ICS 35.040
L 80

中华人民共和国国家标准

GB/T 20272—2006

信息安全技术
操作系统安全技术要求

Information security technology-
Security techniques requirement for operating system

2006-05-31 发布　　2006-12-01 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

目　　次

前　　言

（略）

引　　言

本标准是信息安全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保护等级的操作系统，主要说明为实现 GB17859—1999 中每一个安全保护等级的要求，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保护等级中具体实现上的差异。

计算机操作系统是信息系统的重要组成部分。计算机操作系统的主要功能是进行计算机资源管理和提供用户使用计算机的界面。操作系统所管理的资源包括各种用户资源和计算机的系统资源。用户资源可以归结为以文件形式表示的数据信息资源。系统资源包括系统程序和系统数据以及为管理计算机硬件资源而设置的各种表格，其在操作系统中也都是以文件的形式表现，分别称为可执行文件、数据文件、配置文件等。可见，对操作系统中资源的保护，实际上是对操作系统中文件的保护。由于操作系统在计算机系统中有着十分重要的地位和作用，所以对计算机系统的攻击和威胁（包括人为的和自然的），操作系统往往成为主要的目标。也正因为如此，操作系统的安全就变得十分重要。操作系统安全既要考虑操作系统的安全运行，也要考虑对操作系统中资源的保护（主要是以文件形式表示的数据信息资源的保护）。由于攻击和威胁既可能是针对系统运行的，也可能是针对信息的保密性、完整性和可用性的，所以对操作系统的安全保护的功能要求，需要从操作系统的安全运行和操作系统数据的安全保护两方面综合进行考虑。根据 GB17859-1999 所列安全要素及 GA/T 20271-2006 关于信息系统安全功能要素的描述，本标准从身份鉴别、自主访问控制、标记和强制访问控制、数据流控制、审计、数据完整性、数据保密性、可信路径等方面对操作系统的安全功能要求进行更加具体的描述。为了确保安全功能要素达到所确定的安全性要求，需要通过一定的安全保证机制来实现，根据 GA/T 20271-2006 关于信息系统安全保证要素的描述，本标准从操作系统安全子系统（SSOOS）自身安全保护、操作系统安全子系统（SSOOS）的设计和实现以及操作系统安全子系统（SSOOS）的安全管理等方面，对操作系统的安全保证要求进行更加具体的描述。操作系统的安全还需要有相应的安全硬件系统（即物理安全）方面的支持，这显然已经超出本标准的范围。

综合以上说明，本标准以 GB17859—1999 五个安全保护等级的划分为基础，对操作系统的每一个安全保护等级的安全功能技术要求和安全保证技术要求做详细的描述。为清晰表示每一个安全等级比较低一级安全等级的安全技术要求的增加和增强，在第 4 章的描述中，每一级新增部分用**“宋体加粗”**表示。

信息安全技术　操作系统安全技术要求

1　范围

本标准依据 GB17859-1999 的五个安全保护等级的划分，根据操作系统在信息系统中的作用，规定了操作系统安全所需要的安全技术的各个安全等级的要求。

本标准适用于按等级化要求进行的安全操作系统的设计和实现，对按等级化要求进行的操作系统安全的测试和管理可参照使用。

2　规范性引用文件

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保护等级划分准则

GB/T 20271-2006　信息安全技术　信息安全等级保护　信息系统安全通用技术要求

3　术语、定义和缩略语

3.1 术语和定义

GB17859—1999 和 GB/T 20271-2006 确立的以及下列术语和定义适用于本标准。

3.1.1

操作系统安全　security of operating system

操作系统所存储、传输和处理的信息的保密性、完整性和可用性的表征。

3.1.2

操作系统安全技术 security technology of operating system

实现各种类型的操作系统安全需要的所有安全技术。

3.1.3

操作系统安全子系统 security subsystem of operating system

操作系统中安全保护装置的总称，包括硬件、固件、软件和负责执行安全策略的组合体。它建立了一个基本的操作系统安全保护环境，并提供安全操作系统要求的附加用户服务。按照 GB17859-1999 对可信计算基（TCB）的定义，SSOOS 就是操作系统的 TCB。

3.1.4

SSOOS 安全策略 SSOOS security policy

对 SSOOS 中的资源进行管理、保护和分配的一组规则。一个 SSOOS 中可以有一个或多个安全策略。

3.1.5

安全功能策略 security function policy

为实现 SSOOS 安全要素要求的功能所采用的安全策略。

3.1.6

安全要素　security element

本标准中各安全保护等级的安全技术要求所包含的安全内容的组成成份。

3.1.7

SSOOS 安全功能 SSOOS security function

正确实施 SSOOS 安全策略的全部硬件、固件、软件所提供的功能。每一个安全策略的实现，组成一个 SSOOS 安全功能模块。一个 SSOOS 的所有安全功能模块共同组成该 SSOOS 的安全功能。

3.1.8

SSF 控制范围 SSF scope of control

SSOOS 的操作所涉及的主体和客体的范围。

3.2 缩略语

下列缩略语适用于本标准：

SFP　安全功能策略　security function policy

SSC　SSF 控制范围　SSF scope of control

SSF　SSOOS 安全功能　SSOOS security functioin

SSOOS　操作系统安全子系统　security subsystem of operating system

SSP　SSOOS 安全策略　SSOOS security policy

4　安全等级保护分等级技术要求

4.1　第一级：用户自主保护级

4.1.1　安全功能

4.1.1.1　身份鉴别

身份鉴别包括对用户的身份进行标识和鉴别。可按 GB/T 20271-2006 中 6.1.3.1 的要求，从以下方面设计和实现操作系统的身份鉴别功能：

a)　按 GB/T 20271-2006 中 6.1.3.1.1 和以下要求设计和实现用户标识功能：

——凡需进入操作系统的用户，应先进行标识（建立账号）；

——操作系统用户标识一般使用用户名和用户标识符（UID）。

b)　按 GB/T 20271-2006 中 6.1.3.1.2 和以下要求设计和实现用户鉴别功能：

——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，并在存储时有安全保护；

——通过对不成功的鉴别尝试的值（包括尝试次数和时间的阈值）进行预先定义，并明确规定达到该值时应采取的措施来实现鉴别失败的处理。

c)　对注册到操作系统的用户，应按以下要求设计和实现用户-主体绑定功能：

——将用户进程与所有者用户相关联，使用户进程的行为可以追溯到进程的所有者用户；

——将注系统进程动态地与当前服务要求者用户相关联，使系统进程的行为可以追溯到当前服务的要求者用户。

4.1.1.2　自主访问控制

可按 GB/T 20271-2006 中 6.1.3.2 的要求，从以下方面设计和实现操作系统的自主访问控制功能：

a)　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访问，并阻止非授权用户对客体访问；

b)　设置默认功能，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该主体设置的默认值。

4.1.1.3　用户数据完整性

可按 GB/T 20271-2006 中 6.1.3.3 的要求，对操作系统内部传输的用户数据完整性保护，如进程通信数据的完整性保护，设计和实现操作系统的用户数据完整性保护功能。

4.1.2 SS0OS 自身安全保护

4.1.2.1 SSF 物理安全保护

可按 **GB/T 20271-2006** 中 **6.1.4.1** 的要求，实现 **SSF** 的物理安全保护，通过对物理安全的检查，发现以物理方式的攻击对 **SSF** 造成的威胁和破坏。

4.1.2.2 SSF 运行安全保护

可按 **GB/T 20271-2006** 中 **6.1.4.2** 的要求，从以下方面实现 **SSF** 的运行安全保护：

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） 操作系统程序与用户程序要进行隔离。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；

d） 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进行定义；

e） 区分普通操作模式和系统维护模式；

f） 补丁的发布和运用：补丁是对操作系统安全漏洞进行修补的程序的总称。操作系统的开发者应针对发现的漏洞及时发布补丁。操作系统的管理者应及时运用补丁对操作系统的漏洞进行修补；

g） 在 SS0OS 失败或中断后，应保护其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 SSF 出现失败时的处理。

4.1.2.3 SSF 数据安全保护

可按 **GB/T 20271-2006** 中 **6.1.4.3** 的要求，对在 SS0OS 内传输的 **SSF** 数据，实现 SS0OS 内 SSF 数据传输的基本保护。

