码修改才允许被加进已交付的源码的基本部分。所有改变应被记载和检查，以确保未危及系统的安全。在软件配置管理系统中，应包含从源码产生出系统新版本、鉴定新生成的系统版本和保护源码免遭未授权修改的工具和规程。通过技术、物理和保安规章三方面的结合，可充分保护生成系统所用到的源码免遭未授权的修改和毁坏。

4.4.3.2 分发和操作

应按照**《通用技术要求》6.4.5.2 条分发和操作**的要求，设计和实现操作系统的 TCB 分发和操作。本安全级的具体要求为：

a) 应以文档形式提供对 TCB 安全地进行分发的过程，以及安装、生成和启动的过程进行说明，并最终生成安全的配置。文档中所描述的内容应包括：

——提供分发的过程；

——安全启动和操作的过程；

——建立日志的过程；

——修改检测的内容；

——对任何安全加强功能在启动、正常操作维护时能被撤消或修改的阐述；

——在故障或硬件、软件出错后恢复系统至安全状态的规程；

——对含有加强安全性的硬件部件，应说明用户或自动的诊断测试的操作环境和使用方法；

——所有诊断测试过程中，为加强安全性的硬件部件所提供例证的结果；

——在启动和操作时产生审计踪迹输出的例证。

b) 对系统的未授权修改的风险，应在交付时控制到最低限度。在包装及安全分送和安装过程中，这种控制应采取软件控制系统的方式，确认安全性会由末端用户考虑，所有安全机制都应以功能状态交付。

c) 所有软件应提供安全安装默认值，在客户不做选择时，默认值应使安全机制有效地发挥安全功能。

d) 随同系统交付的全部默认用户标识码，应在交付时处于非激活状态，并在使用前由管理员激活。

e) 用户文档应同交付的软件一起包装，并应有一套规程确保当前送给用户的系统软件是严格按照最新的系统版本来制作的。

f) 以安全方式开发并交付系统后，仍应提供对产品的长期维护和评估的支持，包括产品中的安

全漏洞和现场问题的解决。

g) 向客户通告新的全问题应用书面说明。

h) 可能受到威胁的所有的安全问题，均描述其特点，并被作为主要的问题对待，直到它被解决或在用户同意下降级使用。

i) 为了支持已交付的软件的每个版本，对所有已有的安全漏洞都应有文档书面说明，并且该文档能在限制的基础上被用户得到。

j) 对安全漏洞的修改不必等到系统升级到下一个版本。安全功能的增加和改进应独立于系统版本的升级，也就是说，应存在适应性独立于系统其它功能的改进。

k) 没有客户授权，不允许在客户正在生产性运行的系统上进行新特性和简易原型的开发、测试和安装。

l) 新的版本应避免违反最初的安全策略和设想，也应避免在维护、增加或功能升级中引入安全漏洞，所有功能的改变和安全结构设置的缺省默认值都应被记录。在新版本交付给用户使用前，用户应能得到该相应的文档。

4.4.3.3 开发

应按照**《通用技术要求》6.3.5.3 条**开发的要求，进行操作系统 TCB 的开发。本安全级的具体要求为：

a) 应按**半形式化功能说明，半形式化高层设计、半形式化高层解释，TSF 的结构化实现，TSF 内部结构复杂性最小化，半形式化低层设计，半形式化一致性说明，以及半形式化的 TCB 安全策略模型**的要求，进行 TCB 的开发。

b) 系统的设计和开发应保护数据的完整性，例如，检查数据更新的规则，二重/多重输入的正确处理，返回状态的检查，中间结果的检查，合理值输入检查，事务处理更新的正确性检查等。

c) 在内部代码检查时，应解决潜在的安全缺陷，关闭或取消所有的后门。

d) 所有交付的软件和文档，应进行关于安全缺陷的定期的和书面的检查，并将检查结果告知用户。

e) 系统控制数据，如口令和密钥，不应在未受保护的程序或文档中以明文形式存储，并以书面形式提供给用户关于软件所有权法律保护的指南。

f) 在操作系统开发的敏感阶段，应保持一个安全环境，该安全环境要求：

——描述操作系统开发所使用的计算机系统的安全使用和维护情况的安全策略和措施应有书面记载，并可供检查；

——系统开发过程中使用的所有计算机系统应接受定期的和有书面记载的内部安全审计，描述审计过程的文件和真实的审计报告应可供检查；

——除授权的分发机构外，不应在开发环境外部复制或分发内部文档；

——开发环境的计算机系统使用的所有软件应当合法地从确定的渠道获得；

——开发者个人独自开发的软件，应在被开发管理者审核后才能用于开发的系统。

4.4.3.4 指导性文档

应按照**《通用技术要求》6.4.5.4 条指导性文档**的要求，编制 TCB 的指导性文档。本安全级的具体要求为：

a) 应为最终用户提供简单概要、分章节或手册形式的文档，保证用户拥有进行安全操作所需要的所有信息。与安全有关的信息应包含在一个特别的手册中或许多标准的文本集中，提供用户查阅所有的安全功能。这些信息可随系统发送，也可明确指出它包含在哪个文本当中。

b) 通过提供指导性文档，应把如何安全使用和维护操作系统的信息交付给系统的用户、系统管理员和系统安全员。对文档的总体要求是：

——应对所有的安全访问和相关过程、特权、功能等适当的管理加以阐述；

——应阐述安全管理和安全服务的交互，并提供新的 TCB 安全生成的指导；

——应详细给出每种审计事件的审计记录的结构，以便考察和维护审计文件和进程；

——应提供一个准则集用于保证附加的说明的一致性不受破坏。

c) 用户文档应提供关于不同用户的可见的安全机制以及如何利用它们的信息，描述没有明示用户的保护结构，并解释它们的用途和提供有关它们使用的指南，不应包括那些如果公开将会危及系统安全的任何信息。

d) 系统管理员文档应提供：

——关于系统的安全开机、操作和重新启动的信息，包括启动系统的过程（如引导系统进入安全方式）、在系统操作失误时恢复安全系统操作的过程、运行软件和数据备份及转储的方法和过程；

——一个单独的安装指南，详细说明设置系统的配置和初始化过程，提供一个新系统版本的安全设置和安装文档，包括对所有用户可见的安全相关过程、软件和数据文档的描述。

e) 安全管理员文档应提供：

——有关如何设置、维护和分析系统安全的详细指导，包括当运行一个安全设备时，需要控制的有关功能和特权的警告；

——与安全有关的管理员功能的详细描述，包括增加和删除一个用户、改变用户的安全特征等；

——提供关于所有审计工具的文档，包括为检查和保持审计文件所推荐的过程、针对每种审计事件的详细审计记录文件、为周期性备份和删除审计记录所推荐的过程、为检查能被目录文件所利用的磁盘剩余空间所推荐的过程；

