GJB

中华人民共和国国家军用标准

FL 0137　　GJB 3395－98

军用计算机网络安全评估准则

Evaluation criterion for military computer network security

1998－07－27 发布　　1999－01－01 实施

中国人民解放军总装备部　批准

目　　次

中华人民共和国国家军用标准

军用计算机网络安全评估准则

Evaluation criterion for military computer network security

GJB 3395－98

1 范围

1.1 主题内容

本标准规定了评估军用计算机网络安全的准则、等级划分及每个等级的要求，同时还描述了其他安全服务要求。

1.2 适用范围

本标准适用于军用计算机网络安全评估，也适用于其他需要进行安全评估的计算机网络。

2 引用文件

GJB 2256－94 军用计算机安全术语

GJB 2646－96 军用计算机安全评估准则

3 定义

3.1 术语

本章未列入的术语，参见 GJB 2256 及 GJB 2646。

3.1.1 网络参考监视器 network reference monitor

协调网络内所有主体对客体访问的抽象机器。

3.1.2 网络安全 network security

网络及其服务对未授权修改、破坏或泄露的保护。保证网络正确完成关键性功能，并且不产生有害的副作用。包括提供信息准确度。

3.1.3 网络负责人 network sponsor

负责制订网络安全策略的个人或机构。他(们)设计执行该策略的网络安全体系结构，保证网络以该策略要求的形式实现。对于商用的网络商品而言，负责人一般是厂商；对于已由某部门安装运行的网络系统，负责人一般是工程项目管理员或系统管理员。

3.1.4 网络可信计算基(NTCB) network trusted computed base (NTCB)

网络系统中保护机制的总和，包括硬件、固件和软件，它们一起负责完成安全策略。

3.1.5 NTCB 分部 NTCB partition

在单个网络部件内为实施其网络策略而分配给该部件的保护机制的总和；也就是 NTCB 在单个网络部件内的那部分。

3.2 缩写词

总装备部 1998－07－27 发布　　1999－01－01 实施

AIS　Automated Information system　自动信息系统
ARPANET　Advanced Research Projects Agency Network　ARPA 网
COMSEC　Communications Security　通信安全性
CRC　Cyclic Redundancy Code or Cyclic Redundancy Check　循环冗余码或循环冗余校验
DAC　Discretionary Access Control　自主访问控制
DOS　Denial-of-Service　拒绝服务
DTLS　Descriptive Top-Level Specification　描述性顶层规格说明
FTLS　Formal Top-Level Specification　形式化顶层规格说明
FTP　File Transfer Protocol　文件传输协议
LAN　Local Area Network　局域网
LRC　Longitudinal Redundancy check　纵向冗余校验
MAC　Mandatory Access Control　强制访问控制
MDC　Manipulation Detection Code　操纵探测码
MSM　Message Stream Modification　消息流修改
MWT　Maximum Waiting Time　最大等待时间
NTCB　Network Trusted Computing Base　网络可信计算基
OSI　Open System Interconnection　开放系统互连
PDU　Protocol Data Unit (a.k.a. packet, datagram)　协议数据单元(即:包、数据报)
TCB　Trusted Computer Base　可信计算机基
TELNET　Telecommunication Network　电信网络
TNI　Trusted Network Interpretations　可信网络说明

4　一般要求

本标准中的安全策略、标号、标识、责任、保证、连续保证等要求见 GJB 2646。

4.1　网络安全体系结构与设计

只有执行“网络安全体系结构与设计”的网络才可依据本标准进行评估。网络安全体系结构与设计必须说明与安全相关的策略、客体和协议。在网络安全设计中,必须详细说明应该嵌入网络的接口与服务,这样该网络能作为可信实体进行评估。

4.2　可分部的 NTCB

可以分布于若干个网络部件上的 NTCB 被认为是可分部的,驻留在指定部件内的那部分 NTCB被认为是一个 NTCB 分部。网络主机可能已经有了一个做为单个系统被评估过的 TCB,而该 TCB 不一定与其主机内具有相同安全范围的 NTCB 分部相重合。该 NTCB 分部与主机 TCB 相比,不论其网络安全策略已怎样重合,它都应达到分配给它的安全策略的程度。

4.3　部件评估

网络部件可以由不同的厂商提供,可以支持不同的网络标准,因此执行网络部件评估不仅必要而且有益。在已评估的网络部件上网后,网络的设计者和评估者可多次使用该结果。

网络部件若是支持某策略,必须支持该策略所需要的所有要求,并满足所有的保证条件。

5 详细要求

本章详细说明计算机网络安全评估准则，与计算机安全评估准则相对应，网络安全评估根据网络处理信息的等级和采取的相应措施，将计算机网络安全分为 D, C, B, A 四等和其余全安全服务。D 为最低等，C 分为 C1 和 C2 级，B 分为 B1、B2、B3 级，A 为 A1 级，随着级别提高，系统安全度也随之增加。

注：在本标准中，凡是使用黑体字的部分均表示在较低等级中不包含的那些要求，或表示对已定义要求的变动和增加；凡是不使用黑体字的部分均表示这些要求与较低等级的那些对应要求相同。

5.1 D 等：最小保护

该等只有一个级别。它适合于已被评估，但无法达到更高评估级别的系统。

5.2 C 等：自主保护

该等应提供自主(须知的)保护功能、审计功能、主体责任以及主体初始化的功能。

5.2.1 C1 级：自主安全保护

这一级网络的 NTCB 通过分离用户与数据达到自主安全要求。它可将一些可靠控制组合起来实现单一基础上的访问控制，也就是说，用户可以保护私有的或工程上的数据不受其他用户偶然地读取或破坏。C1 级环境可允许合作用户在同一安全级上处理数据。以下是 C1 级网络系统的最低要求。

5.2.1.1 安全策略

a. 采用 GJB 2646 说明。

b. 解释

网络负责人应清晰描述 NTCB 所完成的整体网络安全策略。该策略应至少包括 C1 级适用的自主要求。它要求数据保密性或数据完整性或两者兼备。该策略应包括通过对用户或用户组鉴别来保护所处理信息的自主安全策略。

访问控制策略应清晰描述网络的下述要求：防止并检测由未授权的用户或错误引起的对敏感信息的“读取或破坏”。未授权的用户包括：无权使用网络的所有用户；网络的合法使用者，但无权访问被保护信息的特定部分。

注意：“用户”并不包括“网络操作员”、“系统程序员”、“系统维护员”、“系统安全员”以及其他技术人员。这些人员与一般用户有所区别并遵循可信设备手册和系统体系结构要求。这些人员可以修改网络中的系统参数，例如：重新定义组成员。他们也可以具有独立的用户职责。

保密性策略：网络负责人应清晰定义阻止未授权用户访问系统中敏感信息的自主保密性策略。

数据完整性策略：网络负责人应清晰定义阻止未授权用户修改(即写入)敏感信息的自主完整性策略。由网络负责人所定义的数据完整性是：在网络中信息不应受到未授权的修改。

c. 基本原理

“负责人”一词可指“出售商”、“网络集成商”、“制造商”、“开发商”中的某一位。有多种含义的原因是因为在评估网络系统时，某些人可能不是相关人员。

可信网络应控制对共享敏感信息的读与写。控制写操作就可保护信息免受破坏。一般情

况下，网络既要保持信息的保密性也要保护完整性。但是，通常是完整性要比保密性更重要。因此，不论网络被评估为哪个级别，网络都应具备保密性和(或)完整性策略。这些策略的保证程度由网络的评估级别反映。

对修改操作的控制可以保证信息可靠，而且，一旦信息被破坏，仍然可以控制由于该破坏而引起的潜在危险。网络完整性策略既要保护在部件上正被处理的数据，也要保护正在网络中传送的数据。由 NTCB 所完成的访问控制策略与每个部件内主体对客体的访问相关。传递信息的通信完整性在“其余安全服务”中讨论。

5.2.1.1.1 自主访问控制

a. 采用 GJB 2646 说明

TCB 应定义并控制计算机系统中已命名用户和已命名客体(文件或程序)之间的访问操作。执行机制(例如：自身/组/公共控制，访问控制表)应允许用户通过自身/组/二者来指定并控制对客体的共享。

b. 解释

自主访问控制(DAC)机制应以各种方式分布于 NTCB 分部中。网络系统中的指定部件可以完成全部或一部分或不完成 DAC 的功能。尤其是仅仅支持内部主体(不做用户直接代理的主体)的部件，例如公共网络中的包交换，就可以不直接完成 DAC 的机制(例如，它们不包含访问控制表)。

在网络环境中，有多种方法鉴别用户身份。例如：在网络安全策略允许的情况下，可用不同部件(如主机，网关)的网络标识符(如互连地址)做为用户组标识符(如主机 A 的所有用户，网络 Q 的所有用户)，这样就不必鉴别每个用户的身份。

对网络来讲，单独主机会对它的用户施加自主控制——这一点和没有网络连接时所使用的控制相类似(事实上，也可能完全相同)。

当可以使用组标识符执行访问控制操作时，可能会要求其他主机的标识符，以此来避免进行远程用户的身份鉴别。

NTCB 分部的 DAC 机制可以在参考监视器的接口中完成或分布在某主体上(该主体是相同或不同部件中 NTCB 的一部分)。参考监视器管理系统中所有的物理资源并创建它所控制的主客体的抽象。这些主客体中的一部分可以完成 NTCB 的某一部分功能。

若网络自主安全策略包含完整性，以上说明尤其适用于控制已被鉴别的用户或用户组在每个部件上进行的修改操作，也就是写访问。

c. 基本原理

在 C1 级，支持整体 DAC 机制的元素被视为不可信的主体。网络环境中的增强型 DAC 机制由 C2 级提供。

典型的 DAC 情况是在某主机上为远程用户创建一个代理进程，该代理进程可在主机 NTCB 分部的控制下访问客体。本标准要求 NTCB 为每一个这样的进程指定并保留一个用户标识符，于是代理进程就可以受到与本地用户一样的自主访问控制。然而，本标准可以允许在一定范围内指定用户标识符。

最明显的情况是如果每一个主机都可以使用网络用户的全局数据库(例如命名服务器)，

那么所有用户标识符都是全局有效的。

某些 NTCB 分部可以为局部注册的用户保持一个局部使用的数据库。在这种情况下，或者禁止为局部未注册的用户创建代理进程，或者允许为预选的用户或用户组创建代理进程。这些进程可标识运行在某远程主机上的用户组。本标准中的审计一词表明了最小的可审计度。审计要求 NTCB 分部的审计设施判定当某代理进程产生时，到底是谁在远程用户的主机上注册运行。

标识与鉴别机制负责建立用户标识符与代理进程的联系。这就意味着代理进程的用户标识符对 DAC 是局部适用的，数据通过网络回到用户主机的传输过程以及在用户主机上为数据做备份不是 DAC 的工作。

只支持内部主体的部件将要影响到 DAC 的实现，这是由于要完成 DAC 判定的部件需要得到一个提供服务的信息(如用户标识符)，关于这种情况的一个例子是主机 A 上的某个用户试图访问主机 B 上的某个文件。通常是由主机 A 向主机 B 传送一个用户标识符，而在主机 B 上完成 DAC 的判定。

有若干种机制可以做到唯一用户标识过程。其中包括：

第一，要求在执行访问操作的主机上提供唯一标识和鉴别过程。

第二，确认由另一主机鉴别的有效网络地址，并将其发送至执行访问操作的主机；

第三，对支持网络全局的用户唯一标识符进行管理，该标识符可能是如在第二中所述的由另一主机鉴别和发送来的，或由一个指定的网络标识和鉴别服务器鉴别和发送来的。

完成第二和第三的协议应遵循系统体系结构要求。

除上述典型方式外，DAC 的网络支持还有其他方式，通常建议集中式访问控制方式。访问控制中心完成 DAC 的所有判定，或控制主机对主机的连接，来减少各主机的负担，这样可使一个主机只需要控制有限个远程主机上的用户对客体的访问。在这种情况下，访问控制中心提供面向抽象连接和 DAC 整体网络安全策略之间的连接。在上述所有情况下，应由客体所在的主机实现该判定。

5.2.1.2 责任

5.2.1.2.1 标识与鉴别

a. 采用 GJB 2646 说明

TCB 要求用户在开始操作前对其自身进行用户标识。而且，TCB 会利用保护机制(如口令)来鉴别用户身份。TCB 应保护鉴别数据以防止被未授权的用户读取。

b. 解释

用户标识与鉴别要求与网络系统对计算机系统的要求一致。标识与鉴别工作可以由用户直接连接的部件负责，也可以由其他的部件(如标识鉴别服务器)负责。当 NTCB 欲以用户或用户组名义作主机或其他网络部件的媒体时，NTCB 将使用主机的标识和鉴别功能而不用单用户的标识鉴别功能。

如果 NTCB 能保证信息避免受到未授权的破坏，那么，当从一个部件到另一个部件时，可以无需再次进行信息鉴别，包括已鉴别的用户身份。这种保护机制至少应达到与鉴别机制和鉴别数据相对称的保证级别。

c. 基本原理

在网络系统中，责任要求没有改变。把 NTCB 分布于若干部件之上，既不增加也不减少要求。即依旧存在单一责任。然而，在 C 1 级网络上(此处无须明显的单一用户责任)，可通过主机或其他部件的标识来满足“单一责任”。另外，在网络这样的分布式系统中，当用户通过主体与远程主体操作时，无须在每一个节点上再次鉴别用户。

自主访问控制(DAC)由部件标识符和(或)鉴别信息的传递实现。这种支持机制使得 DAC 允许用户访问不同 NTCB 分部上的存储客体而不只是用户鉴别的客体。使用向前的标识机制说明了通信路径对源和部件的依赖性。

5.2.1.3 保证

5.2.1.3.1 操作保证

5.2.1.3.1.1 系统体系结构

a. 采用 GJB 2646 说明

TCB 应保持自身运行域。以防止外部干扰或窜改(如修改 TCB 代码或数据结构)。TCB 控制的资源可能是计算机系统中已定义的主体或客体的子集。

b. 解释

所有的 NTCB 分部均必须满足系统体系结构准则。只有当所有 NTCB 分部均保持自身运行域时，NTCB 才可能保持自身运行域。

NTCB 所控制的网络资源子集是各 NTCB 分部所控制的资源子集之和。必须保护属于 NTCB 的代码与数据结构和在 NTCB 主体(即在 NTCB 内部，参考监视器外部的主体)中传送的属于不同 NTCB 分部的代码与数据，以防止其受到外部的干扰和窜改。可用密码检验和或物理手段来保护 NTCB 分部之间交换的用户鉴别数据。

c. 基本原理

NTCB 分部之间的通信保护要求特别针对 NTCB 分部上的主体。任何 NTCB 分部以外主体的此类要求均属于安全策略完整性要求的范畴。

5.2.1.3.1.2 系统完整性

a. 采用 GJB 2646 说明

应提供硬件和(或)软件特性，能够使用它们来定期验证 TCB 中现场硬件和固件元素操作的正确性。

b. 解释

要求的实现是通过能够用于定期验证每个 NTCB 分部部件中的硬件和固件元素是否正确操作硬件和(或)软件来部分完成的。在网络系统合并以及在全系统中进行操作之前，应提供验证同一性和修正部件操作的特性。例如：应设计一种协议，能使 NTCB 分部的部件定期交换消息并验证彼此的正确应答。该协议还应能决定远程实体的应答能力。NTCB 分部还应提供向网络管理员报告在其他 NTCB 分部中检测到故障的能力。

应该设计一种在 NTCB 内实现的部件之间的协议，在发生网络通信或单独部件失效的情况下，用它来提供正确操作。网络中的自主访问控制策略可能会要求可信主体间的通信(该主体是不同部件上的 NTCB 分部的一部分)。这种通信通常由主体间的协议以平等实体的方式

实现。NTCB 分部与其它部件通信的失效不应引起部件内的错误访问。

c. 基本原理

该“解释”的第一段是对网络系统正文和在网络准则中所定义的 NTCB 分部要求的直接延伸。

NTCB 协议应足够强壮，以便当局部错误发生时，可以保证系统正确地运行。这种保护机制可以保持 NTCB 自身的完整性。任何时侯，网络中的一个或多个部件都可能无法工作，将这种故障对其他部件的影响减至最小是至关重要的。其余的完整性与拒绝服务事件将在“其余安全服务”中讨论。

5.2.1.3.2 生命周期保证

5.2.1.3.2.1 安全测试

a. 采用 GJB 2646 说明

应测试计算机(网络)系统以证明其确实可以如系统文档所要求的正常工作。测试的目的是保证系统不允许未授权用户的通行或以其他方式破坏 TCB 的安全保护体系(参见 GJB 2646 附录 C(补充件))。

b. 解释

部件测试需要利用一个测试台来测试部件的接口与协议。网络系统中的安全机制的测试是通过综合测试过程进行的，测试过程包括实现这一安全机制的一个 NTCB 分部的所有部件。把这种综合测试附加到网络系统评估时任何单个部件的评估中。负责人应能标识出包括网络大小的系统配置的许可集。可利用分析或测试过程与工具来测试这些配置的限制。在配置许可集内的配置变动无须再次测试。

c. 基本原理

测试是验证安全机制正确完成预定功能的首要方法。

5.2.1.4 文档

5.2.1.4.1 安全特性用户指南

a. 采用 GJB 2646 说明

用户文档的摘要、章条或手册应描述由 TCB 提供的保护机制、保护机制的使用说明及保护机制间的交互过程。

b. 解释

该用户文档描述了用户可见的全局(网络系统)级的、每一部件用户接口上的以及他们之间交互过程中的保护机制。

c. 基本原理

该“解释”是对网络系统和在网络标准中所定义的 NTCB 分部的延伸。单个部件提供的保护机制的文档由适用于单个部件的可信计算机标准提供。

5.2.1.4.2 可信设备手册

a. 采用 GJB 2646 说明

在计算机系统管理手册中应指出：当安全设备运行时，对有关功能与特权应加以说明，并提出警告。

b. 解释

该手册中应包含说明与过程，以协助系统管理员了解系统的配置情况。这些说明与过程包括以下几种情况：

网络本身的硬件配置；

如何向网络中增加新部件；

当某部件阶段性地离开网络(如被破坏或断开连接)后再次上网的情况；

影响网络安全性能的网络配置，例如手册应向网络系统管理员说明影响网络体系结构的部件间的互连；

加载或修改 NTCB 软件或固件。

应规定物理上的和管理环境上的控制。网络中任一安全性假设均应说明。例如所有通信链都应有物理级上的保护。

c. 基本原理

多种系统管理员可能有各种各样的责任。这些手册中的技术安全措施应与其他安全措施结合使用，以保证网络系统的安全性。其他安全措施包括管理安全、物理安全、辐射安全等。

该手册中应增加网络配置部分的标准，因为，部件之间正确的互连对于网络体系结构的实现至关重要。

密码技术是保护通信线路的常用机制。未授权用户不可以读加密信息。通常密文的安全级比较低，如欲使用加密算法，应由国家和军队安全主管部门认可。

加密算法与其实现过程不在本标准讨论范围。加密算法及其实现可能由某个单独设备完成或是某个部件的主体功能。本标准不加区别地把任一加密实现包看做是加密机制。

5.2.1.4.3 测试文档

a. 采用 GJB 2646 说明

系统负责人应向评估者提供一份文档，该文档包括：测试计划、安全机制的测试过程，以及安全机制功能测试的结果。

b. 解释

测试计划应说明测试的组成，亦应标识出不属于评估系统的测试部件。该计划应包括这类部件中与测试相关的功能，以及评估系统这类部件的接口。网络测试计划说明应明确表示测试可以完全覆盖网络安全策略。测试应包括在系统体系结构和系统完整性中所描述的特性。测试亦应包括网络体系结构和大小。

c. 基本原理

被评估实体可能是一个网络子系统(参见附录 A(补充件))，应增加其他部件才能构成一个完整网络系统，在这种情况下，该文档应包括一些与上下文有关的定义说明。在评估时，若没有测试网络子系统的说明，就无法验证测试计划的正确性。

5.2.1.4.4 设计文档

a. 采用 GJB 2646 说明

设计文档应提供负责人描述的保护原理及其在 TCB 上的实现，如果 TCB 由不同的模块构成，应描述模块之间的接口。

b. 解释

在说明 NTCB 如何实现负责人所描述的保护原理时，应说明 NTCB 的分布方式。亦应说明安全策略。NTCB 模块间的接口应包括：NTCB 分部与分部内模块间的接口（若存在模块的话）。负责人应描述安全体系结构与设计，其中包括部件间安全要求的分布情况。附录 A（补充件）说明有关部件的评估。

c. 基本原理

该解释是对在网络系统正文中所定义的网络说明要求的直接延伸。另外还要求在其他如描述部件或描述操作环境的文档中把网络子系统或网络系统描述为功能，例如在可信设备手册中。

为进行评估，网络系统应有相关的网络安全体系结构与设计（和网络安全体系结构与设计无关的部件的互连见附录 C（补充件））。网络安全体系结构必须包括与安全相关的策略、客体和协议。网络安全设计说明了网络中应包含的接口与服务，因此，能够可信地评估该网络。也许有多种设计构成同一个体系结构，但可能会出现不兼容或无法工作的情况（遵循互连规则的除外）。要求在设计中以可见接口方式描述部件间合作和安全相关的机制，不可见接口不在本标准讨论范畴。

在进行网络或部件评估之前，负责人应提供网络安全体系结构与设计。网络安全体系结构与设计必须充分实现，而某些明显和不明显的缺陷要经过基于该特定结构的可信网络评议会议的同意。

当设计部件或欲评估部件时，当用部件组装网络或欲评估该网络时，均必须首先证明满足网络安全体系结构与设计。也就是说，用遵循网络安全体系结构与设计的每一种方法，能将多个部件构成网络，使之达到评估说明规定的可信网络要求。

为了由部件组成的可信网络能独立构造，网络安全体系结构与设计应完整而无二义性地定义部件的安全功能与部件间的接口。应该评估网络安全体系结构与设计，以保证遵循它的说明而建立的网络是可信的，也就是说该网络可由本标准来评估。

5.2.2 C2 级：可控访问保护

这一级网络可以达到比 C1 级粒度更细的自主访问控制。用户可通过注册过程、审计安全事件和资源隔离等手段，对自己的每个行为负责。以下是 C2 级网络系统的最低要求。

5.2.2.1 安全策略

a. 采用 GJB 2646 说明。

b. 解释

网络负责人应清晰描述 NTCB 所完成的整体网络安全策略。该策略应至少包括 C1 级适用的自主要求。它要求数据保密性或数据完整性或两者兼备。该策略应包括通过对用户或用户组鉴别来保护所处理信息的自主安全策略。

访问控制策略应清晰描述网络的下述要求：防止并检测由未授权的用户或错误引起的对敏感信息的“读取或破坏”。未授权的用户包括：无权使用网络的所有用户；网络的合法使用者，但无权访问被保护的信息的特定部分。

注意：“用户”并不包括“网络操作员”、“系统程序员”、“系统维护员”、“系统安全员”以及其

他技术人员。这些人员与一般用户有所区别并遵循可信设备手册和系统体系结构要求。这些人员可以修改网络中的系统参数，例如重新定义组成员。他们也可以具有独立的用户职责。

保密性策略：网络负责人应清晰定义阻止未授权用户访问系统中敏感信息的自主保密性策略。

数据完整性策略：网络负责人应清晰定义阻止未授权用户修改(即写入)敏感信息的自主完整性策略。由网络负责人所定义的数据完整性是：在网络中信息不应受到未授权的修改。

c. 基本原理

“负责人”一词可指“出售商”、“网络集成商”、“制造商”、“开发商”中的某一位。有多种含义的原因是因为在评估网络系统时，某些人可能不是相关人员。

可信网络应控制对共享敏感信息的读与写。控制写操作就可保护信息免受破坏，一般情况下，网络既要保持信息的保密性也要保护完整性。但是，通常是完整性要比保密性更重要。因此，不论网络被评估为哪个级别，网络都应具备保密性和(或)完整性策略。这些策略的保证程度由网络的评估级别反映。

对修改操作的控制可以保证信息可靠，而且，一旦信息被破坏，仍然可以控制由于该破坏而引起的潜在危险。网络完整性策略既要保护在部件上正被处理的数据，也要保护正在网络中传送的数据。由 NTCB 所完成的访问控制策略与每个部件内主体对客体的访问相关。传递信息的通信完整性在“其余安全服务”中讨论。

5.2.2.1.1 自主访问控制

a. 采用 GJB 2646 说明

TCB 应定义并控制计算机系统中已命名用户和已命名客体(文件或程序)之间的访问操作。执行机制(例如自身/组/公共控制，访问控制表)应允许用户通过自身/组/二者来指定并控制对客体的共享。**执行机制还应控制访问权限的传播。自主访问控制机制应可以通过显性的用户行为或默认方式防止客体受到未授权的访问。这种访问控制应包括或排除单用户粒度的访问操作。只有授权用户才可以允许未得到访问许可的用户访问客体。**

b. 解释

自主访问控制机制应以各种方式分布于 NTCB 分部中。网络系统中的指定部件可以完成全部或一部分或不完成 DAC 的功能。尤其是仅仅支持内部主体(不做用户直接代理的主体)的部件，例如公共网络中的包交换，就可以不直接完成 DAC 的机制(例如，它们不包含访问控制表)。

在网络环境中，有多种方法鉴别用户身份。例如：在网络安全策略允许的情况下，可用不同部件(如主机、网关)的网络标识符(如互连地址)做为用户组标识符(如主机 A 的所有用户，网络 Q 的所有用户)，这样就不必鉴别每个用户的身份。**例如：主机 A 可以使用一个特定的组标识符，并保持一个显性用户组列表，于是，主机 A 可利用该表与主机 B 进行通信。**

对网络来讲，单个主机会对它的用户在已命名个体的基础上施加自主控制——这一点和没有网络连接时所使用的控制相类似(事实上，也可能完全相同)。

当可以使用组标识符执行访问控制操作时，可能会要求其他主机的标识符，以此来避免进行远程用户的身份鉴别。C2 级或 C2 以上级的网络必须保证：当使用组标识符时，应利用审计

记录来确切地标识(立即或以后)该组标识符所代表的单个用户。在组成员的改变以及相应的实现访问控制时刻的不同步过程中,可以允许稍有偏差。

NTCB 分部的 DAC 机制可以在参考监视器的接口中完成或分布在某主体上(该主体是相同或不同部件中 NTCB 的一部分)。参考监视器管理系统中所有的物理资源并创建它所控制的主客体的抽象。这些主客体中的一部分可以完成 NTCB 的某一部分功能。**当某个 DAC 资源分布于 NTCB 主体上(可能在参考监视器外)时,DAC 的设计与实现机制的保证要求应符合 C2 级或 C2 以上各级网络的要求。**

若网络自主安全策略包含完整性,以上说明尤其适用于控制已被鉴别的用户或用户组在每个部件上进行的修改操作,也就是写访问。

c. 基本原理

在 C2 级,支持整体 DAC 机制的元素需要隔离支持 DAC 的信息(即客体)以便于审计(参见"系统体系结构")。可利用 X.25 中的同一协议的方法,例如网络第三层 X.25 协议的同一方法。使用该网络标识符来标识用户组或用户自身。支持整体 DAC 机制的元素被视为不可信的主体。网络环境中的增强型 DAC 机制由 C2 级提供。

典型的 DAC 情况是在某主机上为远程用户创建一个代理进程,该代理进程可在主机 NTCB 分部的控制下访问客体。本标准要求 NTCB 为每一个这样的进程指定并保留一个用户标识符,于是代理进程就可以受到与本地用户一样的自主访问控制。然而,本标准可以允许在一定范围内指定用户标识符。

最明显的情况是:如果每一个主机都可以使用网络用户的全局数据库(例如命名服务器),那么所有用户标识符都是全局有效的。

某些 NTCB 分部可以为局部注册的用户保持一个局部使用的数据库。在这种情况下,或者禁止为局部未注册的用户创建代理进程;或者允许为预选的用户或用户组创建代理进程。这些进程可标识运行在某远程主机上的用户组。本标准中的审计一词表明了最小的可审计度。审计要求 NTCB 分部的审计设施判定当某代理进程产生时,到底是谁在远程用户的主机上注册运行。

标识与鉴别机制负责建立用户标识符与代理进程的联系。这就意味着代理进程的用户标识符对 DAC 是局部适用的,数据通过网络回到用户主机的传输过程以及在用户主机上为数据做备份不是 DAC 的工作。

只支持内部主体的部件将要影响到 DAC 的实现,这是由于要完成 DAC 判定的部件需要得到一个提供服务的信息(如用户标识符),关于这种情况的一个例子是主机 A 上的某个用户试图访问主机 B 上的某个文件。通常是由主机 A 向主机 B 传送一个用户标识符,而在主机 B 上完成 DAC 判定。

有若干种机制可以做到唯一用户标识过程。其中包括:

第一,要求在执行访问操作的主机上提供唯一标识和鉴别过程。

第二,确认由另一主机鉴别的有效网络地址,并将其发送至执行访问操作的主机;

第三,对支持网络全局的用户唯一标识符进行管理,该标识符可能是如在第二中所述的由另一主机鉴别和发送来的,或由一个指定的网络标识和鉴别服务器鉴别和发送来的。

完成第二和第三的协议应遵循系统体系结构要求。

除上述典型方式外，DAC的网络支持还有其他方式，通常建议集中式访问控制方式。访问控制中心完成DAC的所有判定，或控制主机对主机的连接，来减少各主机的负担，这样可使一个主机只需要控制有限个远程主机上的用户对客体的访问。在这种情况下，访问控制中心提供面向抽象连接和DAC整体网络安全策略之间的连接。在上述所有情况下，应由客体所在的主机实现该判定。

5.2.2.1.2 客体重用

a. 采用自GJB 2646说明

在向一个主体初始转让、分配或重分配TCB未使用的存储器客体池之前，应删除所有包含在存储器客体内的信息授权。对已释放回系统的客体，有访问权的任何主体都不能再使用由原主体产生的任何信息，包括已加密的信息。

b. 解释

NTCB应保证它所控制的任一存储客体（如某部件上NTCB分部控制下的消息缓冲区）不包含该部件主体内未获授权的信息。这种要求应由每个NTCB分部完成。

c. 基本原理

在网络系统中，人们对NTCB直接控制下的存储客体感兴趣，如部件上的消息缓冲区。网络系统里的每一个部件都应满足客体重用要求。例如DAC要求消息缓冲区处于NTCB分部的控制下。分配给某内部主体的缓冲区可以被某个保证消息流完整性的主体所重用。这种可控的客体可以在物理资源如缓冲区、磁盘扇区、磁带和主存上实现或在某部件如网络开关上实现。

5.2.2.2 责任

5.2.2.2.1 标识与鉴别

a. 采用GJB 2646说明

TCB要求用户在开始操作前对其自身进行用户标识。而且，TCB会利用保护机制（如口令）来鉴别用户身份。TCB应保护鉴别数据以防止被未授权的用户读取。**TCB应该能够很好地识别计算机系统内的每一个用户，以此实现个体责任。TCB还应该提供把这种标识与该单个用户发生的所有可审计动作相联系的能力。**

b. 解释

用户标识与鉴别要求与网络系统对计算机系统的要求一致。标识与鉴别工作可以由用户直接连接的部件负责，也可以由其他的部件（如标识鉴别服务器）负责。当NTCB欲以用户或用户组名义作主机或其他网络部件的媒体时，NTCB将使用主机的标识和鉴别功能而不用单用户的标识鉴别功能。**部件标识功能在进行鉴别时，应隐含与标识功能有直接联系的特定的用户组。这一要求并不适合于内部主体。**

如果NTCB能保证信息避免受到未授权的破坏，那么，当从一个部件到另一个部件时，可以无需再次进行信息鉴别，包括已鉴别的用户身份。这种保护至少应达到与鉴别机制和鉴别数据的保护相同的保证级别。

c. 基本原理

在网络系统中，责任要求没有改变。把 NTCB 分布于若干部件之上，既不增加也不减少要求。即依旧存在单一责任。同样，在 C2 级或更高级的网络系统中，“单一责任”可由主机或其他部件中的标识功能完成，只要能追踪单个用户或满足活动主体的特定单用户要求即可。在追踪过程中允许有偏差，因为组成员可能有变化，而且，完成访问控制也需要时间。另外，在网络这样的分布式系统中，当用户通过主体与远程主体操作时，无需在每一个节点上再次鉴别用户。

自主访问控制（DAC）由部件标识符和（或）鉴别信息的传递实现。这种支持机制使得 DAC 允许用户访问不同 NTCB 分部上的存储客体而不只是用户鉴别的客体。使用前向的标识机制指明通信路径上源和部件的依赖性。

5.2.2.2.2 审计

a. 采用自 GJB 2646 说明

TCB 应能建立、维护和保护对客体（它所保护的）访问的审计跟踪，防止修改、未授权访问或破坏。审计数据应受 TCB 保护。对它的读访问应限制在对审计数据已授权的那些人。TCB 应能记录下述类型的事件：标识和鉴别机制的使用、把客体引入到一个用户的地址空间（如打开文件，启动程序）、删除客体、计算机操作员和系统管理员和（或）系统安全员的动作，以及其他有关的安全事件。对每个已记录的事件来说，审计记录应标出：事件的日期和时间、用户、事件的类型、事件的成功或失败。对于标识和鉴别事件，请求的起点（如终端 ID）应包括在审计记录中。对于把客体引入用户地址空间的事件和客体删除事件，审计记录应包括客体名。计算机系统管理员应能以个体标识为基础有选择地审计任意一个或更多个用户的活动。

b. 解释

负责人必须能分辨出哪些事件是可审计的。如果 NTCB 本身（如“其余安全服务”中所标识的那些）无法分辨此类事件，审计机制应提供一个接口，授权主体可利用该接口中的参数来产生审计记录。这样的审计记录要与 NTCB 的审计记录有所区别。在网络系统中，“其余安全相关事件”（与网络体系结构和安全策略有关）可能有以下几种：

. 标识每一个访问事件（如在网络的两个主机之间建立或不建立连接）及其参数（如访问过程中两个主机的标识符）；

利用本地时间或全局同步时间来标识每一个访问过程的起止时间；

在两个主机交互过程中，标识与安全相关的意外情况（如破坏数据完整性事件）；

使用密码术；

改变网络配置（如某部件加入或离开网络）。

另外，如果必要，审计追踪记录中应包含标识信息，以允许所有相关的审计记录（如：不同主机上的审计记录）可相关。而且，网络中的某部件可能具有所要求的审计功能（如存入、取出、减少、分析），而其他部件则可能不存储审计数据，但却可以将审计数据传送到指定的收集部件。由于资源的不可得性，应控制审计数据的丢失。

在网络系统中，由于引入和删除客体事件而使其“用户地址空间”被扩展，包括远程用户（或主机）的代理正在使用的那些地址空间。尽管如此，其重点仍在用户而不是 DAC 准则中讨论过的内部主体。另外，审计信息应以机器可读的形式存储。

c. 基本原理

对远程用户来讲，可利用网络标识符(如互连地址)来表示单个用户或用户组标识符(如主机 A 的所有用户)，以避免当远程用户需要使用标识时应进行的维护过程。在 C2 级，必须能标识出(立即或以后)一个组标识符表示哪些单个用户。在其它各方面，该说明是网络系统准则的直接延伸。

5.2.2.3 保证

5.2.2.3.1 操作保证

5.2.2.3.1.1 系统体系结构

a. 采用 GJB 2646 说明

TCB 应保持自身运行域，以防止外部干扰或窜改(如修改 TCB 代码或数据结构)。TCB 控制的资源可以是计算机系统中已定义的主体或客体的子集。**TCB 应隔离被保护的资源，以使它们受到访问控制并满足审计要求。**

b. 解释

所有的 NTCB 分部均必须满足系统体系结构准则。只有当所有 NTCB 分部均保持自身运行域时，NTCB 才可能保持自身运行域。

NTCB 所控制的网络资源子集是 NTCB 各分部所控制的资源子集之和。必须保护属于 NTCB 的代码与数据结构和在 NTCB 主体(即在 NTCB 内部，参考监视器外部的主体)中传送的属于不同 NTCB 分部的代码与数据，以防止其受到外部的干扰和窜改。可用密码验证和或物理手段来保护 NTCB 分部之间交换的用户鉴别信息。

每一个 NTCB 分部应按照网络体系结构与安全策略的要求隔离部件内受保护的资源。

c. 基本原理

NTCB 分部之间的通信保护要求特别针对 NTCB 分部上的主体。任何 NTCB 分部以外主体的此类要求均属于安全策略完整性要求的范畴。

与 C1 级比较，隔离受保护的资源，为依赖于资源(例如，DAC 和用户标识)的机制的正确操作提供更多的保护。

5.2.2.3.1.2 系统完整性

a. 采用 GJB 2646 说明

应提供硬件和(或)软件特性，能够使用它们来定期验证 TCB 中现场硬件和固件元素操作的正确性。

b. 解释

要求的实现是通过能够用于定期验证每个 NTCB 分部部件中的硬件和固件元素是否正确操作硬件和(或)软件来部分完成的。在网络系统合并以及在全系统中进行操作之前，应提供验证同一性和修正部件操作的特性。例如：应设计一种协议，能使 NTCB 分部的部件定期交换消息并验证彼此的正确应答。该协议还应能决定远程实体的应答能力。NTCB 分部还应提供向网络管理员报告在其他 NTCB 分部中检测到故障的能力。

应该设计一种在 NTCB 内实现的部件之间的协议，在发生网络通信或单独部件失效的情况下，用它来提供正确操作。网络中的自主访问控制策略可能会要求可信主体间的通信(该主

体是不同部件上的 NTCB 分部的一部分)。这种通信通常由主体间的协议以平等实体的方式来实现。NTCB 分部与其他部件通信的失效不应引起部件内的错误访问。

c. 基本原理

该“解释”的第一段是对网络系统正文和在网络准则中所定义的 NTCB 分部要求的直接延伸。

NTCB 协议应足够强壮,以便当局部故障发生时,可以保证系统正确地运行。这种保护机制可以保持 NTCB 自身的完整性。任何时侯,网络中的一个或多个部件都可能无法工作,将这种故障对其他部件的影响减至最小是至关重要的。其余的完整性与拒绝服务事件将在“其余安全服务”中讨论。

5.2.2.3.2 生命周期保证

5.2.2.3.2.1 安全测试

a. 采用 GJB 2646 说明

应测试计算机系统以证明其确实可以如系统文档所要求的正常工作。测试的目的,是保证系统不允许未授权用户的通行或以其他方式破坏 TCB 的安全保护体系。测试还应包括搜索明显的缺陷,这些缺陷会使资源隔离遭到破坏或允许对审计数据或鉴别数据进行未授权的访问(参见 GJB 2646 附录 C(补充件))。

b. 解释

部件测试需要利用一个测试台来测试部件的接口与协议,并包括意外情况下的测试。网络系统中的安全机制测试是通过综合测试过程进行的,测试过程包括实现这一安全机制的一个 NTCB 分部的所有部件。把这种综合测试附加到网络系统评估时任何单个部件的评估中。负责人应能标识出包括网络大小的系统配置的许可集。可利用分析或测试过程与工具来测试这些配置的限制。在配置许可集内的配置变动无须再次测试。

c. 基本原理

测试是验证安全机制正确完成预定功能的首要方法。

5.2.2.4 文档

5.2.2.4.1 安全特性用户指南

a. 采用 GJB 2646 说明

用户文档的摘要、章条或手册应描述由 TCB 提供的保护机制、保护机制的使用说明及保护机制间的交互过程。

b. 解释

该用户文档描述了用户可见的全局(网络系统)级的、每一部件用户接口上的以及它们之间交互过程中的保护机制。

c. 基本原理

该“解释”是对网络系统和在网络标准中所定义的 NTCB 分部的延伸。由单个部件提供的保护机制的文档由适用于单个部件的可信计算机标准提供。

5.2.2.4.2 可信设备手册

a. 采用 GJB 2646 说明

在计算机系统管理手册中应指出：当安全设备运行时，对有关功能与特权应加以说明，并提出警告。对各类审计事件，应给出提供检查和维护审计文件用的程序以及详细的审计记录结构。

b. 解释

该手册中应包含说明与过程，以协助系统管理员了解系统的配置情况。这些说明与过程包括以下几种情况：

网络本身的硬件配置；

如何向网络中增加新部件；

当某部件阶段性地离开网络（如被破坏或断开连接）后再次上网的情况；

影响网络安全性能的网络配置，例如手册应向网络系统管理员说明影响网络体系结构的部件间的互连；

加载或修改 NTCB 软件或固件。

应规定物理上的和管理环境上的控制。网络中任一安全性假设均应说明。例如：所有通信链都应有物理级上的保护。

c. 基本原理

多种系统管理员可能有各种各样的责任。这些手册上的技术安全措施必须与其他安全措施结合使用，以保证网络系统的安全性。其他安全措施包括管理安全、物理安全、辐射安全等。

该手册中应增加网络配置部分的标准，因为，部件之间正确的互连对于网络体系结构的实现至关重要。

密码技术是保护通信线路的常用机制。未授权用户不可以读加密信息。通常密文的安全级比较低，如欲使用加密算法，应由国家和军队安全主管部门认可。

加密算法与其实现过程不在本标准讨论范围。加密算法及其实现可能由某个单独设备完成或是某个部件的主体功能。本标准不加区别地把任一加密实现包看做是加密机制。

5.2.2.4.3 测试文档

a. 采用 GJB 2646 说明

系统负责人应向评估者提供一份文档，该文档包括测试计划、安全机制的测试过程，以及安全机制功能测试的结果。

b. 解释

测试计划应说明测试的组成，亦应标识出不属于评估系统的测试部件。该计划还应包括这类部件中与测试相关的功能，以及评估系统这类部件的接口。网络测试计划说明应明确表示测试可以完全覆盖网络安全策略。测试应包括在系统体系结构和系统完整性中所描述的特性。测试亦应包括网络体系结构和大小。

c. 基本原理

被评估实体可能是一个网络子系统（参见附录 A（补充件）），应增加其他部件才能构成一个完整网络系统，在这种情况下，该文档应包括一些与上下文有关的定义说明。在评估时，若没有测试网络子系统的说明，就无法验证测试计划的正确性。