4.1.2.4 资源利用

可按 **GB/T 20271-2006** 中 **6.1.4.4** 的要求，从以下方面实现 SS0OS 的资源利用：

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

b）采取适当的策略，按有限服务优先级，提供主体使用 TSC 内某个资源子集的优先级，进行 SS0OS 资源的管理和分配；

c）按资源分配中最大限额的要求，进行 SS0OS 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。

4.1.2.5 SS0OS 访问控制

可按 **GB/T 20271-2006** 中 **6.1.4.5** 的要求，从以下方面实现 SS0OS 的访问控制：

a） 按会话建立机制的要求，对会话建立的管理进行设计；

b） 按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。在基于基本标识的基础上，SSF 应限制系统的并发会话的最大数量，并应利用默认值作为会话次数的限定数；

c） 按可选属性范围限定的要求，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。

4.1.3 SS0OS 设计和实现

4.1.3.1 配置管理

可按 **GB/T 20271-2006** 中 **6.1.5.1** 的要求，从以下方面实现 SS0OS 的配置管理：

a) 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 SS0OS 样本完全对应。

4.1.3.2 分发和操作

可按 **GB/T 20271-2006** 中 **6.1.5.2** 的要求，从以下方面实现 SS0OS 的分发和操作：

a) 以文档形式提供对 SS0OS 安全地进行分发的过程，并对安装、生成和启动的过程进行说明，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，确认安全性会由最终用户考虑，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作用；

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最新的系统版本来制作的。

4.1.3.3 开发

可按 **GB/T 20271-2006** 中 **6.1.5.3** 的要求，从以下方面进行 SS0OS 的开发：

a) 按非形式化功能说明、描述性高层设计、SSF 子集实现、SSF 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 SS0OS 的设计；

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) 由系统控制的敏感数据，如口令和密钥等，不应在未受保护的程序或文档中以明文形式储存；

f) 应以书面形式向用户提供关于软件所有权法律保护的指南。

4.1.3.4 文档要求

可按 **GB/T 20271-2006** 中 **6.1.5.4** 的要求，从以下方面编制 SS0OS 的文档：

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，并解释它们的用途和提供有关它们使用的指南；

b) 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；

c) 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。

4.1.3.5 生存周期支持

可按 **GB/T 20271-2006** 中 **6.1.5.5** 的要求，从以下方面实现 SS0OS 的生存周期支持：

a) 按开发者定义生存周期模型进行开发；

b) 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) 操作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

可按 GB/T 20271-2006 中 6.1.5.6 的要求，从以下方面对 SSOOS 进行测试：

a) 通过一般功能测试和相符独立性测试，确认 SSOOS 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；

c) 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；

d) 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 SSOOS 安全管理

可按 GB/T 20271-2006 中 6.1.6 的要求，从以下方面实现 SSOOS 的安全管理：

a) 对相应的 SSOOS 的访问控制、鉴别控制、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。

4.2 第二级：系统审计保护级

4.2.1 安全功能

4.2.1.1 身份鉴别

身份鉴别包括对用户的身份进行标识和鉴别。应按 GB/T 20271-2006 中中 6.2.3.1 的要求，从以下方面设计和实现操作系统的身份鉴别功能：

a) 按 GB/T 20271-2006 中 6.2.3.1.1 和以下要求设计和实现用户标识功能：

——凡需进入操作系统的用户，应先进行标识（建立账号）；

——操作系统用户标识应使用用户名和用户标识（UID），并在操作系统的整个生存周期实现用户的唯一性标识，以及用户名或别名、UID 等之间的一致性。

b) 按 GB/T 20271-2006 中 6.2.3.1.2 和以下要求设计和实现用户鉴别功能：

——采用强化管理的口令鉴别/基于令牌的动态口令鉴别等机制进行身份鉴别，并在每次用户登录系统时进行鉴别；

——鉴别信息应是不可见的，并在存储和传输时进行安全保护；

——通过对不成功的鉴别尝试的值（包括尝试次数和时间的阈值）进行预先定义，并明确规定达到该值时应采取的措施来实现鉴别失败的处理。

c) 对注册到操作系统的用户，应按以下要求设计和实现用户-主体绑定功能：

——将用户进程与所有者用户相关联，使用户进程的行为可以追溯到进程的所有者用户；

——将注系统进程动态地与当前服务要求者用户相关联，使系统进程的行为可以追溯到当前服务的要求者用户。

4.2.1.2 自主访问控制

宜按 GB/T 20271-2006 中 6.2.3.2 的要求，从以下方面设计和实现操作系统的自主访问控制功能：

a) 允许命名用户以用户的身份规定并控制对客体的访问，并阻止非授权用户对客体的访问；

b) 设置默认功能，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具有该主体设置的默认值；

c) 有更细粒度的自主访问控制，将访问控制的粒度控制在单个用户；对系统中的每一个客体，都能够实现由客体的创建者以用户指定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由创建者用户授予；

d) 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；

e) 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；

f) 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、执行等；客

体的访问控制属性应包含可分配给主体的读、写和执行等权限；

g) 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；

h) 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，同时应指出主体和客体对这些规则应用的类型。

4.2.1.3 安全审计

宜按 GB/T 20271-2006 中 **6.2.2.3** 的要求，从以下方面设计和实现操作系统的安全审计功能：

a) 安全审计功能应与身份鉴别、自主访问控制等安全功能紧密结合；

b) 提供审计日志，潜在侵害分析，基本审计查阅和有限审计查阅，安全审计事件选择，以及受保护的审计踪迹存储等功能；

c) 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；

d) 能够创建并维护一个对受保护客体访问的审计踪踪，保护审计记录不被未授权的访问、修改和破坏；

e) 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、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、系统管理员及系统安全管理员进行的操作等。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；

f) 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。对于身份标识和鉴别事件，应记录请求的源（如末端号或网络地址）；对于创建和删除客体的事件，应记录客体的名字和客体的安全属性；

g) 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鉴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使用、修改和删除审计；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。

4.2.1.4 用户数据完整性

按 **GB/T 20271-2006** 中 **6.2.3.3** 的要求，从以下方面设计和实现操作系统的用户数据完整性保护功能：

a) 在对数据进行访问操作时，检查存储在存储介质上的用户数据是否出现完整性错误。操作系统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；

——将磁盘表面的问题自动记录下来；

——随时检查、诊断磁盘上的错误；

b) 对操作系统内部传输的用户数据，如进程间的通信，应提供保证数据完整性的功能；

c) 对操作系统中处理的用户数据，应按回退的要求设计相应的 SSOOS 安全功能模块，进行异常情况的操作序列回退，以确保用户数据的完整性。

4.2.1.5 用户数据保密性

宜按 **GB/T 20271-2006** 中 **6.2.3.4** 的要求，从以下方面设计和实现操作系统的用户数据保密性保护功能：

a) 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影响系统的运行；
c) 在多用户系统中，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。

4.2.2 SSOOS 自身安全保护

4.2.2.1 SSF 物理安全保护

宜按 **GB/T 20271-2006 中 6.2.4.1** 的要求，实现 SSF 的物理安全保护，通过对物理攻击的检查，发现以物理方式的攻击对 SSF 造成的威胁和破坏。

4.2.2.2 SSF 运行安全保护

宜按 **GB/T 20271-2006 中 6.2.4.2** 的要求，从以下方面实现 SSF 的运行安全保护：

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) 操作系统程序与用户程序要进行隔离。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；
d) 提供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；
e) 应区分普通操作模式和系统维护模式；
f) 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；
g) 对备份或不影响 SSOOS 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；
h) 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；
i) 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；
j) 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；
k) 在 SSOOS 失败或中断后，应确保其以最小的损害得到恢复。并按失败保护中所描述的内容，实现对 SSF 出现失败时的处理；
l) 操作系统环境应控制和审计系统控制台的使用情况；
m) 补丁的发布、管理和使用：补丁是对操作系统安全漏洞进行修补的程序的总称。操作系统的开发者应针对发现的漏洞及时发布补丁。操作系统的管理者应及时获取、统一管理并及时运用补丁对操作系统的漏洞进行修补。

4.2.2.3 SSF 数据安全保护

宜按 **GB/T 20271-2006 中 6.2.4.3** 的要求，对在 SSOOS 内传输的 SSF 数据进行以下安全保护：

a) 实现 SSOOS 内 SSF 数据传输的基本保护；

b） SSOOS 内 SSF 数据复制的一致性保护。

4.2.2.4 资源利用

宜按 **GB/T 20271-2006 中 6.2.4.4** 的要求，从以下方面实现 SSOOS 的资源利用：

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，SSF 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 SSOOS 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 SSOOS 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） 当系统资源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） 系统应提供维护状态中运行的能力，在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。