——关于设置所有文件和目录的最低访问许可的建议；

——运行文件系统或磁盘完整性检测所做的建议；

——如何进行系统自我评估的章节（带有网络管理、口令要求、拨号访问控制、意外事故计划的安全报告），为灾害恢复计划所做的建议；

——描述普通侵入技术和其它威胁，并查出和阻止它们的内容。

f) 安全管理员文档应提供安全管理员了解如何用安全的方式管理系统，除了给出一般的安全忠告，还要明确：

——在系统用安全的方法设置时，围绕用户、用户帐号、用户组成员关系、主体和客体的属性等，应如何安装或终止安装；

——在系统的生命周期内如何用安全的方法维护系统，包括为了防止系统被破坏而进行的每天、每周、每月的安全常规备份等；

——如何用安全的方法重建部分 TCB（如内核）的方法（如果允许在系统上重建 TCB）；

——说明审计跟踪机制，使授权用户可以有效地使用审计跟踪来执行本地的安全策略；

——必要时，如何调整系统的安全默认配置。

g) 文档中不应提供任何一旦泄露将会危及系统安全的信息。有关安全的指令和文档应划分等级分别提供给用户、系统管理员和系统安全员。这些文档应为独立的文档，或作为独立的章节

插入到管理员指南和用户指南中。文档也可为硬拷贝、电子文档或联机文档。如果是联机文档应控制对其的访问。

4.4.3.5 生命周期支持

应按照**《通用技术要求》6.4.5.5 条生命周期支持**的要求，设计和实现操作系统的 TCB。本安全级的具体要求为：

a) 应按标准的生命周期模型进行开发，**提供充分的安全措施，应用部分的工具和技术应遵照实现标准。**

b) 所有安全软件应提供安全安装默认值。在未做特殊选择时,应按默认值安装安全机制。

c) 随同系统交付的全部默认用户标识号，在安装完时应处于非激活状态，并由系统管理员加以激活。

d) 文档应详细阐述安全启动和操作的过程，详细说明安全功能在启动、正常操作维护时是否能被撤消或修改，说明在故障或系统出错时如何恢复系统至安全状态。

e) 如果系统含有加强安全性的硬件，那么管理员、终端用户或自动的诊断测试，应能在各自的操作环境中运行它并详细说明操作过程。

4.4.3.6 测试

应按照**《通用技术要求》6.4.5.6 条测试**的要求，对操作系统的 TCB 进行测试。本安全级的具体要求为：

a) 应通过一般功能测试和抽样性独立测试，**严格的测试范围分析**，高层设计测试、低层设计测试、实**现表示测试**，顺序的功能测试等，确认 TCB 的功能与所要求的功能相一致。

b) 所有系统的安全特性，应被全面测试，包括查找漏洞，如允许违反系统访问控制要求、允许违反资源访问控制要求、允许拒绝服务、允许多审计或验证数据进行未授权访问等。所有被发现的漏洞应被改正、消除或使其无效，并在消除漏洞后重新测试，以证实它们已被消除，且没有引出新的漏洞。

c) 应提供测试文档，详细描述测试计划、测试过程、测试结果。

4.4.3.7 脆弱性评定

应按照《通用技术要求》6**.4.5.7 条脆弱性评定**所描述的要求对所开发的 TCB 进行脆弱性评定。本安全级的具体要求为：

a) 应从**一般性的和/或系统化的隐蔽信道分析**，指南检查、分析确认、**对安全状态的检查和分析**，TCB 安全功能强度评估，开发者脆弱性分析、独立脆弱性分析、**中级抵抗力分析**等方面进行脆弱性评定。

4.4.4 TCB 安全管理要求

应按照**《通用技术要求》6.4.6 条 TCB 安全管理**所描述的要求，实现 TCB 的安全管理。本安全级的具体要求为：

a) 对相应的 TCB 的访问控制、鉴别控制、审计和安全属性管理等相关的功能，以及与一般的安装、配置和维护有关的功能，制定相应的操作、运行规程和行为规章制度。

b) 根据本级中安全功能技术要求所涉及的自主访问控制、标记、强制访问控制、身份鉴别、客体重用、审计、数据完整性、**隐蔽信道分析、可信路径**和安全保证技术要求所涉及的配置管理、分发和操作、开发、指导性文档、生命周期支持、测试、脆弱性评定等所涉及的有关内容设计 TCB 安全管理。

c) 应将系统管理员、安全员和审计员等重要安全角色分别设置专人担任，并按“最小授权原则”

分别授予他们各自为完成自身任务所需的最小权限，并形成相互制约的关系。

4.5 第五级：访问验证保护级

4.5.1 安全功能

4.5.1.1 自主访问控制

应按照**《通用技术要求》6.5.3.3 条**的要求，设计和实现操作系统的自主访问控制功能。

在本安全级中，要求有更细粒度的自主访问控制，并将自主访问控制扩展到计算机信息系统的所有主体与客体。对系统中的每一个客体，都应能够实现由客体的创建者（用户）以用户指定方式或默认方式确定其对该客体的访问权限，而别的同组用户或非同组的用户和用户组对该客体的访问权则应由创建者用户授予，并将访问控制的粒度控制在单个用户，做到只有授权用户才能对该客体实施所授权的访问，而阻止那些非授权的用户对该客体进行任何访问，也阻止授权用户以非授权的操作形式对该客体进行访问。本级还要求自主访问控制能与身份鉴别和审计相结合，通过确认用户身份的真实性和记录用户的各种成功的或不成功的访问，使用户对自己的行为承担明确的责任。

本级中，对自主访问控制的要求应包括：

——定义访问控制属性，并保护这些属性。主体的访问控制属性至少应有：读、写、运行等；客体的访问控制属性应包含可分配给主体的读、写和执行的权限。

——定义分配和修改主体和客体的访问控制属性的规则，并执行对主体和客体的访问控制属性的分配和修改，规则的结果应达到只有被授权的用户才允许访问一个客体。

——定义主体对客体的访问授权规则。该规则应基于主体对客体的访问控制属性，授权的范围应包括主体和客体及相关的访问控制属性，同时应指出主体和客体对这些规则应用的类型。

——所有主体和客体的创建和删除应由系统来进行。主体可请求系统创建和删除主体和客体，但不允许它自己去做这些，从而保证主体和客体不能以危害由系统包含的信息的方式来创建。无论何时一个主体或客体被创建，系统应保证被用于创建该主体或客体的资源不能包含以前使用的任何信息，这些资源主要有：存储器、文件、目录、符号连接、管道、消息队列、信号灯、共享主存等。

实现操作系统自主访问控制的具体方法有：

a) 基于目录表访问的自主访问控制，应为每个实施访问的主体建立一张可以被该主体访问的“客体目录表”。每个用户在其文件目录表中依次列出文件名，并逐一标明对这些文件的访问权限。权限一般分为四种：读、写、执行和属主。每个客体应有唯一的属主。属主具有访问权和分配、回收其他用户的访问权的权限。文件目录表的修改只有文件的属主才能实施，其他任何用户不允许在文件目录表中写，因此，操作系统应在文件的拥有者控制下维护所有的文件目录。

b) 基于存取控制表的自主访问控制，应决定任何一个确定的主体是否可对某一客体进行访问，并识别存取文件的单个用户或用户组。对系统中每一个需要保护的客体，都应为其附加一个主体明细表，表中的每一项包括主体的身份以及对该客体的访问权。这些信息应贮存在某个地方，清楚地与客体相连，高效地标识可存取文件的用户。

c) 访问控制矩阵模型，应用状态和状态转换进行访问关系定义。访问控制矩阵可是一张表格，每行代表一个用户（主体），每列代表一个存取目标（客体），表中的每个元素是该主体对客体的访问权集合。访问的权限应包括读、写、执行和删除。访问控制矩阵一般是稀疏的，矩阵内多数的项为空，即多数主体无权访问多数客体。访问控制矩阵根据不同类型的客体被允