5.2.2.4.4 设计文档

a. 采用 GJB 2646 说明

设计文档应提供负责人描述的保护原理及其在 TCB 上的实现，如果 TCB 由不同的模块构成，应描述模块之间的接口。

b. 解释

在说明 NTCB 如何实现负责人所描述的保护原理时，应说明 NTCB 的分布方式。亦应说明安全策略。NTCB 模块间的接口应包括：NTCB 分部与分部内模块间的接口（若存在模块的话）。负责人应描述安全体系结构与设计，其中包括部件间安全要求的分布情况。附录 A（补充件）说明有关部件的评估。

c. 基本原理

该解释是对在网络系统正文中所定义的网络说明要求的直接延伸。另外还要求在其他如描述部件或描述操作环境的文档中把网络子系统或网络系统描述为功能，例如在可信设备手册中。

为进行评估，网络系统应有相关的网络安全体系结构与设计（和网络安全体系结构与设计无关的部件的互连见附录 C（补充件））。网络安全体系结构必须包括与安全相关的策略、客体和协议。网络安全设计说明了网络中应包含的接口与服务，因此，能够可信地评估该网络。也许有多种设计构成同一个体系结构，但可能会出现不兼容或无法工作的情况（遵循互连规则的除外）。要求在设计中以可见接口方式描述部件间合作和安全相关的机制，不可见接口不在本标准讨论范畴。

在进行网络或部件评估之前，负责人应提供网络安全体系结构与设计。网络安全体系结构与设计必须充分实现，而某些明显和不明显的缺陷要经过基于该特定结构的可信网络评议会议的同意。

当设计部件或欲评估部件时，当用部件组装网络或欲评估该网络时，均必须首先证明满足网络安全体系结构与设计。也就是说，用遵循网络安全体系结构与设计的每一种方法，能将多个部件构成网络，使之达到评估说明规定的可信网络要求。

为了由部件组成的可信网络能独立构造，网络安全体系结构与设计应完整而无二义性地定义部件的安全功能与部件间的接口。应该评估网络安全体系结构与设计，以保证遵循它的说明而建立的网络是可信的，也就是说该网络可由本标准来评估。

5.3 B 等：强制保护

B 等的主要要求是 NTCB 保护敏感标号的完整性，并使用它们去实施一组强制性访问控制规则。本等级网络系统必须将敏感标号与系统主要数据结构一起传送。系统负责人还需要提供安全策略模型（NTCB 将以此为基础）和一份 NTCB 的规范说明，还必须提供参考监视器概念已被实现的证据。

5.3.1 B1 级：有标号的安全保护

B1 级的网络系统要求具有 C2 级的全部特征。另外，必须提出安全策略模型的非形式化的描述、数据标号和命名主体对客体强制性访问控制。对输出信息必须有正确的标号能力。必须排除经测试而标识的任何缺陷。以下是 B1 级网络系统的最低要求。

5.3.1.1 安全策略

a. 采用 GJB 2646 说明

b. 解释

网络负责人应清晰描述 NTCB 所完成的整体网络安全策略。该策略应至少包括本级适用的自主和强制访问控制要求。它要求数据保密性或数据完整性或两者兼备。**该策略是由自主性和强制性两部分组成的访问控制策略。**该策略应包括通过对用户或用户组鉴别来保护所处理的信息的自主安全策略。该访问控制策略应清晰描述网络的下述要求：防止并检测由未授权的用户或错误引起的对敏感信息的“读取或破坏”。**强制性策略必须定义它所支持的敏感标号集。对于 B1 级或更高级别，强制性策略应基于敏感标号（该敏感标号反映了按保密性和（或）完整性规定的信息的安全级）和用户标号（该标号用于鉴别用户，以允许其访问某类信息）。**未授权的用户包括：无权使用网络的所有用户；网络的合法使用者，但无权访问被保护信息的持定部分。

注意：“用户”并不包括“网络操作员”、“系统程序员”、“系统维护员”、“系统安全员”以及其他技术人员。这些人员与一般用户有所区别并遵循可信设备手册和系统体系结构要求。这些人员可以修改网络中的系统参数，例如：重新定义组成员。他们也可以具有独立的用户职责。

保密性策略：网络负责人应清晰定义阻止未授权用户访问系统中敏感信息的自主和强制保密性策略。

数据完整性策略：网络负责人应清晰定义阻止未授权用户修改（即：写入）敏感信息的自主和强制完整性策略。由网络负责人所定义的数据完整性是：在网络中信息不应受到未授权的修改。**一般情况下，由 NTCB 实施的强制完整性策略不能防止信息在部件间传输中被修改。然而，完整性敏感标号可以使信息在传输过程中由于受到保护而不会发生传输错误。这种要求有别于标号完整性要求。**

c. 基本原理

“负责人”一词可指“出售商”、“网络集成商”、“制造商”、“开发商”中的某一位。有多种含义的原因是因为在评估网络系统时，某些人可能不是相关人员。

可信网络应控制对共享敏感信息的读与写。控制写操作就可保护信息免受破坏，一般情况下，网络既要保持信息的保密性也要保护完整性。但是，通常是完整性要比保密性更重要。因此，不论网络被评估为哪个级别，网络都应具备保密性和（或）完整性策略。这些策略的保证程度由网络的评估级别反映。

对修改操作的控制可以保证信息可靠，而且，一旦信息被破坏，仍然可以控制由于该破坏而引起的潜在危险。网络完整性策略既要保护在部件上正被处理的数据，也要保护正在网络中传送的数据。由 NTCB 所完成的访问控制策略与每个部件内主体对客体的访问相关。传递信息的通信完整性在“其余安全服务”中讨论。

在某些体系结构中的强制完整性策略（B1 级或更高级）可以用来支持面向连接的抽象或网络中部件之间的连接。例如，在端对端加密过程中的密钥配发中心，就可以指定一类特定的完整性范畴，以防止密钥产生的代码和数据受到该部件上其他支持过程（如操作员接口和审计）的修改。

某些体系结构中的强制完整性策略，可以定义一个完整性敏感标号，它反映了为确保信息既不会受到超过指定限度的随机错误的破坏，也不会受到未授权消息流修改(MSM)的特定要求。与完整性敏感标号相关的特定矩阵一般反映了网络中的指定应用。

5.3.1.1.1 自主访问控制

a. 采用 GJB 2646 说明

TCB 应定义并控制计算机系统中已命名用户和已命名客体(文件或程序)之间的访问操作。执行机制(例如：自身/组/公共控制，访问控制表)应允许用户通过自身/组/二者来指定并控制对客体的共享。执行机制还应控制访问权限的传播。自主访问控制机制应可以通过显性的用户行为或默认方式防止客体受到未授权的访问。这种访问控制应包括或排除单用户粒度的访问操作。只有授权用户才可以允许未得到访问许可的用户访问客体。

b. 解释

自主访问控制(DAC)机制应以各种方式分布于 NTCB 分部中。网络系统中的指定部件可以完成全部或一部分或不完成 DAC 的功能。尤其是仅仅支持内部主体(不做用户直接代理的主体)的部件，例如公共网络中的包交换，就可以不直接完成 DAC 的机制(例如它们不包含访问控制表)。

在网络环境中，有多种方法鉴别用户身份。例如在网络安全策略允许的情况下，可用不同部件(如主机，网关)的网络标识符(如互连地址)做为用户组标识符(如主机 A 的所有用户，网络 Q 的所有用户)，这样就不必鉴别每个用户的身份。例如，主机 A 可以使用一个特定的组标识符，并保持一个显性用户组列表，于是，主机 A 可利用该表与主机 B 进行通信。

对网络来讲，单个主机会对它的用户在已命名个体的基础上施加自主的控制——这一点和没有网络连接时所使用的控制相类似(事实上，也可能完全相同)。

当可以使用组标识符执行访问控制操作时，可能会要求其他主机的标识符，以此来避免进行远程用户的身份鉴别。C2 级或 C2 以上级的网络必须保证：当使用组标识符时，应利用审计记录来确切地标识(立即或以后)该组标识符所代表的单个用户。在组成员的改变以及相应的实现访问控制时刻的不同步过程中，可以允许稍有偏差。

NTCB 分部的 DAC 机制可以在参考监视器的接口中完成或分布在某个主体上(该主体是相同或不同部件中 NTCB 的一部分)。参考监视器管理系统中所有的物理资源并创建它所控制的主客体的抽象。这些主客体中的一部分可以完成 NTCB 的某一部分功能。当某 DAC 资源分布于 NTCB 主体上(可能在参考监视器外)时，DAC 的设计与实现机制的保证要求应符合 C2 级或 C2 以上各级网络的要求。

若网络自主安全策略包含完整性，以上说明尤其适用于控制已被鉴别的用户或用户组在每个部件上进行的修改操作，也就是写访问。

c. 基本原理

在这一级，支持整体 DAC 机制的元素需要隔离支持 DAC 的信息(即客体)以便于审计(参见“系统体系结构”)。可利用 X.25 中的同一协议的方法，例如网络协议第三层 X.25 中的同一方法，使用该网络标识符标识用户组或用户自身。支持整体 DAC 机制的元素被视为不可信的主体。

典型的 DAC 情况是在某主机上为远程用户创建一个代理进程，该代理进程可在主机 NTCB 分部的控制下访问客体。本标准要求 NTCB 为每一个这样的进程指定并保留一个用户标识符，于是代理进程就可以受到与本地用户一样的自主访问控制。然而，本标准可以允许在一定范围内指定用户标识符。

最明显的情况是：如果每一个主机都可以使用网络用户的全局数据库（例如命名服务器），那么所有用户标识符都是全局有效的。

某些 NTCB 分部可以为局部注册的用户保持一个局部使用的数据库。在这种情况下，或者禁止为局部未注册的用户创建代理进程，或者允许为预选的用户或用户组创建代理进程。这些进程可标识运行在某远程主机上的用户组。本标准中的审计一词表明了最小的可审计度。审计要求 NTCB 分部的审计设施判定当某代理进程产生时，到底是谁在远程用户的主机上注册运行。

标识与鉴别机制负责建立用户标识符与代理进程的联系。这就意味着代理进程的用户标识符对 DAC 是局部适用的，数据通过网络回到用户主机的传输过程以及在用户主机上为数据做备份不是 DAC 的工作。

只支持内部主体的部件将要影响到 DAC 的实现，这是由于要完成 DAC 判定的部件需要得到一个提供服务的信息（如用户标识符），关于这种情况的一个例子是主机 A 上的某个用户试图访问主机 B 上的某个文件。通常是由主机 A 向主机 B 传送一个用户标识符，而在主机 B 上完成 DAC 判定。

有若干种机制可以做到唯一用户标识过程。其中包括：

第一，要求在执行访问操作的主机上提供唯一标识和鉴别过程；

第二，确认由另一主机鉴别的有效网络地址，并将其发送至执行访问操作的主机；

第三，对支持网络全局的用户唯一标识符进行管理，该标识符可能是如在第二中所述的由另一主机鉴别和发送来的，或由一个指定的网络标识和鉴别服务器鉴别和发送来的。

完成第二和第三的协议应遵循系统体系结构要求。

除上述典型方式外，DAC 的网络支持还有其他方式，通常建议集中式访问控制方式。访问控制中心完成 DAC 的所有判定，或控制主机对主机的连接，来减少各主机的负担，这样可使一个主机只需要控制有限个远程主机上的用户对客体的访问。在这种情况下，访问控制中心提供面向抽象连接和 DAC 整体网络安全策略之间的连接。在上述所有情况下，应由客体所在的主机实现该判定。

有两种分布实现 DAC 的机制，一种是在不同的部件上分布实现，另一种在某个部件中的 NTCB 分部的主体上支持 DAC。由于“计算机系统”表示为整体“计算机网络”，每个部件都有责任完成分配给它的安全机制以保证网络安全策略的实现。对于传统的主机系统，DAC 机制可以与参考监视器中的强制访问控制（MAC）一起，使用如虚拟机器监控器等几种方法，在接口外支持 DAC。

与全局固定的强制性策略不同，DAC 是非常网络和系统专用化的，它的特性反映了系统的自然用途。常见情况是，单独主机以命名个体方式控制本地用户，这就像没有网络一样。然而，在大型网络中，集中地管理所有用户显然是很困难的。因此，其余主机的用户通常都被分

组，以便于网络 DAC 策略的控制要求实际上是以这些主机或其他部件的标识为基础。网关是此类部件的一个例子。

保证要求是可信系统的关键所在。它可以决定某个系统或网络是否适合于指定的环境。在单个系统中，DAC 是合成在参考监视器中的，而与其他部分很难区分清楚。在网络系统中，由于 DAC 的分布实现，区分就比较容易。如果主要的网络部件可以较简便地设计实现，而又不会降低安全策略的要求，那么可信网络也就容易实现。

5.3.1.1.2 客体重用

a. 采用自 GJB 2646 说明

在向一个主体初始转让、分配或重分配 TCB 未使用的存储器客体池之前，应删除所有包含在存储器客体内的信息授权。对已释放回系统的客体有访问权的任何主体都不能再使用由原主体产生的任何信息，包括已加密的信息。

b. 解释

NTCB 应保证它所控制的任一存储客体（如某部件上 NTCB 分部控制下的消息缓冲区）不包含该部件主体内未获授权的信息。这种要求应由每个 NTCB 分部完成。

c. 基本原理

在网络系统中，人们对 NTCB 直接控制下的存储客体感兴趣，如部件上的消息缓冲区。网络系统里的每一个部件都应满足客体重用要求。例如 DAC 要求消息缓冲区处于 NTCB 分部的控制下。分配给某内部主体的缓冲区可以被某个保证消息流完整性的主体所重用。这种可控的客体可以在物理资源如缓冲区、磁盘扇区、磁带和主存上实现或在某部件如网络开关上实现。

5.3.1.1.3 标号

a. 采用 GJB 2646 说明

TCB 应保持与每个主体及该主体控制下的存储客体（如过程、文件、段、设备）相关的敏感标号。强制访问控制判断应以这些标号为基础。为输入无标号的数据，TCB 应提出请求，并从授权用户那里接收该数据的安全等级，而且 TCB 将对所有这些活动进行审计。

b. 解释

在 NTCB 分部控制下输入的无标号数据将由输入它的单级设备强行指定一个标号。标号应包括由网络负责人所描述的与网络安全策略完全一致的保密性与完整性两部分。本说明中所有的“标号”一词都包括上述两个部分。同样，“单级”和“多级”两词都以该策略的保密性和完整性为基础。强制完整性策略应特别具有下述要求，如未被判定的消息流修改的可能性应在被保护数据的标号中有所反映。例如，当输入数据时，能够以密码机制为基础赋给它一个完整性标号，来保证达到该策略的要求。NTCB 应保证这种机制受到保护，而且能基于一个标号调用它。

c. 基本原理

该“解释”是对网络系统要求和在网络说明中所定义的 NTCB 分部的延伸。单级设备可以看作是主体或者也可以看作是客体。多级设备可以看作是有一定保密范围的可信主体，即该主体的保密范围位于期望在该设备上传输数据的最小至最大范围之间。

针对保密性或完整性或二者的敏感标号，可以反映未划分的等级或划分的等级或二者。

5.3.1.1.3.1 标号完整性

a. 采用 GJB 2646 说明

敏感标号应准确表示特定主体或客体的安全级，该主体和客体由此而相联系。当 TCB 输出时，敏感标号应准确而无二义性地表示内部标号，并与正在输出的信息相联系。

b. 解释

“TCB 输出”是指从一个部件上的客体到另一个部件上的客体的信息传送过程。在 NTCB 分部间传送的信息在“系统完整性”中讨论。内部与外部敏感标号的形式可能不同，但其意义相同。另外，NTCB 还应保证敏感标号与网络中正在传输的信息之间的正确关系。

正如在“可信设备手册”中所述，未授权用户不可读加密信息。一般来讲，密文的安全级低于明文的。明文与密文包含在不同的客体中，各有自己的标号。明文的标号应加以保护，并与密文相关，当密文解为明文时，它可以被恢复。如果明文与单级设备相关联，其标号可以是隐含的。标号也可以隐含于密钥中。

当信息被输出到某个环境，在那里它可能受到有意或无意的修改时，TCB 应支持如密码检验和方法以保证标号的准确性。当具备强制完整性策略时，该策略应定义完整性标号的含义。

c. 基本原理

加密算法与其实现过程不在本标准讨论范围。加密算法及其实现可以由一个单独设备完成或是某部件的主体功能。本标准不加区别地把任意一个实现包看做是加密机制。加密算法应得到国家和军队的安全主管部门批准。加密过程是某部件上 NTCB 分部的一部分。

加密机制不一定是多级设备或多级主体。由定义可知，加密过程是多级的。明文与密文接口带有不同安全级的信息。加密机制不会因在数据上执行逻辑或数学的操作而产生新的数据。加密机制中的明文或密文接口应分别标识为单级或多级。若接口是单级的，数据的安全级为可信单体，并与接口隐性相关联，“单级设备输出准则”适合于此处。

若接口是多级的，则数据必须加以标号，“多级设备输出准则”适合此处。网络体系结构可任意挑选可用的机制，将客体与标号相联系。可能发生的有关加密客体的例子如下：

在客体的协议定义中，包含标号域；

通过密钥将标号与客体隐式相联系，也就是说，密钥唯一标识安全级，在数据的加密级上，必须保护单独或私用的密钥。

5.3.1.1.3.2 有标号信息的输出

a. 采用 GJB 2646 说明

TCB 应对每个通信信道和 I/O 设备标明单级或多级。这个标志的任何变化都应由人工实现，并可由 TCB 审计。TCB 应维护并且审计任何与通信信道或 I/O 设备有关的安全级或标号的变化。

b. 解释

应指定每个通信信道和网络部件为单级或多级。该指定的任何改变应经过由负责受影响部件的管理员或安全员批准，或由 NTCB 的管理员或安全员批准。这种改变可被网络审计。

NTCB 应维护并能审计与单级通信信道相关联的设备标号或者与多级通信信道或部件相关联范围的任何改变。NTCB 还应能审计与在多级通信信道或部件上传送的信息相关联的安全级集合的任何变化。

c. 基本原理

网络中的通信信道或部件与独立系统中的通信信道或 I/O 设备相似。必须把它们指定为多级(可以区分不同安全级的信息)或单级。在 GJB 2646 中，单级设备只可以连接在单级信道上。

若要改变向部件或通信信道发送信息的级或级的集合,应得到网络或部件安全员的认可与批准(若没有安全员,系统管理员也可以)。这一要求可以保证未经有关人员的批准,不会发生与安全相关的改动。

5.3.1.1.3.2.1 向多级设备的输出

a. 采用 GJB 2646 说明

当 TCB 将一个客体输出到一个多级 I/O 设备时,与该客体有关的敏感标号也应相应输出。并以输出信息相同的形式(如机器可读或人可读形式)驻留在同一物理介质上。当 TCB 在多级通信信道上输出或输入一个客体时，该信道使用的协议可以无二义性地把敏感标号和被发送或被接收的有关信息联系起来。

b. 解释

网络中的部件,包括主机,应通过多级通信信道或多个单级通信信道良好地互连,以保护多安全级的信息。联系安全级与输出信息的协议应提供唯一所需要的信息,将安全级与单个部件上 NTCB 分部之间通信信道上传送的信息联系起来。这种协议的定义必须指定敏感标号的表示和语义(如机器可读的标号必须唯一表示安全级)。

安全级与通信信息之间“无二义”的联系,应达到 NTCB 内其余任何标号的精确度(在“标号完整性”中已讨论)。这种机制可由受保护且高度可靠的直接物理层连接完成,或由传统的可以有效地发现传输过程中错误的密码链保护完成,或者也可以使用分离的信道完成。

c. 基本原理

协议必须定义敏感标号的表示与语义。(见附录 B(补充件)中的“强制访问控制策略”)。多级设备与(不可信)主体的接口,或由参考监视器的接口完成,或由一个多级主体完成(例如,在 Bell-LaPadula 模型定义的“受委托主体”),该主体提供一个以 NTCB 分部的内部标号为基础的标号。

当今的技术水平限制了安全网络中强制策略的支撑能力。控制网络中每一个主体操作的参考监视器应完全由单个 NTCB 分部提供,该 NTCB 分部还应提供其主体的 NTCB 接口。这就意味着在安全策略模型(该主体通过传输调用能更改该模型)中表示的“安全状态”必须包含在同一个部件中。

对于驻留某个 NTCB 分部的部件之外的事件(例如到达一个消息)可以影响该 NTCB 分部的安全状态。这种影响可在另外的部件或分部上的事件初始化后异步地产生。例如,不确定的延迟可能发生在以下三种情况中,即一个部件初始化某消息、消息到达另一个部件的 NTCB 分部和第二个部件上安全状态改变。由于网络各部件是并行工作的,所以需要网络的全局控

制(如网络全局时钟)以实现安全状态的同步转换。一般来说,这种设计既不实用也不被接受。因此,NTCB 分部之间的交互仅限于一对(至少是逻辑上的)设备之间的通信,如果设备可接/发多级信息的话,应为多级设备。对于广播型信道来讲,通信对是发送者与预定接收者。然而,如果广播信道带多级信息,还需要另外的机制(如 TCB 保持的加密检验和)来实现分离与发送。

当两个位于不同部件上的多级设备进行互连时,在信道上使用的协议中需要有一个通用表示的敏感标号,使得发送者与接收者都能理解。在整个网络策略中每一个安全级都必须在那些标号中唯一表示出来。

在某个单独的 TCB 中,敏感标号的精确度一般是由很简单的技术(如很短的物理连接)来保证的,也可以使用单独印刷电路板或通过内部总线来达到。在许多网络环境中,很可能发生偶然的错误或蓄意引入的错误,此时更需要良好的保护措施。

5.3.1.1.3.2.2 向单级设备输出

a. 采用 GJB 2646 说明

单级 I/O 设备和单级通信信道不需要维护其处理信息的敏感标号。然而,TCB 应包含一种机制,用这种机制 TCB 和一个受权用户进行可靠地通信,该通信信息具有指定的单安全级,且通过单级信道或 I/O 设备完成输入或输出。

b. 解释

如果两个直接相连的部件之一或全都不能可信地将不同安全级信息分离,或者这两个部件有一个共同的单安全级,那么,这两个部件应通过单级信道通信。单级部件或单级通信信道并不需要保持其处理信息的敏感标号,因此 NTCB 应包含一个可靠机制,使得 NTCB 与一个授权用户或 NTCB 分部内的主体可利用该机制指定信息的安全级,该信息由单级信道或网络部件输入或输出。

c. 基本原理

网络中的单级通信信道和单级部件与独立系统的单级信道和 I/O 设备类似,它们都不能可信地分离不同安全级的信息,因此,在这类信道与部件上传送的与数据相关的标号是隐含的;这是因为信道或部件而不是位流的显性部分使得 NTCB 将数据与标号连系起来。注意,加密信息的安全级是密文的级而非明文的原有级。

5.3.1.1.3.2.3 人可读的输出标号

a. 采用 GJB 2646 说明

计算机系统管理员应规定与输出敏感标号相关联的可打印的标号名。TCB 应对所有人员可读的输出、编页的输出以及带有可识别敏感标号的硬拷贝输出(如行打印机输出)的开始和结束做出标记,以便正确表示该输出的敏感性①。TCB 应按默认值对所有人可读的输出、编页的输出以及带有可识别敏感标号的硬拷贝输出(如行打印机输出)的每页的顶部和底部做标记,以便正确表示该页信息的敏感性。TCB 应该按默认值,并以适当方法标记具有人可读敏感标号的其他形式的人可读的输出(如映象、图形),以便正确表示该输出的敏感性。这些标记

① 在人可读的敏感标号内划分等级的部分应等于与输出这些标号相关联的所有已划分等级信息的最大部分;未划分等级的部分应包括与输出这些标号相关联的所有未划分等级的信息,而不再有其它未划分等级的信息。

默认值的任何滥用都应由 TCB 审计。

b. 解释

本标准对于产生人不可读输出的部件不加要求。对于产生人可读输出的部件，在网络中定义的每一个安全级在所有的部件中都应有统一的含义。网络管理员与其任何相关的部件管理员，都可指定与已定义安全级相关联的人可读标号。

c. 基本原理

该"解释"是对网络系统和在网络说明中所定义的 NTCB 分部要求的直接延伸。

5.3.1.1.4 强制访问控制

a. 采用 GJB 2646 说明

TCB 应对全部主体及其控制下的存储客体(如进程、文件、段、设备)执行强制访问控制策略。应给这些主体和客体指定敏感标号，这些标号是划分等级和不划分等级的结合，而且应作为强制性访问控制判断的基础。对于受 TCB 控制的主体和客体之间的全部访问应掌握下列要求：仅当主体安全级中划分的等级大于等于客体安全级中划分的等级，而且主体安全级中未划分的等级包括了客体安全级中全部未划分的等级时，主体才能读一个客体；仅当主体安全级中划分的等级小于等于客体安全级中划分的等级，而且主体安全级中未划分的等级被包含在客体安全级中未划分的等级时，主体才能写一个客体。TCB 应该用标识和鉴别数据来鉴别一个用户的标识，并保证 TCB 可以创建它以外主体的安全级及授权，从而使得批准和授权的那个用户去支配该用户。

b. 解释

每一个 NTCB 分部，都对它所控制下的部件上的所有主体、客体执行强制访问控制策略。在网络中，NTCB 分部的责任包括 TCB 在单个系统部件上施加的所有强制性访问控制。与其他部件进行通信用的主体和客体，更处于 NTCB 分部的控制下。强制访问控制包括保密性与完整性控制，这一点，网络负责人已在整体网络安全策略中有所描述。

两部件间与通信相关的概念化实体，如扇区、连接和虚电路，可视为有两个端点，每一端存在于一个部件上，而每个端点可视为局域客体。通信过程可视为从一端的客体上把信息拷贝到另一端的客体上。透明的携带数据的实体，如数据报和包，既可视为存储在其他客体上的信息，也可视为分别处在通信路径两端的携带数据的实体。

可通过保密性或完整性级别来达到"两个或两个以上"安全级的要求。在强制完整性策略中，读与写的要求通常为当且仅当某主体的安全级可控制另一主体的安全级时，该主体可读另一主体；当且仅当客体的安全级可控制主体的安全级时，主体可写客体。以完整性策略为基础，网络负责人应定义对所有标号的控制关系，例如，通过将保密性和完整性的点阵结合起来去定义这个关系。

c. 基本原理

NTCB 分部只可以对它部件上的主体和客体保持访问控制。某部件上的一个主体如欲访问另一部件上客体的信息，就要在远程部件上创建一个主体，以此作为第一个主体的代理。

强制访问控制必须在每一个 NTCB 分部的参考监视器接口上实施(即控制物理处理资源的机制)。这种机制为它所控制的主体和客体创建抽象。可以指定参考监视器外的一些主体

去完成部分 NTCB 分部的强制策略，如使用在 Bell-LaPadula 模型中定义的“可信主体”。

对于在 I/O 设备上传输的标号信息的更高要求，保证了连接于通信路径上客体敏感标号之间的一致性。网络体系结构必须能识别整体强制性网络安全策略与面向抽象之间的联系。例如，单独的携带数据的实体（如数据报）可以有单独的敏感标号，并以这些标号接受每一部件上的强制访问控制。单级连接的抽象由某个体系结构隐含地完成，而连接由单级主体实现，该单级主体只能使用同级的数据报。

基本的可信系统技术允许 DAC 机制分布实现，这一点与强制访问控制要求相反。对于网络而言，MAC 与 DAC 机制的分离是规则而非意外情况。

用来代表强制性访问控制（包括数据保密性和完整性）策略中所有安全级的总体敏感标号集，总是形成部分有序集。不失一般性，该有序集总可以延伸成一个包括所有未划分等级总和的点阵。对于任意一个点阵，全体敏感标号就定义了一个控制关系。为便于管理，最好有一个可控制其余标号的最大级。

5.3.1.2 责任

5.3.1.2.1 标识与鉴定

a. 采用 GJB 2646 说明

TCB 要求用户在开始操作前对其自身进行用户标识。因此，TCB 应维持鉴别数据，该数据包括验证单个用户身份的信息（如口令），用于确定批准和授权单个用户的信息。TCB 用这种数据来鉴别用户身份及保证 TCB 外部的可代表单个用户建立动作的主体的安全等级和授权能力，并由已批准和授权用户支配它。TCB 应保护鉴别数据以防止被未授权的用户读取。TCB 应该能够很好地识别计算机系统内的每一个用户，以此实现个体责任。TCB 还应该提供把这种标识与该单个用户发生的所有可审计动作相联系的能力。

b. 解释

用户标识与鉴别要求与网络系统对计算机系统的要求一致。标识与鉴别工作可以由用户直接连接的部件负责，也可以由其他的部件（如标识鉴别服务器）负责。当 NTCB 欲以用户或用户组名义作主机或其他网络部件的媒体时，NTCB 将使用主机的标识和鉴别功能而不用单用户的标识鉴别功能。部件标识功能在进行鉴别时，应隐含与标识功能有直接联系的特定的用户组。这一要求并不适合于内部主体。

如果 NTCB 能保证信息避免受到未授权的破坏，那么，当从一个部件到另一个部件时，可以无需再次进行信息鉴别，包括已鉴别的用户身份。这种保护至少应达到与鉴别机制和鉴别数据的保护相同的保证级别。

c. 基本原理

在网络系统中，责任要求没有改变。把 NTCB 分布于若干部件之上，既不增加也不减少要求。即依旧存在单一责任。同样，在 C2 级或更高级的网络系统中，“单一责任”可由主机或其他部件中的标识功能完成，只要能追踪单个用户或满足活动主体的特定单用户要求即可。在追踪过程中允许有偏差，因为组成员可能有变化，而且，完成访问控制也需要时间。另外，在网络这样的分布系统中，当用户通过主体与远程主体操作时，无需在每一个节点上再次鉴别用户。

自主访问控制(DAC)由部件标识符和(或)鉴别信息的传递实现。这种支持机制使得DAC允许用户访问不同NTCB分部上的存储客体而不只是用户鉴别的客体。使用前向的标识机制指明通信路径上源和部件的依赖性。**如果用已授权的标识作为确定某主体敏感标号的基础，它必须满足"标号完整性准则"。**

一个已授权的标识可在部件间前向传递，并被某些部件用来标识与主体相关联的安全级，该主体是已标识用户的代理所创建的。

5.3.1.2.2 审计

a. 采用GJB 2646说明

TCB应能建立、维护和保护对客体(它所保护的)访问的审计跟踪，防止修改、未授权访问或破坏。审计数据应受TCB保护。对它的读访问应限制在对审计数据已授权的那些人。TCB应能记录下述类型的事件：标识和鉴定机制的使用、把客体引入到一个用户的地址空间(如打开文件，启动程序)、删除客体、计算机操作员和系统管理员和(或)系统安全员的动作，以及其他有关的安全事件。**TCB还应能审计人可读的输出标号的任何滥用。**对每个已记录的事件来说，审计记录应标出：事件的日期和时间、用户、事件的类型、事件的成功或失败。对于标识和鉴别事件，请求的起点(如终端ID)应包括在审计记录中。对于把客体引入用户地址空间的事件和客体删除事件，审计记录应包括客体名**和客体的安全级**。计算机系统管理员应能以个体标识和**(或)客体的安全级**为基础有选择地审计任意一个或更多个用户的活动。

b. 解释

负责人必须能分辨出哪些事件是可审计的。如果NTCB本身(如"其余安全服务"中所标识的那些)无法分辨此类事件，审计机制应提供一个接口，授权主体可利用该接口中的参数来产生审计记录。这样的审计记录要与NTCB的审计记录有所区别。在网络系统中，"其余安全相关事件"(与网络体系结构和安全策略有关)可能有以下几种：

标识每一个访问事件(如在网络的两个主机之间建立或不建立连接)及其参数(如访问过程中两个主机的标识符)；

利用本地时间或全局同步时间来标识每一个访问过程的起止时间；

在两个主机交互过程中，标识与安全相关的意外情况(如破坏数据完整性事件)；

使用密码术；

改变网络配置(如某部件加入或离开网络)。

另外，如果必要，审计追踪记录中应包含标识信息，以允许所有相关的审计记录(如不同主机上的审计记录)可相关。而且，网络中的某部件可能具有所要求的审计功能(如存入、取出、减少、分析)，而其他部件则可能不存储审计数据，但却可以将审计数据传送到指定的收集部件。由于资源的不可得性，应控制审计数据的丢失。

在网络系统中，由于引入和删除客体事件而使其"用户地址空间"被扩展，包括远程用户(或主机)的代理正在使用的那些地址空间。尽管如此，其重点仍在用户而不是DAC准则中讨论过的内部主体。另外，审计信息必须以机器可读的形式存储。

c. 基本原理

对远程用户来讲，可利用网络标识符(如互连地址)来表示单个用户或用户组标识符(如主

机 A 的所有用户),以避免当远程用户需要使用标识时应进行的维护过程。在这一级,它必须能标识出(立即或以后)一个组标识符表示哪些单个用户。在其它各方面,该说明是网络系统准则的直接延伸。

5.3.1.3 保证

5.3.1.3.1 操作保证

5.3.1.3.1.1 系统体系结构

a. 采用 GJB 2646 说明

TCB 应保持自身运行域。以防止外部干扰或篡改(如修改 TCB 代码或数据结构)。TCB 控制的资源可以是计算机系统中已定义的主体或客体的子集。**TCB 应在其控制下,通过提供不同的地址空间来维护进程隔离。**TCB 应隔离被保护的资源,以使它们受到访问控制并满足审计要求。

b. 解释

所有的 NTCB 分部均必须满足系统体系结构准则.只有当所有 NTCB 分部均保持自我运行域时,NTCB 才可能保持自身运行域。**由于每一个部件在整个网络系统中都是一个独立的区域,因此在特定情况下,若部件上只有一个主体,就可以通过不同的地址空间来达到进程隔离的要求。**

NTCB 所控制的网络资源子集是各 NTCB 分部所控制的资源子集之和。必须保护属于 NTCB 的代码与数据结构和在 NTCB 主体(即在 NTCB 内部参考监视器外部的主体)中传送的属于不同 NTCB 分部的代码与数据,以防止其受到外部的干扰和窜改。可用密码检验和或物理手段来保护 NTCB 分部之间交换的用户鉴别数据。

每一个 NTCB 分部都按照网络体系结构与安全策略隔离部件内受保护的资源。**因此,网络系统中安全机制的"支持元素"(如 DAC 和用户标识)与 C2 级相比,由于提供了 NTCB 控制下的不同地址空间,从保证观点来看更强了。**

如在自主访问控制中已讨论的,某 NTCB 分部的 DAC 机制可以在参考监视器接口上实现,或者可以分布在同一个部件或不同部件内 NTCB 部分的主体中。若是分布在 NTCB 的主体内(即在参考监视器之外),DAC 设计与实现的保证要求应该与 C2 级或更高级网络相同。

c. 基本原理

NTCB 分部之间的通信保护要求特别针对 NTCB 分部上的主体。对于 NTCB 分部以外主体此类保护的任何要求均属于安全策略完整性要求的范畴。

在 NTCB 控制下能保证区分地址空间,这就提供了按照安全级来隔离主体的能力。这个要求在 B1 级提出,因为它是实现强制访问控所绝对必要的。

5.3.1.3.1.2 系统完整性

a. 采用 GJB 2646 说明

应提供硬件和(或)软件特性,能够使用它们来定期验证 TCB 中现场硬件和固件元素操作的正确性。

b. 解释

要求的实现是通过能够用于定期验证每个 NTCB 分部部件中的硬件和固件元素是否正

确操作硬件和(或)软件来部分完成的。在网络系统合并以及在全系统中进行操作之前，应提供验证同一性和修正部件操作的特性。例如，应设计一种协议，能使 NTCB 分部的部件定期交换消息并验证彼此的正确应答。该协议还应能决定远程实体的应答能力。NTCB 分部还应提供向网络管理员报告在其他 NTCB 分部检测到故障的能力。

应该设计一种在 NTCB 内实现的部件之间的协议，在发生网络通信或单独部件失效的情况下，用它来提供正确操作。网络中的强制和自主访问控制策略可能会要求可信主体间的通信(该主体是不同部件上的 NTCB 分部的一部分)。这种通信通常由主体间的协议以平等实体的方式来实现。NTCB 分部与其他部件通信的失效不应引起部件内的错误访问。

c. 基本原理

该“解释”的第一段是对网络系统正文和在网络准则中所定义的 NTCB 分部要求的直接延伸。

NTCB 协议应足够强壮，以便当局部故障发生时，可以保证系统正确地运行。这种保护机制可以保持 NTCB 自身的完整性。任何时侯，网络中的一个或多个部件都可能无法工作，将这种故障对其他部件的影响减至最小是至关重要的。其余的完整性与拒绝服务事件将在“其余安全服务”中讨论。

5.3.1.3.2 生命周期保证

5.3.1.3.2.1 安全测试

a. 采用 GJB 2646 说明

应测试计算机系统，以证明其的确可以如系统文档所要求的正常工作。一个充分熟悉 TCB 特定实现的小组应详细分析和测试它的设计文档、源代码和目标代码。他们的目标是暴露全部设计和实现的缺陷，这些缺陷可以允许一个 TCB 外的主体去读、改变或删除通常在 TCB 执行强制或自主安全策略时拒绝的数据；并且保证没有主体(未授权去这样做)能使 TCB 进入不能对其它用户启动的通信做出响应的状态。应排除所有已发现的缺陷，或使其无效，而且 TCB 应被重新测试，以便验证已排除了缺陷，并且没有产生新的缺陷(参见 GJB 2646 附录 C(补充件))。

b. 解释

部件测试需要利用一个测试台来测试部件的接口与协议，并包括意外情况下的测试。为满足该准则。网络系统中的安全机制测试是通过综合测试过程进行的，测试过程包括实现这一安全机制的一个 NTCB 分部的所有部件。把这种综合测试附加到网络系统评估时任何单个部件的评估中。负责人应能标识出包括如网络大小的系统配置的许可集。可利用分析或测试过程与工具来测试这些配置的限制。在配置许可集内的配置变动无须再次测试。

对每一部件的测试应包括该部件上 NTCB 分部以外所引进的主体，该主体可读、改变或删除一般情况下已被废弃的数据。如果该部件的一般接口不能提供创建完成此类测试所需要的主体的方法，那么，这一部分测试将对部件使用一个不可信软件的特定版本，来完成在主体内的这些测试，应保存测试结果以进行测试分析。这样的特定版本将有一个 NTCB 分部，它与在评估时该部件通常配置的 NTCB 分部是相同的。

强制性控制的测试应包括：证明向部件输入和(或)从部件输出的信息标号准确表示该部

件使用的、被 NTCB 分部所维护的、作为强制访问控制判定基础的标号。测试亦应包括由该部件支持的单级或多级每一种类型的设备。

c. 基本原理

"没有主体(未授权去这样做)能使 TCB 进入不能对其它用户启动的通信做出响应的状态"涉及到拒绝服务问题的安全服务及协议实现的正确。

测试是验证安全机制正确完成预定功能的重要方法。测试的主要目的是证明系统能对从不可信主体到 NTCB 分部的输入(有可能是蓄意的)做出响应。

一般系统允许动态输入新程序和创建新进程(由此也就引进了新主体),并由用户指定其安全特性。而与此相反,许多网络部件则没有在一般操作过程中引进新程序和(或)新进程的方法。由此,相关的测试程序就必须做为软件的特定版本而引进,而不是测试小组的一般输入所产生的结果。但是,必须保证用于这样测试的 NTCB 分部与评估时的 NTCB 分部完全相同。

敏感标号在保持网络强制访问控制中占有关键地位。对网络安全尤其重要的是部件间通信的信息标号规则——多级设备的显性标号和单级设备的隐性标号。因此,对标号的正确性测试就尤为重要。