4.2.2.5 SSOOS 访问控制

宜按 **GB/T 20271-2006 中 6.2.4.5** 的要求，从以下方面实现操 SSOOS 的访问控制：

a) 按会话建立机制的要求，对会话建立的管理进行设计。**在建立 SSOOS 会话之前，应鉴别用户的身份。登录机制不允许鉴别机制本身被旁路；**

b） 按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。在基于基本标识的基础上，SSF 应限制系统的并发会话的最大数量，并应利用默认值作为会话次数的限定数；

c） 按可选属性范围限定的要求，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；

d） 成功登录系统后，SSOOS 应记录并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鉴别失败的情况；

——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 SSOOS 设计和实现

4.2.3.1 配置管理

宜按 **GB/T 20271-2006 中 6.2.5.1** 的要求，从以下方面实现 SSOOS 的配置管理：

a） 在配置管理能力方面应实现对版本号等方面的要求；

b） 在 SSOOS 的配置管理范围方面，应将 SSOOS 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

宜按 **GB/T 20271-2006 中 6.2.5.2** 的要求，从以下方面实现 SSOOS 的分发和操作：

a) 应以文档形式提供对 SS0OS 安全地进行分发的过程，并对安装、生成和启动的过程进行说明，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；

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，确认安全性会由最终用户考虑，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最新的系统版本来制作的。

4.2.3.3 开发

宜按 **GB/T 20271-2006 中 6.2.5.3** 的要求，从以下方面进行 SS0OS 的开发：

a) 要求按**非形式化安全策略模型、完全定义的外部接口、**描述性高层设计、SSF 子集实现、SSF 内部结构**层次化**、描述性低层设计、非形式化对应性说明的要求，进行 SS0OS 的设计；

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) 由系统控制的敏感数据，如口令和密钥等，不应在未受保护的程序或文档中以明文形式储存；

f) 应以书面形式向用户提供关于软件所有权法律保护的指南。

4.2.3.4 文档要求

宜按 **GB/T 20271-2006 中 6.2.5.4** 的要求，从以下方面编制 SS0OS 的文档：

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；

——描述普通入侵技术和其它威胁，及查出和阻止它们的方法；

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 生存周期支持

宜按 **GB/T 20271-2006 中 6.2.5.5** 的要求，从以下方面实现 SS0OS 的生存周期支持：

a) 应按开发者定义生存周期模型和**明确定义开发工具的要求**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、最终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

宜按 **GB/T 20271-2006 中 6.2.5.6** 的要求，从以下方面对 SS0OS 进行测试：

a) 应通过一般功能测试，相符独立性测试，**范围证据和范围分析，高层设计的测试**，确认 SS0OS 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

宜按 GB/T 20271-2006 中 6.2.5.7 的要求，从以下方面对 SS0OS 进行脆弱性评定：

a) 对防止误用的评定，通过对文档的检查，查找 SS0OS 以不安全的方式进行使用或配置而不为人们所察觉的情况；

b) 对 SS0OS 安全功能强度评估，通过对安全机制的安全行为的合格性或统计结果的分析，证明其达到或超过安全目标要求所定义的最低强度；

c) 开发者脆弱性分析，通过确定明显的安全脆弱性的存在，并确认在所期望的环境中所存在的脆弱性不会被利用。

4.2.4 SS0OS 安全管理

宜按 **GB/T 20271-2006 中 6.2.6** 的要求，从以下方面实现 SS0OS 的安全管理：

a) 对相应的 SS0OS 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和安全保证技术要求所涉及的安全属性，设计 SSOOS 安全属性管理；**

c) **根据本级中安全功能技术要求和安全保证技术要求所涉及的安全数据，设计 SSOOS 安全数据管理。**

4.3 第三级：安全标记保护级

4.3.1 安全功能

4.3.1.1 身份鉴别

身份鉴别包括对用户的身份进行标识和鉴别。一般应按 **GB/T 20271-2006 中 6.3.3.1** 的要求，从以下方面设计和实现操作系统的身份鉴别功能：

a) 按 GB/T 20271-2006 中 6.3.3.1.1 和以下要求设计和实现用户标识功能：

——凡需进入操作系统的用户，应先进行标识（建立账号）；

——操作系统用户标识应使用用户名和用户标识（UID），并在操作系统的整个生存周期实现用户的唯一性标识，以及用户名或别名、UID 等之间的一致性；

b) 按 **GB/T 20271-2006 中 6.3.3.1.2** 和以下要求设计和实现用户鉴别功能：

——采用强化管理的口令鉴别/基于令牌的动态口令鉴别/生物特征鉴别/**数字证书鉴别等机制**进行身份鉴别，并在每次用户登录系统时进行鉴别；

——鉴别信息应是不可见的，**在存储和传输时应按 GB/T 20271-2006 中 6.3.3.8 的要求，用加密方法进行安全保护；**

——通过对不成功的鉴别尝试的值（包括尝试次数和时间的阈值）进行预先定义，并明确规定达到该值时应采取的措施来实现鉴别失败的处理。

c) 对注册到操作系统的用户，应按以下要求设计和实现用户-主体绑定功能：

——将用户进程与所有者用户相关联，使用户进程的行为可以追溯到进程的所有者用户；

——将系统进程动态地与当前服务要求者用户相关联，使系统进程的行为可以追溯到当前服务的要求者用户。

4.3.1.2 自主访问控制

一般应按 **GB/T 20271-2006 中 6.3.3.3** 的要求，从以下方面设计和实现操作系统的自主访问控制功能：

a) 允许命名用户以用户的身份规定并控制对客体的访问，并阻止非授权用户对客体的访问。

b) 设置默认功能，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具有该主体的默认值；

c) 有更细粒度的自主访问控制，将访问控制的粒度控制在单个用户。对系统中的每一个客体，都应能够实现由客体的创建者以用户指定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；

d) 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；

e) 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；

f) 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、执行等；客体的访问控制属性应包含可分配给主体的读、写和执行等权限；

g) 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；

h） 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。

4.3.1.3 标记

一般应按 GB/T 20271-2006 中 6.3.3.4 的要求，从以下方面设计和实现操作系统的标记功能：

a） 采用标记的方法为操作系统 SSOOS 安全功能控制范围内的主体和客体设置敏感标记。这些敏感标记构成多级安全模型的的属性库。操作系统主、客体的敏感标记应以默认方式生成或由安全员进行建立、维护和管理；

b) 当信息从 SSOOS 控制范围之内向 SSOOS 控制范围之外输出时，可带有或不带有敏感标记；当信息从 SSOOS 控制范围之外向 SSOOS 控制范围之内输入时，应通过标记标明其敏感标记。

4.3.1.4 强制访问控制

一般应按 GB/T 20271-2006 中 6.3.3.5 的要求，从以下方面设计和实现操作系统的**强制访问控制功能：**

a） 由专门设置的系统安全员统一管理操作系统中与强制访问控制等安全机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，按职能分割原则分别授予它们各自为完成自己所承担任务所需的权限，并形成相互制约关系；

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，对客体的控制范围涉及操作系统内部的存储、处理和传输过程；

c) 运行于网络环境的分布式操作系统，应统一实现强制访问控制功能；

d) 运行于网络环境的多台计算机系统上的网络操作系统，在需要进行统一管理时，应考虑各台计算机操作系统的主、客体安全属性设置的一致性，并实现跨网络的 SSOOS 间用户数据保密性和完整性保护。

4.3.1.5 数据流控制

对于以数据流方式实现数据交换的操作系统，一般应按 GB/T 20271-2006 中 6.3.3.6 的要求，设计和实现操作系统的数据流控制功能。

4.3.1.6 安全审计

一般应按 GB/T 20271-2006 中 **6.3.2.4** 的要求，从以下方面设计和实现操作系统的安全审计功能：

a） 安全审计功能应与身份鉴别、自主访问控制、**标记、强制访问控制及完整性控制**等安全功能紧密结合；

b） 提供审计日志、**实时报警生成**，潜在侵害分析、**基于异常检测**，基本审计查阅、有限审计查阅和**可选审计查阅**，安全审计事件选择，以及受保护的审计踪迹存储和**审计数据的可用性确保**等功能；

c） 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；

d） 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；

e） 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、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；

f) 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。对于身份标识和鉴别事件，应记录请求的源（如末端号或网络地址）；对于创建和删除客体的事件，应记录客体的名字和客体的安全属性；

g) 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鉴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 用户数据完整性