许实施的操作规定存取的种类。矩阵状态的转换通过命令集合将命令规定成一系列基本操作实现，主要包括：

——在 A[S,O]中增加权力 R；

——在 A[S,O]中删除权力 R；

——生成主体 S；

——生成客体 O；

——删除主体 S；

——删除客体 O。

d) 能力表是存取矩阵的另一种改进类型。能力表与主体相关，每个用户应有一个能力表，决定用户是否可以对客体进行访问以及进行何种模式的访问（读、写、执行）。一个拥有一定能力的主体允许依照一定的模式访问客体，在进程运行期间，可删除或添加某些能力。一个用户的能力可以转让，也可以回收，还可以包含在程序、数据文件、硬件、软件中，并采用一定措施进行保护。

e) 拥有者/同组/其他访问控制机制，是在每个文件上附加一段有关存取控制信息的二进制位，这些位应反映不同类型用户的存取方式，一般不超过四类：文件的拥有者、与文件拥有者同组的用户、特定的系统用户和其他用户。每一类用户都应有一组权限，每组权限有三个权限标志位来控制以下权限：

——可读（r）：如果被设置，则文件或目录可读。

——可写（w）：如果被设置，文件或目录可以被写入或修改。

——可执行（x）：如果被设置，文件或目录可以被执行和搜索。

f) 客体的拥有者应是唯一有权修改客体访问权限的主体，拥有者对其拥有的客体应具有全部控制权，但是，不允许客体拥有者把该客体的控制权分配给其他主体。因此，客体拥有者在任何时候都可以改变其所属客体的访问控制表，并可对其他主体授予或撤消对该客体的任何一种访问模式。另外，可设立系统管理员（也称为超级用户），有权修改系统中所有客体的访问控制表，并可对所有客体进行所有模式的访问。

4.5.1.2 强制访问控制

应按照**《通用技术要求》6.5.3.5 条强制访问控制**的要求，设计和实现所需要的强制访问控制功能。本安全级的具体要求为：

a) 应由专门设置的系统安全员统一管理计算机信息系统中与强制访问控制有关的事件和信息，并将系统的常规管理、与安全有关的管理以及审计管理，分别由系统管理员、系统安全员和系统审计员来承担，按最小授权原则分别授予它们各自为完成自己所承担任务所需的最小权限，在三者之间形成相互制约的关系。

b) 强制访问控制应与用户身份鉴别、标记等安全功能密切配合，使系统对用户的安全控制包含从用户进入系统到退出系统的全过程。本安全级，**要求将强制访问控制扩展到计算机信息系统中的所有主体与客体；**要求对客体的控制范围涉及信息系统内部的存储、处理和传输过程，**及将信息进行输入、输出操作的过程，即无论信息以何种形式存在，都应有一定的安全属性与其相关联，并按强制访问控制规则对其进行控制。**

c) 对运行于网络环境的分布式操作系统，应设计统一的 TCB，考虑到跨网络的情况，应在分布式控制中心设置 TCB 安全功能模块，统一实现强制访问控制功能。

d) 对运行于网络环境的多台计算机系统上的操作系统，应在每一台计算机操作系统内设计一个

完整的 TCB，实现强制访问控制功能，并在需要时实现跨网络的 TCB 间用户数据保密性和完整性保护，还应统一考虑各台计算机系统的主、客体安全属性设置的一致性。

4.5.1.3 标记

应按照**《通用技术要求》6.5.3.4 条标记**的要求，设计和实现标记功能。本安全级的具体要求为：

a) 应采用标记的方法为操作系统 TCB 安全功能控制范围内的主体和客体设置安全属性。这些安全属性构成采用多级安全模型的强制访问控制机制的属性库——强制访问控制的基础数据。操作系统用户的安全属性应在用户建立注册帐户后由系统安全员通过 TCB 所提供的安全员界面进行标记；客体的安全属性应在数据输入到由 TCB 安全功能所控制的范围内时以缺省方式生成或由安全员进行标记。

b) 本级要求将标记扩展到信息系统中的所有主体与客体。当信息从 TCB 控制范围之内向 TCB 控制范围之外输出时，应带有安全属性，如打印输出的数据等，应明显标示出该数据的安全标记；当信息从 TCB 控制范围之外向 TCB 控制范围之内输入时，应通过标记标明其安全属性。

4.5.1.4 身份鉴别

应按照**《通用技术要求》6.5.3.1 条用户标识和《通用技术要求》6.5.3.2 条用户鉴别**的要求，设计和实现操作系统的身份鉴别功能。本安全级的具体要求为：

a) 在以请求访问方式引起信息流动时，除可采用口令进行鉴别，并在每次用户登录系统时对请求者的身份进行鉴别外，还应有更加严格的身份鉴别，如采用智能 IC 卡、指纹、视网膜等特殊信息进行身份鉴别，并应在每次用户登录系统之前进行鉴别。智能 IC 卡身份鉴别以密码技术为基础，并符合 X .509 协议。

b) 在以交换方式引起信息流动时，应进行通行双方身份的真实性和双方对对信交换行为的不可抵赖性鉴别。

c) 在某些情况下，除了要求确保用户身份的唯一性和真实性外，还要求对某些用户的身份进行特别保护，使其不被其他用户发现或滥用。

4.5.1.5 客体重用

应按照**《通用技术要求》6.5.3.6 条客体重用**的要求设计操作系统的客体重用功能。本安全级的具体要求为：

a) 应确保动态分配与管理的资源，在保持信息安全的情况下被再利用，主要包括：

——确保非授权用户不能查找在使用后返还系统的记录介质中的信息内容；

——确保非授权用户不能查找系统现已分配给他的记录介质中以前的信息内容。

b) 存储器保护应包括:

——对存储单元的地址的保护，使非法用户不能访问那些受到保护的存储单元；

——对被保护的存储单元的操作提供各种类型的保护。最基本的保护类型是“读/写”和“只读”。不能读/写的存储单元，若被用户读/写时，系统应及时发出警报或中断程序执行。