5.3.1.3.2.2 设计规格说明与验证

a. 采用 GJB 2646 说明

应在计算机系统的整个生命周期内维持由 TCB 支撑的安全策略的非形式化的或形式化的模型,并证明它与其原理一致。

b. 解释

该模型所表示的整体网络安全策略将提供由 NTCB 施加在网络内主体和存储客体上的强制访问控制策略基础。该策略也将成为由 NTCB 完成的控制已命名用户对已命名客体访问的自主访问控制策略的基础。数据完整性要求表明:未授权的 MSM 影响无须包含在该模型中。整体网络策略必须分解在适当部件上的策略元素中,并用来作为这些部件安全策略模型的基础。

模型的抽象级别、模型中显式表示的主体和客体集都将受 NTCB 分部影响。如果某些网络部件的 NTCB 分部对主体和客体实行访问控制,那么,该主体和客体必须显式地表示在模型中,模型应为结构化的,以保证单个网络部件的原理和实体是明显的。分配给部件的全局网络策略元素应由该部件的模型表示。

c. 基本原理

模型的实现方法在很大程度上依赖于分布系统中通信服务的完整,在紧耦合的分布系统中,该模型非常类似于独立的计算机系统中的模型。

其余情况下,每一分部的模型都将表示在每种部件上 NTCB 分部的规则。它使模型更清晰,而且,尽管不是模型的一部分,也显示了系统设计所隐含的访问限制,例如,代表协议实体的主体只能访问处于协议同一层的包含数据单元的客体。主体和客体在不同协议层上的分配是协议的设计问题,它无须反映在安全策略模型中。

5.3.1.4 文档

5.3.1.4.1 安全特性用户指南

a. 采用 GJB 2646 说明

用户文档的摘要、章条或手册应描述由 TCB 提供的保护机制、保护机制的使用说明及保护机制间的交互过程。

b. 解释

该用户文档描述了用户可见的全局(网络系统)级的、每一部件用户接口上的以及它们之间交互过程中的保护机制。

c. 基本原理

该"解释"是对网络系统和在网络标准中所定义的 NTCB 分部要求的延伸。由单个部件提供的保护机制的文档由适用于单个部件的 GJB 2646 提供。

5.3.1.4.2 可信设备手册

a. 采用 GJB 2646 说明

在计算机系统管理手册中应指出:当安全设备运行时,对有关功能与特权应加以说明,并提出警告。对各类审计事件,应给出提供检查和维护审计文件用的程序以及详细审计记录结构。手册应描述操作员和管理员有关安全功能和用户安全特性的变化。它应提供有关系统保护特性的一致和有效的用法。如它们怎样互相作用,怎样安全地生成一个新的 TCB。手册还应提供设备程序、警告和需要受控的特权,以便安全地操作该设备。

b. 解释

该手册中应包含说明与过程,以协助系统管理员了解系统的配置情况。这些说明与过程包括以下几种情况:

网络本身的硬件配置;

如何向网络中增加新部件;

当某部件阶段性地离开网络(如被破坏或断开连接)后再次上网的情况;

影响网络安全性能的网络配置,例如,手册应向网络系统管理员说明影响网络体系结构的部件间的互连;

加载或修改 NTCB 软件或固件。

应规定物理上的和管理环境上的控制。网络中任一安全性假设均应说明。例如,所有通信链都应有物理级上的保护。

c. 基本原理

多种系统管理员可能有各种各样的责任。这些手册上的技术安全措施必须与其他安全措施结合使用,以保证网络系统的安全性。其他安全措施包括管理安全、物理安全、辐射安全等。

该手册中应增加网络配置标准,因为,部件之间正确的互连对于网络体系结构的实现至关重要。

密码技术是保护通信线路的常用机制。未授权用户不可以读加密信息。通常密文的安全级比较低,如欲使用加密算法,应由国家和军队安全主管部门认可。

加密算法与其实现过程不在本标准讨论范围。加密算法及其实现可能由某个单独设备完成或是某部件的主体功能。本标准不加区别地把任一加密实现包看做是加密机制。

5.3.1.4.3 测试文档

a. 采用 GJB 2646 说明

系统负责人应向评估者提供一份文档，该文档包括测试计划、安全机制测试过程以及安全机制功能测试结果。

b. 解释

测试计划应说明测试的组成，亦应标识出不属于评估系统的测试部件。该计划还应包括这类部件中与测试相关的功能，以及评估系统这类部件的接口。网络测试计划说明应明确表示测试可以完全覆盖网络安全策略。测试应包括在系统体系结构和系统完整性中所描述的特性。测试亦应包括网络体系结构和大小。

c. 基本原理

被评估实体可能是一个网络子系统(参见附录 A(补充件))，应增加其他部件才能构成一个完整网络系统，在这种情况下，该文档应包括一些与上下文有关的定义说明。在评估时，若没有测试网络子系统的说明，就无法验证测试计划的正确性。

5.3.1.4.4 设计文档

a. 采用 GJB 2646 说明

设计文档应提供负责人描述的保护原理及其在 TCB 上的实现，如果 TCB 由不同的模块构成，应描述模块之间的接口。**由 TCB 实施的形式化或非形式化描述的安全策略模型都应是可用的，并且应证明它对实施安全策略是足够的。应当标识特定的 TCB 保护装置，而且给出一种解释表示它们满足该模型。**

b. 解释

在说明 NTCB 如何实现负责人所描述的保护原理时，应说明 NTCB 的分布方式。亦应说明安全策略。NTCB 模块间的接口应包括 NTCB 分部与分部内模块间的接口(若存在模块的话)。负责人应描述安全体系结构与设计，其中包括部件间安全要求的分布情况。附录 A(补充件)说明有关部件的评估。

正如在 B 等级的简介中所述，负责人必须证明 NTCB 使用了参考监视器的概念。安全策略模型必须是针对参考监视器的模型。

完成参考监视器的每一分部的安全策略模型应能充分表示由该分部所支持的访问控制策略，包括针对保密性和(或)完整性的自主和强制安全策略。对于强制性策略，应准确定义包括保密性和(或)完整性部件的敏感标号的单独支配关系。

c. 基本原理

该解释是对在网络系统正文中所定义的网络说明要求的直接延伸。另外还要求在其他如描述部件或描述操作环境的文档中把网络子系统或网络系统描述为功能，例如在可信设备手册中。

为进行评估，网络系统应有相关的网络安全体系结构与设计(和网络安全体系结构与设计无关的部件的互连见附录 C(补充件))。网络安全体系结构必须包括与安全相关的策略、客体和协议。网络安全设计说明了网络中应包含的接口与服务，因此，能够可信地评估该网络。也许有多种设计构成同一个体系结构，但可能会出现不兼容或无法工作的情况(遵循互连规则的除外)。要求在设计中以可见接口方式描述部件间合作和安全相关的机制，不可见接口不在本

标准讨论范畴。

在进行网络或部件评估之前，负责人应提供网络安全体系结构与设计。网络安全体系结构与设计必须充分实现，而某些明显和不明显的缺陷要经过基于该特定结构的可信网络评议会议的同意。

当设计部件或欲评估部件时，当用部件组装网络或欲评估该网络时，均必须首先证明满足网络安全体系结构与设计。也就是说，用遵循网络安全体系结构与设计的每一种方法，能将多个部件构成网络，使之达到评估说明规定的可信网络要求。

为了由部件组成的可信网络能独立构造，网络安全体系结构与设计应完整而无二义性地定义部件的安全功能与部件间的接口。应该评估网络安全体系结构与设计，以保证遵循它的说明而建立的网络是可信的，也就是说该网络可由本标准来评估。

“模型”一词在网络中有许多不同的含义，如“协议参考模型”、“正式网络模型”等等。只有“安全策略模型”一词为本要求所用，而且特指接口模型（如参考监视器的“安全参数”），它必须完成所有 GJB 2646 定义的要求。并必须显示出 TCB 的所有部分都是安全协议模型的合法解释，即除非在模型中已有表示，安全状态不会改变。

5.3.2 B2 级：结构化保护

B2 级网络系统中的 NTCB 应基于清晰定义和用文档表示的形式化安全策略模型，该模型要求在 B1 级网络中所有的自主和强制性访问控制延伸至网络中的所有主体和客体。另外，还应具备隐蔽信道。必须精心地构造 NTCB，使之成为严格被保护的单元和不严格被保护的单元两部分。应良好定义 NTCB 接口，而且其设计与实现可使它经受更完备的测试与更完整的浏览。在 B2 级，加强了鉴别机制，以系统管理员和操作员功能的支持形式提供了可信设备管理，提出了加强严格的配置管理控制。系统对于入侵有一定的抵抗力。以下是 B2 级的最低要求。

5.3.2.1 安全策略

a. 采用 GJB 2646 说明。

b. 解释

网络负责人应清晰描述 NTCB 所完成的整体网络安全策略。该策略应至少包括本级适用的自主和强制访问控制要求。它要求数据保密性或数据完整性或两者兼备。该策略是由自主性和强制性两部分组成的访问控制策略。该策略应包括通过对用户或用户组的鉴别来保护所处理的信息的自主安全策略。该访问控制策略应清晰描述网络的下述要求：防止并检测由未授权的用户或错误引起的对敏感信息的“读取或破坏”。强制性策略必须定义它所支持的敏感标号集。对于 B1 级或更高级，强制性策略应基于敏感标号（该敏感标号反映了按保密性和（或）完整性规定信息的安全级）和用户标号（该标号用于鉴别用户，以允许其访问某类信息）。未授权的用户包括：无权使用网络的所有用户；网络的合法使用者，但无权访问被保护信息的特定部分。

注意：“用户”并不包括“网络操作员”、“系统程序员”、“系统维护员”、“系统安全员”以及其他技术人员。这些人员与一般用户有所区别并遵循可信设备手册和系统体系结构要求。这些人员可以修改网络中的系统参数，例如重新定义组成员。他们也可以具有独立的用户职责。

保密性策略：网络负责人应清晰定义阻止未授权用户访问系统中敏感信息的自主和强制保密性策略。

数据完整性策略：网络负责人应清晰定义阻止未授权用户修改(即写入)敏感信息的自主和强制完整性策略。由网络负责人所定义的数据完整性是：在网络中信息不应受到未授权的修改。一般情况下，由 NTCB 实施的强制完整性策略不能防止信息在部件间传输中被修改。然而，完整性敏感标号可以使信息在传输过程中由于受到保护而不会发生传输错误。这种要求有别于标号完整性要求。

c. 基本原理

“负责人”一词可指“出售商”、“网络集成商”、“制造商”、“开发商”中的某一位。有多种含义的原因是因为在评估网络系统时，某些人可能不是相关人员。

可信网络应控制对共享敏感信息的读与写。控制写操作就可以保护信息免受破坏，一般情况下，网络既要保持信息的保密性也要保护完整性。但是，通常是完整性要比保密性更重要。因此，不论网络被评估为哪个等级，网络都应具备保密性和(或)完整性策略。这些策略的保证程度由网络的评估级别反映。

对修改操作的控制可以保证信息可靠，而且，一旦信息被破坏，仍然可以控制由于该破坏而引起的潜在危险。网络完整性策略既要保护在部件上正被处理的数据，也要保护正在网络中传送的数据。由 NTCB 所完成的访问控制策略与每个部件内主体对客体的访问相关。传递信息的通信完整性在“其余安全服务”中讨论。

在某些体系结构中的强制完整性策略(B1 级或更高级)可以用来支持面向连接的抽象或网络中部件之间的连接。例如，在端对端加密过程中的密钥配发中心，就可以指定一类特定的完整性范畴，以防止密钥产生的代码数据受到该部件上其他支持过程(如操作员接口和审计)的修改。

某些体系结构中的强制完整性策略，可以定义一个数据完整性敏感标号，它反映了为确保信息既未受到超过指定限度的随机错误的破坏，也未受到未授权 MSM 的特定要求。与完整性敏感标号相关的特定矩阵一般反映了网络中的指定应用。

5.3.2.1.1 自主访问控制

a. 采用 GJB 2646 说明

TCB 应定义并控制计算机系统中已命名用户和已命名客体(文件或程序)之间的访问操作。执行机制(例如自身/组/公共控制，访问控制表)应允许用户通过自身/组/二者来指定并控制对客体的共享。执行机制还应控制访问权限的传播。自主访问控制机制应可以通过显性的用户行为或默认方式防止客体受到未授权的访问。这种访问控制应包括或排除单用户粒度的访问操作。只有授权用户才可以允许未得到访问许可的用户访问客体。

b. 解释

自主访问控制(DAC)机制应以各种方式分布于 NTCB 分部中。网络系统中的指定部件可以完成全部或一部分或不完成 DAC 的功能。尤其是仅仅支持内部主体(不做用户直接代理的主体)的部件，例如公共网络中的包交换，就可以不直接完成 DAC 的机制(例如它们可能不包含访问控制表)。

在网络环境中，有多种方法鉴别用户身份。例如在网络安全策略允许的情况下，可用不同部件(如主机，网关)的网络标识符(如互连地址)做为用户组标识符(如主机 A 的所有用户，网络 Q 的所有用户)，这样就不必鉴别每个用户的身份。例如，主机 A 可以使用一个特定的组标识符，并保持一个显性用户组列表，于是，主机 A 可利用该表与主机 B 进行通信。

对网络来讲，单个主机会对它的用户在已命名个体的基础上施加自主的控制——这一点和没有网络连接时所使用的控制相类似(事实上，也可能完全相同)。

当可以使用组标识符执行访问控制操作时，可能会要求其他主机的标识符，以此来避免进行远程用户的身份鉴别。C2 级或 C2 以上级的网络必须保证：当使用组标识符时，应利用审计记录来确切地标识(立即或以后)该组标识符所代表的单个用户。在组成员的改变以及相应的实现访问控制时刻的不同步过程中，可以允许稍有偏差。

NTCB 分部的 DAC 机制可以在参考监视器的接口中完成或分布在某主体上(该主体是相同或不同部件中 NTCB 的一部分)。参考监视器管理系统中所有的物理资源并创建它所控制的主客体的抽象。这些主客体中的一部分可以完成 NTCB 的某一部分功能。当某 DAC 资源分布于 NTCB 主体(可能在参考监视器外)时，DAC 的设计与实现机制的保证要求应符合 C2 级或 C2 以上级网络的要求。

若网络自主安全策略包含完整性，以上说明尤其适用于控制已被鉴别的用户或用户组在每个部件上进行的修改操作，也就是写访问。

c. 基本原理

在这一级，支持整体 DAC 机制的元素需要隔离支持 DAC 的信息(即客体)以便于审计(参见“系统体系结构”)。可利用 X.25 中同一协议的方法，例如网络协议第三层 X.25 中的同一方法，使用该网络标识符标识用户组或用户自身。支持整体 DAC 机制的元素被视为不可信的主体。

典型的 DAC 情况是在某主机上为远程用户创建一个代理进程，该代理进程可在主机 NTCB 分部的控制下访问客体。本标准要求 NTCB 为每一个这样的进程指定并保留一个用户标识符，于是代理进程就可以受到与本地用户一样的自主访问控制。然而，本标准可以允许在一定范围内指定用户标识符。

最明显的情况是：如果每一个主机都可以使用网络用户的全局数据库(例如命名服务器)，那么所有用户标识符都是全局有效的。

某些 NTCB 分部可以为局部注册的用户保持一个局部使用的数据库。在这种情况下，或者禁止为局部未注册的用户创建代理进程，或者允许为预选的用户或用户组创建代理进程。这些进程可标识运行在某远程主机上的用户组。本标准中的审计一词表明了最小的可审计度。审计要求 NTCB 分部的审计设施判定当某代理进程产生时，到底是谁在远程用户的主机上注册运行。

标识与鉴别机制负责建立用户标识符与代理进程的联系。这就意味着代理进程的用户标识符对 DAC 是局部适用的，数据通过网络回到用户主机的传输过程以及在用户主机上为数据做备份不是 DAC 的工作。

只支持内部主体的部件将要影响到 DAC 的实现，这是由于要完成 DAC 判定的部件需要

得到一个提供服务的信息(如用户标识符),关于这种情况的一个例子是主机 A 上的某个用户试图访问主机 B 上的某个文件。通常是由主机 A 向主机 B 传送一个用户标识符,而在主机 B 上完成 DAC 判定。

有若干种机制可以做到唯一用户标识过程。其中包括:

第一,要求在执行访问操作的主机上提供唯一标识和鉴别过程;

第二,确认由另一主机鉴别的有效网络地址,并将其发送至执行访问操作的主机;

第三,对支持网络全局的用户唯一标识符进行管理,该标识符可能是如在第二中所述的由另一主机鉴别和发送来的,或由一个指定的网络标识和鉴别服务器鉴别和发送来的。

完成第二和第三的协议应遵循系统体系结构要求。

除上述典型方式外,DAC 的网络支持还有其他方式,通常建议集中式访问控制方式。访问控制中心完成 DAC 的所有判定,或控制主机对主机的连接,来减少各主机的负担,这样可使一个主机只需要控制有限个远程主机上的用户对客体的访问。在这种情况下,访问控制中心提供面向抽象连接和 DAC 整体网络安全策略之间的连接。在上述所有情况下,应由客体所在的主机实现该判定。

有两种分布实现 DAC 的机制,一种是在不同的部件上分布实现,另一种在某个部件中的 NTCB 分部的主体上支持 DAC。由于"计算机系统"表示为整体"计算机网络",每个部件都有责任完成分配给它的安全机制以保证网络安全策略的实现。对于传统的主机系统,DAC 机制可以与参考监视器中的 MAC 一起,使用如虚拟机器监控器等几种方法,在接口外支持 DAC。

与全局固定的强制性策略不同,DAC 是非常网络和系统专用化的,它的特性反映了系统的自然用途。常见情况是,单独主机以命名个体方式控制本地用户,这就像没有网络一样。然而,在大型网络中,集中地管理所有用户显然是很困难的。因此,其余主机的用户通常都被分组,以便于网络 DAC 策略的控制要求实际上是以这些主机或其他部件的标识为基础。网关是此类部件的一个例子。

保证要求是可信系统的关键所在。它可以决定某个系统或网络是否适合于指定的环境。在单个系统中,DAC 是合成在参考监视器中的,而与其他部分很难区分清楚。在网络系统中,由于 DAC 的分布实现,区分就比较容易。如果主要的网络部件可以较简便地设计实现,而又不会降低安全策略的要求,那么可信网络也就容易实现。

5.3.2.1.2 客体重用

a. 采用 GJB 2646 说明

在向一个主体初始转让、分配或重分配 TCB 未使用的存储器客体池之前,应删除所有包含在存储器客体内的信息授权。对已释放回系统的客体有访问权的任何主体,都不能再使用由原主体产生的任何信息,包括已加密的信息。

b. 解释

NTCB 应保证它所控制的任一存储客体(如某部件上 NTCB 分部控制下的消息缓冲区)不包含该部件主体内未获授权的信息。这种要求应由每个 NTCB 分部完成。

c. 基本原理

在网络系统中,人们对 NTCB 直接控制下的存储客体感兴趣,如部件上的消息缓冲区。

网络系统里的每个部件都应满足客体重用要求。例如 DAC 要求消息缓冲区处于 NTCB 分部的控制下。分配给某内部主体的缓冲区可以被某个保证消息流完整性的主体所重用。这种可控的客体可以在物理资源如缓冲区、磁盘扇区、磁带和主存上实现或在某部件如网络开关上实现。

5.3.2.1.3 标号

a. 采用 GJB 2646 说明

TCB 应保存 TCB 外部主体所直接或间接访问的与每一个计算机系统资源(如主体、存储客体、ROM)有关的敏感标号。强制访问控制判断应以这些标号为基础。为输入无标号的数据，TCB 应提出请求，并从授权用户那里接收该数据的安全等级，而且 TCB 将对所有这些活动进行审计。

b. 解释

在 NTCB 分部控制下输入的无标号数据将由输入它的单级设备的**设备标号**强行指定一个标号。标号应包括由网络负责人所描述的与网络安全策略完全一致的保密性与完整性两部分。本说明中所有的“标号”一词都包括上述两部分。同样，“单级”和“多级”两词都以该策略的保密性和完整性为基础。强制完整性策略应特别具有下述要求，如未被判定的消息流修改的可能性应在被保护数据的标号中有所反映。例如，当输入数据时，能够以密码机制为基础赋给它一个完整性标号，来保证达到该策略的要求。NTCB 应保证这种机制受到保护，而且能基于一个标号调用它。

如果安全策略包括完整性策略，所有在传输过程中可能引起 MSM 的活动，都将视为对数据完整性有破坏的、未授权的访问。NTCB 应自动测试、发现、报告这类超出网络完整性策略要求的错误或破坏。应标识 MSM 抗干扰措施。应选择强有力的技术以抵抗 MSM。若使用了加密方法，它应被国家和军队安全主管部门批准。

必须给网络中每一部件内的所有客体分配标号，以便用它们可信地维持多级信息的分离，而与单级部件有关的任何客体的标号应该与该部件的标号相同。必须给用来存储网络控制信息的客体及其它网络结构(如路径表)分配标号，为的是防止未授权的访问和(或)修改。

c. 基本原理

该“解释”是对网络系统要求和在网络说明中所定义的 NTCB 分部的延伸。单级设备可以看作是主体或者也可以看作是客体。多级设备可以看作是有一定保密范围的可信主体，即该主体的保密范围位于期望在该设备上传输数据的最小至最大范围之间。

针对保密性或完整性或二者的敏感标号，可以反映未划分的等级或划分的等级或二者。

本要求适合于所有 B2 级或更高级别的网络。

如果网络存在完整性策略，由 NTCB 负责完成，NTCB 必须实施确保将信息准确地从源传送到目的地(不考虑中间连接点的个数)的策略。NTCB 必须能防御设备故障、环境遭破坏、人和进程未授权修改数据的动作。完成代码或格式转换的协议应保护数据和控制信息的完整性。

可以规定尚未发现的传输错误的概率作为网络安全策略的一部分，因此，可以确定网络能满足预定应用的程度。当在部件中处理数据时，能在与该数据相关的完整性敏感标号内反映

出由该数据要满足的特定度量值(例如,未被发现的修改概率)。要区分不同的应用和操作环境有不同的完整性要求。

网络应具有自动测试、发现和报告超过操作模式要求阈值错误的能力。完整性抗干扰的有效性必须与其他安全相关特性(如保密性)同样精确。

经常使用密码术作为数据完整性保证的基础,也可以使用操纵检测码(MDC)机制。加密或 MDC 算法的充分性、协议逻辑的正确性以及实现的充分性必须在 MSM 抗干扰设计中被证实。

5.3.2.1.3.1 标号完整性

a. 采用 GJB 2646 说明

敏感标号应准确表示特定主体或客体的安全级,该主体和客体由此而相联系。当 TCB 输出时,敏感标号应准确而无二义性地表示内部标号,并与正在输出的信息相联系。

b. 解释

"TCB 输出"是指信息从一个部件上的客体到另一部件上的客体的传送过程。在 NTCB 分部间的传送的信息在"系统完整性"中讨论。内部与外部敏感标号的形式可能不同,但其意义相同。另外,NTCB 还应保证敏感标号与网络中正在传输的信息之间的正确关系。

正如在"可信设备手册"中所述,未授权用户不可读加密信息。一般来讲,密文的安全级低于明文的。明文与密文包含在不同的客体中,各有自己的标号。明文的标号应加以保护,并与密文相关,当密文解为明文时,它可以被恢复。如果明文与单级设备相关联,其标号可以是隐含的。标号也可以隐含于密钥中。

当信息被输出到某个环境,在那里它可能受到有意或无意的修改时,TCB 应支持如密码检验和的方法,以保证标号的准确性。当具备强制完整性策略时,该策略应定义完整性标号的含义。

c. 基本原理

加密算法与其实现过程不在本标准讨论范围。加密算法及其实现可以由一个单独设备完成或是某部件的主体功能。本标准不加区别地把任意一个实现包看做是加密机制。加密算法应得到国家和军队安全主管部门批准。加密过程是某部件上 NTCB 分部的一部分。

加密机制不一定是多级设备或多级主体。由定义可知,加密过程是多级的。明文与密文接口带有不同安全级的信息。加密机制不会因在数据上执行逻辑或数学的操作而产生新的数据。加密机制中的明文或密文接口应分别标识为单级或多级。若接口是单级的,数据的安全级为可信单体,并与接口隐性相关联,"单级设备输出准则"适合于此处。

若接口是多级的,则数据必须加以标号,"多级设备输出准则"适合此处。网络体系结构可任意挑选可用的机制,将客体与标号相联系。可能发生的有关加密客体的例子如下:

在客体的协议定义中,包含标号域;

通过密钥将标号与客体隐式相联系,也就是说,密钥唯一标识安全级,在数据的加密级上,必须保护单独或私用的密钥。

5.3.2.1.3.2 有标号信息的输出

a. 采用 GJB 2646 说明

TCB 应对每个通信信道和 I/O 设备标明单级或多级。这个标志的任何变化都应由人工实现，并可由 TCB 审计。TCB 应维护并且审计任何与通信信道或 I/O 设备有关的安全等级或标号的变化。

b. 解释

应指定每个通信信道和网络部件为单级或多级。该指定的任何改动需经由负责受影响部件的管理员或安全员批准，或由 NTCB 的管理员或安全员批准。这种改变可被网络审计。

NTCB 应维护并能审计与单级通信信道相关联的设备标号或者与多级通信信道或部件相关联的范围的任何改变。NTCB 还应能审计与在多级通信信道或部件上传送的信息相关联的安全级集合的任何变化。

c. 基本原理

网络中的通信信道或部件与独立系统中的通信信道或 I/O 设备相似。必须把它们指定为多级(可以区分不同安全级的信息)或单级。在 GJB 2646 中，单级设备只可以连接在单级信道上。

若要改变向部件或通信信道发送信息的级或级的集合，应得到网络或部件安全员的认可与批准(若没有安全员，系统管理员也可以)。这一要求可以保证未经有关人员的批准，不会发生与安全相关的改动。

5.3.2.1.3.2.1 向多级设备的输出

a. 采用 GJB 2646 说明

当 TCB 将一个客体输出到一个多级 I/O 设备时，与该客体有关的敏感标号也应相应输出。并以输出信息相同的形式(如机器可读或人可读形式)驻留在同一物理介质上。当 TCB 在多级通信信道上输出或输入一个客体时，该信道使用的协议可以无二义性地把敏感标号和被发送或被接收的有关信息联系起来。

b. 解释

网络中的部件，包括主机，应通过多级通信信道或多个单级通信信道良好地互连，以保护多安全级的信息。联系安全级与输出信息的协议，应提供唯一所需要的信息，将安全级与单个部件上 NTCB 分部之间通信信道上传送的信息联系起来。这种协议的定义必须指定敏感标号的表示和语义(如机器可读的标号必须唯一表示安全级)。

安全级与通信信息之间“无二义”的联系应达到 NTCB 内其余任何标号的精确度(在“标号完整性”中已讨论)。这种机制可由受保护且高度可靠的直接物理层连接完成，或由传统的可以有效发现传输过程中错误的密码链保护完成，或者也可以使用分离的信道完成。**输入或输出的信息域必须与有关的设备标号相关联。**

c. 基本原理

协议必须定义敏感标号的表示与语义(见附录 B(补充件)中的“强制访问控制策略”)。多级设备与(不可信)主体的接口，或由参考监视器完成，或由一个多级主体完成(例如，在 Bell-LaPadula 模型定义的“受委托主体”)，该主体提供一个以 NTCB 分部的内部标号为基础的标号。

当今的技术水平限制了安全网络中强制策略的支撑能力。控制网络中每一个主体操作的

参考监视器应完全由单个 NTCB 分部提供，该 NTCB 分部还应提供其主体的 NTCB 接口。这就意味着在安全策略模型（该主体能通过传输调用更改该模型）中表示的“安全状态”必须包含在同一个部件中。

对于驻留某个 NTCB 分部的部件之外的事件（例如到达一个消息）可以影响该 NTCB 分部的安全状态。这种影响可在另外的部件或分部上的事件初始化后异步地产生。例如，不确定的延迟可能发生在以下三种情况中，即一个部件初始化某消息、消息到达另一个部件的 NTCB 分部和第二个部件上安全状态改变。由于网络各部件是并行工作的，所以需要网络的全局控制（如网络全局时钟）以实现安全状态的同步转换。一般来说，这种设计既不实用也不被接受。因此，NTCB 分部之间的交互仅限于一对（至少是逻辑上的）设备之间的通信，如果设备可接/发多级信息的话，应为多级设备。对于广播型信道而言，通信对是发送者与预定接收者。然而，如果广播信道带多级信息，还需要另外的机制（如 TCB 保持的加密检验和）来实现分离与发送。

当两个位于不同部件上的多级设备进行互连时，在信道上使用的协议中需要有一个通用表示的敏感标号，使得发送者与接收者都能理解。在整个网络策略中每一安全级都必须在那些标号中唯一表示出来。

在某个单独的 TCB 中，敏感标号的精确度一般是由很简单的技术（如很短的物理连接）来保证的，也可以使用单独印制电路板或通过内部总线来达到。在许多网络环境中，很可能发生偶然的错误或蓄意引入的错误，此时更需要良好的保护措施。

5.3.2.1.3.2.2 向单级设备输出

a. 采用 GJB 2646 说明

单级 I/O 设备和单级通信信道不需要维护其处理信息的敏感标号。然而，TCB 应包含一种机制，用这种机制 TCB 和一个受权用户进行可靠的通信，该通信信息具有指定的单安全级，且通过单级信道或 I/O 设备完成输入或输出。

b. 解释

如果两个直接相连的部件之一或全部都不能可信地将不同的安全级信息分离，或者这两个部件有一个共同的单安全级，那么，这两个部件应通过单级信道通信。单级部件或单级通信信道并不需要保持其处理信息的敏感标号，因此 NTCB 应包含一个可靠机制，使得 NTCB 与一个授权用户或 NTCB 分部内的主体可利用该机制指定信息的安全级，该信息由单级信道或网络部件输入或输出。

c. 基本原理

网络中的单级通信信道和单级部件与独立系统的单级信道和 I/O 设备类似，它们都不能可信地分离不同安全级的信息，因此，在这类信道与部件上传送的与数据相关联的标号是隐含的；这是因为信道或部件而不是位流的显性部分使得 NTCB 将数据与标号连系起来。注意，加密信息的安全级是密文的级而非明文的原有级。

5.3.2.1.3.2.3 人可读的输出标号

a. 采用 GJB 2646 说明

计算机系统管理员应规定与输出敏感标号相关联的可打印的标号名。TCB 应对所有人

员可读的输出、编页的输出以及带有可识别敏感标号的硬拷贝输出(如行打印机输出)的开始和结束做出标记,以便正确表示该输出的敏感性。TCB 应按默认值对所有人可读的输出、编页的输出以及带有可识别敏感标号的硬拷贝输出(如行打印机输出)的每页的顶部和底部做标记、以便正确表示该页信息的敏感性。TCB 应该按默认值,并以适当方法标记具有人可读敏感标号的其他形式的人可读的输出(如映象、图形),以便正确表示该输出的敏感性。这些标记默认值的任何滥用都应由 TCB 审计。

b. 解释

本标准对于产生人不可读输出的部件不加要求。对于产生人可读输出的部件,在网络中定义的每一个安全级在所有的部件中都应有统一的含义。网络管理员与其任何相关的部件管理员,都可指定与已定义安全级相关联的人可读标号。

c. 基本原理

该"解释"是对网络系统和在网络说明中所定义的 NTCB 分部要求的直接延伸。

5.3.2.1.3.3 主体敏感标号

a. 采用 GJB 2646 说明

在交互对话期间,与终端用户相关联的安全级的每个变化,TCB 都应立即通知该用户,当终端用户想要显示该主体完整的敏感标号时,他应能向 TCB 进行询问。

b. 解释

任何与某终端用户相关联的安全级的改动,NTCB 分部应立即通知属于该部件的终端用户。

c. 基本原理

该局部 NTCB 分部必须保证那个用户理解从终端发出或发到终端的信息的安全级。当某用户在另一部件上有代理进程时,为保持和该用户的通信,可能要调整它的级,可以异步产生这种变化。这种调整对适合于通信线路上的客体强制访问控制是必要的。

5.3.2.1.3.4 设备标号

a. 采用 GJB 2649 说明

对各种附加的物理设备,TCB 应支持最小和最大的安全级的分配,并利用这些安全级满足安放该设备的物理环境所强加的约束条件。

b. 解释

这种要求适合于针对每一个 NTCB 分部的写操作,以使得基于安全级的独立信息是可信的。在部件内每一个用于与其他网络部件通信的 I/O 设备,都应分配一个包括最大及最小标号集合的设备区域。设备区域通常包括(不是必须包括)最大和最小标号之间的所有可能标号。

NTCB 总是为通过设备输出的信息提供一个精确的标号,利用单级设备输入或输出的信息,其标号隐含于设备的安全级中。多级设备上的信息输入或输出时,必须通过统一认可的协议加以标号,如果使用总是负载单级的通信线路,可隐含标号。

若将给定安全级的信息输出至某个输入设备时,该输入设备区域必须包含这个标号给定的级或具有更高的级。若输入设备不包含这个标号给定的级,输出信息将重新加以标号至更

高级，以符合该输入设备区域。其余情况不会重新标号。

c. 基本原理

设备标号的目的是反映并约束设备所处的物理环境中已授权信息的安全级。

从一个设备到另一个设备反复传送的信息可以使用单工通信(即无应答)，当两个设备区域没有公共的级时，只须要求发送设备区域中每一级都低于接收设备区域的一些级。而绝不允许将具有给定级的信息发送到其设备区域不包含高于该级的设备。(参看附录 C 中有关 AIS 观点的类似的互连规则)。

5.3.2.1.4 强制访问控制

a. 采用 GJB 2646 说明

TCB 应对由 TCB 外部主体直接或间接访问的所有的资源(如主体、存储客体和 I/O 设备)执行强制性访问控制策略。应给这些主体和客体指定敏感标号，这些标号是划分等级的和未划等级的结合，而且应作为强制性访问控制判断的基础。对于所有 TCB 外部的主体以及由这些主体直接或间接存储的所有客体应掌握下列要求：仅当主体安全级中划分的等级大于等于客体安全级中划分的等级，而且主体安全级中未划分的等级包括了客体安全级中全部未划分的等级时，主体才能读一个客体；仅当主体安全级中划分的等级小于等于客体安全级中划分的等级，而且主体安全级中未划分的等级被包含在客体安全级中未划分的等级时，主体才能写一个客体。TCB 应该用标识和鉴别数据来鉴别一个用户的标识，并保证 TCB 可以创建它以外主体的安全级及授权，从而使得批准和授权的那个用户去支配该用户。

b. 解释

每一 NTCB 分部，都对它所控制下的部件上的所有主体、客体执行强制访问控制策略。在网络中，NTCB 分部的责任包括 TCB 在单个系统部件上施加的所有强制性访问控制。与其他部件进行通信用的主体和客体，更处于 NTCB 分部的控制下。强制访问控制包括保密性与完整性控制，这一点，网络负责人已在整体网络安全策略中有所描述。

两部件间与通信相关的概念化的实体，如扇区、连接和虚电路，可视为有两个端点，每一端存在于一个部件上，而每个端点可视为局域客体。通信过程可视为从一端的客体上把信息拷贝到另一端的客体上。透明的携带数据的实体，如数据报和包，既可视为存储在其他客体上的信息，也可视为分别处在通信路径两端的携带数据的实体。

可通过保密性或完整性级别来达到“两个或两个以上”安全级的要求。在强制完整性策略中，读与写的要求通常为当且仅当某主体的安全级可控制另一主体的安全级时，该主体可读另一主体；当且仅当客体的安全级可控制主体的安全级时，主体可写客体。以完整性策略为基础，网络负责人应定义对所有标号的控制关系，例如，通过将保密性和完整性的点阵结合起来去定义这个关系。

c. 基本原理

NTCB 分部只可以对它部件上的主体和客体保持访问控制。某部件上的一个主体如欲访问另一部件上客体的信息，就要在该远程部件上创建一个主体，以此作为第一个主体的代理。

强制访问控制必须在每一个 NTCB 分部的参考监视器接口上实施(即控制物理处理资源的机制)。这种机制为它所控制的主体和客体创建抽象。可以指定参考监视器外的一些主体

去完成部分 NTCB 分部的强制策略，如使用在 Bell-LaPadula 模型中定义的“可信主体”。

对于在 I/O 设备上传输的标号信息的更高要求，保证了连接于通信路径上客体敏感标号之间的一致性。网络体系结构必须能识别整体强制性网络安全策略与面向抽象之间的联系。例如，单独携带数据的实体（如数据报）可以有单独的敏感标号，并以这些标号接受每个部件上的强制访问控制。单级连接的抽象是由某体系结构隐含完成的，而连接是由单级主体实现的，该单级主体只能使用同级的数据报。

基本的可信系统技术允许 DAC 机制分布实现，这一点与强制访问控制要求相反。对于网络而言，MAC 与 DAC 机制的分离是规则而非意外情况。

用来代表强制性访问控制（包括数据保密性和完整性）策略中所有安全级的总体敏感标号集总是形成部分有序集。不失一般性，该有序集总可以延伸成一个包括所有未划分等级总和的点阵。对于任一点阵，全体敏感标号就定义了一个控制关系。为便于管理，最好有一个可控制其余标号的最大级。

5.3.2.2 责任

5.3.2.2.1 标识与鉴别

a. 采用 GJB 2646 说明

TCB 要求用户在开始操作前对其自身进行用户标识。因此，TCB 应维持鉴别数据，该数据包括验证单个用户身份的信息（如口令），用于确定批准和授权单个用户的信息。TCB 用这种数据来鉴别用户身份及保证 TCB 外部的可代表单个用户建立动作的主体的安全级和授权能力，并由已批准和授权的用户支配它。TCB 应保护鉴别数据以防止被未授权的用户读取。TCB 应该能够很好地识别计算机系统内的每一个用户，以此实现个体责任。TCB 还应该提供把这种标识与该单个用户发生的所有可审计动作相联系的能力。

b. 解释

用户标识与鉴别要求和网络系统对计算机系统的要求一致。标识与鉴别工作可以由用户直接连接的部件负责，也可以由其他的部件（如标识鉴别服务器）负责。当 NTCB 欲以用户或用户组名义作主机或其他网络部件的媒体时，NTCB 将使用主机的标识和鉴别功能而不用单用户的标识鉴别功能。在进行鉴别时，部件标识功能应隐含与标识功能有直接联系的特定的用户组。这一要求并不适合于内部主体。

如果 NTCB 能保证信息避免受到未授权的破坏，那么，当从一个部件到另一个部件时，可以无须再次进行信息鉴别，包括已鉴别的用户身份。这种保护至少应达到与鉴别机制和鉴别数据的保护相同的保证级别。

c. 基本原理

在网络系统中，责任要求没有改变。把 NTCB 分布于若干部件之上，既不增加也不减少要求。即依旧存在单一责任。同样，在 C2 级或更高级的网络系统中，“单一责任”可由主机或其他部件中的标识功能完成，只要能追踪单个用户或满足活动主体的特定单用户要求即可。在追踪过程中允许有偏差，因为组成员可能有变化，而且，完成访问控制也需要时间。另外，在网络这样的分布式系统中，当用户通过主体与远程主体操作时，无须在每一个节点上再次鉴别用户。

自主访问控制(DAC)由部件标识符和(或)鉴别信息的传递实现。这种支持机制使得DAC允许用户访问不同NTCB分部上的存储客体而不只是用户鉴别的客体。使用前向的标识机制指明了通信路径上源和部件的依赖性。

如果用已授权的标识作为确定某主体敏感标号的基础,它必须满足"标号完整性准则"。

一个已授权的标识可在部件间前向传递,并被某些部件用来标识与主体相关联的安全级,该主体是已标识用户的代理所创建的。

5.3.2.2.1.1 可信路径

a. 采用GJB 2646说明

TCB应在自身与负责初始注册和已鉴别的用户之间提供一个可信通信路径。每次只能有一个用户互斥地通过该路径进行通信。

b. 解释

可信路径由用户(例如人)及该用户直接相连的部件上的NTCB分部所支持。

c. 基本原理

当用户在某远程部件上注册进入时,用户标识符可以安全地在本地与远程NTCB分部间传递,以满足标识和鉴别的要求。

当发生与安全相关的活动时,可信路径是保证用户只与NTCB进行通信的必要措施。不过,可信路径并不提供在NTCB内的通信,而只提供用户与NTCB间的通信。因此,如果某部件不支持与用户的直接通信,则该部件就无须包含保证NTCB与用户直接通信的机制。

NTCB分部之间的可信通信的要求将在"系统体系结构"中详述。这种要求有别于用户到NTCB的可信路径通信要求。然而,一个NTCB分部与另一个NTCB分部之间的可信通信有利于实现用户与远程NTCB分部之间的可信通信。