一般应按 **GB/T 20271-2006 中 6.3.3.7** 的要求，从以下方面设计和实现操作系统的用户数据完整性保护功能：

a) **应为操作系统 SS0OS 安全功能控制范围内的主体和客体设置完整性标签（IL），并建立完整性保护策略模型，保护用户数据在存储、传输和处理过程中的完整性；**

b) 在对数据进行访问操作时，检查存储在存储介质上的用户数据是否出现完整性错误，**并在检测到完整性错误时进行恢复。可通过密码支持系统所提供的完整性功能，对加密存储的数据进行完整性保护。**操作系统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；

——将磁盘表面的问题自动记录下来；

——随时检查、诊断和**修复**磁盘上的错误；

——修复扇区交错和扇区流失；

——将数据移到好的扇区；

——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；

c) 在操作系统内部传输的用户数据，如进程间的通信，应提供保证用户数据完整性的功能。**完整性标签应随数据一起流动，系统应保证低完整性的数据不能插入、覆盖到高完整性的数据；**

d) 对操作系统中处理的数据，应按回退的要求设计相应的 SS0OS 安全功能模块，进行异常情况的操作序列回退，以确保用户数据的完整性。**系统应保证在处理过程中不降低数据完整性的级别。**

4.3.1.8 用户数据保密性

一般应按 **GB/T 20271-2006 中 6.3.3.8** 的要求，从以下方面设计和实现操作系统的用户数据保密性保护功能：

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影响系统的运行；

c) 在多用户系统中，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。

4.3.2 SS0OS 自身安全保护

4.3.2.1 SSF 物理安全保护

一般应按 **GB/T 20271-2006 中 6.3.4.1** 的要求，实现 SSF 的物理安全保护，通过对物理攻击的检查和**自动报告，及时发现**以物理方式的攻击对 SSF 造成的威胁和破坏。

4.3.2.2 SSF 运行安全保护

一般应按 **GB/T 20271-2006 中 6.3.4.2** 的要求，从以下方面实现 SSF 的运行安全保护：

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) 操作系统程序与用户程序要进行隔离。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；

d) 提供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；

e) 应区分普通操作模式和系统维护模式；

f) 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；

g) 对备份或不影响 SS0OS 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；

h) 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；

i) 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；

j) 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；

k) 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；

l) 为操作系统安全管理人员提供一种机制，来产生安全参数值的详细报告；

m) 在 SS0OS 失败或中断后，应确保其以最小的损害得到恢复。并按失败保护中所描述的内容，实现对 SSF 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；**

n) 操作系统环境应控制和审计系统控制台的使用情况；

o) 补丁的发布、管理和使用：补丁是对操作系统安全漏洞进行修补的程序的总称。操作系统的开发者应针对发现的漏洞及时发布补丁。操作系统的管理者应及时获取、统一管理并及时运用补丁对操作系统的漏洞进行修补。

4.3.2.3 SSF 数据安全保护

一般应按 GB/T 20271-2006 中 6.3.4.3 的要求，对在 SS0OS 内传输的 SSF 数据，从以下方面实现安全保护：

a) **实现对输出 SSF 数据可用性、保密性、和完整性保护；**

b) 实现 SS0OS 内 SSF 数据传输的基本保护、**数据分离传输、数据完整性保护**；

c) **实现 SSF 间的 SSF 数据的一致性和** SS0OS 内 SSF 数据复制的一致性**保护。**

4.3.2.4 资源利用

一般应按 **GB/T 20271-2006 中 6.3.4.4** 的要求，从以下方面实现 SS0OS 的资源利用：

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，SSF 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 SS0OS 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 SS0OS 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） 当系统资源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） 系统应提供维护状态中运行的能力，在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。

4.3.2.5 SS0OS 访问控制

一般应按 **GB/T 20271-2006 中 6.3.4.5** 的要求，从以下方面实现 SS0OS 的访问控制：

a) 按会话建立机制的要求，对会话建立的管理进行设计。在建立 SSOOS 会话之前，应鉴别用户的身份。登录机制不允许鉴别机制本身被旁路；

b) 按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。在基于基本标识的基础上，SSF 应限制系统的并发会话的最大数量，并应利用默认值作为会话次数的限定数；

c) 按可选属性范围限定的要求，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；

d) 成功登录系统后，SSOOS 应记录并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鉴别失败的情况；

——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；

e) 在规定的未使用时限后，系统应断开会话或重新鉴别用户，系统应提供时限的默认值；

f) 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；

g) 当用户鉴别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；

h) 系统应提供一种机制，能按时间、进入方式、地点、网络地址或端口等条件规定哪些用户能进入系统。

4.3.3 SS0OS 设计和实现

4.3.3.1 配置管理

一般应按 **GB/T 20271-2006 中 6.3.5.1** 的要求，从以下方面实现 SS0OS 的配置管理：

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) **在配置管理自动化方面要求部分的配置管理自动化；**

c) 在 SS00S 的配置管理范围方面，应将 SS00S 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跟踪，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

一般应按 **GB/T 20271-2006 中 6.3.5.2** 的要求，从以下方面实现 SS00S 的分发和操作：

a) 以文档形式提供对 SS00S 安全地进行分发的过程，并**对修改检测**的过程进行说明，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；

——修改内容的检测；

——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，确认安全性会由最终用户考虑，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) 应采用书面说明的方式向客户通告新的安全问题。

h) 对可能受到威胁的所有的安全问题，均应描述其特点，并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，并且用户能在限制的基础上得到该文档；

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） 只有经过客户授权，才允许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默认值都应作记录。在新版本交付给用户使用前，用户应能得到相应的文档。

4.3.3.3 开发

一般应按 **GB/T 20271-2006 中 6.3.5.3** 的要求，从以下方面进行 SS0OS 的开发：

a） 按非形式化安全策略模型、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、SSF 完全实现、**SSF 内部结构层次化、描述性低层设计、非形式化对应性说明的要求，进行 SS0OS 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） 由系统控制的敏感数据，如口令和密钥等，不应在未受保护的程序或文档中以明文形式储存；

f） 应以书面形式向用户提供关于软件所有权法律保护的指南；

g） **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 文档要求

一般应按 **GB/T 20271-2006 中 6.3.5.4** 的要求，从以下方面编制 SS0OS 的文档：

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） **应通过提供所要求文档，将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 SS0OS 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；

——描述普通入侵技术和其它威胁，及查出和阻止它们的方法；

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、用户账户、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；

——在系统的生存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 SS0OS（如内核）的方法（如果允许在系统上重建 SS0OS）；

——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 生存周期支持

一般应按 **GB/T 20271-2006 中 6.3.5.5** 的要求，从以下方面实现 SS0OS 的生存周期支持：

a) **按标准的生存周期模型和**明确定义开发工具的要求进行开发，并提供安全措施说明**和基本的缺陷纠正**；

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、最终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

一般应按 **GB/T 20271-2006 中 6.3.5.6** 的要求，从以下方面对 SS0OS 进行测试：

a) 通过范围证据和范围分析，高层设计测试和**低层设计测试，顺序的功能测试，**相符独立性测试和**抽样独立性测试等**，确认 SS0OS 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；

c) 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；

d) 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

一般应按 **GB/T 20271-2006 中 6.3.5.7** 的要求，从以下方面对 SS0OS 进行脆弱性评定：

a) 对防止误用的评定，通过对文档的检查和**分析确认**，查找 SS0OS 以不安全的方式进行使用或配置而不为人们所察觉的情况；

b) 对 SS0OS 安全功能强度评估，通过对安全机制的安全行为的合格性或统计结果的分析，证明其达到或超过安全目标要求所定义的最低强度；

c) **独立脆弱性分析，应通过独立穿透测试，确定 SS0OS 可以抵御的低攻击能力攻击者发起的攻击。**

4.3.4 SS0OS 安全管理

一般应按 **GB/T 20271-2006 中 6.3.6** 的要求，从以下方面实现 SS0OS 的安全管理：

a) 对相应的 SS0OS 的访问控制、鉴别控制、审计等相关的安全功能，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和安全保证技术要求所涉及的安全属性，设计 SS0OS 安全属性管理；

c) 根据本级中安全功能技术要求和安全保证技术要求所涉及的安全数据，设计 SS0OS 安全数据管理；

d) 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“职能分离原则”分别授予他们各自为完成自身任务所需的权限，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 身份鉴别