——可采用逻辑隔离的方法进行存储器保护，具体有：界限地址寄存器保护法、内存标志法、锁保护法和特征位保护法等。

c) 在单用户系统中，存储器保护应防止用户进程不影响系统的运行。

d) 在一个多用户系统中，存储器保护应保证系统内各个用户之间互不干扰。

4.5.1.6 审计

应按照**《通用技术要求》6.5.2.4 条审计**的要求设计操作系统的审计功能。本安全级的具体要求

为：

a) 审计功能应与用户标识与鉴别、自主访问控制、**标记及强制访问控制**等安全功能的设计紧密结合。

b) 应能够生成、维护及保护审计过程，使其免遭修改、非法访问及破坏，特别要保护审计数据，要严格限制未经授权的用户访问。

c) 应记录以下类型的事件：

——使用识别与鉴别机制（如注册过程）；

——将某个客体引入某个用户的地址空间（如打开文件）；

——删除客体及计算机操作员、系统管理员与系统安全管理员进程的操作。

d) 每个审计记录应记录事件发生的日期与时间、产生这一事件的用户、事件的类型以及该事件成功与否。对于识别与鉴别事件，审计记录应记录事件发生的源地点；对于将一个客体信息引入某个用户地址空间中的事件以及删除客体的事件，审计记录应包括客体名及客体的安全级别。

e) 本安全级要求基本的审计功能主要包括：

——授权控制和审计跟踪，应能够创建并维护一个对受保护客体访问的审计跟踪，保护审计记录不被未授权的访问、修改和破坏。

——可记录的安全相关事件，应能指出可记录的审计事件的最少类型，包括建立会话登录成功和失败，使用的系统接口，系统数据库管理的改变（改变用户账户属性、审计跟踪设置和分析、为程序分配设置用户 ID、附加或改变系统程序或进程、改变日期和时间等），超级用户命令改变用户身份等。当审计激活时应确保审计跟踪事件的完整性；应提供一个机制来显示当前选择的审计事件，这个机制的使用者应是有限的授权用户。

——每个事件的数据记录，应包括的信息有：事件发生的日期和时间、触发事件的用户、事件的类型、事件成功或失败等。对于身份识别和认证事件，应记录请求的源（如终端号或网络地址）；对于创建和删除客体的事件，应记录客体的名字和属性。

——审计跟踪控制、管理和检查，应提供一个受保护的打开和关闭审计的机制。该机制能选择和改变审计事件，并在系统工作时处于默认状态；该机制的使用应受到系统管理员的授权限制，系统管理员应能够选择一个或多个基于身份识别或客体属性的用户的审计活动；审计工具应能够授权个人监察和浏览审计数据，同时数据应得到授权的使用、修改和删除；应提供对审计跟踪管理功能的保护，使之可以完成审计跟踪的创建、破坏、腾空和存档；系统管理员应能够定义超过审计跟踪极限的阈值；当存储空间被耗尽时，应能按管理员的指定决定采取的措施，包括：报警并丢弃未记录的审计信息、暂停审计、覆盖以前的审计记录等。

4.5.1.7 数据完整性

应按照**《通用技术要求》6.5.3.7 条数据完整性**的要求，设计和实现操作系统的数据完整性功能。本安全级的具体要求为：

a) 应通过对系统中的信息采取有效措施，防止其遭受非授权用户的修改、破坏或删除。

b) 进程应具有高完整性，确保系统能正确运行，不致混乱或崩溃。为此，需要设计相应的 TCB 来实现有关功能。

c) 对在操作系统中经网络传输信息的完整性保护，要求 TCB 提供监视用户数据完整性的功能，即能检测出被传输的用户数据被篡改、删除、插入和重用等情况发生，并进行报警。

d) 对存储在 TCB 安全控制范围内的用户数据应进行完整性保护，实现存储数据的完整性监视，并进行报警。

e) 对磁盘设备中存储的数据，可通过增加磁盘扫描程序实现以下功能：

——自动检查文件与磁盘表面是否完好；

——修复扇区交错和扇区流失；

——将磁盘表面的问题自动记录下来；

——将数据移到好的扇区；

——随时检查、诊断和修复磁盘上的错误。

——可在系统中增加计算机病毒检测、诊断和预防程序；

——也可增加硬盘数据备份和修复程序，将硬盘中的数据压缩、备份，并在必要时恢复。

g) 对在操作系统中进行处理的信息的完整性保护，应通过对各种异常情况事务的回退，以事务的完整性确保数据的完整性。

4.5.1.8 隐蔽通道分析

应按照**《通用技术要求》6.5.3.8 条一般性隐蔽信道分析**的要求进行隐蔽信道分析。本安全级的具体要求为：

a) 操作系统开发者应根据实际测量和工程估算，分析系统中存在的隐蔽信道，并采取相应措施进行防范。

4.5.1.9 可信路径

应按《通用技术要求》6.5.3.9 条用可信路径所描述的要求进行设计。本安全级的具体要求为：

a) 在对用户进行初始登录和/或鉴别时，TCB 应在它与用户之间建立一条安全的信息传输通路。

4.5.1.10 可信恢复

应按照《通用技术要求》6.5.2.6 条备份与故障恢复的要求，设计和实现操作系统的可信恢复功能。本安全级的具体要求为：

a) 按照自我信息备份、增量备份、局部系统备份、热备份、全系统备份和主机系统远地备份的要求，设计备份功能，按照手动恢复、自动恢复和灾难恢复的方法，设计恢复功能，以便在操作系统发生故障时进行必要的恢复工作。

4.5.2 TCB 自身安全保护

4.5.2.1 TSF 保护

应按照**《通用技术要求》6.5.4.1 条 TSF 保护**的要求，设计和实现操作系统的 TSF 保护。本安全级中，操作系统 TSF 保护的具体要求为：

a） 系统在设计时不应留有“后门”。即不应设计有会违反或绕过安全规则的为了维护、支持或操作所需的任何类型的入口，也不应设计有系统文档中未说明的为了维护、支持或操作所需的任何模式的入口。

b） 安全结构应是一个独立的、很好定义的系统软件的一个子集，同时应防止外部干扰，如修改其代码或数据结构。

c） 操作系统应进行分层设计，对操作系统程序和用户程序要进行隔离。

d） 一个进程的虚地址空间至少应被分为两个段：用户空间和系统空间，两者的隔离应是静态的。驻留在内存中的操作系统允许由所有进程共享。用户进程之间应是彼此隔离的。应禁止在用户模式下运行的进程对系统段进行写操作，而当在系统模式下运行时，则允许进程对所有的

虚存空间进行读、写操作。用户模式到系统模式的转换应由一个特殊的指令完成，该指令将限制进程只能对部分系统空间进程访问，这些访问限制一般应是由硬件根据该进程的特权模式来实施的。

e） TCB 应提供一个设置和升级配置参数的安装机制。在初始化和保护与安全有关的数据结构之前，对用户和管理员的安全策略属性应进行定义。

f） TCB 应区分普通操作模式和系统维护模式，TCB 的恢复、全系统操作恢复的启动、配置 TCB 内部的数据库和表等动作应在维护模式中执行。

g） TCB 应防止一个普通用户从未经允许的系统进入维护模式，并应防止一个普通用户与系统内维护模式交互。从而保证在普通用户访问系统之前，系统能以一个安全的方式进行安装和配置。安全机制应在维护模式中保护普通用户的入口。

h） 不要求所有的系统维护都在维护模式中执行，如备份或常规的系统维护不影响 TCB，损坏的资源的修理不是 TCB 的一部分，并且访问对管理员应有限制，因此不需要在维护模式中执行。