5.3.2.2.2 审计

a. 采用GJB 2646说明

TCB应能建立、维护和保护对它所保护的客体访问的审计跟踪,防止修改、未授权访问或破坏。审计数据应受TCB保护,因此对审计数据已获授权的那些人能对它进行读访问。TCB应能记录下述类型的事件:标识和鉴别机制的使用、把客体引入到一个用户的地址空间(如打开文件、启动程序)、删除客体、计算机操作员和系统管理员和(或)系统安全员的动作、以及其他有关的安全事件。TCB还应能审计人可读的输出标号的任何滥用。对每个已记录的事件来说,审计记录应标出:事件的日期和时间、用户、事件的类型、事件的成功或失败。对于标识和鉴别事件,请求的起点(如终端ID)应包括在审计记录中。对于把客体引入用户地址空间的事件和删除客体事件,审计记录应包括客体名和客体的安全级。计算机系统管理员应能以个体标识和(或)客体的安全级为基础有选择地审计任意一个或更多个用户的活动。**TCB应能审计利用隐蔽存储信道的已标识事件。**

b. 解释

负责人必须能分辨出哪些事件是可审计的。如果NTCB本身(如"其余安全服务"中所标识的那些)无法分辨此类事件,审计机制应提供一个接口,授权主体可利用该接口中的参数来产生审计记录。这样的审计记录要与NTCB的审计记录有所区别。在网络系统中,"其余安

全相关事件”(与网络体系结构和安全策略有关)可能有以下几种：

标识每一个访问事件(如在网络的两个主机之间建立或不建立连接)及其参数(如访问过程中两个主机的标识符)；

利用本地时间或全局同步时间来标识每一个访问过程的起止时间；

在两个主机交互过程中，标识与安全相关的意外情况(如破坏数据完整性事件)；

使用密码术；

改变网络配置(如某部件加入或离开网络)。

另外，如果必要，审计追踪记录中应包含标识信息，以允许所有相关的审计记录(如不同主机上的审计记录)可相关。而且，网络中的某部件可能具有所要求的审计功能(如存入、取出、减少、分析)，而其他部件则可能不存储审计数据，但却可以将审计数据传送到指定的收集部件。由于资源的不可得性，应控制审计数据的丢失。

在网络系统中，由于引入和删除客体事件而使其“用户地址空间”被扩展，包括远程用户(或主机)的代理正在使用的那些地址空间。尽管如此，其重点仍在用户而不是DAC准则中讨论过的内部主体。另外，审计信息必须以机器可读的形式存储。

TCB应能审计利用隐蔽存储信道的已标识事件。为实现该功能，每个NTCB分部必须审计由网络带来的、在本地发生的、可能导致使用隐蔽存储信道的事件。

c. 基本原理

对远程用户来讲，可利用网络标识符(如互连地址)来表示单个用户或用户组标识符(如主机A的所有用户)，以避免当远程用户需要使用标识时应进行的维护过程。在这一级，它必须能标识出(立即或以后)一个组标识符表示哪些单个用户。在其它各方面，该说明是网络系统准则的直接延伸。

5.3.2.3 保证

5.3.2.3.1 操作保证

5.3.2.3.1.1 系统体系结构

a. 采用GJB 2646说明

TCB应保持自身运行域，以避免受到外部干扰或窜改(如修改其代码或数据结构)。TCB应在其控制下，通过提供不同的地址空间来隔离进程。TCB内部应由定义恰当的基本独立的模块构成。它应有效地使用可获得的硬件，把严格保护的单元与不严格保护的单元分离。TCB模块应按可执行最小特权的原则设计。应利用硬件中分段的特点支持逻辑上截然不同的存储器客体，这些客体具有分散的属性(如可读、可写)。应完整地定义用户与TCB的接口，并标识所有TCB单元。

b. 解释

所有的NTCB分部均必须满足系统体系结构准则。只有当所有NTCB分部均保持自身运行域时，NTCB才可能保持自身运行域。由于每一个部件在整个网络系统中都是独立的区域，因此在特定情况下，若部件上只有一个主体，就可以通过不同的地址空间来达到隔离进程的要求。

NTCB内部应由恰当定义的独立模块构成，并符合硬件要求。因此要求每一NTCB分部

都如此构成，使 NTCB 能控制所有的网络资源。NTCB 所控制的网络资源子集是 NTCB 各分部所控制的资源子集之和。必须保护属于 NTCB 的代码与数据结构和在 NTCB 主体(即在 NTCB 内部，参考监视器外部的主体)中传送的属于不同的 NTCB 分部的代码与数据，以防止其受到外部干扰和窜改。可用密码检验和或物理手段来保护 NTCB 分部间交换的用户鉴别数据。

每一个 NTCB 分部都必须实施部件内的最小特权法则，而且，NTCB 必须是结构化的，以保证在整个系统中实施最小特权法则。

每一个 NTCB 分部都按照网络体系结构与安全策略隔离部件内的资源。因此，网络系统中安全机制的“支持元素”(如 DAC 和用户标识)与 C2 级相比，由于提供了 NTCB 控制下的不同地址空间，从保证观点来看更强。

如在自主访问控制中已讨论的，某 NTCB 分部的 DAC 机制可能在参考监视器接口上实现，或者可以分布在同一个部件或不同部件内 NTCB 部分的主体中。若是分布在 NTCB 的主体内(即在参考监视器之外)，DAC 设计与实现的保证要求应该与 C2 级或更高级网络相同。

c. 基本原理

NTCB 必须模块化并符合硬件要求，这一点也适用于不同部件上的 NTCB 分部。

最小特权法则要求只能对每个用户或其他欲访问系统的个体授予实现该作业的资源和授权。每一个支持用户或其他个体的 NTCB 分部都必须在系统内执行这一法则。例如，禁止管理人员访问 NTCB 分部外的客体(如游戏)，就可减少被特洛伊木马破坏的机会。

NTCB 分部之间的通信保护要求特别针对 NTCB 分部上的主体。对于 NTCB 分部以外主体此类保护的任何要求均属于安全策略完整性的要求范畴。

在 NTCB 控制下能保证区分地址空间，这就提供了按照安全级来隔离主体的能力。这个要求在 B1 级提出，因为它是实现强制访问控制所绝对必要的。

5.3.2.3.1.2 系统完整性

a. 采用 GJB 2646 说明

应提供硬件和(或)软件特性，能够使用它们来定期验证 TCB 中现场硬件和固件元素操作的正确性。

b. 解释

要求的实现是通过能够用于定期验证每个 NTCB 分部部件中的硬件和固件元素是否正确操作硬件和(或)软件来部分完成的。在网络系统合并以及在全系统中进行操作之前，应提供验证同一性和修正部件操作的特性。例如，应设计一种协议，能使 NTCB 分部的部件定期交换消息并验证彼此的正确的应答。该协议还应能决定远程实体的应答能力。NTCB 分部还应提供向网络管理员报告在其他 NTCB 分部中检测到故障的能力。

应设计一种在 NTCB 内实现的部件之间的协议，在发生网络通信或单独部件失效的情况下，用它来提供正确操作。网络中的强制和自主访问控制策略可能会要求可信主体间的通信(该主体是不同部件上的 NTCB 分部的一部分)。这种通信通常由主体间的协议以平等实体的方式来实现。NTCB 分部与其他部件通信的失效不应引起部件内的错误访问。

c. 基本原理

该“解释”的第一段是对网络系统正文和在网络准则中所定义的 NTCB 分部要求的直接延伸。

NTCB 协议应足够强壮，以便局部错误发生时，可以保证系统正确地运行。这种保护机制可以保持 NTCB 自身的完整性。任何时候，网络中的一个或多个部件都可能无法工作，将这种故障对其他部件的影响减至最小是至关重要的。其余的完整性与拒绝服务事件将在“其余安全服务”中讨论。

5.3.2.3.1.3 隐蔽信道分析

a. 采用 GJB 2646 说明

系统开发者应对隐蔽存储信道作彻底的搜查，并且通过实际测量或工程估计的方法确定每个已标识信道的最大带宽（参见 GJB 2646 附录 A（补充件））。

b. 解释

GJB 2646 隐蔽信道指南中的要求适合于此处。在网络部件之间通信时，可能出现其他的隐蔽信道情况。

c. 基本原理

使用网络协议信息（如信息头）可能会引起隐蔽存储信道。这一点在有关文献中有所阐述。

5.3.2.3.1.4 可信设备管理

a. 采用 GJB 2646 说明

TCB 应支持操作员与管理员的职能分隔。

b. 解释

这一要求适用于整体网络和的单独部件的这类人员。

c. 基本原理

在已分配策略元素的基础上，一些部件可以无须人机接口即可操作。

5.3.2.3.2 生命周期保证

5.3.2.3.2.1 安全测试

a. 采用 GJB 2649 说明

应测试计算机系统，以证明其的确可以如系统文档所要求的正常工作。一个充分熟悉 TCB 规定实现的小组应详细分析和测试它的设计文档、源代码和目标代码。他们的目标是暴露全部设计和实现的缺陷，这些缺陷可以允许一个 TCB 外的主体去读、改变或删除通常在 TCB 执行强制或自主安全策略时拒绝的数据，并且保证没有主体（未授权去这样做）能使 TCB 进入不能对其它用户启动的通信做出响应的状态。TCB 应对入侵有一定的抵抗力。应排除所有已发现的缺陷，或使其无效，而且 TCB 应被重新测试，以便验证已排除的缺陷，并验证没有产生新的缺陷，测试应该可以验证 TCB 的实现与最高层规格说明一致。（参见 GJB 2646 附录 C（补充件））。

b. 解释

部件测试需要用一个测试台来测试部件的接口与协议，并包括意外情况下的测试。为满足该准则，网络系统中的安全机制测试是通过综合测试过程进行的，测试过程包括实现这一安

全机制的一个 NTCB 分部的所有部件。把这种综合测试附加到网络系统评估时任何单个部件的评估中。负责人应能标识出包括如网络大小的系统配置的许可集。可利用分析或测试过程与工具来测试这些配置的限制，在配置许可集内的配置变动无须再次测试。

对每一部件的测试应包括该部件上 NTCB 分部以外所引进的主体，该主体可以读、改变或删除一般情况下已被废弃的数据。如果该部件的一般接口不能提供创建完成此类测试所需要的主体的方法，那么，这一部分测试将对部件使用一个不可信软件的特殊版本，来完成在主体内的这些测试。应保存测试结果以进行测试分析。这样的特定版本将有一个 NTCB 分部，它与在评估时该部件通常配置的 NTCB 分部是相同的。

强制性控制的测试应包括：证明向部件输入和(或)从部件输出的信息标号准确表示该部件使用的、被 NTCB 分部所维护的、作为强制访问控制判定基础的标号。测试亦应包括由该部件支持的单级或多级每一种类型的设备。

NTCB 应对入侵有一定的抵抗力。这一点适用于 NTCB 整体以及本级中某一部件的 NTCB 分部。

c. 基本原理

“没有主体(未授权去这样做)能使 TCB 进入不能对其它用户启动的通信做出响应的状态”涉及到拒绝服务问题的安全服务及协议实现的正确。

测试是验证安全机制正确完成预定功能的重要方法。测试的主要目的是证明系统能对从不可信主体到 NTCB 分部的输入(有可能是蓄意的)做出响应。

一般系统允许动态输入新程序和创建新进程(由此也就引进了新主体)，并由用户指定其他安全特性。而与此相反，许多网络部件则没有在一般操作过程中引进新程序和(或)新进程的方法。由此，相关的测试程序就必须做为软件的特定版本而引进，而不是测试小组的一般输入所产生的结果，但是，必须保证用于这样测试的 NTCB 分部与评估时的 NTCB 完全相同。

敏感标号在保持网络强制访问控制中占有关键地位。对网络安全尤其重要的是部件间通信的信息标号规则——多级设备的显性标号和单级设备的隐性标号。因此，对标号的正确性测试就尤为重要。**测试 NTCB 的实现与描述性顶层规格说明(DTLS)的一致性是 GJB 2646 要求在网络系统的延伸。**

5.3.2.3.2.2 设计规范说明与验证

a. 采用 GJB 2646 说明

应在计算机系统的整个生命周期内维持由 TCB 支持的安全策略的形式化模型，并证明它与其原理一致。**应维护 TCB 的 DTLS，利用异常、错误消息和影响等术语完整和准确地描述 TCB 和 TCB 接口。**

b. 解释

该模型所表示的整体网络安全策略将提供 NTCB 施加在网络内主体和存储客体上强制访问控制策略的基础。该策略也将成为由 NTCB 完成的控制已命名用户对已命名客体访问的自主访问控制的基础。数据完整性要求，表明未授权的 MSM 影响无须包含在该模型中。整体网络策略必须分解在适当部件上的策略元素中，并用来作为这些部件安全策略模型的基础。

模型的抽象级别、模型中显式表示的主体和客体集都将受 NTCB 分部影响。如果某些网络部件的 NTCB 分部对主体和客体实行访问控制，那么，该主体和客体必须显式地表示在模型中，模型应为结构化的，以保证单个网络部件的原理和实体是明显的。分配给部件的全局网络策略元素，应由该部件的模型表示。

网络 DTLS 要求详见“设计文档”。

c. 基本原理

模型的实现方法在很大程度上依赖于分布系统中通信服务的完整，在紧耦合的分布系统中，该模型非常类似于独立计算机系统中的模型。

其余情况下，每一分部的模型都将表示在每种部件上 NTCB 分部的规则。它使模型更清晰，而且，尽管不是模型的一部分，也显示了系统设计所隐含的访问限制，例如，代表协议实体的主体只能访问和处于协议同一层的包含数据单元的客体。主体和客体在不同协议层上的分配是协议的设计问题，它无须反映在安全策略模型中。

5.3.2.3.2.3 配置管理

a. 采用 GJB 2646 说明

在整个生命周期中，如 TCB 设计、开发和维护期间，应把配置管理放在适当的位置，使之能控制所有安全相关的硬件、固件和软件的形式化控制模型、描述性或形式化顶层规范说明、其他设计数据、执行文件、源代码、目标代码的执行版本以及辅助测试工具和文档等方面的改变。配置管理系统应保证与当前 TCB 版本相关联的所有文档和代码之间的一致性。应提供将源代码生成新的 TCB 版本的工具。另外，还应具备 TCB 新旧版本比较的工具，以便查明实际用作新版本的 TCB 的代码只发生了所要求的改动。

b. 解释

要求如上所述并有以下延伸：

配置管理系统必须置于每一个 NTCB 分部内；

配置管理计划应属于整体系统，如果配置管理系统由不同 NTCB 分部上的配置管理系统构成，配置管理计划应说明配置控制是如何适用于整体系统的。

c. 基本原理

每一个 NTCB 分部都应有配置管理系统，否则在整体 NTCB 上不能实现有效的配置管理系统。其余部分只是网络实际工作的反映。

5.3.2.4 文档

5.3.2.4.1 安全特性用户指南

a. 采用 GJB 2646 说明

用户文档中的摘要、章条或手册应描述由 TCB 提供的保护机制、保护机制的使用说明及保护机制间的交互过程。

b. 解释

该用户文档描述了用户可见的全局级的(网络系统)、每一部件用户接口上的以及它们之间交互过程中的保护机制。

c. 基本原理

该"解释"是对网络系统和在网络准则中所定义的 NTCB 分部要求的延伸。由单个部件提供的保护机制的文档由适用于单个部件的 GJB 2646 提供。

5.3.2.4.2 可信设备手册

a. 采用 GJB 2646 说明

在计算机系统管理手册中应指出：当安全设备运行时，对有关功能与特权应加以说明，并提出警告。对各类审计事件，应给出提供检查和维护审计文件用的程序以及详细审计记录结构。手册应描述操作员和管理员有关安全功能和用户安全特性的变化。它应提供有关系统保护特性的一致和有效的用法。如它们怎样互相作用，怎样安全地生成一个新的 TCB。手册还应提供设备程序、警告和需要受控的特权，以便安全地操作该设备。**应标识基准确认机制的 TCB 模块。TCB 的任何模块修改以后，应描述由源代码安全生成新 TCB 的过程。**

b. 解释

该手册中应包含说明与过程，以协助系统管理员了解系统的配置情况。这些说明与过程包括以下几种情况：

网络本身的硬件配置；

如何向网络中增加新部件；

当某部件阶段性地离开网络(如被破坏或断开连接)后再次上网的情况；

影响网络安全性能的网络配置，例如，手册应向网络系统管理员说明影响网络体系结构的部件间的互连；

加载或修改 NTCB 软件或固件；

增量性修改，即应标明网络中哪个部件可能会变化而其余不变化。

应规定物理上的和管理环境上的控制。网络中任一安全性假设均应说明。例如，所有通信链都应有物理级上的保护。

应标明构成 NTCB 的网络部件。而且应标识包含在 NTCB 分部内的模块(该 NTCB 分部可能包含合法性参考机制)。

应描述由源代码安全生成的每一个 NTCB 分部新版本的过程。应标识由于网络配置变化所需要的安全生成 NTCB 的过程与要求。

c. 基本原理

多种系统管理员可能有各种各样的责任。这些手册上的技术安全措施必须与其他安全措施结合使用，以保证网络系统的安全性。其他安全措施包括管理安全、物理安全、辐射安全等。

该手册中应增加网络配置准则，因为，部件之间正确的互连对于网络体系结构的实现至关重要。

密码技术是保护通信线路的常用机制。未授权用户不可读加密信息。通常密文的安全级比较低，如欲使用加密算法，应由国家和军队安全主管部门认可。

加密算法与其实现过程不在本标准讨论范围。加密算法及其实现可能由某个单独设备完成或是某部件的主体功能。本标准不加区别地把任一加密实现包看做是加密机制。

构成 NTCB 的模块和部件的生成与标识要求，是 GJB 2646 在网络部分的扩展。当负责人不提供源代码时，应要求他提供可接受的安全生成的过程。

5.3.2.4.3 测试文档

a. 采用 GJB 2646 说明

负责人应向评估者提供一份文档，该文档包括测试计划、安全机制测试过程以及安全机制功能测试结果。**测试应包括减少隐蔽信道带宽方法的有效性。**

b. 解释

测试计划应说明测试的组成，亦应标识出不属于评估系统的测试部件。该计划还应包括这类部件中与测试相关的功能，以及评估系统这类部件的接口。网络测试计划说明应明确表示测试可以完全覆盖网络安全策略。测试应包括在系统体系结构和系统完整性中所描述的特性。测试亦应包括网络体系结构和大小。

c. 基本原理

被评估实体可能是一个网络子系统(参见附录 A(补充件))，应增加其他部件才能构成一个完整网络系统，在这种情况下，该文档应包括一些与上下文有关的定义说明。在评估时，若没有测试网络子系统的说明，就无法验证测试计划的正确性。

5.3.2.4.4 设计文档

a. 采用 GJB 2646 说明

设计文档应该提供负责人描述的保护原理及其在 TCB 上的实现，如果 TCB 由不同的模块构成，应描述模块之间的接口。由 TCB 实施的形式化描述的安全策略模型都应是可用的，并且应证明它对实施安全策略是足够的。应当标识特定的 TCB 保护机制，而且给出一种解释表示它们满足该模型。**DTLS 应当表明 TCB 接口的准确描述。该文档应描述 TCB 怎样实现参考监视器概念，并解释它如何防篡改，如何不能被旁越，以及如何被正确实现。该文档应描述 TCB 的结构如何便于测试和执行最小特权，还应描述隐蔽信道分析的结果，以及与限定该信道的折衷方案。应当标识所有利用已知隐蔽信道的可审计事件。应提供已知隐蔽存储信道的带宽，因为审计机制无法检测该隐蔽信道带宽的使用。**

b. 解释

在说明 NTCB 如何实现负责人所描述的保护原理时，应说明 NTCB 分部的方式。亦应说明安全策略。NTCB 模块间的接口应包括 NTCB 分部与分部内模块间的接口(若存在模块的话)。负责人应描述安全体系结构与设计，其中包括部件间安全要求的分布情况。附录 A 说明有关部件的评估。

正如在 B 等简要说明中所述，负责人必须证明 NTCB 使用了参考监视器概念。安全策略模型必须是针对参考监视器的模型。

完成参考监视器每一分部的安全策略模型应能充分表示由该分部所支持的访问控制策略，包括针对保密性和(或)完整性的自主和强制安全策略。对于强制性策略，应准确定义其敏感标号的单一主导关系，包括保密性和(或)完整性部件。

c. 基本原理

该解释是对在网络系统正文中所定义的网络说明要求的直接延伸。另外还要求在其他如描述部件或描述操作环境的文档中把网络子系统或网络系统描述为功能，例如在可信设备手册中。

为进行评估，网络系统应有相关的网络安全体系结构与设计(和网络安全体系结构与设计无关的部件的互连见附录 C(补充件))。网络安全体系结构必须包括与安全相关的策略、客体和协议。网络安全设计说明了网络中应包含的接口与服务，因此，能够可信地评估该网络。也许有多种设计构成同一个体系结构，但可能会出现不兼容或无法工作的情况(遵循互连规则的除外)。要求在设计中以可见接口方式描述部件间合作和安全相关的机制，不可见接口不在本标准讨论范畴。

在进行网络或部件评估之前，负责人必须提供网络安全体系结构与设计。网络安全体系结构与设计必须充分实现，而某些明显和不明显的缺陷要经过基于该特定结构的可信网络评议会议的同意。

当设计部件或欲评估部件时，当用部件组装网络或欲评估该网络时，均必须首先证明满足网络安全体系结构与设计。也就是说，用遵循网络安全体系结构与设计的每一种方法，能将多个部件构成网络，使之达到评估说明规定的可信网络要求。

为了由部件组成的可信网络能独立构造，网络安全体系统构与设计必须完整而无二义性地定义部件的安全功能与部件间的接口。亦须评估网络安全体系结构与设计，以保证遵循它的说明而建立的网络是可信的，也就是说该网络可由本标准来评估。

“模型”一词在网络中有许多不同的含义，如“协议参考模型”、“正式网络模型”等等。只有“安全策略模型”一词为本要求所用，而且特指接口模型(如参考监视器的“安全参数”)，它必须完成所有 GJB 2646 所定义的要求。并能显示出 TCB 的所有部分都是安全协议模型的合法解释，即除非在模型中被表示，安全状态不会改变。

5.3.3 B3 级：安全域

B3 级 NTCB 必须满足参考监视器的要求，为的是仲裁所有主体对客体的访问。它必须是防篡改的，而且足够小，以便分析和测试。因此，在 NTCB 设计及实现中，要用有效的系统工程方法，使 NTCB 的结构不包括对安全策略的实施不必要的代码，从而使其复杂性达到最小。支持安全管理员，并把审计机制扩展到有关安全信号事件，并且需要提供系统恢复过程。该系统应高度反入侵。下文是 B3 级系统的最低要求。

5.3.3.1 安全策略

a. 采用 GJB 2646 说明

b. 解释

网络负责人应清晰描述 NTCB 所完成的整体网络安全策略。该策略应至少包括本级适用的自主和强制要求。它要求数据保密性或数据完整性或两者兼备。该策略是由自主性和强制性两部分组成的访问控制策略。该策略应包括通过对用户或用户组鉴别来保护所处理的信息的自主安全策略。该访问控制策略应清晰描述网络的下述要求：防止并检测由未授权用户或错误引起对敏感信息的“读取或破坏”。强制性策略必须定义它所支持的敏感标号集。对于 B1 级或更高级，强制性策略应基于敏感标号(该敏感标号反映了按保密性和(或)完整性规定信息的安全级)和用户标号(该标号用于鉴别用户，以允许其访问某类信息)。未授权的用户包括：无权使用网络的所有用户；网络的合法使用者，但无权访问被保护信息的特定部分。

注意：“用户”并不包括“网络操作员”、“系统程序员”、“系统维护员”、“系统安全员”以及

其他技术人员。这些人员与一般用户有所区别并遵循可信设备手册和系统体系结构要求。这些人员可以修改网络中的系统参数，例如重新定义组成员。他们也可以具有独立的用户职责。

保密性策略：网络负责人应清晰定义阻止未授权用户访问系统中敏感信息的自主和强制保密性策略。

数据完整性策略：网络负责人应清晰定义阻止未授权用户修改(即写入)敏感信息的自主和强制完整性策略。由网络负责人所定义的数据完整性是：在网络中信息不应受到未授权的修改。一般情况下，由 NTCB 实施的强制完整性策略不能防止信息在部件间传输中被修改。然而，完整性敏感标号可以使信息在传输过程中由于受到保护而不会发生传输错误。这种要求有别于标号完整性要求。

c. 基本原理

“负责人”一词可指“出售商”、“网络集成商”、“制造商”、“开发商”中的某一位。有多种含义的原因是因为在评估网络系统时，某些人可能不是相关人员。

可信网络应控制对共享敏感信息的读与写。控制写操作就可保护信息免受破坏，一般情况下，网络既要保持信息的保密性也要保护完整性。但是，通常是完整性要比保密性更重要。因此，不论网络被评估为哪个等级，网络都应具备保密性和(或)完整性策略。这些策略的保证程度由网络的评估级别反映。

对修改操作的控制可以保证信息可靠，而且，一旦信息被破坏，仍然可以控制由于该破坏而引起的潜在危险。网络完整性策略既要保护在部件上正被处理的数据，也要保护正在网络中传送的数据。由 NTCB 所完成的访问控制策略与每个部件内主体对客体的访问相关。传递信息的通信完整性在“其余安全服务”中讨论。

在某些体系结构中的强制完整性策略(B1 级或更高级)可以用来支持面向连接的抽象或网络中部件之间的连接。例如，在端对端加密过程中的密钥发配中心，就可以指定一类特定的完整性范畴，以防止密钥产生的代码和数据受到该部件上其他支持过程(如操作员接口和审计)的修改。

某些体系结构中的强制完整性策略，可以定义一个完整性敏感标号，它反映了为确保信息既未受到超过指定限度的随机错误的破坏，也未受到未授权 MSM 的特定要求。与完整性敏感标号相关的特定矩阵一般反映了网络中的指定应用。

5.3.3.1.1 自主访问控制

a. 采用 GJB 2646 说明

TCB 应定义并控制计算机系统中已命名用户和已命名客体(文档或程序)之间的访问操作。执行机制(例如自身/组/公共控制，访问控制表)应允许用户通过自身/组/二者来指定并控制对客体的共享。执行机制还应控制访问权限的传播。自主访问控制机制应可以通过显性的用户行为或默认方式防止客体受到未授权的访问。**这些访问控制应该为每一个已命名的客体规定一份已命名的用户表和一份已命名的用户组表，以表示他们对该客体相应的访问方式。此外，对每个如此已命名的客体，也应指定一份不能访问该客体的已命名用户表和已命名用户组表。**只有授权用户才可以允许未得到访问许可的用户访问客体。

b. 解释

自主访问控制(DAC)机制应以各种方式分布于 NTCB 分部中。网络系统中的指定部件可以完成全部或一部分或不完成 DAC 的功能。尤其是仅仅支持内部主体(不做用户直接代理的主体)的部件,例如公共网络中的包交换,就可以不直接完成 DAC 的机制(例如它们不包含访问控制表)。

在网络环境中,有多种方法鉴别用户身份。例如在网络安全策略允许的情况下,可用不同部件(如主机、网关)的网络标识符(如互连地址)做为用户组标识符(如主机 A 的所有用户、网络 Q 的所有用户),这样就不必鉴别每个用户的身份。例如,主机 A 可以使用一个特定的组标识符,并保持一个显性用户组列表,于是,主机 A 可利用该表与主机 B 进行通信。

对网络来讲,单个主机会对它的用户在已命名个体的基础上施加自主控制——这一点和没有网络连接时所使用的控制相类似(事实上,也可能完全相同)。

当可以使用组标识符执行访问控制操作时,可能会要求其他主机的标识符,以此来避免进行远程用户的身份鉴别。C2 级或 C2 以上级的网络必须保证:当使用组标识符时,应利用审计记录来确切地标识(立即或以后)该组标识符所代表的单个用户。在组成员的改变以及相应的实现访问控制的时刻不同步过程中,可以允许稍有偏差。

NTCB 分部的 DAC 机制可以在参考监视器的接口中完成或分布在某主体上(该主体是相同或不同部件中 NTCB 的一部分)。参考监视器管理系统中所有的物理资源并创建它所控制的主客体的抽象。这些主客体中的一部分可以完成 NTCB 的某一部分功能。当某 DAC 资源分布于 NTCB 主体(可能在参考监视器外)时,DAC 的设计与实现机制的保证要求应符合 C2 级或 C2 以上级网络的要求。

若网络自主安全策略包含完整性,以上说明尤其适用于控制已被鉴别的用户或用户组在每个部件上进行的修改操作,也就是写访问。

c. 基本原理

在这一级,支持整体 DAC 机制的元素需要隔离支持 DAC 的信息(即客体),以便于审计(参见"系统体系结构")。可利用 X.25 中同一协议的方法,例如网络协议第三层 X.25 中的同一方法,使用该网络标识符标识用户组或用户自身。支持整体 DAC 机制的元素被视为不可信的主体。

典型的 DAC 情况是在某主机上为远程用户创建一个代理进程,该代理进程可在主机 NTCB 分部的控制下访问客体。本标准要求 NTCB 为每一个这样的进程指定并保留一个用户标识符,于是代理进程就可以受到与本地用户一样的自主访问控制。然而,本标准可以允许在一定范围内指定用户标识符。

最明显的情况是:如果每一个主机都可以使用网络用户的全局数据库(例如命名服务器),那么所有用户标识符都是全局有效的。

某些 NTCB 分部可以为局部注册的用户保持一个局部使用的数据库。在这种情况下,或者禁止为局部未注册的用户创建代理进程,或者允许为预选的用户或用户组创建代理进程。这些进程可标识运行在某远程主机上的用户组。本标准中的审计一词表明了最小的可审计度。审计要求 NTCB 分部的审计设施判定当某代理进程产生时,到底是谁在远程用户的主机上注册运行。

标识与鉴别机制负责建立用户标识符与代理进程的联系。这就意味着代理进程的用户标识符对 DAC 是局部适用的，数据通过网络回到用户主机的传输过程以及在用户主机上为数据做备份不是 DAC 的工作。

只支持内部主体的部件将要影响到 DAC 的实现，这是由于要完成 DAC 判定的部件需要得到一个提供服务的信息(如用户标识符)，关于这种情况的一个例子是主机 A 上的某个用户试图访问主机 B 上的某个文件。通常是由主机 A 向主机 B 传送一个用户标识符，而在主机 B 上完成 DAC 判定。

有若干种机制可以做到唯一用户标识过程。其中包括：

第一，要求在执行访问操作的主机上提供唯一标识和鉴别过程；

第二，确认由另一主机鉴别的有效网络地址，并将其发送至执行访问操作的主机；

第三，对支持网络全局的用户唯一标识符进行管理，该标识符可能是如在第二中所述的由另一主机鉴别和发送来的，或由一个指定的网络标识和鉴别服务器鉴别和发送来的。

完成第二和第三的协议应遵循系统体系结构要求。

除上述典型方式外，DAC 的网络支持还有其他方式，通常建议集中式访问控制方式。访问控制中心完成 DAC 的所有判定，或控制主机对主机的连接，来减少各主机的负担，这样可使一个主机只需要控制有限个远程主机上的用户对客体的访问。在这种情况下，访问控制中心提供面向抽象连接和 DAC 整体网络安全策略之间的连接。在上述所有情况下，应由客体所在的主机实现该判定。

有两种分布实现 DAC 的机制，一种是在不同的部件上分布实现，另一种在某个部件中的 NTCB 分部的主体上支持 DAC。由于“计算机系统”表示为整体“计算机网络”，每个部件都有责任完成分配给它的安全机制以保证网络安全策略的实现。对于传统的主机系统，DAC 机制可以与参考监视器中的 MAC 一起，使用如虚拟机器监控器等几种方法，在接口外支持 DAC。

与全局固定的强制性策略不同，DAC 是非常网络和系统专用化的，它的特性反映了系统的自然用途。常见情况是，单独主机以命名个体方式控制本地用户，这就像没有网络一样。然而，在大型网络中，集中地管理所有用户显然是很困难的。因此，其余主机的用户通常都被分组，以便于网络 DAC 策略的控制要求实际上是以这些主机或其他部件的标识为基础。网关是此类部件的一个例子。

保证要求是可信系统的关键所在。它可以决定某个系统或网络是否适合于指定的环境。在单个系统中，DAC 是合成在参考监视器中的，而与其他部分很难区分清楚。在网络系统中，由于 DAC 的分布实现，区分就比较容易。如果主要的网络部件可以较简便地设计实现，而又不会降低安全策略的要求，那么可信网络也就容易实现。

5.3.3.1.2　客体重用

a. 采用 GJB 2646 说明

在向一个主体初始转让、分配或重分配 TCB 未使用的存储器客体池之前，应删除所有包含在存储器客体内的信息授权。对已释放回系统的客体有访问权的任何主体，都不能再使用由原主体产生的任何信息，包括已加密的信息。

b. 解释

NTCB 应保证它所控制的任一存储客体(如某部件上 NTCB 分部控制下的消息缓冲区)不包含该部件主体内未获授权的信息。这种要求应由每个 NTCB 分部完成。

c. 基本原理

在网络系统中,人们对 NTCB 直接控制下的存储客体感兴趣,如部件上的消息缓冲区。网络系统里的每个部件都应满足客体重用要求。例如 DAC 要求使得消息缓冲区处于 NTCB 分部的控制下。分配给某内部主体的缓冲区可以被某个保证消息流完整性的主体所重用。这种可控的客体可以在物理资源如缓冲区、磁盘扇区、磁带和主存上实现或在某部件如网络开关上实现。

5.3.3.1.3 标号

a. 采用 GJB 2646 说明

TCB 应保存 TCB 外部主体所直接或间接访问的与每一个计算机系统资源(如主体、存储客体、ROM)有关的敏感标号。强制访问控制判断应以这些标号为基础。为输入无标号的数据,TCB 应提出请求,并从授权用户那里接收该数据的安全等级,而且 TCB 将对所有这些活动进行审计。

b. 解释

在 NTCB 分部控制下输入的无标号数据将由输入它的单级设备的设备标号强行指定一个设备标号。标号应包括由网络负责人所描述的与网络安全策略完全一致的保密性与完整性两部分。本说明中所有的"标号"一词都包括上述两个部分。同样,"单级"和"多级"两词都以该策略的保密性和完整性为基础。强制完整性策略应特别具有下述要求,如未被判定的消息流修改的可能性应在被保护数据的标号中有所反映。例如,当输入数据时,能够以密码机制为基础赋给它一个完整性标号,来保证达到该策略的要求。NTCB 应保证这种机制受到保护,而且能基于一个标号调用它。

如果安全策略包括完整性策略,所有在传输过程中可能引起 MSM 的活动,都将视为对数据完整性有破坏的、未授权的访问。NTCB 应自动测试、发现、报告这类超出网络完整性策略要求的错误或破坏。应标识 MSM 防范措施。应保证 MSM 强度,若使用了加密机制,它应被国家和军队安全主管部门批准。

必须给网络中每一部件内的所有客体分配标号,以便用它们可信地维持多级信息的分离,而与单级部件有关的任何主体的标号应该与该部件的标号相同。必须给用来存储网络控制信息的客体及其它网络结构(如路径表)分配标号,为的是防止未授权的访问和(或)修改。

c. 基本原理

该"解释"是对网络系统要求和在网络说明中所定义的 NTCB 分部的延伸。单级设备可以是主体或者也可以看作是客体。多级设备可以看作是有一定保密范围的可信主体,即该主体的保密范围位于期望在该设备上传输数据的最小至最大范围之间。

针对保密性或完整性或二者的敏感标号,可以反映未划分的等级或划分的等级或二者。

本要求适合于所有 B2 级或更高级别的网络。

如果网络存在完整性策略,由 NTCB 负责完成。NTCB 必须实施确保将信息准确地从源传送到目的地(不考虑中间连接点的个数)的策略。NTCB 必须能防御设备故障、环境遭破坏、

人和进程未授权修改数据的动作。完成代码或格式转换的协议应保护数据和控制信息的完整性。

可以规定尚未发现的传输错误的概率作为网络安全策略的一部分，因此，可以确定网络能满足预定应用的程度。当在部件中处理数据时，能在与该数据相关的完整性敏感标号内反映出由该数据要满足的特定度量值(例如，未被发现的修改概率)。要区分不同的应用和操作环境有不同的完整性要求。

网络应具有自动测试、发现和报告超过操作模式要求阈值错误的能力。完整性抗干扰的有效性必须与其他安全相关特性(如保密性)同样精确。

经常使用密码术作为数据完整性保证的基础，可以使用操纵检测码(MDC)机制。加密或MDC算法的充分性、协议逻辑的正确性以及实现的充分性必须在MSM抗干扰设计中被证实。

5.3.3.1.3.1 标号完整性

a. 采用GJB 2646说明

敏感标号应准确表示特定主体或客体的安全级，该主体和客体由此而相联系。当TCB输出时，敏感标号应准确而无二义性地表示内部标号，并与正在输出的信息相联系。

b. 解释

“TCB输出”是指信息从一个部件上的客体到另一部件上的客体的传送过程。在NTCB分部间传送的信息在“系统完整性”中讨论。内部与外部敏感标号的形式可能不同，但其意义相同。另外，NTCB还应保证敏感标号与网络中正在传输的信息之间的正确关系。

正如在“可信设备手册”中所述，未授权用户不可读加密信息。一般来讲，密文的安全级低于明文的。明文与密文包含在不同的客体中，各有自己的标号。明文的标号应加以保护，并与密文相关，当密文解为明文时，它可以被恢复。如果明文与单级设备相关联，其标号可以是隐含的。标号也可以隐含于密钥中。

当信息被输出到某个环境，在那里它可能受到有意或无意的修改时，TCB应支持如密码检验和的方法，来保证标号的准确性。当具备强制完整性策略时，该策略应定义完整性标号的含义。

c. 基本原理

加密算法与其实现过程不在本标准讨论范围。加密算法及其实现可以由某一个单独设备完成或是某部件的主体功能。本标准不加区别地把任意一个实现包看做是加密机制。加密算法应得到国家和军队安全主管部门批准。加密过程是某部件上NTCB分部的一部分。

加密机制不一定是多级设备或多级主体。由定义可知，加密过程是多级的。明文与密文接口带有不同安全级的信息。加密机制不会因在数据上执行逻辑或数学的操作而产生新的数据。加密机制中的明文或密文接口应分别标识为单级或多级。若接口是单级的，数据的安全级为可信单体，并与接口隐性相关联，“单级设备输出准则”适合于此处。

若接口是多级的，则数据必须加以标号，“多级设备输出准则”适合此处。网络体系结构可任意挑选可用的机制，将客体与标号相联系。可能发生的有关加密客体的例子如下：

在客体的协议定义中，包含标号域；

通过密钥将标号与客体隐式相联系，也就是说，密钥唯一标识安全级，在数据的加密级上，必须保护单独或私用的密钥。

5.3.3.1.3.2 有标号信息的输出

a. 采用 GJB 2646 说明

TCB 应对每个通信信道和 I/O 设备标明单级或多级。这个标志的任何变化都应由人工实现，并可由 TCB 审计。TCB 应维护并且审计任何与通信信道或 I/O 设备有关的安全等级或标号的变化。

b. 解释

应指定每个通信信道和网络部件为单级或多级。该指定的任何改动需经由负责受影响部件的管理员或安全员批准，或由 NTCB 的管理员或安全员批准。这种改变可被网络审计。

NTCB 应保持并审计与连接在单级通信信道、多级通信信道或部件的设备有关的当前安全级的任何改变。NTCB 也可以审计在多级通信信道或部件上传送的与信息相关的安全级集合的任何变化。

c. 基本原理

网络中的通信信道或部件与独立系统中的通信信道或 I/O 设备相似。必须把他们指定为多级(可以区分不同安全级的信息)或单级。在 GJB 2646 中，单级设备只可以连接在单级信道上。

若要改变向部件或通信信道发送信息的级或级的集合，应得到网络或部件安全员的认可与批准(若没有安全员，系统管理员也可以)。这一要求可以保证未经有关人员的批准，不会发生与安全相关的改动。

5.3.3.1.3.2.1 向多级设备的输出

a. 采用 GJB 2646 说明

当 TCB 将一个客体输出到一个多级 I/O 设备时，与该客体有关的敏感标号也应相应输出。并以输出信息相同的形式(如机器可读或人可读形式)驻留在同一物理介质上。当 TCB 在多级通信信道上输出或输入一个客体时，该信道使用的协议可以无二义性地把敏感标号和被发送或被接收的有关信息联系起来。

b. 解释

网络中的部件，包括主机，应通过多级通信信道或多个单级通信信道良好地互连，以保护多安全级的信息。联系安全级与输出信息的协议应提供唯一所需要的信息，将安全级与单个部件上 NTCB 分部之间通信信道上传送的信息联系起来。这种协议的定义必须指定敏感标号的表示和语义(如机器可读的标号必须唯一表示安全级)。