身份鉴别包括对用户的身份进行标识和鉴别。一般应按 **GB/T 20271-2006 中 6.4.3.1** 的要求，从以下方面设计和实现操作系统的身份鉴别功能：

a) 按 GB/T 20271-2006 中 **6.4.3.1.1** 和以下要求设计和实现用户标识功能：

——凡需进入操作系统的用户，应先进行标识（建立账号）；

——操作系统用户标识应使用用户名和用户标识（UID），并在操作系统的整个生存周期实现用户的唯一性标识，以及用户名或别名、UID 等之间的一致性；

b) 按 **GB/T 20271-2006 中 6.4.3.1.2** 和以下要求设计和实现用户鉴别功能：

——采用**强化口令管理和/或**基于令牌的动态口令和/或**生物特征鉴别和/或数字证书等相结合的方式，采用多鉴别机制，**实现对用户身份的真实性鉴别，并在每次用户登录系统时进行鉴别；

——鉴别信息应是不可见的，**在存储和传输时应按 GB/T 20271-2006 中 6.4.3.8 的要求，用加密方法进行安全保护；**

——通过对不成功的鉴别尝试的值（包括尝试次数和时间的阈值）进行预先定义，并明确规定达到该值时应采取的措施来实现鉴别失败的处理。

c） 对注册到操作系统的用户，应按以下要求设计和实现用户-主体绑定功能：

——将用户进程与所有者用户相关联，使用户进程的行为可以追溯到进程的所有者用户；

——将系统进程动态地与当前服务要求者用户相关联，使系统进程的行为可以追溯到当前服务的要求者用户。

4.4.1.2 自主访问控制

一般应按 **GB/T 20271-2006 中 6.4.3.3** 的要求，从以下方面设计和实现操作系统的自主访问控制功能：

a） 允许命名用户以用户的身份规定并控制对客体的访问，并阻止非授权用户对客体的访问；

b） 设置默认功能，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该主体设置的默认值；

c） 有更细粒度的自主访问控制，将访问控制的粒度控制在单个用户。对系统中的每一个客体，都应能够实现由客体的创建者以用户指定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；

d） 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；

e） 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；

f） 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、执行等；客体的访问控制属性应包含可分配给主体的读、写和执行等权限；

g） 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；

h） 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。

4.4.1.3 标记

一般应按 **GB/T 20271-2006 中 6.4.3.4** 的要求，从以下方面设计和实现操作系统的标记功能：

a） 采用标记的方法为操作系统 SS0OS 安全功能控制范围内的主体和客体设置敏感标记。这些敏感标记构成多级安全模型的的属性库。操作系统主、客体的敏感标记应以默认方式生成或由安全员进行建立、维护和管理；

b） **本级要求将标记扩展到操作系统中的所有主体与客体。**当信息从SS0OS控制范围之内向SS0OS控制范围之外输出时，**应带有敏感标记，如打印输出的数据等，应明显标示出该数据的敏感标记**；当信息从 SS0OS 控制范围之外向 SS0OS 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 强制访问控制

一般应按 **GB/T 20271-2006 中 6.4.3.5** 的要求，从以下方面设计和实现操作系统的强制访问控制功能：

a） 由专门设置的系统安全员统一管理操作系统中与强制访问控制等安全机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，按职能分割和**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，并形成相互制约关系；

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，**将强制访问控制扩展到信息系统中的所有主体与客体，**对客体的控制范围涉及操作系统内部的存储、处理和传输过程，**及信息进行输入、输出**

操作的过程；

c) 运行于网络环境的分布式操作系统，应统一实现强制访问控制功能；

d) 运行于网络环境的多台计算机系统上的网络操作系统，在需要进行统一管理时，应考虑各台计算机操作系统的主、客体安全属性设置的一致性，并实现跨网络的 SS0OS 间用户数据保密性和完整性保护。

4.4.1.5 数据流控制

对于以数据流方式实现数据交换的操作系统，一般应按 GB/T 20271-2006 中 **6.4.3.6** 的要求，设计和实现操作系统的数据流控制功能。

4.4.1.6 安全审计

一般应按 GB/T 20271-2006 中 **6.4.2.4** 的要求，从以下方面设计和实现操作系统的安全审计功能：

a) 安全审计功能应与身份鉴别、自主访问控制、标记、强制访问控制及完整性控制等安全功能紧密结合；

b) 提供审计日志、实时报警生成和**违例进程终止**，潜在侵害分析、基于异常检测和**简单攻击探测**，基本审计查阅、有限审计查阅和可选审计查阅，安全审计事件选择，以及受保护的审计踪迹存储、审计数据的可用性确保和**防止审计数据丢失的措施**等功能；

c) 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；

d) 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；

e) 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、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；

f) 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。对于身份标识和鉴别事件，应记录请求的源（如末端号或网络地址）；对于创建和删除客体的事件，应记录客体的名字、客体的安全属性和**客体的完整性标签**；

g) 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鉴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 用户数据完整性

一般应按 **GB/T 20271-2006 中 6.4.3.7** 的要求，从以下方面设计和实现操作系统的用户数据完整性保护功能：

a) 为操作系统 SS0OS 安全功能控制范围内的主体和客体设置完整性标签（IL），**并建立半形式化的完整性安全策略模型，**来保护信息在存储、传输和处理过程中的完整性；

b) 在对数据进行访问操作时进行完整性检测和恢复，检查存储在存储介质上的用户数据是否出

现完整性错误，并在检测到完整性错误时进行恢复。可通过密码支持系统所提供的完整性功能，对加密存储的数据进行完整性保护。操作系统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；

——将磁盘表面的问题自动记录下来；

——随时检查、诊断和修复磁盘上的错误；

——修复扇区交错和扇区流失；

——将数据移到好的扇区；

——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；

c) 在操作系统内部进行的数据传输，如进程间的通信，应提供保证数据完整性的功能。完整性标签应随数据一起流动，系统应保证低完整性的数据不能插入、覆盖到高完整性的数据；

d) 对操作系统中处理的数据，应按回退的要求设计相应的 SSOOS 安全功能模块，进行异常情况的操作序列回退，以确保数据的完整性。系统应保证在处理过程中不降低数据完整性的级别。

4.4.1.8 用户数据保密性

一般应按 GB/T 20271-2006 中 **6.4.3.8** 的要求，从以下方面设计和实现操作系统的用户数据保密性保护功能：

a) 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影响系统的运行；

c) 在多用户系统中，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。

4.4.1.9 可信路径

一般应按 GB/T 20271-2006 中 6.4.3.9 的要求，从以下方面设计和实现操作系统的可信路径：

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

4.4.2 SSOOS 自身安全保护

4.4.2.1 SSF 物理安全保护

一般应按 **GB/T 20271-2006 中 6.4.4.1** 的要求，实现 SSF 的物理安全保护，通过对物理攻击的检查、自动报告和**抵抗，防止**以物理方式的攻击对 SSF 造成的威胁和破坏。

4.4.2.2 SSF 运行安全保护

一般应按 **GB/T 20271-2006 中 6.4.4.2** 的要求，从以下方面实现 SSF 的运行安全保护：

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) 操作系统程序与用户程序要进行隔离。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；

d) 提供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；
e) 应区分普通操作模式和系统维护模式；
f) 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；
g) 对备份或不影响 SS0OS 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；
h) 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；
i) 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；
j) 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；
k) 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；
l) 为操作系统安全管理人员提供一种机制，来产生安全参数值的详细报告；
m) 在 SS0OS 失败或中断后，应确保其以最小的损害得到恢复。并按失败保护中所描述的内容，实现对 SSF 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；
n) 操作系统环境应控制和审计系统控制台的使用情况；
o) 补丁的发布、管理和使用：补丁是对操作系统安全漏洞进行修补的程序的总称。操作系统的开发者应针对发现的漏洞及时发布补丁。操作系统的管理者应及时获取、统一管理并及时运用补丁对操作系统的漏洞进行修补。