i） 当操作系统安装完成后，在普通用户访问之前，系统中应配置好初始用户和管理员职责、根目录、审计参数、系统审计跟踪设置以及对文件和目录的合适的访问控制。

j） 执行系统所提供的实用程序，应（默认地）尽可能限定于对系统的有效使用，只允许系统管理员修改或替换系统提供的实用程序。

k） 操作环境应为用户提供一个机制，来控制命令的目录/路径的查找顺序。

l） 系统应提供一个实用程序来校验文件系统和磁盘的完整性。此实用程序应由操作系统自动执行。

m） 系统应为系统管理员提供一种机制，来产生安全参数值的详细报告。

n） 在 TCB 失败或中断后，进程应保证保护文本以最小的损害得到恢复。在本级中，要求按照失败保护中所描述的内容，实现对 TSF 出现失败时的处理。系统因故障或其它原因中断后，应有一种机制去恢复系统。系统应提供在管理维护状态中运行的能力，管理维护状态只能被系统管理员使用，各种安全功能全部失效。

o） 操作系统环境应控制和审计系统控制台的使用情况。

p） 系统应能识别由通信渠道接收的信息的来源者，所有待确认的数据应能从进入点被安全地传送到确认系统，如口令不应由公共的或共享的网络以明文发送，可使用数据加密设备或通过加密信道用加密模式传送。通过通信信道传送信息时，应有差错检测协议。

4.5.2.2 资源利用

应按照**《通用技术要求》6.5.4.2 条资源利用**的要求，设计和实现操作系统的资源利用。在本安全级中，资源利用设计的具体要求为：

a） 应通过一定措施确保当系统出现某些确定的故障情况时，TSF 也能维持正常运行，如系统应检测和报告系统的服务水平已降低到预先规定的最小值；

b） 应采取适当的策略，有限服务优先级提供主体使用 TSC 内某个资源子集的优先级，进行 TCB 资源的管理和分配；

c） 应按资源分配中最大限额的要求，进行 TCB 资源的管理和分配，要求配额机制确保用户和主体将不会独占某种受控的资源；

d） 系统应确保在被授权的主体发出请求时，资源能被访问和利用；

e） 当系统的服务水平降低到预先规定的最小值时，应能检测和发出报告；

f） 系统应提供管理维护状态中运行的能力，在管理维护状态下各种安全性能全部失效，系统只

允许由系统管理员使用；

g） 系统应以每个用户或每个用户组为基础，提供一种机制，控制他们对磁盘的消耗和对 CPU 的使用；

h） 系统应提供软件及数据备份和复原的过程，在系统中应加入再启动的同步点，以便于系统的复原；

i） 操作系统应能提供任一命名的或用户可访问的系统资源的修改历史记录；

j） 系统应提供能用于定期确认系统正确操作的机制和过程，这些机制或过程应涉及系统资源的监督、硬件和固件单元的正确操作、对可能在全系统内传播的错误状态的检测以及超过用户规定的门限的通讯差错的检测等内容。

4.5.2.3 TCB 访问

应按照**《通用技术要求》6.5.4.3 条 TCB 访问控制**的要求，设计和实现操作系统的 TCB 访问控制。本安全级中，操作系统 TCB 访问控制设计的具体要求为：

a） 应按照可选属性范围限定最小级的要求，选择某种会话安全属性的所有失败的尝试 ，对用来建立会话的安全属性的范围进行限制；

b） 应按照多重并发会话限定中基本限定的要求，提供适用于 TSF 内所有用户的限制实现对会话管理的设计，允许用户会话建立的所有尝试；

e） 应按照 TCB 访问历史所描述的要求，实现对会话管理的设计，在会话成功建立的基础上，TSF 应显示用户上一次成功/不成功的会话建立的日期，时间，方法，位置，以及从上一次成功的会话建立以来的不成功的尝试的次数。

f） 应按照 TCB 会话建立所描述的要求，实现对会话管理的设计，TSF 应根据属性允许或拒绝该次会话的建立，这些属性包括：访问地址或端口，用户安全属性（如用户身份、许可证等级、完整性等级、角色中的成员资格），时间范围（如一天中的某些时间、一周的某些天、某些特定日期），或上述属性的组合。

按照以上要求，本级要求在操作系统中应采取的措施主要有：

a) 在建立 TCB 会话之前，认证机制应用这个用户的认证数据由 TCB 校验用户的身份。登录机制不允许认证机制本身被旁路。

b) 为给用户提供系统登录活动的有关信息，让用户识别入侵的企图，采取行动防止可能的未授权使用，成功登录系统后，TCB 应向用户显示以下数据：

——日期、时间、来源和上次成功登录系统的情况；

——上次成功访问系统以来身份识别失败的情况；

——应显示口令到期的天数；

——成功或不成功的事件次数的显示可以用整数计数、时间戳列表等表述方法。

c) 在规定的未使用时限后，系统应断开会话或重新认证用户，系统应提供期限的默认值。

d) 系统应提供锁定用户键盘的机制，键盘开锁过程应要求验证用户。

e) 当用户认证过程不正确的次数达到系统规定的次数时，系统应退出登录过程并终止与用户的交互。系统应提供门限默认值。当门限值被超过时，系统应立即通知系统管理员，同时系统可以指定一段停顿时间，在这段时间之后，才允许重新开始登录程序。系统应具有在连续的侵入尝试下，增加时间间隔的能力，从而延长系统被攻破的时间。

f) 系统应保证即使输入的用户标识是无效的，也应进行完整的用户验证过程，出错的反馈信息

不应暴露是哪一部分的验证信息是错误的。

g) 系统应提供一种机制，能按钟点、周日、年月日等条件规定哪些用户能进入系统，哪些用户不能进入系统。

h) 系统应提供一种机制，能按照进入方式或地点拒绝或接受用户。系统应提供限制被授权的用户通过拨号设备或网络设备访问系统的机制。

i) 系统应提供一种机制，能限制用户在指定的网络地址或端口访问系统。例如，限制系统管理员只能通过系统控制台访问系统。

j) 系统应提供一种机制，限制指定的用户或用户组只能进行不修改的访问。

4.5.3 TCB 设计和实现

4.5.3.1 配置管理

应按照**《通用技术要求》6.5.5.1 条配置管理**所描述的要求进行设计。本安全级的具体要求为：

a) 在配置管理自动化方面要求完全的配置管理自动化。

b) 在配置管理能力方面应对版本号、配置项、授权控制、生成支持和验收过程及进一步的支持等方面均达到要求。

c) 在 TCB 的配置管理范围方面，应将 TCB 的实现表示、设计文档、测试文档、用户文档、管理员文档以及配置管理文档等置于配置管理之下，要求实现对配置管理范围内的问题，特别是安全缺陷问题进行跟踪。还要求包括开发工具配置管理。

d) 在系统的整个生存期，即在它的开发、测试和维护期间，应有一个软件配置管理系统处于保持对改变源码和文件的控制状态。只有被授权的代码和代码修改才允许被加进已交付的源码的基本部分。所有改变应被记载和检查，以确保未危及系统的安全。在软件配置管理系统中，应包含从源码产生出系统新版本、鉴定新生成的系统版本和保护源码免遭未授权修改的工具和规程。通过技术、物理和保安规章三方面的结合，可充分保护生成系统所用到的源码免遭未授权的修改和毁坏。