安全级与通信信息之间“无二义”的联系应达到 NTCB 内其余任何标号的精确度(在“标号完整性”中已讨论)。这种机制可由受保护且高度可靠的直接物理层连接完成，或由传统的可有效地发现传输过程中错误的密码链保护完成，或者也可以使用分离的信道完成。输入或输出的信息域必须与有关的设备标号相关联。

c. 基本原理

协议必须定义敏感标号的表示与语义(见附录 B(补充件)中的“强制访问控制策略”)多级

设备与(不可信)主体的接口，或由参考监视器完成或由一个多级主体完成(例如，在 Bell-La-Padula 模型定义的“受委托主体”)。该主体提供一个以 NTCB 分部的内部标号为基础的标号。

当今的技术水平限制了安全网络中强制策略的支撑能力。控制网络中每一个主体操作的参考监视器应完全由单个 NTCB 分部提供，该 NTCB 分部还应提供其主体的 NTCB 接口。这就意味着在安全策略模型(该主体能通过传输调用更改该模型)中表示的“安全状态”必须包含在同一个部件中。

对于驻留某个 NTCB 分部的部件之外的事件(例如到达一个消息)可以影响该 NTCB 分部的安全状态。这种影响可在另外的部件或分部上的事件初始化后异步地产生。例如，不确定的延迟可能发生在以下三种情况中，即一个部件初始化某消息、消息到达另一个部件的 NTCB 分部和第二个部件上安全状态改变。由于网络各部件是并行工作的，所以需要网络的全局控制(如网络全局时钟)以实现安全状态的同步转换。一般来说，这种设计既不实用也不被接受。因此，NTCB 分部之间的交互仅限于一对(至少是逻辑上的)设备之间的通信，如果设备可接/发多级信息的话，应为多级设备。对于广播型信道而言，通信对是发送者与预定接收者。然而，如果广播信道带多级信息，还需要另外的机制(如 TCB 保持的加密检验和)来实现分离与发送。

当两个位于不同部件上的多级设备进行互连时，在信道上使用的协议中需要有一个通用表示的“敏感标号”，使得发送者与接收者都能理解。在整个网络策略中每一个安全级都必须在那些标号中唯一表示出来。

在某个单独的 TCB 中，敏感标号的精确度一般是由很简单的技术(如很短的物理连接)来保证的，也可以使用单独印制电路板或通过内部总线来达到。在许多网络环境中，很可能发生偶然的错误或蓄意引入的错误，此时更需要良好的保护措施。

5.3.3.1.3.2.2 向单级设备输出

a. 采用 GJB 2646 说明

单级 I/O 设备和单级通信信道不需要维持其处理信息的敏感标号。然而，TCB 应包含一种机制，用这种机制 TCB 和一个受权用户进行可靠的通信，该通信信息具有指定的单安全级，且通过单级信道或 I/O 设备完成输入或输出。

b. 解释

如果两个直接相连的部件之一或全都不能可信地将不同安全级信息分离，或者这两个部件有一个共同的单安全级，那么，这两个部件应通过单级信道通信。单级部件或单级通信信道并不需要保持其处理信息的敏感标号，因此 NTCB 应包含一个可靠机制，使得 NTCB 与一个授权用户或 NTCB 分部内的主体可利用该机制指定信息的安全级，该信息由单级信道或网络部件输入或输出。

c. 基本原理

网络中的单级通信信道和单级部件与独立系统的单级信道和 I/O 设备类似，它们都不能可信地分离不同安全级的信息，因此，在这类信道与部件上传送的与数据相关的标号是隐含的；这是因为信道或部件而不是位流的显性部分使得 NTCB 将数据与标号连系起来。注意，

加密信息的安全级是密文的级而非明文的原有级。

5.3.3.1.3.2.3 人可读的输出标号

a. 采用 GJB 2646 说明

计算机系统管理员应规定与输出敏感标号相关联的可打印的标号名。TCB 应对所有人员可读的输出、编页的输出以及带有可识别敏感标号的硬拷贝输出(如行打印机输出)的开始和结束做出标记,以便正确表示该输出的敏感性。TCB 应按默认值对所有人可读的输出、编页的输出以及带有可识别敏感标号的硬拷贝输出(如行打印机输出)的每页的顶部和底部做标记,以便正确表示该页信息的敏感性。TCB 应该按默认值,并以适当方法标记具有人可读敏感标号的其他形式的人可读的输出(如映象、图形),以便正确表示该输出的敏感性。这些标记默认值的任何滥用都应由 TCB 审计。

b. 解释

本标准对于产生人不可读输出的部件不加要求。对于产生人可读输出的部件,在网络中定义的每一个安全级在所有的部件中都应有统一的含义。网络管理员与其任何相关的部件管理员,都可指定与已定义安全级相关联的人可读标号。

c. 基本原理

该"解释"是对网络系统和在网络说明中所定义的 NTCB 分部要求的直接延伸。

5.3.3.1.3.3 主体敏感标号

a. 采用 GJB 2646 说明

在交互对话期间,与终端用户相关联的安全级的每个变化,TCB 都应立即通知该用户,当终端用户想要显示该主体完全的敏感标号时,他应能向 TCB 进行询问。

b. 解释

任何与某终端用户相关联的安全级的改动,NTCB 分部应立即通知属于该部件的终端用户。

c. 基本原理

该局部 NTCB 分部必须保证那个用户理解从终端发出或发到终端的信息的安全级。当某用户在另一部件上有代理进程时,为保持和该用户的通信,可能要调整它的级,可以异步产生这种变化。这种调整对适合于通信线路上的客体强制访问控制是必要的。

5.3.3.1.3.4 设备标号

a. 采用 GJB 2646 说明

对各种附加的物理设备,TCB 应支持最小和最大的安全级的分配,并利用这些安全级满足安放该设备的物理环境所强加的约束条件。

b. 解释

这种要求适合于针对每一个 NTCB 分部的写操作,以使得基于安全级的独立信息是可信的。在部件内每一个用于与其他网络部件通信的 I/O 设备,都应分配一个包括最大及最小标号集合的设备区域。设备区域通常包括(不是必须包括)最大和最小标号之间的所有可能标号。

NTCB 总是为通过设备输出的信息提供一个精确的标号,利用单级设备输入或输出的信

息，其标号隐含于设备的安全级中。多级设备上的信息输入和输出时，必须通过统一认可的协议加以标号，如果使用总是负载单级的通信线路，可隐含标号。

若将给定安全级的信息输出至某个输入设备时，该输入设备区域必须包含这个标号给定的级或具有更高的级。若输入设备不包含这个标号给定的级，输出信息将重新加以标号至更高级，以符合该输入设备区域。其余情况不会重新标号。

c. 基本原理

设备标号的目的是反映并约束设备所处的物理环境中已授权信息的安全级。

从一个设备到另一个设备反复传送的信息可以使用单工通信(即无应答)，当两个设备区域没有公共的级时，只须要求发送设备区域中每一级都低于接收设备区域的一些级。而绝不允许将具有给定级的信息发送到其设备区域不包含高于该级的设备(参看附录 C(补充件)中有关 AIS 观点的类似的互连规则)。

5.3.3.1.4 强制访问控制

a. 采用 GJB 2646 说明

TCB 应对由 TCB 外部主体直接或间接访问的所有的资源(如主体、存储客体和 I/O 设备)执行强制性访问控制策略。应给这些主体和客体指定敏感标号，这些标号是划分等级的和未划分等级的结合，而且应作为强制性访问控制判断的基础。对于所有 TCB 外部的主体以及由这些主体直接或间接存储的所有客体应掌握下列要求：仅当主体安全级中划分的等级大于等于客体安全级划分的等级，而且主体安全级中未划分的等级包括了客体安全级中全部未划分的等级时，主体才能读一个客体；仅当主体安全级中划分的等级小于等于客体安全级中划分的等级，而且主体安全级中未划分等级被包含在客体安全级中未划分的等级时，主体才能写一个客体。TCB 应该用标识和鉴别数据来鉴别一个用户的标识，并保证 TCB 可以创建它以外主体的安全级及授权，从而使得批准和授权的那个用户去支配该用户。

b. 解释

每一个 NTCB 分部，都对它所控制下的部件上的所有主体、客体执行强制访问控制策略。在网络中，NTCB 分部的责任包括 TCB 在单个系统部件上施加的所有强制性访问控制。与其他部件进行通信用的主体和客体，更处于 NTCB 分部的控制下。强制访问控制包括保密性与完整性控制，这一点，网络负责人已在整体网络安全策略中有所描述。

两部件间与通信相关的概念化的实体，如扇区、连接和虚电路，可视为有两个端点，每一端存在于一个部件上，而每个端点可视为局域客体。通信过程可视为从一端的客体上把信息拷贝到另一端的客体上。透明的携带数据的实体，如数据报和包，既可视为存储在其他客体上的信息，也可视为分别处在通信路径两端的携带数据的实体。

可通过保密性或完整性级别来达到“两个或两个以上”安全级的要求。在强制完整性策略中，读与写的要求通常为当且仅当某主体的安全级可控制另一主体的安全级时，该主体可读另一主体；当且仅当客体的安全级可控制主体的安全级时，主体可写客体。以完整性策略为基础，网络负责人应定义对所有标号的控制关系，例如，通过将保密性和完整性的点阵结合起来去定义这个关系。

c. 基本原理

NTCB 分部只可以对它部件上的主体和客体保持访问控制。某部件上的一个主体如欲访问另一部件上客体的信息，就要在该远程部件上创建一个主体，以此作为第一个主体的代理。

强制访问控制必须在每一个 NTCB 分部的参考监视器接口上实施(即控制物理处理资源的机制)。这种机制为它所控制的主体和客体创建抽象。可以指定参考监视器外的一些主体去完成部分 NTCB 分部的强制策略，如使用在 Bell-LaPadula 模型中定义的“可信主体”。

对于在 I/O 设备上传输的标号信息的更高要求保证了连接于通信路径上客体敏感标号之间的一致性。网络体系结构必须能识别整体强制性网络安全策略与面向抽象之间的联系。例如，单独携带数据的实体(如数据报)可以有单独的敏感标号，并由这些标号接受每个部件上的强制访问控制。单级连接的抽象是由某体系结构隐含完成的，而连接是由单级主体实现的，该单级主体只能使用同级的数据报。

基本的可信系统技术允许 DAC 机制分布实现，这一点与强制访问控制要求相反。对于网络而言，MAC 与 DAC 机制的分离是规则而非意外情况。

用来代表强制性访问控制(包括数据保密性和完整性)策略中所有安全级的全部敏感标号集总是形成部分有序集。不失一般性，该有序集总可以延伸成一个包括所有未划分等级总和的点阵。对于任一点阵，全体敏感标号就定义了一个控制关系。为便于管理，最好有一个可控制其余标号的最大级。

5.3.3.2 责任

5.3.3.2.1 标识与鉴别

a. 采用 GJB 2646 说明

TCB 要求用户在开始操作前对其自身进行用户标识。因此，TCB 应维持鉴别数据，该数据包括验证单个用户身份的信息(如口令)，用于确定批准和授权单个用户的信息。TCB 用这种数据来鉴别用户身份及保证 TCB 外部的可代表单个用户建立动作的主体的安全级和授权能力，并由已批准和授权的用户支配它。TCB 应保护鉴别数据以防止被未授权的用户读取。TCB 应该能够很好地识别计算机系统内的每一个用户，以此实现个体责任。TCB 还应该提供把这种标识与该单个用户发生的所有可审计动作相联系的能力。

b. 解释

用户标识与鉴别要求和网络系统对计算机系统的要求一致。标识与鉴别工作可以由用户直接连接的部件负责，也可以由其他的部件(如标识鉴别服务器)负责。当 NTCB 欲以用户或用户组名义作主机或其他网络部件的媒体时，NTCB 将使用主机的标识和鉴别功能而不用单用户的标识鉴别功能。在进行鉴别时，部件标识功能应隐含与标识功能有直接联系的特定的用户组。这一要求并不适合于内部主体。

如果 NTCB 能保证信息避免受到未授权的破坏，那么，当从一个部件到另一个部件时，可以无须再次进行信息鉴别，包括已鉴别的用户身份。这种保护至少应达到与鉴别机制和鉴别数据的保护相同的保证级别。

c. 基本原理

在网络系统中，责任要求没有改变。把 NTCB 分布于若干部件之上，既不增加也不减少要求。即依旧存在单一责任。同样，在 C2 级或更高级的网络中，“单一责任”可由主机或其他

部件中的标识功能完成，只要能追踪单个用户或满足活动主体的特定单用户要求即可。在追踪过程中允许有偏差，因为组成员可能有变化，而且，完成访问控制也需要时间。另外，在网络这样的分布式系统中，当用户通过主体与远程主体操作时，无须在每一个节点上再次鉴别用户。

自主访问控制（DAC）由部件标识符和（或）鉴别信息的传递实现。这种支持机制使得DAC允许用户访问不同NTCB分部上的存储客体而不只是用户鉴别的客体。使用前向的标识机制指明了通信路径上源和部件的依赖性。

如果用已授权的标识作为确定某主体敏感标号的基础，它必须满足“标号完整性准则”。

一个已授权的标识可在部件间前向传递，并被某些部件用来标识与主体相关联的安全级，该主体是已标识用户的代理所创建的。

5.3.3.2.1.1 可信路径

a. 采用GJB 2646说明

TCB应在自身与用户之间提供一个可信通信路径，以供TCB与用户进行正确连接（如注册、改变主体安全级）时使用。经过该可信路径的通信应完全由用户或TCB激活。该路径逻辑上应与其他路径隔离，并与之完全区分开。

b. 解释

可信路径由用户（例如人）及该用户直接相连的部件上的NTCB分部所支持。

c. 基本原理

当用户在某远程部件上注册进入时，用户标识符可以安全地在本地与远程NTCB分部间传递，以满足标识和鉴别要求。

当发生与安全相关的活动时，可信路径是保证用户只与NTCB进行通信的必要措施。不过，可信路径并不提供在NTCB内的通信，而只提供用户与NTCB间的通信。因此，如果某部件不支持与用户的直接通信，则该部件就无须包含保证NTCB与用户直接通信的机制。

一个NTCB分部与另一个NTCB分部之间的可信通信的要求将在“系统体系结构”中详述。这种要求有别于用户到NTCB的可信路径通信要求。然而，一个NTCB分部与另一个NTCB分部之间的可信通信有利于实现用户与远程NTCB分部之间的可信通信。

5.3.3.2.2 审计

a. 采用GJB 2646说明

TCB应能建立、维护和保护对它所保护的客体访问的审计跟踪，防止修改、未授权访问或破坏。审计数据应受TCB保护，对审计数据已获授权的那些人能对它进行读访问。TCB应能记录下述类型的事件：标识和鉴别机制的使用、把客体引入到一个用户的地址空间（如打开文件，启动程序）、删除客体、计算机操作员和系统管理员和（或）系统安全员的动作，以及其他与安全有关的事件。TCB还应能审计人可读的输出标号的任何滥用。对每个已记录的事件来说，审计记录应标出：事件的日期和时间、用户、事件的类型，事件的成功或失败。对于标识和鉴别事件，请求的起点（如终端ID）应包括在审计记录中。对于把客体引入用户地址空间的事件和删除客体事件，审计记录应包括客体名和客体的安全级。计算机系统管理员应能以个体标识和（或）客体的安全级为基础有选择地审计任意一个或更多用户的活动。TCB应能审

计利用隐蔽存储信道的已标识事件。TCB 应包含一种机制，它能监控安全可审计事件的发生和积累，从而表明当前对安全策略的破坏。当超过阈值时，该机制应能立即通知安全管理员，而且如果这些有关安全事件的发生或积累再继续，系统应采取破坏最小的操作来终止该事件。

b. 解释

负责人必须能分辨出哪些事件是可审计的。如果 NTCB 本身(如“其余安全服务”中所标识的那些)无法分辨此类事件，审计机制应提供一个接口，授权主体可利用该接口中的参数来产生审计记录。这样的审计记录要与 NTCB 的审计记录有所区别。在网络系统中，“其余安全相关事件”(与网络体系结构和安全策略有关)可能有以下几种：

标识每一个访问事件(如在网络的两个主机之间建立或不建立连接)及其参数(如访问过程中两个主机的标识符)；

利用本地时间或全局同步时间来标识每一个访问过程的起止时间；

在两个主机交互过程中，标识与安全相关的意外情况(如破坏数据完整性事件)；

使用密码术；

改变网络配置(如某部件加入或离开网络)。

另外，如果必要，审计追踪记录中应包含标识信息，以允许所有相关的审计记录(如不同主机上的审计记录)可相关。而且，网络中的某部件可能具有所要求的审计功能(如存入、取出、减少、分析)，而其他部件则可能不存储审计数据，但却可以将审计数据传送到指定的收集部件。由于资源的不可得性，应控制审计数据的丢失。

在网络系统中，由于引入和删除客体事件而使其“用户地址空间”被扩展，包括远程用户(或主机)的代理正在使用的那些地址空间。尽管如此，其重点仍在用户而不是 DAC 准则中讨论过的内部主体。另外，审计信息必须以机器可读的形式存储。

TCB 应能审计利用隐蔽存储信道的已标识事件。为实现该功能，每个 NTCB 分部必须审计由网络带来的、在本地发生的、可能导致使用隐蔽存储信道的事件。

负责人应标识特定的、可能导致违反安全策略的可审计事件。当类似事件发生并积累而超过阈值时，检测到该事件的部件必须能够通知有关管理员。如果积累仍继续，应启动操作来终止该事件。例如，注册时间超过阈值时，应终止不成功的注册操作。

c. 基本原理

对远程用户来讲，可利用网络标识符(如互连地址)来表示单个用户或用户组标识符(如主机 A 的所有用户)，以避免当远程用户需要使用标识时应进行的维护过程。在这一级，它必须能标识出(立即或以后)一个组标识符表示哪些单个用户。在其它各方面，该说明是网络系统准则的直接延伸。

由于并发和同步问题，可能无法实时地检测到不同 NTCB 分部上发生的安全可审计事件的积累。然而，每一个具有审计责任的 NTCB 分部，都必须能检测到本地发生的这类事件的积累，并通知该分部安全管理员或网络安全管理员来启动操作在局部范围终内终止该事件。

5.3.3.3 保证

5.3.3.3.1 操作保证

5.3.3.3.1.1 系统体系结构

a. 采用 GJB 2646 说明

TCB 应保持自身运行域，以避免受到外部干扰或篡改(如修改其代码或数据结构)。TCB 应在其控制下，通过提供不同的地址空间来隔离进程。TCB 内部应由定义恰当的基本独立的模块构成。它应有效地使用可获得的硬件，把严格保护的单元与不严格保护的单元分离。TCB 模块应按可执行最小特权的原则设计。应利用硬件中分段的特点支持逻辑上截然不同的存储器客体，这些客体具有分散的属性(如可读、可写)。应完整地定义用户与 TCB 的接口，并标识所有 TCB 单元。**应使用一种完整的、原理简单且具有精确定义语义的保护机制来设计和构造 TCB。这一机制应在 TCB 和系统内部结构有效方面起到重要作用。TCB 应把分层、抽象和数据隐藏有效地结合使用。有效的系统工程将会使 TCB 的复杂性最小，而且能排除没有严格被保护的 TCB 模块。**

b. 解释

所有的 NTCB 分部均必须满足系统体系结构准则. 只有当所有 NTCB 分部均保持自身运行域时，NTCB 才可能保持自身运行域。由于每一个部件在整个网络系统中都是独立的区域，因此在特定情况下，若部件上只有一个主体，就可以通过不同的地址空间来达到隔离进程的要求。

NTCB 内部应由恰当定义的独立模块构成，并符合硬件要求。因此要求每一个 NTCB 分部也都如此构成，使 NTCB 能控制所有的网络资源。NTCB 所控制的网络资源子集是 NTCB 各分部所控制的资源子集之和。必须保护属于 NTCB 的代码与数据结构和在 NTCB 主体(即在 NTCB 内部，参考监视器外部的主体)中传送的属于不同 NTCB 分部的代码与数据，以防止其受到外部干扰和窜改。可用密码检验和(或)物理手段来保护 NTCB 分部间交换的用户鉴别数据。

每一个 NTCB 分部都必须实施部件内的最小特权法则。而且，NTCB 必须是结构化的，以保证在整个系统中实施最小特权法则。

必须按照网络安全体系结构，使用完整的、原理简单的保护机制来设计和构造 NTCB。而且，每一个 NTCB 分部也应如此来设计和构造。

有效的系统工程应使 NTCB 及其每一个 NTCB 分部的复杂性最小。应注意排除 NTCB 内不严格被保护的模块(和部件)。

尽管某些模块和(或)部件不是直接严格被保护的，但在 NTCB 内也可能需要包含它们，则它们必须满足 NTCB 的要求。为了正确操作严格被保护的模块和(或)部件，有必要正确操作这些模块和(或)部件，然而，这些模块和(或)部件的数目与大小应严格控制在最小。

每一个 NTCB 分部都按照网络体系结构与安全策略隔离部件内的资源。因此，网络系统中安全机制的“支持元素”(如 DAC 和用户标识)与 C2 级相比，由于提供了 NTCB 控制下的不同地址空间，从保证观点看更强了。

如在自主访问控制中已讨论的，某 NTCB 分部的 DAC 机制可能在参考监视器接口上实现，或者可以分布在同一个部件或不同部件内 NTCB 部分的主体中。若是分布在 NTCB 的主体内(即在参考监视器之外)，DAC 设计与实现的保证要求应该与 C2 级或更高级网络相同。

c. 基本原理

NTCB 必须模块化并符合硬件要求，这一点也适用于不同部件上的 NTCB 分部。

最小特权法则要求只能对每个用户或其他欲访问系统的个体授予实现该作业的资源和授权。每一个支持用户或其他个体的 NTCB 分部都必须在系统内执行这一法则。例如，禁止管理人员访问 NTCB 分部外的客体(如游戏)就可减少被特洛伊木马破坏的机会。

NTCB 分部之间的通信保护要求特别针对 NTCB 分部上的主体。对于 NTCB 分部以外主体的此类保护的任何要求均属于安全策略完整性的要求范畴。

网络中有些部分(模块和(或)部件)可能不是直接严格被保护的，因此在访问控制判断中就不包含它们，不直接受到审计，也不包含于标识/鉴别过程中。然而，网络的安全性必须依赖于这些模块和(或)部件的正确操作。例如单级包交换，虽然，通常它不直接包含于自主安全策略的执行中，这个交换是可信的，不会与不同消息流的数据混淆。如果该交换没有正确操作，数据就可能混淆，而且会发生非授权访问。因此，这些模块和(或)部件必须包含在 NTCB 中，还必须满足适合于 NTCB 策略元素责任的要求。

5.3.3.3.1.2 系统完整性

a. 采用 GJB 2646 说明

应提供硬件和(或)软件特性，能够使用它们来定期地验证 TCB 中现场硬件和固件元素操作的正确性。

b. 解释

要求的实现是通过能够用于定期验证每个 NTCB 分部部件中的硬件和固件元素是否正确操作硬件和(或)软件来部分完成的。在网络系统合并以及在全系统中进行操作之前，应提供验证同一性和修正部件操作的特性。例如，应设计一种协议能使 NTCB 分部的部件定期交换消息并验证彼此的正确应答。该协议还应能决定远程实体的应答能力。NTCB 分部还应提供向网络管理员报告在其他 NTCB 分部中检测到故障的能力。

应设计一种在 NTCB 内实现的部件之间的协议，在发生网络通信或单独部件失效的情况下，用它来提供正确操作。网络中的强制和自主访问控制策略可能会要求可信主体间的通信(该主体是不同部件上的 NTCB 分部的一部分)。这种通信通常由主体间的协议以平等实体的方式来实现。NTCB 分部与其他部件通信的失效不应引起部件内的错误访问。

c. 基本原理

该“解释”的第一段是对网络系统正文和在网络准则中所定义的 NTCB 分部要求的直接延伸。

NTCB 协议应足够强壮，以便局部错误发生时，可以保证系统正确地运行。这种保护机制可以保持 NTCB 自身的完整性。任何时候网络中的一个或多个部件都可能无法工作，将这种故障对其他部件的影响减至最小是至关重要的。其余的完整性与否认服务事件将在“其余安全服务”中讨论。

虽然，有一些完整性和否认服务特性可能存在于 NTCB 之外。换句话说，网络内的所有软件都应在 NTCB 之内。每个有可能写一些数据或写协议域的软件都是“可信的”，以便于保护完整性或不会引起某种程度的否认服务。例如，必须“信任”TELNET 可以正确传送用户数据和传送包。FTP 也必须是“可信的”，不会不适当地修改和传送文件。然而，(从保护观点出

发)可以在 NTCB 外设计这些协议。这样做对于这类安全工程是有益的。因此,不会泄露数据而又必须是可信的代码的总量是最小的。把所有东西放入 NTCB 内有悖于实现"有效的系统工程应使 TCB 的复杂性最小,而且能排除没有严格被保护的 TCB 模块"的要求,而这一点正是 B2 与 B3 级的首要区别。如果所有东西都必须放在 NTCB 内以保证数据完整性和针对否认服务的保护,就无法保证最大限度地对泄露进行保护。

5.3.3.3.1.3 隐蔽信道分析

a. 采用 GJB 2646 说明

系统开发者应对隐蔽存储信道作彻底的搜查,并且通过实际测量或工程估计的方法确定每个已标识信道的最大带宽(参见 GJB 2646 附录 A(补充件))。

b. 解释

GJB 2646 隐蔽信道指南中的要求适合于此处。在网络部件之间通信时,可能出现其他的隐蔽信道情况。

c. 基本原理

使用网络协议信息(如信息头)可能会引起隐蔽存储信道。使用传送频率可能引起隐蔽时间信道。S 这一点在有关文献中有所阐述。

5.3.3.3.1.4 可信设备管理

a. 采用 GJB 2646 说明

TCB 应将操作员与管理员的功能分隔开。应标识在安全管理员任务中所执行的功能。只有在计算机系统上发生了与安全管理任务截然不同的可审计活动后,计算机系统管理员才能执行安全管理功能。在安全管理任务中所能执行的非安全功能应严格限制在对有效执行安全任务必不可少的功能范围内。

b. 解释

这一要求适用于整体网络和单独部件的这类人员。

c. 基本原理

在已分配策略元素的基础上,一些部件可以无须人机接口即可操作。

5.3.3.3.1.5 可信恢复

a. 采用 GJB 2646 说明

在计算机系统发生故障或产生其他间断后,应提供程序和(或)机制以保证在不危及保护的情况下得到恢复。

b. 解释

在任意 NTCB 分部发生故障或产生其他间断后,恢复进程必须不危及保护来完成恢复。在整个 NTCB 发生故障后,恢复进程也必须可以使之恢复。

c. 基本原理

这是该要求在网络正文中的直接扩展,同时考虑到系统中一部分部件失效后,另一部分仍可以继续工作的情况。这可能是一件安全相关事件,所以必须是可审计的。

5.3.3.3.2 生命周期保证

5.3.3.3.2.1 安全测试

a. 采用 GJB 2646 说明

应测试计算机系统，以证明其的确可以如系统文档所要求的正常工作。一个充分熟悉 TCB 规定实现的小组应详细分析和测试它的设计文档、源代码和目标代码。他们的目标是暴露全部设计和实现的缺陷，这些缺陷可以允许一个 TCB 外的主体去读、改变或删除通常在 TCB 执行强制或自主安全策略时拒绝的数据，并且保证没有主体(未授权去这样做)能使 TCB 进入不能对其它用户启动的通信做出响应的状态。TCB 应对入侵有一定的抵抗力。应排除所有已发现的缺陷，或使其无效，而且 TCB 应重新测试，以便验证已排除的缺陷，并验证没有产生新的缺陷，测试应该可以验证 TCB 的实现与最高层规格说明一致。(参见 GJB 2646 附录 C(补充件))。**在测试中不能发现设计缺陷，允许有几个可纠正的执行缺陷，而且这种情况也应极少发生。**

b. 解释

部件测试需要用一个测试台来测试部件的接口与协议，并包括意外情况下的测试。为满足该准则，网络系统中的安全机制测试是通过综合测试过程进行的，测试过程包括实现这一安全机制的一个 NTCB 分部的所有部件。把这种综合测试附加到网络系统评估时任何单个部件的评估中。负责人应能标识出如网络大小的系统配置的许可集。可利用分析或测试过程与工具来测试这些配置的限制。在配置许可集内的配置变动无须再次测试。

对每一个部件的测试应包括该部件上 NTCB 分部以外引进的主体，该主体可以读、改变或删除一般情况下已被废弃的数据。如果该部件的一般接口不能提供创建完成此类测试所需要的主体的方法，那么，这一部分测试将对部件使用一个不可信软件的特定版本，来完成在主体内的这些测试。应保存测试结果以进行测试分析。这样的特定版本将有一个 NTCB 分部，它与在评估时该部件通常配置的 NTCB 分部是相同的。

强制性控制的测试应包括：证明向部件输入和(或)从部件输出的信息标号准确表示该部件使用的被 NTCB 分部所维护的、作为强制访问控制判定基础的标号。测试亦应包括由该部件支持的单级或多级的每一种类型的设备。

NTCB 应对入侵有一定的抵抗力。这一点适用于 NTCB 整体以及本级别中某一部件的 NTCB 分部。

c. 基本原理

“没有主体(未授权去这样做)能使 TCB 进入不能对其它用户启动的通信做出响应的状态”涉及到拒绝服务问题的安全服务及协议实现的正确。

测试是验证安全机制正确完成预定功能的重要方法。测试的主要目的是证明系统能对从不可信主体到 NTCB 分部的输入(有可能是蓄意的)做出响应。

一般系统允许动态输入新程序和创建新进程(由此也就引进了新主体)，并由用户指定其安全特性。而与此相反，许多网络部件则没有在一般操作过程中引进新程序和(或)新进程的方法。由此，相关的测试程序就必须做为软件的特定版本而引进，而不是测试小组的一般输入所产生的结果。但是，必须保证用于这样测试的 NTCB 分部与评估时的 NTCB 完全相同。

敏感标号在保持网络强制访问控制中占有关键地位。对网络安全尤其重要的是部件间通信的信息标号规则——多级设备的显性标号和单级设备的隐性标号。因此，对标号的正确性

测试就尤为重要。测试 NTCB 的实现与描述性顶层规格说明(DTLS)的一致性是 GJB 2646 要求在网络系统的延伸。

5.3.3.3.2.2 设计规范说明与验证

a. 采用 GJB 2646 说明

应在计算机系统的整个生命周期内维持由 TCB 支持的安全策略的形式化模型，并证明与其原理一致。应维护 TCB 的 DTLS，利用异常、错误消息和影响等术语完整和准确地描述 TCB 和 TCB 接口。应提供 DTLS 与模型一致的有力证据。

b. 解释

该模型所表示的整体网络安全策略将提供 NTCB 施加在网络内主体和存储客体上强制访问控制策略的基础。该策略也将成为由 NTCB 完成的控制已命名用户对已命名客体访问的自主访问控制的基础。数据完整性要求，表明未授权的 MSM 影响无须包含在该模型中。整体网络策略必须分解在适当的部件上的策略元素中，并用来作为这些部件的安全策略模型的基础。

模型的抽象级别、模型中显式表示的主体和客体集都将受 NTCB 分部影响。如果某些网络部件的 NTCB 分部对主体和客体实行访问控制，那么，该主体和客体必须显式地表示在模型中，模型应为结构化的，以保证单个网络部件的原理和实体是明显的。分配给部件的全局网络策略元素，应由该部件的模型表示。

网络 DTLS 要求详见“设计文挡”。

c. 基本原理

模型的实现方法在很大程度上依赖于分布系统中通信服务的完整，在紧耦合的分布系统中，该模型非常类似于独立计算机系统中的模型。

其余情况下，每一分部的模型都将表示在每种部件上 NTCB 分部的规则。它使模型更清晰，而且，尽管不是模型的一部分，也显示了系统设计所隐含的访问限制，例如，代表协议实体的主体只能访问和处于协议同一层的包含数据单元的客体。主体和客体在不同协议层上的分配是协议的设计问题，它无须反映在安全策略模型中。

5.3.3.3.2.3 配置管理

a. 采用 GJB 2646 说明

在整个生命周期中，如 TCB 设计、开发和维护期间，应把配置管理放在适当的位置，使之能控制所有安全相关硬件、固件和软件的形式化控制模型、描述性或形式化顶层规范说明、其他设计数据、执行文件、源代码、目标代码的执行版本以及辅助测试工具和文档等方面的改变。配置管理系统应保证与当前 TCB 版本相关联的所有文档和代码之间的一致性。应提供将源代码生成新的 TCB 版本的工具。另外，还应具备 TCB 新旧版本比较的工具，以便查明实际用作新版本的 TCB 的代码只发生了所要求的改动。

b. 解释

要求如上所述并有以下延伸：

配置管理系统必须置于每一个 NTCB 分部内；

配置管理计划应属于整体系统，如果配置管理系统由不同 NTCB 分部上的配置管理系统

构成，配置管理计划应说明配置控制是如何适用于整体系统的。

c. 基本原理

每一个 NTCB 分部都应有配置管理系统，否则在整体 NTCB 上不能实现有效的配置管理系统。其余部分只是网络实际工作的反映。

5.3.3.4 文挡

5.3.3.4.1 安全特性用户指南

a. 采用 GJB 2646 说明

用户文档中的摘要、章条或手册应描述由 TCB 提供的保护机制、保护机制的使用说明及保护机制间的交互过程。

b. 解释

该用户文档描述了用户可见的全局级的(网络系统)、每一部件用户接口上的以及它们之间交互过程中的保护机制。

c. 基本原理

该“解释”是对网络系统和在网络准则中所定义的 NTCB 分部要求的延伸。由单个部件提供的保护机制的文档由适用于单个部件的 GJB 2646 提供。

5.3.3.4.2 可信设备手册

a. 采用 GJB 2646 说明

在计算机系统管理手册中应指出：当安全设备运行时，对有关功能与特权应加以说明，并提出警告。对各类审计事件，应给出提供检查和维护审计文档用的程序以及详细审计记录结构。手册应描述操作员和管理员有关安全功能和用户安全特性的变化。它应提供有关系统保护特性的一致和有效的用法。如它们怎样互相作用，怎样安全地生成一个新的 TCB。手册还应提供设备程序、警告和需要受控的特权，以便安全地操作该设备。应标识基准确认机制的 TCB 模块。TCB 的任何模块修改以后，应描述由源代码安全生成新 TCB 的过程。**还应包括在系统运行任何失效发生后能安全恢复系统操作的过程。**

b. 解释

该手册中应包含说明与过程，以协助系统管理员了解系统的配置情况。这些说明与过程包括以下几种情况：

网络本身的硬件配置；

如何向网络中增加新部件；

当某部件阶段性地离开网络(如被破坏或断开连接)后再次上网的情况；

影响网络安全性能的网络配置，例如，手册应向网络系统管理员说明影响网络体系结构的部件间的互连；

加载或修改 NTCB 软件或固件；

增量性修改，即应标明网络中哪个部件可能会变化而其余不变化。

应规定物理上的和管理环境上的控制。网络中任一安全性假设均应说明。例如，所有通信链都应有物理级上的保护。

应标明构成 NTCB 的网络部件。而且应标识包含在 NTCB 分部内的模块(该 NTCB 分部

可能包含合法性参考机制)。

应描述由源代码安全生成的每一个 NTCB 新版本的过程。应标识由于网络配置变化所需要的安全生成 NTCB 的过程与要求。

应标明以安全状态启动每一个 NTCB 分部的过程,也应包括在系统或分系统操作间断后继续开始安全运行的程序。

c. 基本原理

多种系统管理员可能有各种各样的责任。这些手册上的技术安全措施必须与其他安全措施结合使用,以保证网络系统的安全性。其他安全措施包括管理安全、物理安全、辐射安全等。

该手册中应增加网络配置准则,因为,部件之间正确的互连对于网络体系结构的实现至关重要。

密码技术是保护通信线路的常用机制。未授权用户不可读加密信息。通常密文的安全级比较低,如欲使用加密算法须由国家和军队安全主管部门认可。

加密算法与其实现过程不在本标准讨论范围。加密算法及其实现可能由某个单独设备完成或是某部件的主体功能。本标准不加区别地把任一加密实现包看做是加密机制。

构成 NTCB 的模块和部件的生成与标识要求,是 GJB 2646 在网络部分的扩展。当负责人不提供源代码时,应要求他提供安全生成的可接受的过程。

由于给定的网络系统的特性(如不同的部件在不同的时间死机,而无该部件后网络系统还必须继续运行),必须了解如何安全启动 NTCB 分部和如何恢复安全运行。还必须了解当任何一个 NTCB 分部死机后,如何恢复 NTCB 安全运行。

5.3.3.4.3 测试文挡

a. 采用 GJB 2646 说明

负责人应向评估者提供一份文档,该文档包括测试计划、安全机制测试过程以及安全机制功能测试结果。测试应包括减少隐蔽信道带宽方法的有效性。

b. 解释

测试计划应说明测试的组成,亦应标识出不属于评估系统的测试部件。该计划还应包括这类部件中与测试相关的功能,以及评估系统这类部件的接口。网络测试计划说明应明确表示测试可以完全覆盖网络安全策略。测试应包括在系统体系结构和系统完整性中所描述的特性。测试亦应包括网络体系结构和大小。

c. 基本原理

被评估实体可能是一个网络子系统(参见附录 A(补充件)),应增加其他部件才能构成一个完整网络系统,在这种情况下,该文档应包括一些与上下文有关的定义说明。在评估时,若没有测试网络子系统的说明,就无法验证测试计划的正确性。

可以利用隐蔽信道的带宽决定网络是否适应给定环境。因此,应精确选择用来减少带宽的方法。

5.3.3.4.4 设计文档

a. 采用 GJB 2646 说明

设计文档应该提供负责人描述的保护原理及其在 TCB 上的实现,如果 TCB 由不同的模

块构成，应描述模块之间的接口。由 TCB 实施的形式化描述的安全策略模型都应是可用的，并且应证明它对实施安全策略是足够的。应当标识特定的 TCB 保护机制，而且给出一种解释表示它们满足该模型。DTLS 应当表明 TCB 接口的准确描述。该文档应描述 TCB 怎样实现参考监视器概念，并解释它如何防篡改，如何不能被旁越，以及如何被正确实现。**应非形式地表明 TCB 的实现（如在硬件、固件和软件方面）与 DTLS 相一致。应使用非形式化技术表明 DTLS 元素和 TCB 元素一致。**该文档应描述 TCB 的结构如何便于测试和执行最小特权，还应描述隐蔽信道分析的结果，以及与限定该信道的折衷方案。应当标识所有利用已知隐蔽信道的可审计事件。应提供已知隐蔽存储信道的带宽，因为审计机制无法检测该隐蔽信道带宽的使用。

b. 解释

在说明 NTCB 如何实现负责人所描述的保护原理时，应说明 NTCB 分部的方式。亦应说明安全策略。NTCB 模块间的接口应包括 NTCB 分部与分部内模块间的接口（若存在模块的话）。负责人应描述安全体系结构与设计，其中包括部件间安全要求的分布情况。附录 A（补充件）说明有关部件的评估。

正如在 B 等的简要说明中所述，负责人必须证明 NTCB 使用了参考监视器概念。安全策略模型必须是针对参考监视器的模型。

完成参考监视器每一分部的安全策略模型应能充分表示由该分部所支持的访问控制策略，包括针对保密性和（或）完整性的自主和强制安全策略。对于强制性策略，应准确定义其敏感标号的单一主导关系，包括保密性和（或）完整性部件。

c. 基本原理

该解释是对在网络系统正文中所定义的网络说明要求的直接延伸。另外还要求在其他如描述部件或描述操作环境的文档中把网络子系统或网络系统描述为功能，例如在可信设备手册中。

为进行评估，网络系统应有相关的网络安全体系结构与设计（和网络安全体系结构与设计无关的部件的互连见附录 C（补充件））。网络安全体系结构必须包括与安全相关的策略、客体和协议。网络安全设计说明了网络中应包含的接口与服务，因此能够可信地评估该网络。也许有多种设计构成同一个体系结构，但可能会出现不兼容或无法工作的情况（遵循互连规则的除外）。要求在设计中以可见接口方式描述部件间合作和安全相关的机制，不可见接口不在本标准讨论范畴。

在进行网络或部件评估之前，负责人必须提供网络安全体系结构与设计。网络安全体系结构与设计必须充分实现，而某些明显和不明显的缺陷要经过基于该特定结构的可信网络评议会议的同意。

当设计部件或欲评估部件时，当用部件组装网络或欲评估该网络时，均必须首先证明满足网络安全体系结构与设计。也就是说，用遵循网络安全体系结构与设计的每一种方法，能将多个部件构成网络，使之达到评估说明规定的可信网络要求。