4.4.2.3 SSF 数据安全保护

一般应按 GB/T 20271-2006 中 6.4.4.3 的要求，对在 SS0OS 内传输的 SSF 数据，从以下方面进行安全保护：

a) 实现对输出 SSF 数据可用性、保密性、和完整性保护；
b) 实现 SS0OS 内 SSF 数据传输的基本传输保护、数据分离传输、数据完检测和改正等；
c) 实现 SSF 间的 SSF 数据的一致性和 SS0OS 内 SSF 数据复制的一致性保护；
d) **实现用户与 SSF 间的可信路径。**

4.4.2.4 资源利用

一般应按 **GB/T 20271-2006 中 6.4.4.4** 的要求，从以下方面实现 SS0OS 的资源利用：

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，SSF 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 SS0OS 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 SS0OS 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) 当系统资源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) 系统应提供维护状态中运行的能力，在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。

4.4.2.5 SS0OS 访问控制

一般应按 **GB/T 20271-2006 中 6.4.4.5** 的要求，从以下方面实现 SS0OS 的访问控制：

a) 按会话建立机制的要求，对会话建立的管理进行设计。在建立 SSOOS 会话之前，应鉴别用户的身份。登录机制不允许鉴别机制本身被旁路；

b） 按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。在基于基本标识的基础上，SSF 应限制系统的并发会话的最大数量，并应利用默认值作为会话次数的限定数；

c） 按可选属性范围限定的要求，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；

d） 成功登录系统后，SSOOS 应记录并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鉴别失败的情况；

——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；

e） 在规定的未使用时限后，系统应断开会话或重新鉴别用户，系统应提供时限的默认值；

f） 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；

g） 当用户鉴别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；

h） 系统应提供一种机制，能按时间、进入方式、地点、网络地址或端口等条件规定哪些用户能进入系统。

4.4.3 SS0OS 设计和实现

4.4.3.1 配置管理

一般应按 **GB/T 20271-2006 中 6.4.5.1** 的要求，从以下方面实现 SS0OS 的配置管理：

a） 在配置管理能力方面应实现**生成支持和验收过程**的要求；

b） 在配置管理自动化方面要求部分的配置管理自动化；

c） 在 SS0OS 的配置管理范围方面，应将 SS0OS 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**开发工具配置管理范围的管理；**

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

一般应按 **GB/T 20271-2006 中 6.4.5.2** 的要求，从以下方面实现 SS0OS 的分发和操作：

a） 应以文档形式提供对 SS0OS 安全地进行分发的过程，并对防止修改过程进行说明，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，确认安全性会由最终用户考虑，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) 应采用书面说明的方式向客户通告新的安全问题；
h) 对可能受到威胁的所有的安全问题，均应描述其特点，并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，并且用户能在限制的基础上得到该文档；
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) 只有经过客户授权，才允许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默认值都应作记录。在新版本交付给用户使用前，用户应能得到相应的文档。

4.4.3.3 开发

一般应按 **GB/T 20271-2006 中 6.3.5.3** 的要求，从以下方面进行 SSOOS 的开发：

a) 应按**半形式化的 SSOOS 安全策略模型、半形式化功能说明、半形式化高层设计、SSF 的结构化实现、SSF 内部结构复杂度最小化、半形式化低层设计、半形式化对应性说明**的要求，进行 SSOOS 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) 由系统控制的敏感数据，如口令和密钥等，不应在未受保护的程序或文档中以明文形式存储；
f) 应以书面形式提供给用户关于软件所有权法律保护的指南；
g) 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 文档要求

一般应按 **GB/T 20271-2006 中 6.4.5.4** 的要求，从以下方面编制 SS0OS 的文档：

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) 应通过提供所要求的文档，将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 SS0OS 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；

——描述普通入侵技术和其它威胁，及查出和阻止它们的方法；

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、用户账户、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；

——在系统的生存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 SS0OS（如内核）的方法（如果允许在系统上重建 SS0OS）；

——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 生存周期支持

一般应按 **GB/T 20271-2006 中 6.4.5.5** 的要求，从以下方面实现 SS0OS 的生存周期支持：

a) 按标准的生存周期模型和**遵照实现标准-应用部分的工具和技术的要求**进行开发，并**提供充分的安全措施；**

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、最终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

一般应按 **GB/T 20271-2006 中 6.4.5.6** 的要求，对 SS0OS 进行测试：

a) 应通过范围证据和**严格的范围分析，**高层设计测试、低层设计测试**和实现表示测试，顺序的功能测试，**相符独立性测试和抽样独立性测试等，确认 SS0OS 的功能与所要求的功能相一致；

b) 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 SS0OS 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；

d) 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；

e) 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

一般应按 **GB/T 20271-2006 中 6.4.5.7** 的要求，从以下方面对 SS0OS 进行脆弱性评定：

a) 通过一般性的隐蔽信道分析，对隐蔽存储信道进行搜索，标识出可识别的隐蔽存储信道；

b) 对防止误用的评定，通过对文档的检查和分析确认，查找 SS0OS 以不安全的方式进行使用或配置而不为人们所察觉的情况；

c) 对 SS0OS 安全功能强度评估，通过对安全机制的安全行为的合格性或统计结果的分析，证明其达到或超过安全目标要求所定义的最低强度；

d) **中抵抗力分析，**通过独立穿透测试和对**脆弱性的系统化搜索**，确定 SS0OS 可以抵御**中攻击能力攻击者发起的穿透性攻击**。

4.4.4 SS0OS 安全管理

一般应按 **GB/T 20271-2006 中 6.4.6** 的要求，从以下方面实现 SS0OS 的安全管理：

a) 对相应的 SSOOS 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和安全保证技术要求所涉及的安全属性，设计 SSOOS 安全属性管理；

c) 根据本级中安全功能技术要求和安全保证技术要求所涉及的安全数据，设计 SSOOS 安全数据管理；

d) 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 身份鉴别

身份鉴别包括对用户的身份进行标识和鉴别。一般应按 **GB/T 20271-2006 中 6.5.3.1** 的要求，从以下方面设计和实现操作系统的身份鉴别功能：

a) 按 GB/T 20271-2006 中 6.5.3.1.1 和以下要求设计和实现用户标识功能：

——凡需进入操作系统的用户，应先进行标识（建立账号）；

——操作系统用户标识应使用用户名和用户标识（UID），并在操作系统的整个生存周期实现用户的唯一性标识，以及用户名或别名、UID 等之间的一致性；

b) 应按 **GB/T 20271-2006 中 6.5.3.1.2** 和以下要求设计和实现用户鉴别功能：

——采用强化管理的口令鉴别和/或基于令牌的动态口令鉴别和/或生物特征鉴别和/或数字证书鉴别和/以协议形式化分析为基础的鉴别等相结合的方式，采用多鉴别机制，实现对用户身份的真实性鉴别，并在每次用户登录系统时和系统重新连接时进行鉴别；

——鉴别信息应是不可见的，在存储和传输时应按 GB/T 20271-2006 中 6.5.3.8 的要求，用加密方法进行安全保护；

——通过对不成功的鉴别尝试的值（包括尝试次数和时间的阈值）进行预先定义，并明确规定达到该值时应采取的措施来实现鉴别失败的处理。

c) 对注册到操作系统的用户，应按以下要求设计和实现用户-主体绑定功能：

——将用户进程与所有者用户相关联，使用户进程的行为可以追溯到进程的所有者用户；

——将系统进程动态地与当前服务要求者用户相关联，使系统进程的行为可以追溯到当前服务的要求者用户。

4.5.1.2 自主访问控制

一般应按 **GB/T 20271-2006 中 6.5.3.3** 的要求，从以下方面设计和实现操作系统的自主访问控制功能：

a) 允许命名用户以用户的身份规定并控制对客体的访问，并阻止非授权用户对客体的访问；

b) 设置默认功能，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该主体设置的默认值；

c) 有更细粒度的自主访问控制，将访问控制的粒度控制在单个用户。对系统中的每一个客体，都应能够实现由客体的创建者以用户指定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；

d) 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；

e) 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；

f) 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、执行等；客

体的访问控制属性应包含可分配给主体的读、写和执行等权限；

g) 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；

h) 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。

4.5.1.3 标记

一般应按 **GB/T 20271-2006 中 6.5.3.4** 的要求，从以下方面设计和实现操作系统的标记功能：

a) 应采用标记的方法为操作系统 SS0OS 安全功能控制范围内的主体和客体设置敏感标记。这些敏感标记构成多级安全模型的的属性库。操作系统主、客体的敏感标记应以默认方式生成或由安全员进行建立、维护和管理；

b) 本级要求将标记扩展到操作系统中的所有主体与客体。当信息从 SS0OS 控制范围之内向 SS0OS 控制范围之外输出时，应带有敏感标记，如打印输出的数据等，应明显标示出该数据的敏感标记；当信息从 SS0OS 控制范围之外向 SS0OS 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 强制访问控制