4.5.3.2 分发和操作

应按照**《通用技术要求》6.5.5.2 条分发和操作**的要求，设计和实现操作系统的 TCB 分发和操作。本安全级的具体要求为：

a) 应以文档形式提供对 TCB 安全地进行分发的过程，以及安装、生成和启动的过程进行说明，并最终生成安全的配置。文档中所描述的内容应包括：

——提供分发的过程；

——安全启动和操作的过程；

——建立日志的过程；

——修改检测的内容；

——对任何安全加强功能在启动、正常操作维护时能被撤消或修改的阐述；

——在故障或硬件、软件出错后恢复系统至安全状态的规程；

——对含有加强安全性的硬件部件，应说明用户或自动的诊断测试的操作环境和使用方法；

——所有诊断测试过程中，为加强安全性的硬件部件所提供例证的结果；

——在启动和操作时产生审计踪迹输出的例证。

b) 对系统的未授权修改的风险，应在交付时控制到最低限度。在包装及安全分送和安装过程中，这种控制应采取软件控制系统的方式，确认安全性会由末端用户考虑，所有安全机制都应以功能状态交付。

c) 所有软件应提供安全安装默认值，在客户不做选择时，默认值应使安全机制有效地发挥安全功能。

d) 随同系统交付的全部默认用户标识码，应在交付时处于非激活状态，并在使用前由管理员激活。

e) 用户文档应同交付的软件一起包装，并应有一套规程确保当前送给用户的系统软件是严格按照最新的系统版本来制作的。

f) 以安全方式开发并交付系统后，仍应提供对产品的长期维护和评估的支持，包括产品中的安全漏洞和现场问题的解决。

g) 向客户通告新的全问题应用书面说明。

h) 可能受到威胁的所有的安全问题，均描述其特点，并被作为主要的问题对待，直到它被解决或在用户同意下降级使用。

i) 为了支持已交付的软件的每个版本，对所有已有的安全漏洞都应有文档书面说明，并且该文档能在限制的基础上被用户得到。

j) 对安全漏洞的修改不必等到系统升级到下一个版本。安全功能的增加和改进应独立于系统版本的升级，也就是说，应存在适应性独立于系统其它功能的改进。

k) 没有客户授权，不允许在客户正在生产性运行的系统上进行新特性和简易原型的开发、测试和安装。

l) 新的版本应避免违反最初的安全策略和设想，也应避免在维护、增加或功能升级中引入安全漏洞，所有功能的改变和安全结构设置的缺省默认值都应被记录。在新版本交付给用户使用前，用户应能得到该相应的文档。

4.5.3.3 开发

应按照**《通用技术要求》6.3.5.3 条**开发的要求，进行操作系统 TCB 的开发。本安全级的具体要求为：

a) 应按**形式化功能说明，形式化高层设计，**TSF 的结构化实现，TSF 内部结构复杂性最小化，**形式化低层设计，形式化一致性说明，以及形式化的 TCB 安全策略模型**的要求，进行 TCB 的开发。

b) 系统的设计和开发应保护数据的完整性，例如，检查数据更新的规则，二重/多重输入的正确处理，返回状态的检查，中间结果的检查，合理值输入检查，事务处理更新的正确性检查等。

c) 在内部代码检查时，应解决潜在的安全缺陷，关闭或取消所有的后门。

d) 所有交付的软件和文档，应进行关于安全缺陷的定期的和书面的检查，并将检查结果告知用户。

e) 系统控制数据，如口令和密钥，不应在未受保护的程序或文档中以明文形式存储，并以书面形式提供给用户关于软件所有权法律保护的指南。

f) 在操作系统开发的敏感阶段，应保持一个安全环境，该安全环境要求：

——描述操作系统开发所使用的计算机系统的安全使用和维护情况的安全策略和措施应有书面记载，并可供检查；

——系统开发过程中使用的所有计算机系统应接受定期的和有书面记载的内部安全审计，描述审计过程的文件和真实的审计报告应可供检查；

——除授权的分发机构外，不应在开发环境外部复制或分发内部文档；

——开发环境的计算机系统使用的所有软件应当合法地从确定的渠道获得；

——开发者个人独自开发的软件，应在被开发管理者审核后才能用于开发的系统。

4.5.3.4 指导性文档

应按照**《通用技术要求》6.5.5.4 条指导性文档**的要求，编制 TCB 的指导性文档。本安全级的具体要求为：

a) 应为最终用户提供简单概要、分章节或手册形式的文档，保证用户拥有进行安全操作所需要的所有信息。与安全有关的信息应包含在一个特别的手册中或许多标准的文本集中，提供用户查阅所有的安全功能。这些信息可随系统发送，也可明确指出它包含在哪个文本当中。

b) 通过提供指导性文档，应把如何安全使用和维护操作系统的信息交付给系统的用户、系统管理员和系统安全员。对文档的总体要求是：

——应对所有的安全访问和相关过程、特权、功能等适当的管理加以阐述；

——应阐述安全管理和安全服务的交互，并提供新的 TCB 安全生成的指导；

——应详细给出每种审计事件的审计记录的结构，以便考察和维护审计文件和进程；

——应提供一个准则集用于保证附加的说明的一致性不受破坏。

c) 用户文档应提供关于不同用户的可见的安全机制以及如何利用它们的信息，描述没有明示用户的保护结构，并解释它们的用途和提供有关它们使用的指南，不应包括那些如果公开将会危及系统安全的任何信息。

d) 系统管理员文档应提供：

——关于系统的安全开机、操作和重新启动的信息，包括启动系统的过程（如引导系统进入安全方式）、在系统操作失误时恢复安全系统操作的过程、运行软件和数据备份及转储的方法和过程；

——一个单独的安装指南，详细说明设置系统的配置和初始化过程，提供一个新系统版本的安全设置和安装文档，包括对所有用户可见的安全相关过程、软件和数据文档的描述。

e) 安全管理员文档应提供：

——有关如何设置、维护和分析系统安全的详细指导，包括当运行一个安全设备时，需要控制的有关功能和特权的警告；

——与安全有关的管理员功能的详细描述，包括增加和删除一个用户、改变用户的安全特征等；

——提供关于所有审计工具的文档，包括为检查和保持审计文件所推荐的过程、针对每种审计事件的详细审计记录文件、为周期性备份和删除审计记录所推荐的过程、为检查能被目录文件所利用的磁盘剩余空间所推荐的过程；