为了由部件组成的可信网络能独立构造，网络安全体系结构与设计必须完整而无二义性地定义部件的安全功能与部件间的接口。亦须评估网络安全体系结构与设计，以保证遵循它

的说明而建立的网络是可信的，也就是说该网络可由本标准来评估。

“模型”一词在网络中有许多不同的含义，如“协议参考模型”、“正式网络模型”等等。只有“安全策略模型”一词为本要求所用，而且特指接口模型（如参考监视器的“安全参数”），它必须完成所有 GJB 2646 所定义的要求。并能显示出 TCB 的所有部分都是安全协议模型的合法解释，即除非在模型中被表示，安全状态不会改变。

5.4 A 等：验证保护

本等将利用形式化安全验证方法，来保证网络系统采用的强制和自主安全控制能有效保护该系统存储或处理的保密信息或其他敏感信息。为证明 NTCB 满足设计、开发和实现各方面的安全要求，需要一些扩展文件。

5.4.1 A1 级：验证设计

A1 级系统在功能上与 B3 级相同，没有增加另外的结构特征或策略要求。这一等级系统的显著特征是分析形式化设计规范和验证技术，并高度保证正确实现 NTCB。这种保证是自然的，始于安全策略正式模型的设计和形式化顶层规格说明（FTLS）的设计。由于使用了独立的特殊规格说明语言或验证系统，A1 级设计验证有五条重要准则：

a. 必须清晰描述安全策略的形式化模型并具有文档，其中包括数学证明，证明该模型与其公理一致和该模型支持安全策略是有效的。

b. FTLS 中必须包括 NTCB 所完成功能的抽象定义和支持隔离运行域所使用的硬件和（或）固件机制的抽象定义。

c. 在可能的情况下（即当有验证工具存在时），必须利用形式化技术表明 NTCB 的 FTLS 与其模型相一致，否则也可以用非形式化技术。

d. 必须以非形式化方式表明 NTCB 的实现（如在硬件、固件和软件方面）与 FTLS 相一致，必须用非形式化技术表明 FTLS 元素与 NTCB 元素相对应。FTLS 必须表示满足安全策略要求的统一的保护机制，而且 NTCB 的元素的映射就是这种保护机制的元素。

e. 必须利用形式化分析技术来标识和分析隐蔽信道。也可以使用非形式化技术来标识隐蔽定时信道，必须证明，在系统中已标识的隐蔽信道的继续存在。

为保持 A1 级系统所要求的 NTCB 的扩展设计和开发分析，需要更严格的配置管理，而且具备安全地将该系统分配到现场的过程。应支持系统安全管理员。下文是 A1 级系统的最低要求。

5.4.1.1 安全策略

a. 采用 GJB 2646 说明

b. 解释

网络负责人应清晰描述 NTCB 所完成的整体网络安全策略。该策略应至少包括本级适用的自主和强制访问控制要求。它要求数据保密性或数据完整性或两者兼备。该策略是由自主性和强制性两部分组成的访问控制策略。该策略应包括通过对用户或用户组鉴别来保护所处理的信息的自主安全策略。该访问控制策略应清晰描述网络的下述要求：防止并检测由未授权用户或错误引起对敏感信息的“读取或破坏”。强制性策略必须定义它所支持的敏感标号集。对于 B1 级或更高级，强制性策略应基于敏感标号（该敏感标号反映了按保密性和（或）完

整性规定的信息的安全级)和用户标号(该标号用于鉴别用户,以允许其访问某类信息)。未授权的用户包括：无权使用网络的所有用户;网络的合法使用者,但无权访问被保护的信息的特定部分。

注意："用户"并不包括"网络操作员"、"系统程序员"、"系统维护员"、"系统安全员"以及其他技术人员。这些人员与一般用户有所区别并遵循可信设备手册和系统体系结构要求。这些人员可以修改网络中的系统参数,例如:重新定义组成员。他们也可以具有独立的用户职责。

保密性策略：网络负责人应清晰定义阻止未授权用户访问系统中敏感信息的自主和强制保密性策略。

数据完整性策略：网络负责人应清晰定义阻止未授权用户修改(即写入)敏感信息的自主和强制完整性策略。由网络负责人所定义的数据完整性是信息：在网络中信息不应受到未授权的修改。一般情况下,由 NTCB 实施的强制完整性策略不能防止信息在部件间传输中被修改。然而,完整性敏感标号可以使信息在传输过程中由于受到保护而不会发生传输错误。这种要求有别于标号完整性要求。

c. 基本原理

"负责人"一词可指"出售商"、"网络集成商"、"制造商"、"开发商"中的某一位。有多种含义的原因是因为在评估网络系统时,某些人可能不是相关人员。

可信网络应控制对共享敏感信息的读与写。控制写操作就可以保护信息免受破坏,一般情况下,网络既要保持信息的保密性也要保护完整性。但是,通常是完整性要比保密性更重要。因此,不论网络被评估为哪个等级,网络都应具备保密性和(或)完整性策略。这些策略的保证程度由网络的评估级别反映。

对修改操作的控制可以保证信息可靠,而且,一旦信息被破坏,仍然可以控制由于该破坏而引起的潜在危险。网络完整性策略既要保护在部件上正被处理的数据,也要保护正在网络中传送的数据。由 NTCB 所完成的访问控制策略与每个部件内主体对客体的访问相关。传递信息的通信完整性在"其余安全服务"中讨论。

在某些体系结构中的强制完整性策略(B1 级或更高级)可以用来支持面向连接的抽象或网络中部件之间的连接。例如,在端对端加密过程中的密钥配发中心,就可以指定一类特定的完整性范畴,以防止密钥产生的代码和数据受到该部件上其他支持过程(如操作员接口和审计)的修改。

某些体系结构中的强制完整性策略,可以定义一个完整性敏感标号,它反映了为确保信息既未受到超过指定限度的随机错误的破坏,也未受到未授权 MSM 的特定要求。与完整性敏感标号相关的特定矩阵一般反映了网络中的指定应用。

5.4.1.1.1 自主访问控制

a. 采用 GJB 2646 说明

TCB 应定义并控制计算机系统中已命名用户和已命名客体(文件或程序)之间的访问操作。执行机制(例如自身/组/公共控制,访问控制表)应允许用户通过自身/组/二者来指定并控制对客体的共享。执行机制还应控制访问权限的传播。自主访问控制机制应可以通过显性

的用户行为或默认方式防止客体受到未授权的访问。这些访问控制应该为每一个已命名的客体规定一份已命名的用户表和一份已命名的用户组表，以表示他们对该客体相应的访问方式。此外，对每个如此已命名的客体，也应指定一份不能访问该客体的已命名用户表和已命名用户组表。只有授权用户才可以允许未得到访问许可的用户访问客体。

b. 解释

自主访问控制(DAC)机制应以各种方式分布于 NTCB 分部中。网络系统中指定部件可以完成全部或一部分或不完成 DAC 的功能。尤其是仅仅支持内部主体(不做用户直接代理的主体)的部件，例如公共网络中的包交换，就可以不直接完成 DAC 的机制(例如它们不包含访问控制表)。

在网络环境中，有多种方法鉴别用户身份。例如在网络安全策略允许的情况下，可用不同部件(如主机、网关)的网络标识符(如互连地址)做为用户组标识符(如主机 A 的所有用户、网络 Q 的所有用户)，这样就不必鉴别每个用户的身份。例如，主机 A 可以使用一个特定的组标识符，并保持一个显性用户组列表，于是，主机 A 可利用该表与主机 B 进行通信。

对网络来讲，单个主机会对它的用户在已命名个体的基础上施加自主控制——这一点和没有网络连接时所使用的控制相类似(事实上，也可能完全相同)。

当可以使用组标识符执行访问控制操作时，可能会要求其他主机的标识符，以此来避免进行远程用户的身份鉴别。在 C2 级或 C2 以上级的网络必须保证：当使用组标识符时，应利用审计记录来确切地标识(立即或以后)该组标识符所代表的单个用户。在组成员的改变以及相应的实现访问控制的时刻不同步过程中，可以允许稍有偏差。

NTCB 分部的 DAC 机制可以在参考监视器的接口中完成或分布在某主体上(该主体是相同或不同部件中 NTCB 的一部分)。参考监视器管理系统中所有的物理资源并创建它所控制的主客体的抽象。这些主客体中的一部分可以完成 NTCB 的某一部分功能。当某 DAC 资源分布于 NTCB 主体(可能在参考监视器外)时，DAC 的设计与实现机制的保证要求应符合 C2 级或 C2 以上级网络的要求。

若网络自主安全策略包含完整性，以上说明尤其适用于控制已被鉴别的用户或用户组在每个部件上进行的修改操作，也就是写访问。

c. 基本原理

在这一级，支持整体 DAC 机制的元素需要隔离支持 DAC 的信息(即客体)，以便于审计(参见“系统体系结构”)。可利用 X.25 中的同一协议的方法，例如网络协议第三层 X.25 中同一方法，使用该网络标识符标识用户组或用户自身。支持整体 DAC 机制的元素被视为不可信的主体。

典型的 DAC 情况是在某主机上为远程用户创建一个代理进程，该代理进程可在主机 NTCB 分部的控制下访问客体。本标准要求 NTCB 为每一个这样的进程指定并保留一个用户标识符，于是代理进程就可以受到与本地用户一样的自主访问控制。然而，本标准可以允许在一定范围内指定用户标识符。

最明显的情况是：如果每一个主机都可以使用网络用户的全局数据库(例如命名服务器)，那么所有用户标识符都是全局有效的。

某些 NTCB 分部可以为局部注册的用户保持一个局部使用的数据库。在这种情况下，或者禁止为局部未注册的用户创建代理进程，或者允许为预选的用户或用户组创建代理进程。这些进程可标识运行在某远程主机上的用户组。本标准中的审计一词表明了最小的可审计度。审计要求 NTCB 分部的审计设施判定当某代理进程产生时，到底是谁在远程用户的主机上注册运行。

标识与鉴别机制负责建立用户标识符与代理进程的联系。这就意味着代理进程的用户标识符对 DAC 是局部适用的，数据通过网络回到用户主机的传输过程以及在用户主机上为数据做备份不是 DAC 的工作。

只支持内部主体的部件将要影响到 DAC 的实现，这是由于要完成 DAC 判定的部件需要得到一个提供服务的信息(如用户标识符)，关于这种情况的一个例子是主机 A 上的某个用户试图访问主机 B 上的某个文件。通常是由主机 A 向主机 B 传送一个用户标识符，而在主机 B 上完成 DAC 判定。

有若干种机制可以做到唯一用户标识过程。其中包括：

第一，要求在执行访问操作的主机上提供唯一标识和鉴别过程；

第二，确认由另一主机鉴别的有效网络地址，并将其发送至执行访问操作的主机；

第三，对支持网络全局的用户唯一标识符进行管理，该标识符可能是如在第二中所述的由另一主机鉴别和发送来的，或由一个指定的网络标识和鉴别服务器鉴别和发送来的。

完成第二和第三的协议应遵循系统体系结构要求。

除上述典型方式外，DAC 的网络支持还有其他方式，通常建议集中式访问控制方式。访问控制中心完成 DAC 的所有判定，或控制主机对主机的连接，来减少各主机的负担，这样可使一个主机只需要控制有限个远程主机上的用户对客体的访问。在这种情况下，访问控制中心提供面向抽象连接和 DAC 整体网络安全策略之间的连接。在上述所有情况下，应由客体所在的主机实现该判定。

有两种分布实现 DAC 的机制，一种是在不同的部件上分布实现，另一种在某个部件中的 NTCB 分部的主体上支持 DAC。由于“计算机系统”表示为整体“计算机网络”，每个部件都有责任完成分配给它的安全机制以保证网络安全策略的实现。对于传统的主机系统，DAC 机制可以与参考监视器中的 MAC 一起，使用如虚拟机器监控器等几种方法，在接口外支持 DAC。

与全局固定的强制性策略不同，DAC 是非常网络和系统专用化的，它的特性反映了系统的自然用途。常见情况是，单独主机以命名个体方式控制本地用户，这就像没有网络一样。然而，在大型网络中，集中地管理所有用户显然是很困难的。因此，其余主机的用户通常都被分组，以便于网络 DAC 策略的控制要求实际上是以这些主机或其他部件的标识为基础。网关是此类部件的一个例子。

保证要求是可信系统的关键所在。它可以决定某个系统或网络是否适合于指定的环境。在单个系统中，DAC 是合成在参考监视器中的，而与其他部分很难区分清楚。在网络系统中，由于 DAC 的分布实现，区分就比较容易。如果主要的网络部件可以较简便地设计实现，而又不会降低安全策略的要求，那么可信网络也就容易实现。

5.4.1.1.2　客体重用

a. 采用 GJB 2646 说明

在向一个主体初始转让、分配或重分配 TCB 未使用的存储器客体池之前，应删除所有包含在存储器客体内的信息授权。对已释放回系统的客体有访问权的任何主体，都不能再使用由原主体产生的任何信息，包括已加密的信息。

b. 解释

NTCB 应保证它所控制的任一存储客体（如某部件上 NTCB 分部控制下的消息缓冲区）不包含该部件主体内未获授权的信息。这种要求应由每个 NTCB 分部完成。

c. 基本原理

在网络系统中，人们对 NTCB 直接控制下的存储客体感兴趣，如部件上的消息缓冲区。网络系统里的每个部件都应满足客体重用要求。例如 DAC 要求使得消息缓冲区处于 NTCB 分部的控制下。分配给某内部主体的缓冲区可以被某个保证消息流完整性的主体所重用。这种可控的客体可以在物理资源如缓冲区、磁盘扇区、磁带和主存上实现或在某部件如网络开关上实现。

5.4.1.1.3 标号

a. 采用 GJB 2646 说明

TCB 应保存 TCB 外部主体所直接或间接访问的与每一个计算机系统资源（如主体、存储客体、ROM）有关的敏感标号。强制访问控制判断应以这些标号为基础。为输入无标号的数据，TCB 应提出请求，并从授权用户那里接收该数据的安全等级，而且 TCB 将对所有这些活动进行审计。

b. 解释

在 NTCB 分部控制下输入的无标号数据将由输入它的单级设备的设备标号强行指定一个标号。标号应包括由网络负责人所描述的与网络安全策略完全一致的保密性与完整性两部分。本说明中所有的“标号”一词都包括上述两个部分。同样，“单级”和“多级”两词都以该策略的保密性和完整性为基础。强制完整性策略应特别具有下述要求，如未被判定的消息流修改的可能性应在被保护数据的标号中有所反映。例如，当输入数据时，能够以密码机制为基础赋给它一个完整性标号，来保证达到该策略的要求。NTCB 应保证这种机制受到保护，而且能基于一个标号调用它。

如果安全策略包括完整性策略，所有在传输过程中可能引起 MSM 的活动，都将视为对数据完整性有破坏的、未授权的访问。NTCB 应自动测试、发现、报告这类超出网络完整性策略要求的错误或破坏。应标识 MSM 防范措施。应保证 MSM 强度，若使用了加密机制，它应被国家和军队安全主管部门批准。

必须给网络中每一部件内的所有客体分配标号，以便用它们可信地维持多级信息的分离，而与单级部件有关的任何主体的标号应该与该部件的标号相同。必须给用来存储网络控制信息的客体及其他网络结构（如路径表）分配标号，为的是防止未授权的访问和（或）修改。

c. 基本原理

该“解释”是对网络系统要求和在网络说明中所定义的 NTCB 分部的延伸。单级设备可以是主体或者也可以看作是客体。多级设备可以看作是有一定保密范围的可信主体，即该主

体的保密范围位于期望在该设备上传输数据的最小至最大范围之间。

针对保密性或完整性或二者的敏感标号，可以反映未划分的等级或划分的等级或二者。

本要求适合于所有 B2 级或更高级别的网络。

如果网络存在完整性策略，由 NTCB 负责完成。NTCB 必须实施确保将信息准确地从源传送到目的地(不考虑中间连接点的个数)的策略。NTCB 必须能防御设备故障、环境遭破坏、人和进程未授权修改数据的动作。完成代码或格式转换的协议应保护数据和控制信息的完整性。

可以规定尚未发现的传输错误的概率作为网络安全策略的一部分，因此，可以确定网络能满足预定应用的程度。当在部件中处理数据时，能在与该数据相关的完整性敏感标号内反映出由该数据要满足的特定度量值(例如，未被发现的修改概率)。要区分不同的应用和操作环境有不同的完整性要求。

网络应具有自动测试、发现和报告超过操作模式要求阈值错误的能力。完整性抗干扰的有效性必须与其他安全相关特性(如保密性)同样精确。

经常使用密码术作为数据完整性保证的基础，可以使用操纵检测码(MDC)机制。加密或 MDC 算法的充分性、协议逻辑的正确性以及实现的充分性必须在 MSM 抗干扰设计中被证实。

5.4.1.1.3.1 标号完整性

a. 采用 GJB 2646 说明

敏感标号应准确表示特定主体或客体的安全级，该主体和客体由此而相联系。当 TCB 输出时，敏感标号应准确而无二义性地表示内部标号，并与正在输出的信息相联系。

b. 解释

“TCB 输出”是指信息从一个部件上的客体到另一部件上的客体的传送过程。在 NTCB 分部间传送的信息在“系统完整性”中讨论。内部与外部敏感标号的形式可能不同，但其意义相同。另外，NTCB 还应保证敏感标号与网络中正在传输的信息之间的正确关系。

正如在“可信设备手册”中所述：未授权用户不可读加密信息。一般来讲，密文的安全级低于明文的。明文与密文包含在不同的客体中，各有自己的标号。明文的标号应加以保护，并与密文相关，当密文解为明文时，它可以被恢复。如果明文与单级设备相关联，其标号可以是隐含的。标号也可以隐含于密钥中。

当信息被输出到某个环境，在那里它可能受到有意或无意的修改时，TCB 应如密码检验和的方法，来保证标号的准确性。当具备强制完整性策略时，该策略应定义完整性标号的含义。

c. 基本原理

加密算法与其实现过程不在本标准讨论范围。加密算法及其实现可以由某一个单独设备完成或是某部件的主体功能。本标准不加区别地把任意一个实现包看做是加密机制。加密算法应得到国家和军队安全主管部门批准。加密过程是某部件上 NTCB 分部的一部分。

加密机制不一定是多级设备或多级主体。由定义可知，加密过程是多级的。明文与密文接口带有不同安全级的信息。加密机制不会因在数据上执行逻辑或数学的操作而产生新的数

据。加密机制中的明文或密文接口应分别标识为单级或多级。若接口是单级的，数据的安全级为可信单体，并与接口隐性相关联，“单级设备输出准则”适合于此处。

若接口是多级的，则数据必须加以标号，“多级设备输出准则”适合此处。网络体系结构可任意挑选可用的机制，将客体与标号相联系。可能发生的有关加密客体的例子如下：

在客体的协议定义中，包含标号域；

通过密钥将标号与客体隐式相联系。也就是说，密钥唯一标识安全级。在数据的加密级上，必须保护单独或私用的密钥。

5.4.1.1.3.2 有标号信息的输出

a. 采用 GJB 2646 说明

TCB 应对每个通信信道和 I/O 设备标明单级或多级。这个标志的任何变化都应由人工实现，并可由 TCB 审计。TCB 应维护并且审计任何与通信信道或 I/O 设备有关的安全等级或标号的变化。

b. 解释

应指定每个通信信道和网络部件为单级或多级。该指定的任何改动需经由负责受影响部件的管理员或安全员批准，或由 NTCB 的管理员或安全员批准。这种改变可被网络审计。

NTCB 应保持并审计与连接在单级通信信道、多级通信信道或部件的设备有关的当前安全级的任何改变。NTCB 也可以审计在多级通信信道或部件上传送的与信息相关的安全级集合的任何变化。

c. 基本原理

网络中的通信信道或部件与独立系统中的通信信道或 I/O 设备相似。必须把它们指定为多级(可以区分不同安全级的信息)或单级。在 GJB 2646 中，单级设备只可以连接在单级信道上。

若要改变向部件或通信信道发送信息的级或级的集合，应得到网络或部件安全员的认可与批准(若没有安全员，系统管理员也可以)。这一要求可以保证未经有关人员的批准不会发生与安全相关的改动。

5.4.1.1.3.2.1 向多级设备的输出

a. 采用 GJB 2646 说明

当 TCB 将一个客体输出到一个多级 I/O 设备时，与该客体有关的敏感标号也应相应输出。并以输出信息相同的形式(如机器可读或人可读形式)驻留在同一物理介质上。当 TCB 在多级通信信道上输出或输入一个客体时，该信道使用的协议可以无二义性地把敏感标号和被发送或被接收的有关信息联系起来。

b. 解释

网络中的部件，包括主机，应通过多级通信信道或多个单级通信信道良好地互连，以保护多安全级的信息。联系安全级与输出信息的协议应提供唯一所需要的信息，将安全级与单个部件上 NTCB 分部之间通信信道上传送的信息联系起来。这种协议的定义必须指定敏感标号的表示和语义(如机器可读的标号必须唯一表示安全级)。

安全级与通信信息之间无“无二义”的联系应达到 NTCB 内其余任何标号的精确度(在

“标号完整性”中已讨论)。这种机制可由受保护且高度可靠的直接物理层连接完成,或由传统的可有效地发现传输过程中错误的密码链保护完成,或者也可以使用分离的信道完成。输入或输出的信息域必须与有关的设备标号相关联。

c. 基本原理

协议必须定义敏感标号的表示与语义(见附录 B 中的“强制访问控制策略”)。多级设备与(不可信)主体的接口,或由一个参考监视器完成,或由一个多级主体完成,(例如,在 Bell-LaPadula 模型定义的“受委托主体”),该主体提供一个以 NTCB 分部的内部标号为基础的标号。

当今的技术水平限制了安全网络中强制策略的支撑能力。控制网络中每一个主体操作的参考监视器应完全由单个 NTCB 分部提供,该 NTCB 分部还应提供其主体的 NTCB 接口。这就意味着在安全策略模型(该主体能通过传输调用更改该模型)中表示的“安全状态”必须包含在同一个部件中。

对于驻留某个 NTCB 分部的部件之外的事件(例如到达一个消息)可以影响该 NTCB 分部的安全状态。这种影响可在另外的部件或分部上的事件初始化后异步地产生。例如,不确定的延迟可能发生在以下三种情况中,即一个部件初始化某消息、消息到达另一个部件的 NTCB 分部和第二个部件上安全状态改变。由于网络各部件是并行工作的,所以需要网络的全局控制(如网络全局时钟)以实现安全状态的同步转换。一般来说,这种设计既不实用也不被接受。因此,NTCB 分部之间的交互仅限于一对(至少是逻辑上的)设备之间的通信,如果设备可接/发多级信息的话,应为多级设备。对于广播型信道而言,通信对是发送者与预定接收者。然而,如果广播信道带多级信息,还需要另外的机制(如 TCB 保持的加密检验和)来实现分离与发送。

当两个位于不同部件上的多级设备进行互连时,在信道上使用的协议中需要有一个通用表示的敏感标号,使得发送者与接收者都能理解。在整个网络策略中每一安全级都必须在那些标号中唯一表示出来。

在某个单独的 TCB 中,敏感标号的精确度一般是由很简单的技术(如很短的物理连接)来保证的,也可以使用单独印制电路板或通过内部总线来达到。在许多网络环境中,很可能发生偶然的错误或蓄意引入的错误,此时更需要良好的保护措施。

5.4.1.1.3.2.2 向单级设备输出

a. 采用 GJB 2646 说明

单级 I/O 设备和单级通信信道不需要维持其处理信息的敏感标号。然而,TCB 应包含一种机制,用这种机制 TCB 和一个受权用户进行可靠的通信,该通信信息具有指定的单安全级,且通过单级信道或 I/O 设备完成输入或输出。

b. 解释

如果两个直接相连的部件之一或全都不能可信地将不同安全级信息分离,或者这两个部件有一个共同的单安全级,那么,这两个部件应通过单级信道通信。单级部件或单级通信信道并不需要保持其处理信息的敏感标号,因此 NTCB 应包含一个可靠机制,使得 NTCB 与一个授权用户或 NTCB 分部内的主体可利用该机制指定信息的安全级,该信息由单级信道或网络

部件输入或输出。

c. 基本原理

网络中的单级通信信道和单级部件与独立系统的单级信道和 I/O 设备类似，它们都不能可信地分离不同安全级的信息。因此，在这类信道与部件上传送的与数据相关的标号是隐含的；这是因为信道或部件而不是位流的显性部分使得 NTCB 将数据与标号连系起来。注意，加密信息的安全级是密文的级而非明文的原有级。

5.4.1.1.3.2.3 人可读的输出标号

a. 采用 GJB 2646 说明

计算机系统管理员应规定与输出敏感标号相关联的可打印的标号名。TCB 应对所有人员可读的输出、编页的输出以及带有可识别敏感标号的硬拷贝输出(如行打印机输出)的开始和结束做出标记，以便正确表示该输出的敏感性。TCB 应按默认值对所有人可读的输出、编页的输出以及带有可识别敏感标号的硬拷贝输出(如行打印机输出)的每页的顶部和底部做标记，以便正确表示该页信息的敏感性。TCB 应该按默认值，并以适当方法标记具有人可读敏感标号的其他形式的人可读的输出(如映象、图形)，以便正确表示该输出的敏感性。这些标记默认值的任何滥用都应由 TCB 审计。

b. 解释

本标准对于产生人不可读输出的部件不加要求。对于产生人可读输出的部件，在网络中定义的每一个安全级在所有的部件中都应有统一的含义。网络管理员与其任何相关的部件管理员，都可指定与已定义安全级相关联的人可读标号。

c. 基本原理

该“解释”是对网络系统和在网络准则中所定义的 NTCB 分部要求的直接延伸。

5.4.1.1.3.3 主体敏感标号

a. 采用 GJB 2646 说明

在交互对话期间，与终端用户相关联的安全级的每个变化，TCB 都应立即通知该用户，当终端用户想要显示该主体完全的敏感标号时，他应能向 TCB 进行询问。

b. 解释

任何与某终端用户相关联的安全级的改动，NTCB 分部应立即通知属于该部件的终端用户。

c. 基本原理

该局部 NTCB 分部必须保证那个用户理解从终端发出或发到终端的信息的安全级。当某用户在另一部件上有代理进程时，为保持和该用户的通信，可能要调整它的级，可以异步产生这种变化。这种调整对适合于通信线路上的客体强制访问控制是必要的。

5.4.1.1.3.4 设备标号

a. 采用 GJB 2646 说明

对各种附加的物理设备，TCB 应支持最小和最大的安全级的分配，并利用这些安全级满足安放该设备的物理环境所强加的约束条件。

b. 解释

这种要求适合于针对每一个 NTCB 分部的写操作，以使得基于安全级的独立信息是可信的。在部件内每一个用于与其他网络部件通信的 I/O 设备，都应分配一个包括最大及最小标号集合的设备区域，设备区域通常包括(不是必须包括)最大和最小标号之间的所有可能标号。

NTCB 总是为通过设备输出的信息提供一个精确的标号，利用单级设备输入或输出的信息，其标号隐含于设备的安全级中。多级设备上的信息输入和输出时，必须通过统一认可的协议加以标号，如果使用总是负载单级的通信线路，可隐含标号。

若将给定安全级的信息输出至某个输入设备时，该输入设备区域必须包含这个标号给定的级或具有更高的级。若输入设备不包含这个标号给定的级，输出信息将重新加以标号至更高级，以符合该输入设备区域。其余情况不会重新标号。

c. 基本原理

设备标号的目的是反映并约束设备所处的物理环境中已授权信息的安全级。

从一个设备到另一个设备反复传送的信息可以使用单工通信(即无应答)，当两个设备区域没有公共的级时，只须要求发送设备区域中每一级都低于接收设备区域的一些级。而绝不允许将具有给定级的信息发送到其设备区域不包含高于该级的设备。(参看附录 C(补充件)中有关 AIS 观点的类似的互连规则)。

5.4.1.1.4 强制访问控制

a. 采用 GJB 2646 说明

TCB 应对由 TCB 外部主体直接或间接访问的所有的资源(如主体、存储客体和 I/O 设备)执行强制性访问控制策略。应给这些主体和客体指定敏感标号，这些标号是划分等级的和未划分等级的结合，而且应作为强制性访问控制判断的基础。对于所有 TCB 外部的主体以及由这些主体直接或间接存储的所有客体应掌握下列要求：仅当主体安全级中划分的等级大于等于客体安全级中划分的等级，而且主体安全级中未划分的等级包括了客体安全级中全部未划分的等级时，主体才能读一个客体；仅当主体安全级中划分的等级小于等于客体安全级中划分的等级，而且主体安全级中未划分的等级被包含在客体安全级中未划分的等级时，主体才能写一个客体。TCB 应该用标识和鉴别数据来鉴别用户的标识，并保证 TCB 可以创建它以外主体的安全级及授权，从而使得批准和授权的那个用户去支配该用户。

b. 解释

每一个 NTCB 分部，都对它所控制下的部件上的所有主体、客体执行强制访问控制策略。在网络中，NTCB 分部的责任包括 TCB 在单个系统部件上施加的所有强制性访问控制。与其他部件进行通信用的主体和客体，更处于 NTCB 分部的控制下。强制访问控制包括保密性与完整性控制，这一点，网络负责人已在整体网络安全策略中有所描述。

两部件间与通信相关的概念化的实体，如扇区、连接线、虚电路，可视为有两个端点，每一端存在于一个部件上，而每个端点可视为局域客体。通信过程可视为从一端的客体上把信息拷贝到另一端的客体上。透明的携带数据的实体，如数据报和包，既可视为存储在其他客体上的信息，也可视为分别处在通信路径两端的携带数据的实体。

可通过保密性或完整性级别来达到“两个或两个以上”安全级的要求。在强制完整性策略中，读与写的要求通常为当且仅当某主体的安全级可控制另一主体的安全级时，该主体可读另

一主体；当且仅当客体的安全级可控制主体的安全级时，主体可写客体。以完整性策略为基础，网络负责人应定义对所有标号的控制关系，例如，通过将保密性和完整性的点阵结合起来去定义这个关系。

c. 基本原理

NTCB 分部只可以对它部件上的主体和客体保持访问控制。某部件上的一个主体如欲访问另一部件上客体的信息，就要在该远程部件上创建一个主体，以此作为第一个主体的代理。

强制访问控制必须在每一个 NTCB 分部的参考监视器接口上实施（即控制物理处理资源的机制）。这种机制为它所控制的主体和客体创建抽象。可以指定参考监视器外的一些主体，去完成部分 NTCB 分部的强制策略，如使用在 Bell-Lapadula 模型中定义的“可信主体”。

对于在 I/O 设备上传输的标号信息的更高要求保证了连接于通信路径上客体敏感标号之间的一致性。网络体系结构必须能识别整体强制性网络安全策略与面向抽象之间的联系。例如，单独携带数据的实体（如数据报）可以有单独的敏感标号，并由这些标号接受每个部件上的强制访问控制。单级连接的抽象是由某体系结构隐含完成的，而连接是由单级主体实现的，该单级主体只能使用同级的数据报。

基本的可信系统技术允许 DAC 机制分布实现，这一点与强制访问控制要求相反。对于网络而言，MAC 与 DAC 机制的分离是规则而非意外情况。

用来代表强制性访问控制（包括数据保密性和完整性）策略中所有安全级的全部敏感标号集总是形成部分有序集。不失一般性，该有序集总可以延伸成一个包括所有未划分等级总和的点阵。对于任一点阵，全体敏感标号就定义了一个控制关系。为便于管理，最好有一个可控制其余标号的最大级。

5.4.1.2 责任

5.4.1.2.1 标识与鉴别

a. 采用 GJB 2646 说明

TCB 要求用户在开始操作前对其自身进行用户标识。因此，TCB 应维持鉴别数据，该数据包括验证单个用户身份的信息（如口令），用于确定批准和授权单个用户的信息。TCB 用这种数据来鉴别用户身份及保证 TCB 外部的可代表单个用户建立动作的主体的安全级和授权能力，并由已批准和授权的用户支配它。TCB 应保护鉴别数据以防止被未授权的用户读取。TCB 应该能够很好地识别计算机系统内的每一个用户，以此实现个体责任。TCB 还应该提供把这种标识与该单个用户发生的所有可审计动作相联系的能力。

b. 解释

用户标识与鉴别要求和网络系统对计算机系统的要求一致。标识与鉴别工作可以由用户直接连接的部件负责，也可以由其他的部件（如标识鉴别服务器）负责。当 NTCB 欲以用户或用户组名义作主机或其他网络部件的媒体时，NTCB 将使用主机的标识和鉴别功能而不用单用户的标识鉴别功能。在进行鉴别时，部件标识功能应隐含与标识功能有直接联系的特定的用户组。这一要求并不适合于内部主体。

如果 NTCB 能保证信息避免受到未授权的破坏，那么，当从一个部件到另一个部件时，可以无须再次进行信息鉴别，包括已鉴别的用户身份。这种保护至少应达到与鉴别机制和鉴别

数据的保护相同的保证级别。

c. 基本原理

在网络系统中，责任要求没有改变。把 NTCB 分布于若干部件之上，既不增加也不减少要求。即依旧存在单一责任。同样，在 C2 级或更高级的网络中，“单一责任”可由主机或其他部件中的标识功能完成，只要能追踪单个用户或满足活动主体的特定单用户要求即可。在追踪过程中允许有偏差，因为组成员可能有变化，而且，完成访问控制也需要时间。另外，在网络这样的分布式系统中，当用户通过主体与远程主体操作时，无须在每一个节点上再次鉴别用户。

自主访问控制（DAC）由部件标识符和（或）鉴别信息的传递实现。这种支持机制使得 DAC 允许用户访问不同 NTCB 分部上的存储客体而不只是用户鉴别的客体。使用前向的标识机制指明了通信路径上源和部件的依赖性。

如果用已授权的标识作为确定某主体敏感标号的基础，它必须满足“标号完整性准则”。

一个已授权的标识可在部件间前向传递，并被某些部件用来标识与主体相关联的安全级，该主体是已标识用户的代理所创建的。

5.4.1.2.1.1 可信路径

a. 采用 GJB 2646 说明

TCB 应在自身与用户之间提供一个可信通信路径，以供 TCB 与用户进行正确连接（如注册、改变主体安全级）时使用。经过该可信路径的通信应完全由用户或 TCB 激活。该路径逻辑上应与其他路径隔离，并与之完全区分开。

b. 解释

可信路径由用户（例如人）及该用户直接相连的部件上的 NTCB 分部所支持。

c. 基本原理

当用户在某远程部件上注册进入时，用户标识符可以安全地在本地与远程 NTCB 分部间传递，以满足标识和鉴别要求。

当发生与安全相关的活动时，可信路径是保证用户只与 NTCB 进行通信的必要措施。不过，可信路径并不提供在 NTCB 内的通信，而只提供用户与 NTCB 间的通信。因此，如果某部件不支持与用户的直接通信，则该部件就无须包含保证 NTCB 与用户直接通信的机制。

一个 NTCB 分部与另一个 NTCB 分部之间的可信通信的要求将在“系统体系结构”中详述。这种要求有别于用户到 NTCB 的可信路径通信要求。然而，一个 NTCB 分部与另一个 NTCB 分部之间的可信通信有利于实现用户与远程 NTCB 分部之间的可信通信。

5.4.1.2.2 审计

a. 采用 GJB 2646 说明

TCB 应能建立、维护和保护对它所保护的客体访问的审计跟踪，防止修改、未授权访问或破坏。审计数据应受 TCB 保护，对审计数据已获授权的那些人能对它进行读访问。TCB 应能记录下述类型的事件：标识和鉴别机制的使用、把客体引入到一个用户的地址空间（如打开文件、启动程序）、删除客体、计算机操作员和系统管理员和（或）系统安全员的动作、以及其他有关的安全事件。TCB 还应能审计人可读的输出标号的任何滥用。对每个已记录的事件来

说，审计记录应标出：事件的日期和时间、用户、事件的类型，事件的成功或失败。对于标识和鉴别事件，请求的起点（如终端 ID）应包括在审计记录中。对于把客体引入用户地址空间的事件和删除客体事件，审计记录应包括客体名和客体的安全级。计算机系统管理员应能以个体标识和（或）客体的安全级为基础有选择地审计任意一个或更多用户的活动。TCB 应能审计利用隐蔽存储信道的已标识事件。TCB 应包含一种机制，它能监控安全可审计事件的发生和积累，从而表明当前对安全策略的破坏。当超过阈值时，该机制应能立即通知安全管理员，而且如果这些有关安全事件的发生或积累再继续，系统应采取破坏最小的操作来终止该事件。

b. 解释

负责人必须能分辨出哪些事件是可审计的。如果 NTCB 本身（如“其余安全服务”中所标识的那些）无法分辨此类事件，审计机制应提供一个接口，授权主体可利用该接口中的参数来产生审计记录。这样的审计记录要与 NTCB 的审计记录有所区别。在网络系统中，“其余安全相关事件”（与网络体系结构和安全策略有关）可能有以下几种：

标识每一个访问事件（如在网络的两个主机之间建立或不建立连接）及其参数（如访问过程中两个主机的标识符）；

利用本地时间或全局同步时间来标识每一个访问过程的起止时间；

在两个主机交互过程中，标识与安全相关的意外情况（如破坏数据完整性事件）；

使用密码术；

改变网络配置（如某部件加入或离开网络）。

另外，如果必要，审计追踪记录中应包含标识信息，以允许所有相关的审计记录（如不同主机上的审计记录）可相关。而且，网络中的某部件可能具有所要求的审计功能（如存入、取出、减少、分析），而其他部件则可能不存储审计数据，但却可以将审计数据传送到指定的收集部件。由于资源的不可得性，应控制审计数据的丢失。

在网络系统中，由于引入和删除客体事件而使其“用户地址空间”被扩展，包括远程用户（或主机）的代理正在使用的那些地址空间。尽管如此，其重点仍在用户而不是 DAC 准则中讨论过的内部主体。另外，审计信息必须以机器可读的形式存储。

TCB 应能审计利用隐蔽存储信道的已标识事件。为实现该功能，每个 NTCB 分部必须审计由网络带来的、在本地发生的、可能导致使用隐蔽存储信道的事件。

负责人应标识特定的、可能导致违反安全策略的可审计事件。当类似事件发生并积累而超过阈值时，检测到该事件的部件必须能够通知有关管理员。如果积累仍继续，应启动操作来终止该事件。例如，注册时间超过阈值时，应终止不成功的注册操作。

c. 基本原理

对远程用户来讲，可利用网络标识符（如互连地址）来表示单个用户或用户组标识符（如主机 A 的所有用户），以避免当远程用户需要使用标识时应进行的维护过程。在这一级，它必须能标识出（立即或以后）一个组标识符表示哪些单个用户。在其它各方面，该说明是网络系统准则的直接延伸。

由于并发和同步问题，可能无法实时地检测到不同的 NTCB 分部上发生的安全可审计事件的积累。然而，每一个具有审计责任的 NTCB 分部，都必须能检测到本地发生的这类事件

的积累，并通知该分部安全管理员或网络安全管理员来启动操作在局部范围内终止该事件。

5.4.1.3 保证

5.4.1.3.1 操作保证

5.4.1.3.1.1 系统体系结构

a. 采用 GJB 2646 说明

TCB 应保持自身运行域，以避免受到外部干扰或篡改(如修改其代码或数据结构)。TCB 应在其控制下，通过提供不同的地址空间来隔离进程。TCB 内部应由定义恰当的基本独立的模块构成。它应有效地使用可获得的硬件，把严格保护的单元与不严格保护的单元分离。TCB 模块应按可执行最小特权的原则设计。应利用硬件中分段的特点支持逻辑上截然不同的存储器客体，这些客体具有分散的属性(如可读，可写)。应完整地定义用户与 TCB 的接口，并标识所有 TCB 单元。应使用一种完整的、原理简单且具有精确定义语义的保护机制来设计和构造 TCB。这一机制应在 TCB 和系统内部结构有效方面起到重要作用。TCB 应把分层、抽象和数据隐藏有效地结合使用。有效的系统工程将会使 TCB 的复杂性最小，而且能排除没有严格被保护的 TCB 模块。

b. 解释

所有的 NTCB 分部均必须满足系统体系结构准则。只有当所有 NTCB 分部均保持自身运行域时，NTCB 才可能保持自身运行域。由于每一个部件在整个网络系统中都是独立的区域，因此在特定情况下，若部件上有一个主体，就可以通过不同的地址空间来达到隔离进程的要求。

NTCB 内部应由恰当定义的独立模块构成，并符合硬件要求。因此要求每一个 NTCB 分部也都如此构成，使 NTCB 能控制所有的网络资源。NTCB 所控制的网络资源子集是 NTCB 各分部所控制的资源子集之和。必须保护属于 NTCB 的代码与数据结构和在 NTCB 主体(即在 NTCB 内部，参考监视器外部的主体)中传送的属于不同的 NTCB 分部的代码与数据，以防止其受到外部干扰和篡改。可用密码检验和(或)物理手段来保护 NTCB 间交换的用户鉴别数据。