一般应按 **GB/T 20271-2006 中 6.5.3.5** 的要求，从以下方面设计和实现操作系统的强制访问控制功能：

a) 应由专门设置的系统安全员统一管理操作系统中与强制访问控制等安全机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，按职能分割和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，并形成相互制约关系；

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，将强制访问控制扩展到信息系统中的所有主体与客体，对客体的控制范围涉及操作系统内部的存储、处理和传输过程，及信息进行输入、输出操作的过程；

c) 运行于网络环境的分布式操作系统，应统一实现强制访问控制功能；

d) 运行于网络环境的多台计算机系统上的网络操作系统，在需要进行统一管理时，应考虑各台计算机操作系统的主、客体安全属性设置的一致性，并实现跨网络的 SS0OS 间用户数据保密性和完整性保护。

4.5.1.5 数据流控制

对于以数据流方式实现数据交换的操作系统，一般应按 GB/T 20271-2006 中 **6.5.3.6** 的要求，设计和实现操作系统的数据流控制功能。

4.5.1.6 安全审计

一般应按 GB/T 20271-2006 中 **6.5.2.4** 的要求，从以下方面设计和实现操作系统的安全审计功能：

a) 安全审计功能应与身份鉴别、自主访问控制、标记、强制访问控制及完整性控制等安全功能紧密结合；

b) 提供审计日志、实时报警生成、违例进程终止、**服务取消和用户帐号断开与失效**，潜在侵害分析、基于异常检测和**复杂攻击探测**，基本审计查阅、有限审计查阅和可选审计查阅，安全审计事件选择，以及受保护的审计踪迹存储、审计数据的可用性确保和防止审计数据丢失的措施等功能；

c) 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；

d) 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；

e) 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、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；

f) 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。对于身份标识和鉴别事件，应记录请求的源（如末端号或网络地址）；对于创建和删除客体的事件，应记录客体的名字、客体的安全属性和**客体的完整性标签**；

g) 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鉴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 用户数据完整性

一般应按 **GB/T 20271-2006 中 6.5.3.7** 的要求，从以下方面设计和实现操作系统的用户数据完整性保护功能：

a) 应为操作系统 SSOOS 安全功能控制范围内的主体和客体设置完整性标签（IL），**并建立形式化的完整性安全策略模型，**来保护信息在存储、传输和处理过程中的完整性；

b) 在对数据进行访问操作时进行完整性检测和恢复，检查存储在存储介质上的用户数据是否出现完整性错误，并在检测到完整性错误时进行恢复。可通过密码支持系统所提供的完整性功能，对加密存储的数据进行完整性保护。操作系统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；

——将磁盘表面的问题自动记录下来；

——随时检查、诊断和修复磁盘上的错误；

——修复扇区交错和扇区流失；

——将数据移到好的扇区；

——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；

c) 在操作系统内部进行的数据传输，如进程间的通信，应提供保证数据完整性的功能。完整性标签应随数据一起流动，系统应保证低完整性的数据不能插入、覆盖到高完整性的数据；

d) 对操作系统中处理的数据，应按回退的要求设计相应的 SSOOS 安全功能模块，进行异常情况的操作序列回退，以确保数据的完整性。系统应保证在处理过程中不降低数据完整性的级别。

4.5.1.8 用户数据保密性

一般应按 GB/T 20271-2006 中 **6.5.3.8** 的要求，从以下方面设计和实现操作系统的用户数据保密性保护功能：

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影响系统的运行；

d) 在多用户系统中，存储器保护应保证系统内各个用户之间互不干扰。

4.5.1.9 可信路径

一般应按 **GB/T 20271-2006 中 6.5.3.9** 的要求，从以下方面设计和实现操作系统的 SS0OS 的可信路径：

a) 在对用户进行初始登录和/或鉴别时，SS0OS 应在它与用户之间建立一条安全的信息传输通路。

4.5.2 SS0OS 自身安全保护

4.5.2.1 SSF 物理安全保护

一般应按 **GB/T 20271-2006 中 6.5.4.1** 的要求，实现 SSF 的物理安全保护，通过对物理攻击的检查、自动报告和抵抗，防止以物理方式的攻击对 SSF 造成的威胁和破坏。

4.5.2.2 SSF 运行安全保护

一般应按 **GB/T 20271-2006 中 6.5.4.2** 的要求，从以下方面实现 SSF 的运行安全保护：

a) 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) 操作系统程序与用户程序要进行隔离。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；

d) 提供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；

e) 区分普通操作模式和系统维护模式；

f) 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；

g) 对备份或不影响 SS0OS 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；

h) 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；

i) 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；

j) 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；

k) 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；

l) 为操作系统安全管理人员提供一种机制，来产生安全参数值的详细报告；

m) 在确定不减弱保护的情况下启动 SSOOS，并在 SSF 运行中断后能在不减弱 SSP 保护的情况下以手动或自动方式恢复运行。在 SSOOS 失败或中断后，应确保其以最小的损害得到恢复，并按失败保护中所描述的内容，实现对 SSF 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，其它各种安全功能应全部失效；

n) 操作系统环境应控制和审计系统控制台的使用情况；

o) 补丁的发布、管理和使用：补丁是对操作系统安全漏洞进行修补的程序的总称。操作系统的开发者应针对发现的漏洞及时发布补丁。操作系统的管理者应及时获取、统一管理并及时运用补丁对操作系统的漏洞进行修补。

4.5.2.3 SSF 数据安全保护

一般应按 GB/T 20271-2006 中 6.5.4.3 的要求，对在 SS0OS 内传输的 SSF 数据，从以下方面进行安全保护：

a) 实现对输出 SSF 数据可用性、保密性、和完整性保护；
b) 实现 SS0OS 内 SSF 数据传输的基本传输保护、数据分离传输、数据完检测和改正等；
c) 实现 SSF 间的 SSF 数据的一致性和 SS0OS 内 SSF 数据复制的一致性保护；
d) 实现用户与 SSF 间及 SSF 间的可信路径。

4.5.2.4 资源利用

一般应按 **GB/T 20271-2006 中 6.5.4.4** 的要求，从以下方面实现 SS0OS 的资源利用：

a) 通过一定措施确保当系统出现某些确定的故障情况时，SSF 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) 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 SS0OS 资源的管理和分配；
c) 按资源分配中最大限额的要求，进行 SS0OS 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) 确保在被授权的主体发出请求时，资源能被访问和利用；
e) 当系统资源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) 提供维护状态中运行的能力，在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) 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) 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) 操作系统应能提供用户可访问的系统资源的修改历史记录；
j) 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。

4.5.2.5 SS0OS 访问控制

一般应按 **GB/T 20271-2006 中 6.5.4.5** 的要求，从以下方面实现 SS0OS 的访问控制：

a) 按会话建立机制的要求，对会话建立的管理进行设计。在建立 SSOOS 会话之前，应鉴别用户的身份。登录机制不允许鉴别机制本身被旁路；
b) 按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。在基于基本标识的基础上，SSF 应限制系统的并发会话的最大数量，并应利用默认值作为会话次数的限定数；
c) 按可选属性范围限定的要求，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；
d) 成功登录系统后，SSOOS 应记录并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鉴别失败的情况；
——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；
e) 在规定的未使用时限后，系统应断开会话或重新鉴别用户，系统应提供时限的默认值；
f) 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；
g) 当用户鉴别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；

h） 系统应提供一种机制，能按时间、进入方式、地点、网络地址或端口等条件规定哪些用户能进入系统。

4.5.3 SS0OS 设计和实现

4.5.3.1 配置管理

一般应按 **GB/T 20271-2006 中 6.5.5.1** 的要求，从以下方面实现 SS0OS 的配置管理：

a） 在配置管理能力方面，应安全生成支持和验收过程的进一步支持进行设计；

b） 在配置管理自动化方面要求完全的配置管理自动化；

c） 在配置管理范围方面，应将 SS0OS 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，要求实现对开发工具配置管理范围的管理；