——关于设置所有文件和目录的最低访问许可的建议；

——运行文件系统或磁盘完整性检测所做的建议；

——如何进行系统自我评估的章节（带有网络管理、口令要求、拨号访问控制、意外事故计划的安全报告），为灾害恢复计划所做的建议；

——描述普通侵入技术和其它威胁，并查出和阻止它们的内容。

f) 安全管理员文档应提供安全管理员了解如何用安全的方式管理系统，除了给出一般的安全忠告，还要明确：

——在系统用安全的方法设置时，围绕用户、用户帐号、用户组成员关系、主体和客体的属性等，应如何安装或终止安装；

——在系统的生命周期内如何用安全的方法维护系统，包括为了防止系统被破坏而进行的每天、每周、每月的安全常规备份等；

——如何用安全的方法重建部分 TCB（如内核）的方法（如果允许在系统上重建 TCB）；

——说明审计跟踪机制，使授权用户可以有效地使用审计跟踪来执行本地的安全策略；

——必要时，如何调整系统的安全默认配置。

h) 文档中不应提供任何一旦泄露将会危及系统安全的信息。有关安全的指令和文档应划分等级分别提供给用户、系统管理员和系统安全员。这些文档应为独立的文档，或作为独立的章节插入到管理员指南和用户指南中。文档也可为硬拷贝、电子文档或联机文档。如果是联机文档应控制对其的访问。

4.5.3.5 生命周期支持

应按照**《通用技术要求》6.4.5.5 条生命周期支持**的要求，设计和实现操作系统的 TCB。本安全级的具体要求为：

a) 应按**可测量的生命周期模型**进行开发，提供充分的安全措施，**所有部分的工具和技术应遵照实现标准。**

b) 所有安全软件应提供安全安装默认值。在未做特殊选择时,应按默认值安装安全机制。

c) 随同系统交付的全部默认用户标识号，在安装完时应处于非激活状态，并由系统管理员加以激活。

d) 文档应详细阐述安全启动和操作的过程，详细说明安全功能在启动、正常操作维护时是否能被撤消或修改，说明在故障或系统出错时如何恢复系统至安全状态。

e) 如果系统含有加强安全性的硬件，那么管理员、终端用户或自动的诊断测试，应能在各自的操作环境中运行它并详细说明操作过程。

4.5.3.6 测试

应按照**《通用技术要求》6.5.5.6 条测试**的要求，对操作系统的 TCB 进行测试。本安全级的具体要求为：

a) 应通过一般功能测试和**完全性独立测试**，严格的测试范围分析，高层设计测试、低层设计测试、实现表示测试，顺序的功能测试等，确认 TCB 的功能与所要求的功能相一致。

b) 所有系统的安全特性，应被全面测试，包括查找漏洞，如允许违反系统访问控制要求、允许违反资源访问控制要求、允许拒绝服务、允许多审计或验证数据进行未授权访问等。所有被发现的漏洞应被改正、消除或使其无效，并在消除漏洞后重新测试，以证实它们已被消除，且没有引出新的漏洞。

c) 应提供测试文档，详细描述测试计划、测试过程、测试结果。

4.5.3.7 脆弱性评定

应按照《通用技术要求》6**.5.5.7 条脆弱性评定**所描述的要求对所开发的 TCB 进行脆弱性评定。本安全级的具体要求为：

a) 应从**彻底的隐蔽信道分析**，指南检查、分析确认、对安全状态的检查和分析，TCB 安全功能强度评估，开发者脆弱性分析、独立脆弱性分析、**高级抵抗力分析**等方面进行脆弱性评定。

4.5.4 TCB 安全管理

应按照**《通用技术要求》6.5.6 条 TCB 安全管理**所描述的要求，实现 TCB 的安全管理。本安全级的具体要求为：

a) 对相应的 TCB 的访问控制、鉴别控制、审计和安全属性管理等相关的功能，以及与一般的安装、配置和维护有关的功能，制定相应的操作、运行规程和行为规章制度。

b) 根据本级中安全功能技术要求所涉及的自主访问控制、标记、强制访问控制、身份鉴别、客体重用、审计、数据完整性、隐蔽信道分析、可信路径、**可信恢复**和安全保证技术要求所涉及的配置管理、分发和操作、开发、指导性文档、生命周期支持、测试、脆弱性评定等所涉及的有关内容设计 TCB 安全管理。

c) 应将系统管理员、安全员和审计员等重要安全角色分别设置专人担任，并按“最小授权原则”分别授予他们各自为完成自身任务所需的最小权限，并形成相互制约的关系。

附 录 A

（说明性附录）

标准概念说明

A.1 组成与相互关系

一个安全的操作系统，无论其安全等级达到《准则》所规定的哪一个级，都应从安全功能和安全保证两方面考虑其安全性。

本标准在计算机信息系统安全等级保护通用技术要求（以下简称《通用技术要求》）对安全功能和安全保证所进行的详细说明的基础上，针对操作系统在安全性方面的特殊要求，各个安全等级的不同安全功能要求和不同安全保证要求分别进行详细说明。安全功能要求主要说明操作系统所实现的安全策略和安全机制符合《准则》中哪一级的功能要求；安全保证分别从 TCB 自身安全、TCB 的设计和实现 TCB 安全管理三个方面进行描述。

图 A-1 给出《操作系统技术要求》的主要组成成分与相互关系。

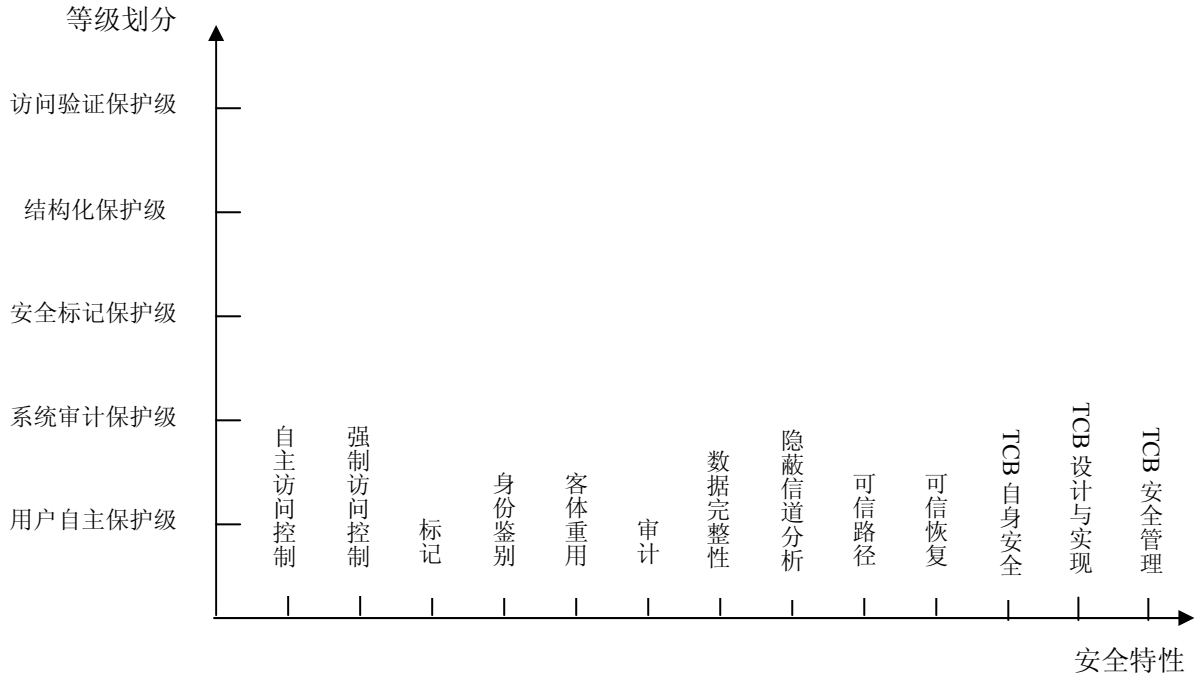

图 A-1 《操作系统技术要求》的组成与相互关系

A.2 关于安全等级划分的说明

计算机操作系统可以是单处理机环境的操作系统，也可以是多处理机环境的操作系统。后者又包括多处理机并行操作系统、分布式操作系统（含分布式计算环境）、网络操作系统等多种情况。对于单处理机环境的操作系统，安全等级的划分相对简单，而对于多处理机环境的操作系统，由于其一般都