每一个 NTCB 分部都必须实施部件内的最小特权法则。而且，NTCB 必须是结构化的，以保证在整个系统中实施最小特权法则。

必须按照网络安全体系结构，使用完整的、原理简单的保护机制来设计和构造 NTCB。而且，每一个 NTCB 分部也应如此来设计和构造。

有效的系统工程应使 NTCB 及其每一个 NTCB 分部的复杂性最小。应注意排除 NTCB 内不严格被保护的模块(和部件)。

尽管某些模块和(或)部件不是直接严格被保护的，但在 NTCB 内也可能需要包含它们，则它们必须满足 NTCB 的要求。为了正确操作严格被保护的模块和(或)部件，有必要正确操作这些模块和(或)部件，然而，这些模块和(或)部件的数目与大小应严格控制在最小。

每一个 NTCB 分部都按照网络体系结构与安全策略隔离部件内的资源。因此，网络系统中安全机制的“支持元素”(如 DAC 和用户标识)与 C2 级相比，由于提供了 NTCB 控制下的不同地址空间，从保证观点看更强了。

如在自主访问控制中已讨论的，某 NTCB 分部的 DAC 机制可能在参考监视器接口上实现，或者可以分布在同一个部件或不同部件内 NTCB 部分的主体中。若是分布在 NTCB 的主体内(即在参考监视器之外)，DAC 设计与实现的保证要求应该与 C2 级或更高级网络相同。

c. 基本原理

NTCB 必须模块化并符合硬件要求，这一点也适用于不同部件上的 NTCB 分部。

最小特权法则要求只能对每个用户或其他欲访问系统的个体授予实现该作业的资源和授权。每一个支持用户或其他个体的 NTCB 分部都必须在系统内执行这一法则。例如，禁止管理人员访问 NTCB 分部外的客体(如游戏)就可减少被特洛伊木马破坏的机会。

NTCB 分部之间的通信保护要求特别针对 NTCB 分部上的主体。对于 NTCB 分部以外主体的此类保护的任何要求均属于安全策略完整性的要求范畴。

网络中有些部分(模块和(或)部件)可能不是直接严格被保护的，因此在访问控制判断中就不包含它们，不直接受到审计，也不包含于标识/鉴别过程中。然而，网络的安全性必须依赖于这些模块和(或)部件的正确操作。例如单级包交换，虽然，通常它不直接包含于自主安全策略的执行中，这个交换是可信的，不会与不同消息流的数据混淆。如果该交换没有正确操作，数据就可能混淆，而且会发生非授权访问。因此，这些模块和(或)部件必须包含在 NTCB 中，还必须满足适合于 NTCB 策略元素责任的要求。

5.4.1.3.1.2 系统完整性

a. 采用 GJB 2646 说明

应提供硬件和(或)软件特性，能够使用它们来定期地验证 TCB 中现场硬件和固件元素操作的正确性。

b. 解释

要求的实现是通过能够用于定期验证每个 NTCB 分部部件中的硬件和固件元素是否正确操作硬件和(或)软件来部分完成的。在网络系统合并以及在全系统中进行操作之前，应提供验证同一性和修正部件操作的特性。例如，应设计一种协议能使 NTCB 分部的部件定期交换消息并验证彼此的正确应答。该协议还应能决定远程实体的应答能力。NTCB 分部还应提供向网络管理员报告在其他 NTCB 分部中检测到故障的能力。

应设计一种在 NTCB 内实现的部件之间的协议，在发生网络通信或单独部件失效的情况下，用它来提供正确操作。网络中的强制和自主访问控制策略可能会要求可信主体间的通信(该主体是不同部件上的 NTCB 分部的一部分)。这种通信通常由主体间的协议以平等实体的方式来实现。NTCB 分部与其他部件通信的失效不应引起部件内的错误访问。

c. 基本原理

该“解释”的第一段是对网络系统正文和在网络准则中所定义的 NTCB 分部要求的直接延伸。

NTCB 协议应足够强壮，以便局部错误发生时，可以保证系统正确地运行。这种保护机制可以保持 NTCB 自身的完整性。任何时侯，网络中的一个或多个部件都可能无法工作，将这种故障对其他部件的影响减至最小是至关重要的。其余的完整性与否认服务事件将在“其余安全服务”中讨论。

显然，有一些完整性和否认服务特性可能存在于 NTCB 之外。换句话说，网络内的所有软件都应在 NTCB 之内。每个有可能写一些数据或写协议域的软件都是“可信的”，以便于保护完整性或不会引起某种程度的否认服务。例如，必须“信任”TELNET 可以正确传送用户数据和传送包。FTP 也必须是“可信的”，不会不适当地修改和传送文件。然而，(从保护观点出发)可以在 NTCB 外设计这些协议。这样做对于这类安全工程是有益的。因此，不会泄露数据而又必须是可信的代码的总量是最小的。把所有东西放入 NTCB 内有悖于实现“有效的系统工程应使 TCB 的复杂性最小，而且能排除没有严格被保护的 TCB 模块”的要求，而这一点正是 B2 与 B3 级的首要区别。如果所有东西都必须放入 NTCB 内以保证数据完整性和针对否认服务的保护，就无法保证最大限度地泄露进行保护。

5.4.1.3.1.3　隐蔽信道分析

a. 采用 GJB 2646 说明

系统开发者应对隐蔽存储信道作彻底的搜查，并且通过实际测量或工程估计的方法确定每个已标识信道的最大带宽(参见 GJB 2646 附录 A(补充件))。

b. 解释

GJB 2646 隐蔽信道指南中的要求适合于此处。在网络部件之间通信时，可能出现其他的隐蔽信道情况。应使用形式化方法分析每个单独部件的设计和实现。

c. 基本原理

使用网络协议信息(如信息头)可能会引起隐蔽存储信道。使用传送频率可能引起隐蔽时间信道。这一点在有关文献中有所阐述。

5.4.1.3.1.4　可信设备管理

a. 采用 GJB 2646 说明

TCB 应将操作员与管理员的功能分隔开。应标识在安全管理员任务中所执行的功能。只有在计算机系统上发生了与安全管理任务截然不同的可审计活动后，计算机系统管理员才能执行安全管理功能。在安全管理任务中所能执行的非安全功能应严格限制在对有效执行安全任务必不可少的功能范围内。

b. 解释

这一要求适用于整体网络和单独部件的这类人员。

c. 基本原理

在已分配策略元素的基础上，一些部件可以无须人机接口即可操作。

5.4.1.3.1.5　可信恢复

a. 采用 GJB 2646 说明

在计算机系统发生故障或产生其他间断后，应提供程序和(或)机制以保证在不危及保护的情况下得到恢复。

b. 解释

在任意 NTCB 分部发生故障或产生其他间断后，恢复进程必须不危及保护来完成恢复。在整个 NTCB 发生故障后，恢复进程也必须可以使之恢复。

c. 基本原理

这是该要求在网络正文中的直接扩展，同时考虑到系统中一部分部件失效后，另一部分仍可以继续工作的情况。这可能是一件安全相关事件，所以必须是可审计的。

5.4.1.3.2 生命周期保证

5.4.1.3.2.1 安全测试

a. 采用 GJB 2646 说明

应测试计算机系统，以证明其的确可以如系统文档所要求的正常工作。一个充分熟悉 TCB 规定实现的小组应详细分析和测试它的设计文档、源代码和目标代码。他们的目标是暴露全部设计和实现的缺陷，这些缺陷可以允许一个 TCB 外的主体去读、改变或删除通常在 TCB 执行强制或自主安全策略时拒绝的数据，并且保证没有主体(未授权去这样做)能使 TCB 进入不能对其他用户启动的通信做出响应的状态。TCB 应对入侵有一定的抵抗力。应排除所有已发现的缺陷，或使其无效，而且 TCB 应重新测试，以便验证已排除的缺陷，并验证没有产生新的缺陷，测试应该可以验证 TCB 的实现与最高层规格说明一致。(参见 GJB 2646 附录 C(补充件))。在测试中不能发现设计缺陷，允许有几个可纠正的执行缺陷，而且这种情况也应极少发生。形式化顶层规格说明(FTLS)到源代码的人工的或其它的映象可以构成穿透能力测试的基础。

b. 解释

部件测试需要用一个测试平台来测试部件的接口与协议，并包括意外情况下的测试。为满足该准则，网络系统中的安全机制测试是通过综合测试过程进行的，测试过程包括实现这一安全机制的一个 NTCB 分部的所有部件。把这种综合测试附加到网络系统评估时任何单个部件的评估中。负责人应能标识出如网络大小的系统配置的许可集。可利用分析或测试过程与工具来测试这些配置的限制。在配置许可集内的配置变动无须再次测试。

对每一个部件的测试应包括该部件上 NTCB 分部以外引进的主体，该主体可以读、改变或删除一般情况下已被废弃的数据。如果该部件的一般接口不能提供创建完成此类测试所需要的主体的方法，那么，这一部分测试将对部件使用一个不可信软件的特定版本，来完成在主体内的这些测试。应保存测试结果以进行测试分析。这样的特定版本将有一个 NTCB 分部，它与在评估时该部件通常配置的 NTCB 分部是相同的。

强制性控制的测试应包括：证明向部件输入和(或)从部件输出的信息标号准确表示该部件使用的、被 NTCB 分部所维护的、作为强制访问控制判定基础的标号。测试亦应包括由该部件支持的单级或多级的每一种类型的设备。

NTCB 应对入侵有一定的抵抗力。这一点适用于 NTCB 整体以及本级中某一部件的 NTCB 分部。

c. 基本原理

“没有主体(未授权去这样做)能使 TCB 进入不能对其它用户启动的通信做出响应的状态”涉及到拒绝服务问题的安全服务及协议实现的正确。

测试是验证安全机制正确完成预定功能的重要方法。测试的主要目的是证明系统能对从不可信主体到 NTCB 分部的输入(有可能是蓄意的)做出响应。

一般系统允许动态输入新程序和创建新进程(由此也就引进了新主体)，并由用户指定其

安全特性。而与此相反，许多网络部件则没有在一般操作过程中引进新程序和(或)新进程的方法。由此，相关的测试程序就必须做为软件的特定版本而引进，而不是测试小组的一般输入所产生的结果。但是，必须保证用于这样测试的 NTCB 分部与评估时的 NTCB 完全相同。

敏感标号在保持网络强制访问控制中占有关键地位。对网络安全尤其重要的是部件间通信的信息标号规则——多级设备的显性标号和单级设备的隐性标号。因此，对标号的正确性测试就尤为重要。测试 NTCB 的实现与描述性顶层规格说明(DTLS)的一致性是 GJB 2646 要求在网络系统的延伸。

5.4.1.3.2.2 设计规范说明与验证

a. 采用 GJB 2646 说明

应在计算机系统的整个生命周期内维持由 TCB 支持的安全策略的形式化模型，并证明与其原理一致。应维护 TCB 的 DTLS，利用异常、错误消息和影响等术语完整和准确地描述 TCB，**应维护 TCB 形式化顶层规格说明(FTLS)，利用异常、错误消息和影响等述语准确地描述 TCB。如果作为实现 TCB 组成部件的硬件和(或)固件的特性在 TCB 接口上是可见的，则 DTLS 和 FTLS 就应包括它们。还应表示 FTLS 是 TCB 接口的准确描述。**应提供 DTLS 与模型一致的有力证据。**应结合使用形式化和非形式化技术来表明 FTLS 与该模型一致，这种验证证据应与形式化规范说明和已用的验证系统所提供的证据相一致，形式化规格说明及验证系统应由国家和军队安全主管部门在现代技术范围内认可，应实现 FTLS 到 TCB 源代码的人工或其它映象，以提供正确实现的证据。**

b. 解释

该模型所表示的整体网络安全策略将提供 NTCB 施加在网络内主体和存储客体上强制访问控制策略的基础。该策略也将成为由 NTCB 完成的控制已命名用户对已命名客体访问的自主访问控制的基础。数据完整性要求表明未授权的 MSM 影响无须包含在该模型中。整体网络策略必须分解在适当的部件上的策略元素中，并用来作为这些部件的安全策略模型的基础。

模型的抽象级别、模型中显式表示的主体和客体集都将受 NTCB 分部影响。如果某些网络部件的 NTCB 分部对主体和客体实行访问控制，那么，该主体和客体必须显式地表示在模型中，模型应为结构化的，以保证单个网络部件的原理和实体是明显的。分配给部件的全局网络策略元素，应由该部件的模型表示。

网络的 FTLS 由每一个独立的可信的网络部件的部件 FTLS 加上适合于多个部件的任何全局描述与断言组成。如果每一部件的模型都表示了所有分配至该部件的全局强制策略元素，就可以不需要任何全局断言。每一部件的 FTLS 应描述与该部件上 NTCB 分部的接口。

网络 DTLS 要求详见“设计文档”。

c. 基本原理

模型的实现方法在很大程度上依赖于分布系统中通信服务的完整，在紧耦合的分布系统中，该模型非常类似于独立计算机系统中的模型。

其余情况下，每一分部的模型都将表示在每种部件上 NTCB 分部的规则。它使模型更清晰，而且，尽管不是模型的一部分，也显示了系统设计所隐含的访问限制，例如，代表协议实体

的主体只能访问和处于协议同一层的包含数据单元的客体。主体和客体在不同协议层上的分配是协议的设计问题，它无须反映在安全策略模型中。

FTLS 必须表示基础的参考监视器以及任何完成强制策略的主体。其他分布在 NTCB 主体中的策略元素无需在 FTLS 中表示(参见“系统体系结构”解释)。

5.4.1.3.2.3 配置管理

a. 采用 GJB 2646 说明

在整个生命周期中，如 TCB 设计、开发和维护期间，应把配置管理系统放在适当的位置，使之能控制所有安全相关的硬件、固件和软件的形式化控制模型、描述性或形式化顶层规格说明、其他设计数据、执行文件、源代码、目标代码的执行版本以及辅助测试工具和文档等方面的改变。配置管理系统应保证与当前 TCB 版本相关联的所有文档和代码之间的一致性。应提供将源代码生成新的 TCB 版本的工具。另外，还应具备 TCB 新旧版本比较的工具，以便查明实际用作新版本的 TCB 的代码只发生了所要求的改动。**应将技术的、物理的和过程化的安全措施相结合，用来保护所有生成 TCB 的资料的主拷贝或拷贝免受非授权的修改或破坏。**

b. 解释

要求如上所述并有以下延伸：

配置管理系统必须置于每一个 NTCB 分部内；

配置管理计划应属于整体系统。如果配置管理系统由不同 NTCB 分部上的配置管理系统构成，配置管理计划应说明配置控制是如何适用于整体系统的。

所有用于生成新版本 NTCB 和每一个 NTCB 分部的资料，不论其物理上存在于何处，均必须受到保护。

c. 基本原理

每一个 NTCB 分部都应有配置管理系统，否则在整体 NTCB 上不能实现有效的配置管理系统。其余部分只是网络实际工作的反映。

这个新的要求显式地管理用于生成 NTCB 分部资料的保护，即使该生成过程发生在某远程部件的下线装载时，亦应如此。

5.4.1.3.2.4 可信分布

a. 采用 GJB 2646 说明

应提供可信的计算机系统控制和分配设备，用来维持在描述当前 TCB 版本的主数据和适合当前版本的现场主拷贝代码之间映射的完整性。还应有一些过程(如现场的安全验收测试)以保证分配给客户的 TCB 软件、固件和硬件的更新是完全由主拷贝指定的。

b. 解释

该要求如上所述。附加要求是，如果使用下线装载，必须具备可信地生成、发送及装载任何相关软件的方法。

c. 基本原理

这是本要求在网络正文中的直接扩展。

5.4.1.4 文档

5.4.1.4.1 安全特性用户指南

a. 采用 GJB 2646 说明

用户文档中的摘要、章条或手册应描述由 TCB 提供的保护机制、保护机制的使用说明及保护机制间的交互过程。

b. 解释

该用户文档描述了用户可见的全局级的(网络系统)、每一部件用户接口上的以及它们之间交互过程中的保护机制。

c. 基本原理

该"解释"是对网络系统和在网络准则中所定义的 NTCB 分部要求的延伸。由单个部件提供的保护机制的文档由适用于单个部件的 GJB 2646 提供。

5.4.1.4.2 可信设备手册

a. 采用 GJB 2646 说明

在计算机系统管理手册中应指出:当安全设备运行时,对有关功能与特权应加以说明,并提出警告。对各类审计事件,应给出提供检查和维护审计文档用的程序以及详细审计记录结构。手册应描述操作员和管理员有关安全功能和用户安全特性的变化。它应提供有关系统保护特性的一致和有效的用法。如它们怎样互相作用,怎样安全地生成一个新的 TCB。手册还应提供设备程序、警告和需要受控的特权,以便安全地操作该设备。应标识基准确认机制的 TCB 模块。TCB 的任何模块修改以后,应描述由源代码安全生成新 TCB 的过程。还应包括在系统运行任何失效发生后能安全恢复系统操作的过程。

b. 解释

该手册中应包含说明与过程,以协助系统管理员了解系统的配置情况。这些说明与过程包括以下几种情况:

网络本身的硬件配置;

如何向网络中增加新部件;

当某部件阶段性地离开网络(如被破坏或断开连接)后再次上网的情况;

影响网络安全性能的网络配置,例如,手册应向网络系统管理员说明影响网络体系结构的部件间的互连;

加载或修改 NTCB 软件或固件;

增量性修改,即应标明网络中哪个部件可能会变化而其余不变化。

应规定物理上的和管理环境上的控制。网络中任一安全性假设均应说明。例如,所有通信链都应有物理级上的保护。

应标明构成 NTCB 的网络部件。而且应标识包含在 NTCB 分部内的模块(该 NTCB 分部可能包含合法性参考机制)。

应描述由源代码安全生成的每一个 NTCB 新版本的过程。应标识由于网络配置变化所需要的安全生成 NTCB 的过程与要求。

应标明以安全状态启动每一个 NTCB 分部的过程,也应包括在系统或分系统操作间断后继续开始安全运行的程序。

c. 基本原理

多种系统管理员可能有各种各样的责任。这些手册上的技术安全措施必须与其他安全措施结合使用，以保证网络系统的安全性。其他安全措施包括管理安全、物理安全、辐射安全等。

该手册中应增加网络配置准则，因为，部件之间正确的互连对于网络体系结构的实现至关重要。

密码技术是保护通信线路的常用机制。未授权用户不可读加密信息。通常密文的安全级比较低，如欲使用加密算法须由国家和军队安全主管部门认可。

加密算法与其实现过程不在本标准讨论范围。加密算法及其实现可能由某个单独设备完成或是某部件的主体功能。本标准不加区别地把任一加密实现包看做是加密机制。

构成 NTCB 的模块和部件的生成与标识要求，是 GJB 2646 在网络部分的扩展。当负责人不提供源代码时，应要求他提供安全生成的可接受的过程。

由于给定的网络系统的特性(如不同的部件在不同的时间死机，而无该部件后网络系统还必须继续运行)，必须了解如何安全启动 NTCB 分部和如何恢复安全运行。还必须了解当任何一个 NTCB 分部死机后，如何恢复 NTCB 安全运行。

5.4.1.4.3 测试文档

a. 采用 GJB 2646 说明

负责人应向评估者提供一份文档，该文档包括测试计划、安全机制测试过程以及安全机制功能测试结果。测试应包括减少隐蔽信道带宽方法的有效性。**应提供形式化顶层规格说明与 TCB 源代码之间的一致性。**

b. 解释

测试计划应说明测试的组成，亦应标识出不属于评估系统的测试部件。该计划还应包括这类部件中与测试相关的功能，以及评估系统这类部件的接口。网络测试计划说明应明确表示测试可以完全覆盖网络安全策略。测试应包括在系统体系结构和系统完整性中所描述的特性。测试亦应包括网络体系结构和大小。

必须检验 FTLS 与 NTCB 源代码之间的映象，以保证在可能的程度上，FTLS 是源代码的正确表示。而且，在网络系统的设计与开发期间，FILS 成为精确的依据。对于网络系统中每一个存在有 FTLS 的部件都必须进行这种检验。

c. 基本原理

被评估实体可能是一个网络子系统(参见附录 A(补充件))，应增加其他部件才能构成一个完整网络系统，在这种情况下，该文档应包括一些与上下文有关的定义说明。在评估时，若没有测试网络子系统的说明，就无法验证测试计划的正确性。

可以利用隐蔽信道的带宽决定网络是否适应给定环境。因此，应精确选择用来减少带宽的方法。

5.4.1.4.4 设计文档

a. 采用 GJB 2646 说明

设计文档应该提供负责人描述的保护原理及其在 TCB 上的实现，如果 TCB 由不同的模块构成，应描述模块之间的接口。由 TCB 实施的形式化描述的安全策略模型都应是可用的，并且应证明它对实施安全策略是足够的。应当标识特定的 TCB 保护机制，而且给出一种解释

表示它们满足该模型。DTLS 应当表明 TCB 接口的准确描述。该文档应描述 TCB 怎样实现参考监视器概念，并解释它如何防篡改，如何不能被旁越，以及如何被正确实现。应非形式地表明 TCB 的实现（如在硬件、固件和软件方面）与 FTLS 相一致。应使用非形式技术表明 FTLS 元素和 TCB 元素一致。该文档应描述 TCB 的结构如何便于测试和执行最小特权，还应描述隐蔽信道分析的结果以及与限定该信道的折衷方案。应当标识所有利用已知隐蔽信道的可审计事件。应提供已知隐蔽存储信道的带宽，因为审计机制无法检测该隐蔽信道带宽的使用。**应该准确描述存在于 TCB 内但与 FTLS 无关的软件、硬件和固件机制（如映射寄存器、直接内存访问（DMA）等）。**

b. 解释

在说明 NTCB 如何实现负责人所描述的保护原理时，应说明 NTCB 分部的方式。亦应说明安全策略。NTCB 模块间的接口应包括 NTCB 分部与分部内模块间的接口（若存在模块的话）。负责人应描述安全体系结构与设计，其中包括部件间安全要求的分布情况。附录 A 说明有关部件的评估。

在说明 FTLS 与 NTCB 在实现上的对应关系时，应先说明每个部件 FTLS 与该部件上 NTCB 分部之间的关系。

正如在 B 等的简要说明中所述，负责人必须证明 NTCB 使用了参考监视器概念。安全策略模型必须是针对参考监视器的模型。

完成参考监视器每一分部的安全策略模型应能充分表示由该分部所支持的访问控制策略，包括针对保密性和（或）完整性的自主和强制安全策略。对于强制性策略，应准确定义其敏感标号的单一主导关系，包括保密性和（或）完整性部件。

c. 基本原理

该解释是对在网络系统正文中所定义的网络说明要求的直接延伸。另外还要求在其他如描述部件或描述操作环境的文档中把网络子系统或网络系统描述为功能。例如在可信设备手册中。

为进行评估，网络系统应有相关的网络安全体系结构与设计（和网络安全体系结构与设计无关的部件的互连见附录 C（补充件））。网络安全体系结构必须包括与安全相关的策略、客体和协议。网络安全设计说明了网络中应包含的接口与服务，因此能够可信地评估该网络。也许有多种设计构成同一个体系结构，但可能会出现不兼容或无法工作的情况（遵循互连规则的除外）。要求在设计中以可见接口方式描述部件间合作和安全相关的机制，不可见接口不在本标准讨论范畴。

在进行网络或部件评估之前，负责人必须提供网络安全体系结构与设计。网络安全体系结构与设计必须充分实现，而某些明显和不明显的缺陷要经过基于该特定结构的可信网络评议会议的同意。

当设计部件或欲评估部件时，当用部件组装网络或欲评估该网络时，均必须首先证明满足网络安全体系结构与设计。也就是说，用遵循网络安全体系结构与设计的每一种方法，能将多个部件构成网络，使之达到评估说明规定的可信网络要求。

为了由部件组成的可信网络能独立构造，网络安全体系结构与设计必须完整而无二义性

地定义部件的安全功能与部件间的接口。亦须评估网络安全体系结构与设计，以保证遵循它的说明而建立的网络是可信的，也就是说该网络可由本标准来评估。

“模型”一词在网络中有许多不同的含义，如“协议参考模型”、“正式网络模型”等等。只有“安全策略模型”一词为本要求所用，而且特指接口模型（如参考监视器的“安全参数”），它必须完成所有 GJB 2646 所定义的要求。并能显示出 TCB 的所有部分都是安全协议模型的合法解释，即除非在模型中被表示，安全状态不会改变。

5.5 其余安全服务

其余安全服务包含另外的网络安全内容。这些内容把单机与网络环境区别开来。其中一些内容着重考虑网络环境下逐渐增长的含义，另一些内容考虑单机上没有的问题。这些内容有些超出了 5.1 至 5.4 中各级的范围，有些缺乏 5.1 至 5.4 中各级所具备的理论基础和形式化分析。其余安全服务将上述内容以附加安全要求的形式表达，可以根据不同应用而变化，而且尽量减少它与 5.1 至 5.4 中各级的矛盾，一旦矛盾发生，都将加以说明。其余安全服务的服务可能由 NTCB 以外的机制提供。

5.5.1 范围

其余安全服务描述与 5.1 至 5.4 中各级不同的安全策略。5.1 至 5.4 中各级得到的等级不受其余安全服务的影响。必须先对每个部件或系统进行 5.1 至 5.4 中各级的评估，并以此作为其余安全服务的基础。其余安全服务的评估虽与 5.1 至 5.4 中各级有所区别，但目的类似，即把安全服务的可靠度提供给网络管理员和安全员，安全员将根据这些评估值来决定操作模式以及网络中可信的敏感信息区域。

网络负责人应标识由系统或部件提供的安全服务，其余安全服务评估这些服务。

5.5.2 准则形式

“其余安全服务”标准一般形式为功能描述、机制强度、保证和一段简短说明。

功能：安全服务的目标和实现方式包括特性、机制和实现。实现方式随不同应用环境的要求而有所变化。

机制强度：某实现方式完成目标的好坏程度，有时参数的选择，如检验和的位数、加密算法中序列的字符个数都会影响机制强度。

保证：功能是否可信的基础。包括对冲击的抵抗力、认可性和对旁越的抵抗力。通常情况下，保证是以理论、测试、软件工程以及合法性和认可性的分析为基础。这些分析是形式化或非形式化的，也可能是理论的或实用的。

例如需要考虑由于修改消息流而破坏通信完整性的保护措施，可以选择的功能有：仅发现（查出）错误、发现并改正错误。用户还可选择该保护是否能有效的发现奇数位错、突发的指定宽度错误或某未发现错误的概率。可选机制包括奇偶校检、纵向冗余校验（LRC）、循环冗余校验（CRC）和密码检验函数。CRC 的强度可由检测未发现错误可能发生的概率而得到，其值由使用的位数确定。除密码检验函数以外，其余机制均没有与安全相关的保证。因为既然算法已知，攻击者就可改变消息内容或重新计算未经密码处理的检验函数，当接收方计算检验函数时，并不会发现消息已被处理。经密码处理的检验函数可抵御这种处理。

5.5.3 评估等级

与 5.1 至 5.4 中的各级的有序等级(如 C1, C2, ……)相比,其余安全服务的评估是定性的。到目前为止,在其余安全服务中采取同样的等级划分既不可能也不必要,对于某些服务,其余安全服务的评估结果通常是:无、最小、中等、好四级。负责人未能提供的服务,一般是"未提供"一级。有时功能评估会限定在"有"或"无"两级。"无"一般指"未提供"安全服务。只能由 5.1 至 5.4 的各级和附录 A(补充件)评估每一服务的保证等级,因为服务的完整性依赖于 NTCB 的保护,表 1 表示了其余安全服务保证等级与 5.1 至 5.4 中各级评估等级的对应关系。

表 1

其余安全服务保证等级	5.1 至 5.4 中各级最小评估或附录 A(补充件)评估等级
最小	C1
中等	C2
好	B2

其余安全服务评估比较定性和主观,比 5.1 至 5.4 中各级评估有更大的可变性,然而,其余安全服务提供了与评估系统能力相关的有用信息,以及对指定应用环境的可用性,如功能、机制和保证是分开评估的,则每一项拥有一个等级。在某些情况下,机制强度可由技术结果定量表示(如:CRC 位数,使用的特殊函数等),这种强度定量的测量可能成为等级的基础。

其余安全服务评估比 5.1 至 5.4 中各级评估对技术进步更加敏感。其余安全服务评估具有敏感性的原因是:与 5.1 至 5.4 中各级的理论基础相比,其余安全服务的某些安全服务以实验为基础。进一步的研究可能会改变这种状况。随着水平的提高,高级评估的阈值也会提高。因此可能要对已评过的等级进行再次评估。

一般来讲,只对(偶然)事故和不能正常工作进行保护的机制,不能在最小级上达到机制强度的最小评估结果(即评估结果不能达到最小级)。机制必须提供对有意攻击(破坏)的保护才能达到好的评估结果。

网络产品的总结报告可能会包含按项列出的 5.1 至 5.4 中各级的评估等级和其余安全服务安全服务及其评估结果。例如:XYZ 网络的等级可能如下:〔B2,安全服务 1:最小,安全服务 2:未提供,安全服务 3:无,…,安全服务 n :(功能:好,机制强度:中等,保证:好)〕。在某些情况下,安全服务不在本标准范围内(如:COMSEC),由外部源得到的评估也可能反映在该报告上。在这种情况下,也可能使用与上述例项不同的术语。

5.5.4 与 ISO－OSI 体系结构的相关性

通过定义适用于开放系统之间通信保护中与安全相关的一般结构单元,可以扩展 ISO－OSI 的体系结构。OSI 安全附则的范围规定由参考模型提供的安全服务及相关机制的一般描述,并指出这些服务和机制在参考模型中的位置。

在 OSI 安全附则和其余安全服务之间有许多冲突。在编写本标准的过程中,OSI 文件也在更新,因此无法详细描述其间关系。所以下述说明可能在将来有所变化。

OSI 安全附则中标明的某些安全服务包含在本标准 5.1 至 5.4 中各级,其余的在其余安

全服务中。重点是应覆盖所有服务。本标准中安全服务及其实现机制与 OSI 安全附则不同。OSI 附则中，一般只说明功能，有时说明机制强度，极少提及保证，而在本标准中，尤其是 5.1 至 5.4，保证是主要因素。

OSI 安全附则的范围是有限的，OSI 安全与终端系统安装和组织所需的安全措施无关，除 OSI 中可见的安全服务外，GJB 2646 与本标准将 OSI 看作做为子集。

5.5.5 为特定环境选择安全服务

其余安全服务中列举的安全服务是用于某些特定环境下的特定网络上的服务。不过，在特定环境下，并不是所有服务都同等重要，而且，某服务的重要性在不同环境中也有所不同。网络管理员应决定在特定准则下某网络获得的等级是否符合应用环境。

例如，网络 XYZ 已获得以下等级〔B2，安全服务 1：最小级，安全服务 2：未提供，…〕。网络 K 的管理员可能不需要安全服务 2，因此 XYZ 虽然未提供这个安全服务，仍不影响选择它。如果网络 Q 的管理员认为安全服务 2 是必须的，就可能认为 XYZ 不合格；如果网络 P 的管理员认为安全服务 1 是至关重要的，而且等级至少为“好”，也可能认为 XYZ 不合格；而网络 R 的管理员可能只需要安全服务 1 为最小级，也就可能选择 XYZ。

再例如，在某应用环境里，如起落飞机或地下储存室中，在电话上窃取情报不构成威胁，这种环境下的 LAN 就无需加密，只利用物理保护就达到系统高安全状态，因为该系统处于被保护的直径内。在这种环境下，管理员认为有标号的和以标号为基础的访问控制能够提供充分保护，如果有足够的机制来保护标号的完整性，密码术是不必要的。再看个反例，如果 LAN 中包含通过未保护的空间进行信息传输，管理员可能要求使用密码的完整性保护机制。

5.5.6 一般保证实现方法

本条讨论适合于多种安全服务保证的实现方法。

协议的逻辑与防范措施的实现，在可能的情况下（如有工具存在），应使用形式化方法证明其正确与有效，否则使用非形式化方法。

为提供安全服务对不同形式外部冲击响应的保证，可使用若干种真实的或模拟的测试方法，其中有：功能测试、阶段性测试、穿透测试、压力测试、死锁和活跃等协议组成安全特性的协议测试。

另外，可信计算机所提供的运行环境对于增强一系列安全服务的保证十分有价值。在设计与实现这些服务时，可使用自主或强制访问控制以达到将无关的服务隔离。于是，复杂而易出错的服务的实现或由未评估供货商提供的服务的实现将不会降低同一部件上其他服务所不易实现的保证。另外，TCB 可保证网络信息最基本的安全与完整性保护不会由于其余安全服务标识不同的安全服务所削弱。

一般而言，保证是可以通过在 NTCB 分部的有序主体集上实现下述特性来达到，NTCB 分部的代码和数据都具有唯一的强制完整性级别以保护对 NTCB 的阻止和冲击。

其余安全服务机制里设计与实现的保证成功的概率与在 5.1 至 5.5 各等级的保证要求相关。下述服务的设计与实现，服务测试，设计说明与验证，配置管理和分布等因素，可为评估提供保证。

5.5.6.1 服务的设计与实现因素

评估等级为“中等”要求服务可以为分离的地址空间提供 TCB，而且服务内部由良好定义的大型独立模块构成。可以利用可用的硬件分离紧要保护的服务和不紧要保护的服务。服务的设计遵循最小特权法则，完整定义用户接口并且描述所有与服务相关的元素。

评估等级为“好”要求服务中采用分层、抽象和数据隐蔽技术，并利用系统工程的方法达到最小复杂性并分离紧要服务模块。

5.5.6.2 服务测试因素

在安全测试方面，“最小”评估等级表示已完成服务测试，并可如系统文件所示工作，可以保证没有明显途径允许未授权用户旁越，从而冲击系统界限和客体。测试应查出明显的缺陷，这些缺陷能造成服务所使用的数据被外部软件修改或错误的服务修改。

“中等”评估等级表示，除满足“最小”等级因素外，还应组织一个能透彻理解指定文件的小组，该小组应详细分析和测试设计文件、源代码和目标代码，并发现所有可能破坏 NTCB 以外的关于主体服务的设计和实现的缺陷。“中等”级别的系统应在某种程度上对故意冲击有抵抗能力。“中等”级别的系统应该改正所有已发现的错误或使之不再发生，并应重新测试，表明这些缺陷确已改正而且不再产生新缺陷。

评估等级为“好”表示除满足“中等”级别的因素外，系统应对故意冲击有更大的抵抗力，并且不存在设计缺陷，测试中只允许出现极小的可修正的实现中的缺陷，对这种缺陷应说明其存在的合理理由。测试以源代码为基础。

5.5.6.3 设计说明与检验因素

在设计说明与检验方面，“最小”评估等级表示在系统的生命周期内始终维持一个服务特性的非形式化模型。“中等”级别没有定义附加的要求。

评估等级为“好”表示除了在系统生命周期内维持一个服务特性的形式化模型外，还应表明与其原则相一致，应该提供一份与安全相关代码的描述说明，并要求完整而精确地描述异常错误信息及其影响。

5.5.6.4 配置管理因素

在配置管理方面，“最小”评估等级表示在开发与维护服务的过程中，始终应该有配置管理系统，以便对说明书、其余设计数据、实现文档、源代码、目标代码的运行版本、测试混合物、测试代码和文档的修改加以控制。

“中等”评估等级表示：配置管理系统应保证始终维持当前版本的文件和代码的映射，并将该新版本与旧版本比较以保证只对相关代码进行了修改。

评估等级“好”表示配置管理系统覆盖整个生命周期，同样适用于所有支持服务的固件和硬件，而且使用技术上的、物理上的和过程的保护等手段，以便防止对主拷贝或产生服务的所有资源拷贝的未授权修改或破坏。

5.5.6.5 分布因素

目前在此方面没有“最小”和“中等”评估级别。

评估等级为“好”表示控制和分配设施可以保持描述当前服务版本的主数据和当前版本代码的主拷贝之间映射的完整性。整个过程都应保证软件，固件和硬件的修改符合主拷贝所表示的分布。

5.5.7 支持性基元

本条描述适合于多种安全服务的机制与保证技术。有关这些技术的详细内容可参见5.5.8条。

在许多安全服务中，密码术是常用的机制，协议是网络的基础。本条讨论的内容将作为5.5.8条的基础。

5.5.7.1 加密机制

5.5.7.1.1 功能因素

加密是保护数据免受泄露和修改的措施。通过它的使用，可防止消息内容、流量分析的泄露，也可发现消息流的修改、拒绝消息服务和伪装。例如描述在通信结构中使用编码技术的ISO文件，现已成为美国ISO体系中密码术安全保护的成员。在可能发生线路窃听的环境里，加密是最重要、使用最广泛的安全机制，某种程度上它已不象是服务了。

加密机制的使用，导致了密钥管理(如人工管理或以密钥分配协议和密钥分配中心管理)的出现。

5.5.7.1.2 机制强度因素

用数学方法和统计分析能得到密码术密码的强度，它主要依赖于未授权解码工作函数的结果。在许多情况下对这些分析进行分类，只有达到最高级分类数据时(这些数据可能由机制保护)，其结果才可用。

当在网络中使用加密机制时，它与网络协议一道来防止泄露。使用密码技术时密码的强度、协议逻辑的正确性以及实现的充分性是数据可信性强度的首要因素。加密算法由国家和军队安全主管部门标识才通过或不通过，通过时给出该算法对所保护信息的敏感度。

5.5.7.1.3 保证因素

加密技术的分析与作为GJB 2646可信基础的形式说明与检验相比区别甚大。这种分析大部分都要分类。最后，由国家和军队安全主管部门提供加密技术的保证。一般情况下不分级表示保证度。

5.5.7.2 协议

5.5.7.2.1 功能因素

协议是决定网络间实体通信行为的规则和格式。其设计与实现对于网络系统和子系统之间信息能正确、有效和高效的传输起关键作用。

许多网络安全服务由协议来帮助完成，协议的失效与缺陷将会引起由协议支持的服务的失效与缺陷。

若在协议中存在某一级设计上的错误或逻辑上的缺陷，表现为某种形式的拒绝服务，使之在正常的操作环境下丧失其功能。这级错误包括死锁、活动阻塞、未说明的接收、缺乏活动性和不可执行的交互。

另一设计要求是不论发生哪一种随机破坏或使通信发生困难时，如噪音、消息丢失和消息被改组，协议都必须保持能工作。注意，大部分网络是分层设计的，每一层基于协议的服务都是通过引用下一层服务而实现的。也就是说如果某一层已提供对某种通信困难的保护，它的上层就无须再将该保护列入设计中。

第三种设计是在发生窃听状态这类故意破坏时，协议仍需继续工作。这类协议要有对MSM的防范措施。

5.5.7.2.2 机制强度因素

协议的缺陷可能出现在设计阶段，也可能出现在实现阶段。实现阶段的缺陷意味着协议说明与软件实现之间不一致。

5.5.7.2.3 保证因素

实现的正确性保证受技术制约，如设计说明与验证和测试等。

理想状态是可以证实所有的网络协议功能都已正常工作。然而，目前进行大量代码的测试是过分昂贵的，因此，应把验证代码控制在最小范围。较为可行的方案是将诸如TCP这样复杂的协议分割成可信的部分(如实现安全相关功能的软件)和不可信的部分(其余软件)。于是只需验证与安全相关部分达到第一部分的要求即可。然而，有一点须加以考虑，即如何标识协议的可信部分，如何对之加以保护。

保证协议设计正确性的方法有使用面向特殊协议问题的工具和技术。任何一种正式的方法或测试手段或两者都可以使用。

仅当把协议建立在某种可理解的模型或技术的基础上时，有可能获得设计正确性的保证。此时需要该模型或技术能解决可能出现的问题。由于实际的协议可能与发行的版本间有区别，所以这样的保证在某种程度上会下降。

5.5.7.2.3.1 形式化方法

协议的定义和合法性的形式化技术适合于对实际协议进行验证，以证明其设计中不存在死锁、活锁和不完整性。如果当前的形式化工具不充分或负责人不愿使用非形式化工具，在协议说明与验证的评估中应说明所使用的验证工具。

协议说明与验证的形式化方法主要基于有限状态机概念，将其加以扩展来表示网络中并发和通信特性。串行通信和PERI网可作为协议的基本模型，基于该模型的实验性自动验证工具也已开发完成。随着保证所需的设计要求不同，也可使用不同的模型和工具。

在协议模型及其实现允许分层的情况下，功能模型、证明、示范证明以及变量都能够可选地适合于某一层或相邻几层。一般来讲，某一层获得的协议保证与下一层协议保证有关或以其为前提。

5.5.7.2.3.2 测试

协议测试是除形式化验证以外保证协议正确性的另一方法。目前已使用协议测试来验证如X.25，TCP，TP4等标准实现的一致性，并已取得相当的成功。

测试类型可分为一致性测试和穿透测试。完成这些测试的目的是获得协议能够正确操作的一定程度的信心。

测试的目标是发现可能引起协议不能完成其功能的设计和实现上的缺陷，并依此来决定MSM的防范措施是否有效。测试试图发现所有逻辑缺陷，如死锁、活锁、未说明的接收、解活锁，不可执行的交互等。应当修改已发现的缺陷并重新对其测试，来验证该缺陷已不再发生而且也未引入新的缺陷。在测试中不存在设计缺陷，只有极少的可改正的执行错误，并且对这些错误应说明合理的原因，这时才能作出测试是否成功的结论。测试的基础是测试说明和源代