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

一般应按 **GB/T 20271-2006 中 6.5.5.2** 的要求，从以下方面实现 SS0OS 的分发和操作：

a） 应以文档形式提供对 SS0OS 安全地进行分发的过程，并对防止修改过程进行说明，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，确认安全性会由最终用户考虑，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） 应采用书面说明的方式向客户通告新的安全问题；

h） 对可能受到威胁的所有的安全问题，均应描述其特点，并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，并且用户

能在限制的基础上得到该文档；

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） 只有经过客户授权，才允许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默认值都应作记录。在新版本交付给用户使用前，用户应能得到相应的文档。

4.5.3.3 开发

一般应按 **GB/T 20271-2006 中 6.3.5.3** 的要求，从以下方面进行 SS0OS 的开发：

a） 应按**形式化的 SS0OS 安全策略模型、形式化功能说明、形式化高层设计、**SSF 的结构化实现、SSF 内部结构复杂度最小化、**形式化低层设计、形式化对应性说明**的要求，进行 SS0OS 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) 由系统控制的敏感数据，如口令和密钥等，不应在未受保护的程序或文档中以明文形式存储；

f) 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；

g） 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 文档要求

一般应按 **GB/T 20271-2006 中 6.5.5.4** 的要求，从以下方面编制 SS0OS 的文档：

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） 应通过提供所要求的文档，将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 SS0OS 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；

——描述普通入侵技术和其它威胁，及查出和阻止它们的方法；

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、用户账户、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；

——在系统的生存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 SS0OS（如内核）的方法（如果允许在系统上重建 SS0OS）；

——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。

4.5.3.5 生存周期支持

一般应按 **GB/T 20271-2006 中 6.4.5.5** 的要求，从以下方面实现 SS0OS 的生存周期支持：

a) 应按**可测量的生存周期模型和遵照实现标准-所有部分的工具和技术的要求**进行开发，并提供充分的安全措施；

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、最终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

一般应按 **GB/T 20271-2006 中 6.5.5.6** 的要求，从以下方面对 SS0OS 进行测试：

a) 应通过范围证据和严格的范围分析，高层设计测试、**低层设计测试和实现表示测试，顺序的**

功能测试，相符独立性测试、抽样性独立测试和**完全独立性测试**等，确认 SS0OS 的功能与所要求的功能相一致；

b） 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 SS0OS 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；

d） 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；

e） 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

一般应按 **GB/T 20271-2006 中 6.5.5.7** 的要求，从以下方面对 SS0OS 进行脆弱性评定：

a） 通过**严格的隐蔽信道分析，对隐蔽信道进行严格搜索，标识出可识别的隐蔽信道；**

b） 对防止误用的评定，应通过对文档的检查和分析确认，查找 SS0OS 以不安全的方式进行使用或配置而不为人们所察觉的情况；

c） 对 SS0OS 安全功能强度评估，应通过对安全机制的安全行为的合格性或统计结果的分析，证明其达到或超过安全目标要求所定义的最低强度；

d） **高抵抗力分析，**应通过独立穿透测试和对脆弱性的系统化搜索和完备性分析，确定 SS0OS 可以抵御**高攻击能力攻击者发起的穿透性攻击**。

4.5.4 SS0OS 安全管理

一般应按 **GB/T 20271-2006 中 6.5.6** 的要求，从以下方面实现 SS0OS 的安全管理：

a） 对相应的 SS0OS 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和安全保证技术要求所涉及的安全属性，设计 SS0OS 安全属性管理；

c） 根据本级中安全功能技术要求和安全保证技术要求所涉及的安全数据，设计 SS0OS 安全数据管理；

d） 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。

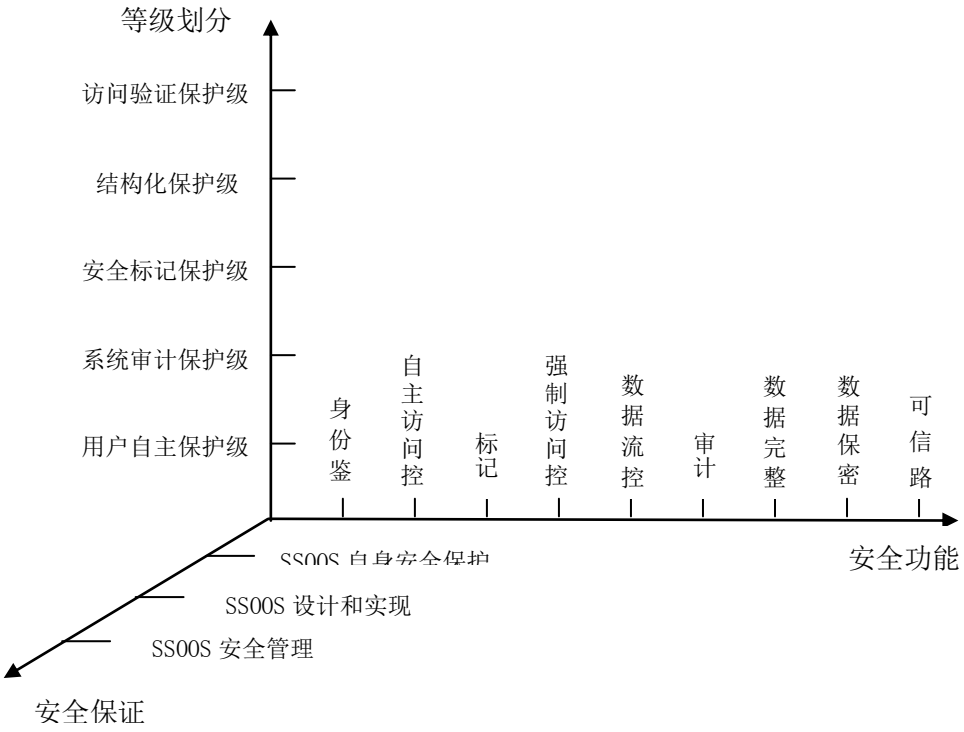
附 录 A
（资料性附录）
标准概念说明

A.1 组成与相互关系

一个安全的操作系统，无论其安全保护等级达到GB17859-1999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GB/T 20271-2006中对信息系统普遍适用的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，对各个安全保护等级的不同安全功能要求和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的每一个安全保护等级所实现的安全策略和安全机制；安全保证分别对每一个安全保护等级的SS0OS自身安全、SS0OS设计和实现、SS0OS安全管理进行描述。

图A.1给出《操作系统安全技术要求》的组成成分与相互关系。



图A.1 《操作系统安全技术要求》的组成与相互关系

A.2 关于安全保护等级划分的说明

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，安全保护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，安全保护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保护等级划分时，应首先考虑各组成部分的安全保护等级划分，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保护等级。这里应把握的基本原则是：各组成部分安全保护等级应不低于整体系统安全保护等级。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保护等级应与该操作系统的安全保护等级相匹配。

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 GB17859-1999 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数据信息。

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 SSOOS、SSF、SSP、SFP 及其相互关系

SSOOS、SSF、SSP、SFP 是《操作系统安全技术要求》中的重要的概念。在操作系统中，SSOOS（操作系统安全子系统）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 SSOOS 可以包含多个 SSF（SSOOS 安全功能模块）,每个 SSF 是一个或多个 SFP（安全功能策略）的实现。SSP（SSOOS 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 SSF 有两种方法，一种是设置前端过滤器，另一种是设置访问监控器。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 SSOOS 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 SSOOS。

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，或将密码技术与操作系统安全技术相结合，组成统一的安全机制。SSF 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。各个安全保护等级的密码技术的具体配置由国家密码主管部门决定。

参　考　文　献

[1] GB/T 18336-1:2001　信息技术　安全技术　IT 安全性评估准则　第 1 部分:简介和一般模型(idt ISO/IEC 15408-1:1999)

[2] GB/T 18336-2：2001　信息技术　安全技术　IT 安全性评估准则　第 2 部分：安全功能要求(idt ISO/IEC 15408-2:1999)

[3] GB/T 18336-3：2001　信息技术　安全技术　IT 安全性评估准则　第 3 部分：安全保证要求(idt ISO/IEC 15408-3:1999)