跨网络运行，安全等级的划分相对复杂。对于多处理机环境的操作系统，由于其操作系统的组成部分具有相对的独立性，并且，这些操作系统运行于网络环境，因而在考虑对其进行安全等级划分时，应首先考虑各组成部分的安全等级划分，并充分考虑网络传输中的安全因素，然后，综合考虑整个操作系统的安全等级。这里应把握的基本原则是：各组成部分安全等级应不低于整体系统安全等级。操作系统的安全性与支持其运行的计算机硬件设备与环境条件密切相关。因此，支持操作系统运行的硬件设备及环境条件的安全等级应与该操作系统的安全等级相匹配。

在设计一个多处理机环境的操作系统时，首先按照安全需求确定整体安全应达到的安全保护等级，再进一步明确该安全保护等级所对应的安全要素所应具有的安全功能和安全保证条件。在具体进行设计时，这些安全要求和安全保证都应落实到组成操作系统的各部分之中，只有各部分都达到了相应的安全要求，该操作系统在总体上才有可能达到所要求的安全保护等级。

A.3 关于主体、客体的进一步说明

在《准则》中，对主体、客体已经进行了定义。为了更确切的地了解主体与客体在操作系统中的地位与作用，这里对其作进一步说明。

在一个操作系统中，每一个实体成分都必须是主体或客体，或者既是主体又是客体。

主体是一个主动的实体，它包括用户、用户组、进程等。系统中最基本的主体应该是用户（包括一般用户和系统管理员、系统安全员、系统审计员等特殊用户）。系统中的所有事件要求，几乎全是由用户激发的。进程是系统中最活跃的实体，用户的所有事件要求都要通过进程的运行来处理。在这里，进程作为用户的客体，同时又是其访问对象的主体。操作系统进程一般分为用户进程和系统进程。用户进程通常运行应用程序，实现用户所要求的运算处理；系统进程则是操作系统完成对用户所要求的事件进行处理的必不可少的组成部分。

客体是一个被动的实体。在操作系统中，客体可以是按照一定格式存储在一定记录介质上的数据信息（通常以文件系统格式存储数据），也可以是操作系统中的进程。操作系统中的进程（包括用户进程和系统进程）一般有着双重身份。当一个进程运行时，它必定为某一用户服务——直接或间接的处理该用户的事件要求。于是，该进程成为该用户的客体，或为另一进程的客体，而这另一进程则是该用户的客体。依此类推，操作系统中运行的任一进程，总是直接或间接为某一用户服务。这种服务关系可以构成一个服务链。服务者是要求者的客体，要求者是服务者的主体，而最原始的主体是用户，最终的客体是一定记录介质上的信息（数据）。

用户进程是固定为某一用户服务的，它在运行中代表该用户对客体资源进行访问，其权限应与所代表的用户相同（通过用户-主体绑定实现）。系统进程是动态的为所有用户提供服务的，因而它的权限是随着服务对象的变化而变化的,通过用户-主体绑定将用户的权限与为其服务的进程的权限动态地相关联。当一个系统进程与一个特定的用户相关联时，这个系统进程在运行中就代表该用户对客体资源进行访问。

A.4 关于 TCB 的进一步说明

TCB、TSF、TSP、SFP 是《操作系统技术要求》中的重要的概念。在操作系统中，TCB（可信计算基）是构成一个安全的操作系统的所有安全保护装置的组合体。一个 TCB 可以包含多个 TSF（TCB 安全功能模块）,每个 TSF 是一个或多个 SFP（安全功能策略）的实现。TSP（TCB 安全功能策略）是这些 SFP 的总称，构成一个安全域，以防止不可信主体的干扰和篡改。实现 TSF 有两种方法，一种是设置前端过滤器，另一种是设置访问监督器。两者都是在一定硬件基础上通过软件实现确定的安全策略，并提供所要求的附加服务。在网络环境下，一个 TCB 可能跨网络实现，构成一个物理上分散、逻辑上

统一的分布式 TCB。

A.5 关于密码技术的说明

密码技术已成为当今操作系统安全保护的关键技术。在不同安全保护等级中所采用的不同安全策略，应选取不同配置的密码技术作为构成操作系统安全保护的重要机制，或将密码技术与系统安全技术相结合，组成统一的安全机制。TSF 可以利用密码功能来满足一些特定的安全要求。这里主要是指由密码系统提供的以下支持：标识与鉴别、抗抵赖、数据加密保护、数据的完整性保护等。各个安全等级密码技术的具体配置由国家密码主管部门决定。

A.6 关于安全操作系统开发方法的说明

开发一个安全的操作系统可以有两种途径。一种是从头设计；另一种是对原有系统进行加固。

从头设计是指开发一个完整的新系统。这时，应将操作系统的功能与所需要的安全功能一起考虑，在实现操作系统功能的同时构建安全的操作系统。用这种途径所实现的系统核心部分往往就是一个按安全功能要求实现的 TCB，当然应包括所需要的操作系统功能。随着操作系统功能的扩展，TCB 的安全功能的控制范围随之扩展，直到操作系统功能全部实现。

对原有操作系统进行加固，是当前常见的增强通用计算机操作系统安全性的方法。这种方法往往只能采用增加外部安全控制模块来实现前端过虑器或访问监督器，其所能实现的安全功能会受到某些限制。比如，对于客体重用的要求很难用加固的方法来实现；隐蔽信道分析的要求对于非信息流控制的系统是无法实现的；要用加固的方法实现一个结构化的 TCB 设计也是十分困难的。因此，采用对已有系统进行加固的方法，目前所能达到的安全保护等级一般最高为第三级：安全标记保护级。如果用外加安全模块（进程）实现安全加固，如何加强安全模块自身的安全保护，防止攻击者破坏或绕过安全模块是一个必须认真解决的重要问题。

参　考　文　献

1. ISO/IEC 15408-1：1999 Information technology—Security techniques—Evaluation Criteria for IT Security Part1:Introduction and general model Part 1:Introduction and general model，Version 2.0

2. ISO/IEC 15408-2：1999 Information technology—Security techniques—Evaluation Criteria for IT Security Part2:Security functional requirements Part2:Security functional requirements，Version 2.0

3. ISO/IEC 15408-3：1999 Information technology—Security techniques—Evaluation Criteria for IT Security Part3:Security assurance requirements Part3:Security assurance requirements，Version 2.0