码。

应充分分析并测试协议对正式和非正式数据类型消息的响应。并在可控制的环境或扩展环境中，进行正常模式和降级模式的测试。

5.5.8 文档

其余安全服务的各类文档标题与 5.1 至 5.4 中各级相同。由这两部分产生的文档，可以合并也可以独立成章，视负责人的需要而定。

5.5.8.1 安全特性用户指南

在用户文档的摘要、各章条和手册中应描述这一部分安全服务使用指南及其与用户的交互方式。

应在该用户文档中描述全局级安全服务、每一部件的用户接口及与用户的交互。

5.5.8.2 可信设备手册

为维持网络安全，在网络和部件子系统管理者的手册中应标识出控制功能和特权；应标明有关安全的操作者和管理者的功能；应提供一致和有效使用网络安全服务的方法及服务间交互的方式；应标识受控制设备的过程、警告和特权。

应标识提供安全服务的软件模块；应描述修改源代码后用来生成新的安全服务目标模块的过程；应描述保证网络从安全状态启动的过程；应描述运行发生故障时，可安全地重新启动的过程。

在说明与过程中应包括：

a. 如何向网络中增加新部件。

b. 当某部件阶段性地离开网络(如：被破坏，或断开连接)后再次上网的情况。

c. 增量性修改，即应标明网络中哪个安全服务可能会变化而其余不变化。

应标明物理上的和管理环境上的控制。网络中任一安全性假设均需说明，例如对所有通信链都必须有物理级上的保护。

5.5.8.3 测试文档

应提供一份测试文档来描述测试计划和测试过程，说明安全服务的测试方式和安全服务功能的测试结果。

在测试计划中应说明测试是如何进行的；还应标明被评估系统组成部分以外附加的测试部件；描述此类部件相关的测试功能，及其与评估系统组成部件的接口；说明测试可以覆盖所有网络安全策略；亦应包括网络配置与大小。

如附录 A 所示，被评估的实体可能是个网络子系统，只有增加另外部件，才能形成网络系统。在这种情况下，测试文档必须增加结构定义。因为没有该网络子系统的结构说明，无法在评估时验证测试计划的合法性。

5.5.8.4 设计文档

在设计文档中应提供网络保护策略说明，解释这种保护策略如何转化为所提供的安全服务，描述安全服务接口并说明安全策略。

在系统描述中，通过说明网络中的安全服务及其支持网络安全目标的合作方式，来说明网络的体系结构和设计。如果网络支持一组安全策略并允许不同策略的部件之间进行通信，则

应定义策略间的关系。

5.5.9 特殊服务

本条描述网络提供的特殊安全服务。描述涉及的网络安全，每一项所涉及的准则以及每一准则的评估范围。

5.5.9.1 通信完整性

通信完整性是下述一系列安全服务的总称。这些服务都是关于计算机通信网络内数据传输的精确度、可靠度、不易腐蚀度以及成功的概率。

完整性是个重要概念，然而，在使用它时却有许多冲突与不一致处。它可以描述诸如一致性、精确性、并发性、数据恢复、修改访问控制(写、增加、删除、修改)以及信息的可靠性等有关进程读写操作的过程。

实现通信完整性的机制与实现自主和强制访问控制的机制极为类似。在 5.1 至 5.4 中的完整性是关于访问控制的，主要是主体修改客体的能力。这一点与其余安全服务不同。

5.5.9.1.1 鉴别

5.5.9.1.1.1 功能

网络应保证数据交换发生在已确定的一对实体之间，还应保证数据资源是已声明过的。如果这一服务由面向连接的组合提供，就称之为对等实体鉴别；如果由无连接组合提供，则称为数据源鉴别。

对等实体鉴别可以防止在错误标识后创建一个对话连接或收回一个已经逻辑初始化的对话队列。

鉴别通常在身份标识之后将已声明的身份标识合法化并提供对欺骗性交互的保护。网络应该对身份标识，鉴别和授权信息提供保护。

适合于鉴别机制的可用技术有：

a. 实体所知的某事(如：口令字)；

b. 密码术；

c. 使用实体特点和(或)拥有物；

将上述机制与 N 层端对端协议一起可以提供对等实体鉴别。

如果欲把信息与指定源相连，必须给信息增加有关显性的或隐性的身份标识信息。针对这一问题指定的方法包括认证可变通信信道，或使用用户唯一的密码鉴别。

如果使用密码进行鉴别服务，则可用译码和签名机制实现。在传统的密钥加密系统中，带有密钥消息的加密自动隐含在数据源鉴别中，因为只有密钥的持有者才能决定消息加密后的形式。然而，由传统的密钥加密系统提供的鉴别，虽可以使发送者和接收者免受第三者攻击，却不能保护这两者中某一方的故意欺骗。因为接收方知道密钥，他可以产生伪装成由发送方传来的加密形式的消息。如果发送方与接收方中有一方不诚实，就需要增加鉴别机制。

在公开密钥加密系统，消息的保密性与消息发送方鉴别机制在功能上是独立的。在取得鉴别之前应先利用发送方的密钥将消息解密，以确保消息源正确，但并不隐藏消息。如果既要求鉴别又要求保密，必须使用公开密钥和签名机制。

基本等级：有或无。

评估范围：无或有。

5.5.9.1.1.2 机制强度

口令机制所提供的安全性在很大程度上取决于密码的选择与保护。由密码提供的安全性依赖于密码的组成、生命期和对泄露和替代的保护。

当使用密码技术时，可以将“握手”协议与“活跃”保证过程相结合以阻止故意破坏与应答。“活跃”保证过程可由以下方式提供：

a. 同步时钟；

b. 两或三种握手方式；

c. 由数字签名和(或)证明机制提供的不抛弃服务

密码强度、协议逻辑的正确度和实现的充分性是利用密码机制进行鉴别的强度的三个首要因素。参见“加密机制”。

等级基础：口令机制。密码机制的强度由国家和军队安全主管部门提供。

评估范围：无到好。

5.5.9.1.1.3 保证

评估保证等级的基础是保证正确地抵抗鉴别威胁，并精确达到控制目标。

这一保证可通过分析鉴别交换机制强度获得。这其中包括口令机制和(或)密码算法分析，以及“握手”协议中死锁、活跃等其他安全特性的自动协议测试。

实现保证的许多方法与其他安全服务相同。

等级基础：见“一般保证实现方法”

评估范围：无到好

5.5.9.1.2 通信域完整性

通信域完整性表示每一通信域对未授权修改的保护。两个广为人知的域是协议信息域和用户数据域。每一协议数据单元(PDU)都包括协议信息，而用户数据可有可无。

还可以划分并表示其他的域，有些通信系统将这类域称为控制域和优先权域。不失一般性，本节认为所有域均包含数据——不论是协议信息或是其他已标识域的信息。为方便起见，把通信域完整性视为数据完整性。数据完整性可由可选域基提供，包括网络体系结构、网络管理或用户。

应加以说明的是，在分层协议中，第 N 层协议信息与用户信息的组合视为第(N－1)层的所有用户数据，应着重注意消息定义以及消息与 PDU 之间的关系。每一 PDU 可能由一条独立消息构成，也可能一组 PDU 由一条消息构成。

5.5.9.1.2.1 功能

数据完整性可抵抗主动冲击并保护数据免受未授权修改。网络应保证信息从源到目的地的正确传输(不论中间连接点的数目有多少)。网络应提供对处理设备失败和个人或进程对数据进行故意的未授权的修改的保证。完成代码格式转换的协议应保证数据和控制信息的完整性。

网络应具备自动检测并报告超出阈值的错误。

由于通信可能受到阻塞/电子欺骗、线路与结点停机、硬软件失效、主动电路窃听等攻击，

因而应具备有效的防范措施以处理可能发生的通信危害。防范措施可能包括策略、过程、自动或物理控制、机制和协议等手段。

等级基础：数据完整性服务是根据对完整性危害的检测能力而评估的。有关特性与评估等级如下所述：

功能评估等级为“最小”应满足：

a. 单个无连接 PDU 的完整性，由已接收的 PDU 是否被修改过而确定；

b. 在无连接 PDU 内部已选域的完整性，由已选域是否被修改过而确定。

功能评估等级为“中等”，除“最小”级要求的以外，还应满足以下任一条件：

a. 在连接上传送已选域的完整性，由已选域是否被修改、插入、删除或重放而决定；

b. 协议层连接上所有用户数据的完整性。此项服务可在整体 PDU 内检测出对任一 PDU 的修改、插入、删除或重放，但不具备恢复功能。

功能的评估等级为“好”应满足：

协议层连接上所有用户数据的完整性。此项服务可在整体 PDU 内检测到任一 PDU 的修改、插入、删除或重放，并能对其进行恢复。

评估范围：无到好。

5.5.9.1.2.2 机制强度

策略、过程、自动或物理控制以及机制和协议可以保证数据不受意外的随机错误和未授权消息流修改的破坏，如修改、替换、重排序、重放和插入。消息流修改(MSM)的防范措施应加以标识并且有效，可选择适当强度的技术来抵抗 MSM。

发生未发现错误的概率是机制强度的象征。网络应具备对超出网络指定要求的通信错误或失效的自动的测试、检测、报告和(或)恢复的能力。

等级基础：如果网络使用加密机制，它将与网络协议一起防止未授权的数据修改。密码的强度、协议逻辑的正确性、实现的充分性是决定使用密码技术的数据完整性机制强度的首要因素。详见“加密机制”一节。

评估范围：无到好。

5.5.9.1.2.3 保证

等级基础：保证表示正确实现数据完整性防范措施，并正确而精确地达到控制目标的成功的概率。

评估范围：无到好。

5.5.9.1.3 否认服务

5.5.9.1.3.1 功能

否认服务可保证数据的装载和(或)接收。

这项服务可防止发送方不承认合法的消息或接收方拒绝接收。网络应提供下面两种功能或其中之一：

a. 向数据接收方提供数据源证明，以防止发送方否认发送过的消息及内容。

b. 向发送方提供发送消息的证明，以防止接收方事后否认曾接收的消息及内容。

等级基础：有或无上述两种功能。

评估范围：无或有。

讨论：数字签名技术适用于否认服务，数字签名由以下两个处理过程确定：

a. 标记一个数据单元；

b. 验证一个已标记的数据单元。

标记过程用加密数据单元或产生数据单元密码的检验函数来完成标记处理。这两种技术将标记者私有信息作为私用密钥。

验证过程将通过使用公用进程和信息以确定签名是否由标记者使用私用密钥而产生。

签名机制的不可遗忘性和可裁定性很重要。即签名只能由标记者的私有信息产生，一旦标记者否认已标记的消息，仲裁机制应可以解决消息标记者与接收者之间的不一致。

通常将数据签名分为以下两种：真实签名和仲裁签名。使用真实签名机制时，由发送者标记的消息直接传送至接收者，后者验证其合法性与鉴定性。使用仲裁机制时，发送者的签名消息通过仲裁(或视为一个公证处)传送至接收者，在这种机制中需要公证机制。

公开密钥加密系统和私用密钥加密系统均可用来产生数字签名。当消息 M 用私用密钥加密系统标记时，该签名是与 M 连接并与之一同发送。在公开密钥实现机制中，标记消息 M 时，应该先用密钥使之变形。这样，签名存在于变形后的消息中。

5.5.9.1.3.2 机制强度

等级基础：否认服务的强度和成功的概率由以下三种实施密码机制成功的概率决定：数字签名机制、协议逻辑正确性、协议实现的充分性。

评估范围：无到好

5.5.9.1.3.3 保证

等级基础：保证正确实现否认服务及达到控制目标成功的概率。

通过对协议逻辑和数字签名机制的分析来证明保证的正确性和有效性。有条件时用形式化方法，否则用非形式化方法。

评估范围：无到好。

5.5.9.2 拒绝服务

保证通信服务的可用性称为服务，而与之相对的拒绝服务称为威胁。不过，通常都延用传统的称法“拒绝服务”。

拒绝服务的检测度依赖于数据完整性检验或检测机制。其他如数据排序、修改、丢失和重放(如序列号、帧计数)等机制也是拒绝服务的防范措施。

当发生吞吐量低于预设的阈值或不能访问远程实体时，就会引起拒绝服务。基于公平机制的用户不能使用资源，也会引起拒绝服务。应考虑使用优先级或类似机制来决定公平性。如果某连接是活跃的，拒绝服务可通过最大等待时间(MWT)或预设的最小吞吐量测出。然而，当某连接处于静态时，位于联结一端的协议实体无法测出与之相对应的实体所发出的下一个包将何时到达，于是就无法测出拒绝服务攻击，因为拒绝服务可能已完全切断了实体间传送包的流程。

拒绝服务一词应包括网络中所有的服务。在下面所讨论的特殊服务中，网络应依赖机制强度来发现、恢复和(或)抵抗拒绝服务。应利用 MISSION 模型，威协模型，生命周期模型及

面向服务模型来具体对待由网络指明的特殊情况。网络管理员或负责人应决定网络中拒绝服务的要求并由此制定出相应的服务准则。

5.5.9.2.1 操作连续性

5.5.9.2.1.1 功能

安全特性可抵抗拒绝服务的外部冲击，而每一特性的目标如下所示：

a. 在网络部件上(如网络节点、连接和控制功能)使用主动或被动的备用件或其他方式的冗余设计可增强可靠度，减少单点故障，增强存活度，并提供剩余能力。

b. 重组能提供网络软件维护的功能，该功能将重组后的软件分布在各网络节点上，并可在移走失败部件后，进行重新初始化和重构，利用备用件进行替换可以隔离和(或)限制网络故障，可以对网络部件的增加和删除进行调整，并隔离已检测到的错误。

c. 由于分布式网络的分布性和灵活性，在一个或几个网络控制部件被破坏后，分布式网络可以减少网络失效的可能性，也可响应瞬时应急要求(如突发的信息量剧增、快速恢复)的灵活控制，可以改善网络拓扑突然改变的响应能力。这样，就可增强存活度及操作的连续性。这其中可能会用到优先权和可剥夺的通信管理技术。

d. 容错机制可处理网络故障，并保持网络操作的连续性。它主要包括：错误或故障检测、应付故障措施、破坏度评价(分析故障后果)、错误或故障恢复、部件或段失效恢复以及网络失效的恢复。

e. 安全控制应包括：创建逻辑子集的完整性，分隔非等级化的强制访问控制目录，保护控制信息免受线路窃听的破坏。

等级基础：网络应保证最小指定连续服务的等级。下述为最小级别要求；

a. 及时检测低于预先指定最小级别的降级服务，并及时报告操作员。

下述服务为“中等”级别：

b. 当个人或进程未授权修改数据而引起设备操作失败时，仍可继续服务。可使用冗余、备份设备或其他方法在出错时进行恢复。可以降级服务，也可以调整服务的优先级。

下述服务为“好”等级：

c. 与 a 相同，但可提供自动的自适应性。

评估范围：无到好。

5.5.9.2.1.2 机制强度

维护网络操作是基于机制的，而机制的健壮程度可能随着网络负载的增加而下降。即使是模拟负载时的下线操作，机制也可能无法保证足够强度的测试。

精确分析可保证算法的正确性，因此可处理“内部故障”，如由资源分配策略或机制实现错误所诱发的部件、段或系统故障；除此之外，还应具备应付“外部冲击”的防范措施。

等级基础：针对上述每一拒绝服务特性，都可以按网络拒绝服务的强度来指定从无到好的等级。例如提供容错机制的主要途径有：

a. 错误或故障检测；

b. 故障处理；

c. 破坏程度评价(故障后果分析)；

d. 错误或故障恢复；

d. 部件或段失效恢复；

f. 网络失效恢复。

评估范围：无到好

5.5.9.2.1.3 保证

保证是提供拒绝服务防范措施正确实现的成功概率，并保证每一特性的目标正确实现。

通过分析网络中资源分配策略或机制的薄弱性或异常，可获得保证，网络可使用不同的形式化模型，如排队理论模型、等级服务模型或资源分配模型(这些模型可用来分析死锁、活跃或其他安全特性)。

等级基础：为保证网络可以响应不同形式的拒绝服务，可采取以下方法：

a. 模拟；

b. 测试：功能性的、阶段性的、入侵性的；

c. 极端情况下测试。

分布式可作为一般保证因素之一，它可提高软件使用时的可靠性，也可提高新软件使用的适应性以及失效恢复时的保证度。另外，闭合开发环境也可提高保证度。

评估范围：无到好。

5.5.9.2.2 基于拒绝服务保护机制的协议

5.5.9.2.2.1 功能

防范拒绝服务的机制通常是基于协议的，其中可能采用测试和检测技术。任何可用于通信的服务应该使用已有的通信协议机制以避免增加网络开销。拒绝服务机制会增加开销，因此，可能给网络性能增加负作用，加权功能的益处可抵消最终性能代价。

例如，为检测拒绝服务的吞吐量，可利用一进程去测试在输出队列中两对实体的传输率。用测得的传输率与预测的最小值比较，可获知拒绝服务的发生并予以警告。

再例如，在指定的时间内使用对两对实体间故障进行检测的协议，来决定远程实体对协议的响应能力。

使用请求应答协议，如交换“你在那儿吗?”一类的信息，可以在静态连接时检测拒绝服务的发生。请求一应答机制阶段性地发送“你好”和“你在那儿吗”消息，以保证两对实体间路径是开放的，应对这类机制加以保护，使其免受可选信息传递的破坏。可以利用对请求——应答机制的响应及响应时间来决定某远程实体的“可用性”，并可检测到拒绝服务的发生。

请求——应答机制一旦遇到硬件故障和(或)不正常负载，就可能使网络失效。有时不同网络互连时，还可能不兼容。应尽可能测量任何脱机以防止拒绝服务的发生。

等级基础：可以使用基于机制的协议数目做为评估基础。若仅提供一种机制，功能可被评为最小；2～3 种机制为中等；3 种以上为好。

评估范围：无到好。

5.5.9.2.2.2 机制强度

等级基础：网络协议的健壮程度随负载加大而下降。下线的模拟负载或操作中的测试，以及精密分析可保证协议在对付“内部故障”时的正确性，而应付“外部错误”是加强机制强度

的正确途径。

评估范围：无到好。

5.5.9.2.2.3 保证

保证是拒绝服务的防范措施及其每一项特性能正确实现成功的概率。

等级基础：可通过分析使用不同形式化模型的网络协议的薄弱性和异常行为来获得评估保证，这些模型包括：排队论模型、分层服务模型、Petri 网或资源分配模型，可以用它们来分析死锁、活跃及其他安全特性。

为保证网络能对不同形式的外部冲击做出反应，可采用下述方法：

a. 模拟；

b. 测试：功能性的，阶段性的，入侵性的；

c. 极端条件下的测试。

分布式可作为一般保证因素之一，它可提高软件使用时的可靠性。也可提高新软件使用的适应性以及失效恢复时的保证度。另外，闭合开发环境也可提高保证度。

评估范围：无到好。

5.5.9.2.3 网络管理

5.5.9.2.3.1 功能

基于系统或消息完整性的拒绝服务防范措施通常有两方面：一是相关通信协议，另一是相关的网络管理(和维护)。在大部分部件上，这两方面独立进行。

网络管理与维护主要针对检测网络健康或错误等可能引起拒绝或降级服务的操作。仅凭吞吐量不能测知其正常的功能。超出承受力的负载、通信量突然加大、重放、因线路噪音而引发的协议重试，都可能将服务降至可接受级别之下，并引起可选的越界管理协议。在现存的协议参考模型中没有很好的描述。

拒绝服务可能引起一对以上的实体连接中断，因此监测与修复工作由相关的网络管理完成。一对实体检测到的潜在的拒绝服务由这些实体上的管理功能层报告。确定拒绝服务冲击由应用管理功能层完成，修复操作由系统管理层完成。

等级基础：有或无

评估范围：无或有

5.5.9.2.3.2 机制强度

网络操作的维护基于机制，而机制的强度随负载递减(如修改例行程序表)。

等级基础：网络中控制的完整性和充分性是解决拒绝服务的关键。在应付“内部错误”(如由于资源分配或机制实现中的错误引起的部件、段或系统的失效)时，不仅可以使用精确的分析来保证算法的正确，还可以使用对付外部冲击(如物理冲击或破坏网络控制)的防范措施。

以上述特点为基础，可为每一级容错机制分配等级，而针对网络提供“容错机制”的强度，也可得到一整体级别。

评估范围：无到好

5.5.9.2.3.3 保证

等级基础：可通过分析使用不同形式化模型的网络协议的薄弱性和异常行为而获得评估

保证，这些模型包括：排队论模型、分层服务模型、Petri 网或资源分配模型，可以用它们来分析死锁、活跃及其他安全特性。

分布式可作为一般保证因素之一，它可提高软件在使用时的可靠性，也可提高新软件使用的适应性以及失效恢复时的保证度。另外，闭合开发环境也可提高保证度。

评估范围：无到好。

5.5.9.3 损害保护

损害保护是所有安全服务的总称。这些服务，如下所述均与计算机通信网内一对实体间的安全性和信息传送的泄露相关。物理保护，如受保护线路可以提供传送安全。网络管理员或负责人应描述物理的、管理的和技术安全的折衷。本标准只讨论技术安全。

5.5.9.3.1 数据机密性

5.5.9.3.1.1 功能

数据机密性是使数据不受未受权泄露的防范措施。数据机密性主要针对防护线路窃听的威胁。主动攻击是侦察链上传输的信息，而且将信息内容泄露给未授权的用户是主要的危害方式。

可采用加密机制来保护信息内容不泄露（见“加密机制”）。密钥分布的粒度是方便性和保密性的折衷。在每一分部的每一安全级上使用一个独立密钥能达到良好粒度，在某时间段内所有的分部使用同一密钥，只能达到粗略粒度。

网络应保护数据不受未授权的泄露。机密性指以下几方面：

a. 在某指定协议层连接中所有用户数据的机密性。注意，由于用户和层的原因，并不需要保护所有的数据。

b. 某独立的未连接的数据报中所有用户数据的机密性。

c. 协议数据单元中用户数据可选域内的机密性。

等级基础：每一特性的有或无。

评估范围：无或有。

5.5.9.3.1.2 机制强度

物理保护和加密是保护数据免受损害的基本技术。通过使用这些技术，可以防止消息内容和通信分析的泄露。

等级基础：数据机密性评估不在本标准范畴。评估组织将按照他们自己的规则与过程评估与指定环境相关的机制。

评估范围：被确认保护的数据安全级

5.5.9.3.1.3 保证

等级基础：保证是使数据机密性不受损害的防范措施成功的概率，以及保证每一特性能正确而准确地实现的概率。黑盒子是 TCB 为实现高性能数据机密性的应用实例。

许多保证数据机密性的措施与其他安全服务相同。详见“一般保证”。

评估范围：无到好。

5.5.9.3.2 通信流机密性

5.5.9.3.2.1 功能

通信流机密性保护数据免受未授权的泄露。通信分析包括分析消息长度、频率及协议部件等，它可能会引起信息泄露。

通信流机密性可屏蔽频率、长度以及通信实体间源——目的的通信模式。加密可以在传输层以上有效地防止泄露，也就是说，可以隐藏过程与应用程序但不是主机结点。

OSI 附则说明："通信填充机制可针对通信分析提供不同级别的保护。这种机制只有在通信填充机制由机密性服务保护时才有效"。

等级基础：无或有

评估范围：无或有

5.5.9.3.2.2 机制强度

物理保护、加密及通信填充是通信分析的主要防范措施。

等级基础：评估通信机密性机制超出本标准的讨论范围。评估组织将按照他们自己的规则与过程评估与指定环境相关的机制。

评估范围：被确认保护的通信安全级。

5.5.9.3.2.3 保证

等级基础：保证是使数据机密性不受损害的防范措施成功的概率，以及保证每一特性能正确而准确地实现的概率。黑盒子 TCB 为实现高性能通信机密性的实例。

许多保护通信机密性的措施与其他安全服务相同。详见"一般保证"。

评估范围：无到好。

5.5.9.3.3 可选路径

5.5.9.3.3.1 功能

路径控制是在选路径过程中的应用规则，用以选择或避免网络、链路或延迟。路径可动态选择或预先设定，因此只能使用物理上安全的子网、延迟或链路。终端系统在检测到连续的攻击后，可能希望网络服务员再建造一条不同的连接路径。安全策略能禁止带有标号的数据通过某些子网、链路和延迟。同样，连接的初始者（或无连接数据单元的发送者）可能对某些路径提供警告并指定避免某些子网、延迟或链路。

例如：有全球性法律和网络管理策略控制个人隐私权，加密和跨界数据流。终端系统用户可以指定信息流不能通过的国家。

等级基础：无或有

评估范围：无或有

5.5.9.3.3.2 机制强度

等级基础："支持性基元"中所讨论的因素。

评估范围：无到好。

5.5.9.3.3.3 保证

等级基础：同"一般保证实现方法"

评估范围：无到好

附录 A
网络部件评估
（补充件）

A1 目的

本标准的 5.1～5.4 条阐述了军用计算机安全评估准则(GJB 2646)，它适于评估作为单独系统且具有单独可信计算基(在网络中称为网络可信计算基 NTCB，它可以从网络部件中逻辑上或物理上划分出来)的计算机和通信设备。因为网络是构成具有独特技术特性的计算机系统重要的和可识别的子集。因此可以专为它们制定可信计算机安全评估准则。

这种网络观点可以延伸为：一个安全网络代表了安全部件的一种组合。这种观点提示我们，评估网络的方法是将系统划分成部件，评估每个部件以确定其相关的安全特征，然后评估由这些部件构成的组合件，得到该网络的总的分类等级。这种方法在两方面有助于鉴定总的网络评估等级：

a. 允许网络部件内部和自身的评估不支持 GJB 2646 要求的所有策略(这将有益于对任何使用这些已被评估的部件构成的网络的总体评估)。

b. 允许在不同的网络中重用这些已被评估的部件，不需要重新评估它们。

这种评估方法并不否认本标准 5.1～5.4 条的任何内容，5.1～5.4 条描述的是一种安全网络的全局特征。为了在在标准内统一和一致，网络说明依据网络是将 GJB 2646 在系统级基础上应用于计算机系统的实例这种观点来进行的。这使得 5.1～5.4 条与 GJB 2646 密切相关，因为在 GJB 2646 下的基本结构模型，即具有单独可信计算基(TCB)的系统结构模型并未改变。

该附录对评估安全网络的单个部件提供指南。该部件评估指南概括了 5.1～5.4 条和 5.5 条所阐述的整个网络说明及其应用，目的是支持对网络或网络子系统产品的最终评估，通过使用 5.1～5.4 条的说明，最终获得一个总的网络等级。注意，5.5 条应用于部件时并无更进一步的说明。在本附录中并未隐含指明所有的网络必须由这些已被评估的部件组成：完整网络可以作为整体用 5.1～5.4 条提拱的系统说明进行评估。然而，在许多实际情况中，该附录所提供的技术应首先考虑单个部件，然后再考虑由这些部件构成的可评估的整体，并在 5.1～5.4 条的规范引导下实际进行系统的评估。

当应用分部的观点时，可信系统的设计者和评估者必须面对三个主要的问题：

a. 应如何分部网络使得对单个部件的评估支持整个网络的最终评估；

b. 评估每个部件时应采用什么评估准则；

c. 应怎样评估由已被评估的部件构成的组合件。

第一个问题将在附录 B(补充件)中论述。其余两个问题将在本附录中说明：第一个在 A1.1 及 A3 节中解释，在 A2 中将说明另一个。

A1.1 介绍了一种部件分类方案，用来处理基于子策略元素的部件，同时也处理单个部件的分级结构。

A2 中对如何组合已被评估的部件提供技术支持和指标，以获取组装后的网络的特定的系统分级。该指标根据所支持的策略元素表示每个部件，这些策略元素可以归纳为四种广义的策略范畴：即强制访问控制、自主访问控制、身份鉴别与验证、审计支持。

依据本标准 5.1～5.4 条中明确说明的网络规范，A3 中提供了特定的评估指标，允许在可信网络中先对单个处理部件分级。这部分内容是根据 A1.1 中定义的部件类型进行组织的。对每种部件类型都可以提供 5.1～5.4 条中适用的说明并按照分类等级进行组织。

A1.1　部件分类法和分级结构

一个处理部件被看作一个较大网络系统的一部分还是一个独立的计算机系统，最主要的区别是若作为一个独立的系统，则必须满足某特定等级的所有的 GJB 2646 要求：对于策略要求(即系统必须支持什么样的特性)，GJB 2646 的目的是在系统范围内执行在操作上的一组特性。然而，在较大系统中，由部件支持的与策略相关的特性的集合不必是独立系统所要求的全集，即系统中不被某个部件支持的特性可以由另一个部件支持。当给某种产品分级以获取其作为一种网络部件的潜在用途时，很想从理论上准确表示其安全性特性，事实上，如果能够表明该部件是属于某一特定类型(即表示出该部件支持的一般策略元素)，属于某一特定的评估等级(它表明提供给每个支持特性的保证程度)和目标结构，结果就是令人满意的。目标结构的描述将包括必须由其它设备提供服务的描述。

为了限制部件类型的数目，我们将由 GJB 2646 定义的 A1 级系统中与策略相关的特征集分割成相对独立的四类，分别支持强制访问控制(MAC)、自主访问控制(DAC)、审计和身份鉴别与验证。(在本附录后面的各种表及文字中，这些类属被分别冠以字符缩略词 M、D、A 和 I)。

一种给定的部件可由部件提供者或由网络提供者要求提供 M、D、A 和 I 功能的任何组合。这样，逻辑上有十六种不同的部件类型可以使用 A3 中提供的指标进行分级。这十六种部件类型分别对应于 M、D、A、I 在理论上可能的十六种组合。在这些组合当中有一种典型的情况(不包含 M、D、A、I 的任何一种)，代表该部件被有意地或被要求不执行任何安全策略，因而不要求满足任何 GJB 2646 要求，也不需要被评估。然而，如果系统的结构允许部件上存在空的子策略，那么仍可以使用这些部件作为安全网络系统的一个部件。其余的部件类型标注为 M、D、I、A、MD、MA、MI、DA、DI、IA、MDA、MDI、MIA、IAD 和 MIAD，其代表的含义是显而易见的(例如，一种“MIA 部件”支持强制访问控制、审计、身份鉴别与验证策略，它恰好具备 A3 中描述的根据评估等级和类型所提供的完全相同的特性)。

除了基于支持性策略元素的类型之外，一个已评估的处理部件可以得到一个单独的评估等级。为能达到某一特定等级，一个部件必须满足该等级要求的所有指标。一般来说，这些指标是 GJB 2646 对要被提供的策略特性子集的直接说明。每种部件类型具有最大和最小等级，如表 A1 所列出。为了达到某一特定等级，一个部件必须满足对于策略、可信度、可计算性及文档的适当的需求。

表 A1　部件类型最大及最小等级

部件类型	最小等级	最大等级
M	B1	A1
D	C1	C2＋
I	C1	C2
A	C2	C2＋
DI	C1	C2＋
DA	C2	C2＋
IA	C2	C2＋
IAD	C2	C2＋
MD	B1	A1
MA	B1	A1
MI	B1	A1
MDA	B1	A1
MDI	B1	A1
MIA	B1	A1
MIAD	B1	A1

每种部件类型的最大等级是从 GJB 2646 推导出的，它是对该部件类型施加的最严格要求的等级。同样地，每种部件类型可用的最小等级是施加于该部件类型之上的最基本的 GJB 2646 评估要求。

为满足 B3 级上的 DAC 和审计支持的要求，我们给出了除上述通用方法外的例外方法，作为这些级别上策略类别的附加支持（也就是对 DAC 提供的 ACL 方法以及对审计的实时警铃），它们并不具备提供给 B3 级 MAC 支持的高级别可信度。对于包括 D 或 A 的部件类型，使用 C2＋级的概念来考虑会更合适，但对包括 M（用来满足 B3 级系统中对 D 或 A 分级的功能性要求）的部件类型却非如此。

支持 I 的部件可能要求提供给 DAC（在相对较低级别的可信度上）或 DAC 和 MAC 二者（在相对较高级别的可信度上）的身份鉴别和验证支持。因而，也提供 I 类型部件从 C1 级到 A1 级范围内的分级层次。B2 级以上的等级反映了对 MAC 标号信息的标号完整性附加的可信度要求，其它特性没有任何附加要求。

要求支持 I 的部件支持 DAC 策略的身份鉴别和验证，因为建立一个用户许可的 GJB 2646

身份鉴别和验证的要求在 M 部件上反映，因此这种要求在建立一个用户的安全标号时至关重要。

对于多重类型部件也给出了基于上述被包括类型的有意义的组合的最小和最大级别。

顺便指出，一个独立的 C1 级系统具有和 C1 级 DI 部件完全相同的验证要求，同样地，一个 C2 级系统和 C2 级 IAD 部件、B1－A1 级系统和 B1－A1 级 MIAD 部件也具有完全相同的验证要求。

A2 组合规则

A2.1 目的

在指定由部件组合而成的(子)系统的等级时，连接网络部件的方式不能与单独评估这些部件时所作的假定冲突。本条介绍将已评估的部件组合成可评估的(子)系统的规则，以及如何给(子)系统指定一个与规则一致的级别的方法。

在本条中，不考虑利用已评估的(子)系统在不同安全级下分隔数据所带来的相对风险。

本条介绍一种给由多个部件组合成的(子)系统指定一个等级的技术基础。这一等级表示被分级的(子)系统作为整体时所能提供的最低安全级。

部件必须提供接口来支持其它被要求的策略。

被评估部件支持的四种策略(即强制访问控制、自主访问控制、审计、身份鉴别与验证)可以组成 15 种可能的组合，组合规则正是据此 15 种组合进行分割的。

A2.2 自主访问控制的组合规则

下面介绍的规则是基于新部件由已评估过的部件组合而成这一概念。本条介绍的规则特别适用于处理负责网络 DAC 策略部件组合。组合 D 部件要求对工程及系统结构作仔细考虑。

当评估 D 部件时，应遵循规定的网络 DAC 策略和已规定的目标网络安全结构。部件定义中将包括一则支持协议，该协议可以传递作为 DAC 决策基础的身份标识。应评估该协议以确保支持目标网络 DAC 策略(例如，如果网络 DAC 策略的访问粒度可以到单个用户，那么将所有用户映射到单个网络 ID 的身份标识协议就不能满足要求)。

下面讨论 D 部件，它是已获取相对于 DAC 的某个级别的部件。(例如，C1～C2＋的 D－Only 部件，C1～C2＋的 DI 部件，B1～A1 的 MD 部件，等。)本条介绍的规则只涉及相关 DAC 策略的部件组合。

A2.2.1 两个 D 部件的组合

任何时候，当直接连接两个 D 部件时，从一个部件向另一个部件传递用于 DAC 决策标识的身份标识传递协议必须在两个部件中保持一致。组合部件提供的身份标识传递协议必须支持目标网络结构的身份标识传递协议。另外，必须表明组合的 DAC 策略能够支持目标网络 DAC 策略，该组合 DAC 策略可以是由一个部件提供的、在其控制下作用于命名主体之上的 DAC 策略的组合或者是由另一部件提供的、在其控制下作用于命名主体之上的 DAC 策略的组合。

A2.2.2 自主访问控制策略组合分级

给定一个如上所述的组合部件，该组合部件相关 DAC 策略的评估等级将是组合部件内任

何 D 部件中的最低级别。

A2.3　身份鉴别与验证(I－Only)组合规则

下面介绍的规则基于新部件由已评估过的部件组合而成这一概念。本条介绍的规则尤其适用于负责网络身份鉴别与验证策略的部件的组合。组合 I 部件要求仔细考虑工程及系统结构。

评估 I 部件时,应遵循已规定的网络身份鉴别与验证策略和已规定的目标网络结构。在部件定义中将包括一则支持性协议声明,该协议声明可以传递用户身份和验证信息以及由 I 部件提供的接口。两个 I 部件的组合必须始终遵守支持网络身份鉴别与验证的协议。此外,由组合 I 部件提供的、支持规定协议的接口必须保持一致。

A2.3.1　身份鉴别与验证组合分级

给定一个如上所述的组合部件,该组合部件的身份鉴别与验证的评估等级将是该组合部件内任一 D 部件的最低等级。

A2.4　审计(A－Only)组合规则

下面介绍的规则基于新部件由已评估过的部件组合而成这一概念。本条介绍的规则尤其适用于负责网络审计策略的部件组合。组合 A 部件要求仔细考虑工程及系统结构。

评估 A 部件时,将针对已规定的网络身份鉴别与验证策略和已规定的目标网络结构。部件定义将包括一则支持性的、该部件用来接收审计信息的协议声明。组合两个 A 部件必须始终遵守支持网络审计的协议。

A2.4.1　审计组合分级

给定一个如上所述的组合部件,该组合部件的审计评估等级将是该组合部件内任何 A 部件的最低等级。

A2.5　强制访问控制(M－Only)组合规则

下面介绍的规则基于新部件由两个直接在物理级上相连的部件组合而成的概念。本条介绍的规则特别适用于负责网络 MAC 策略的部件组合。

MAC 组合规则提供了以下强壮保证,如果网络是由已评估的部件直接连接而成,并且每个连接满足 MAC 组合规则,那么可以支持网络 MAC 策略。这些规则允许基于 MAC 策略的部件的递归定义。下面两条阐述 MAC 组合规则。第一条论述两个直接相连且每个连接端带有多级设备的部件的组合。第二条论述两个直接相连且每个连接端带有单级设备的部件的组合。

下面讨论的 M 部件已获取相对于 MAC 策略的级别。(例如,B1～A1 的 D－Only 部件、B1～A1 的 MD 部件 、B1～A1 的 MI 部件,等)。

A2.5.1　多级设备

任何时候,当两个 M 部件通过通信信道直接相连,并在每个连接的端点带有一个多级设备时,标号协议(如多级设备输出需求所要求的,见 5.3.2.1.3.2.1、5.3.3.1.3.2.1、5.4.1.1.3.2.1)在到两个设备的网络接口处必须完全一致。

任何时候,当一个 B1 级 M 部件直接连接一个 B2～A1 级 M 部件时,由最大级和最小级表示的(系统高和系统低)、与 B1 级 M 部件相关的敏感标号的范围必须与由最大级和最小级表

示的、与 B2～A1 级 M 部件相关的多级设备的敏感标号范围相同。

任何时候，当两个 B2～A1 级 M 部件在每个连接端与一个多级设备直接相连时，由最大级和最小级表示的、与每个被连接的设备相关的敏感标号范围必须相同。

A2.5.2 单级设备

任何时候，当两个 M 部件在每个连接端与一个单级设备直接相连时，与这两个设备相关的安全级必须相同。

任何时候，当两个非 M 部件直接连接时，被这两个非 M 部件处理的数据的最大安全级必须相同。

A2.5.3 自主访问控制策略组合分级

给定一个如 A2.5.1 条和 A2.5.2 中所述的组合部件，该部件的 MAC 评估等级将是组合部件内任一 M 部件的最低级。

A2.6 DI 部件(D－Only 和 I－Only)组合规则

下面介绍的规则基于新部件由已评估的部件组合而成的概念。本条介绍的规则尤其适用于网络负责 DAC 策略和身份鉴别与验证策略的部件组合。组合 DI 部件要求仔细考虑工程及系统结构。

当 I 部件和 D 部件组合成 DI 部件时，该 DI 部件必须保持该 D 部件的网络 DAC 策略。这表明根据 DAC 策略，每个 DAC 接口需要一种用于接收 DAC 信息并返回数据的协议。这种协议必须能够支持该网络 DAC 策略。(注意，如果网络 DAC 策略的定义要求访问决策依赖于用户是“网络组的成员”，也就是说是另一个部件的合法用户，那么该 DAC 接口可能不要求任何传送给 DI 部件的标识。)

另外，对于 C2 级及 C2 以上级，组合的 DI 部件必须保留审计接口，以便输出源于 D 部件和 I 部件的信息。这意味着在该 DI 部件必须提供可以输出由于 DI 部件内各部分动作而产生的审计信息的手段。

DI 部件可能为其它部件提供身份鉴别与验证支持服务。此时必须定义该 DI 部件的身份标识接口，而且要为该接口建立能够支持网络 I/A 策略的协议。DI 部件可能要与其它 D－Only 部件进一步组合形成新的 DI 部件，所用的规则如上所述。

然而，DI 部件不必要为其它部件提供身份鉴别与验证服务。此时该 DI 部件可能仅与其它能满足自身身份鉴别与验证服务的部件(也即是 DI 部件、MIAD 部件、MI 部件等)组合。

如果组合的 DI 部件支持直接连接的用户，则组合 DI 部件的评估等级为 C1 级。

A2.6.1 ⟦STBZ⟧DI 部件组合分级

给定一个如上所述的组合部件，且 I 部件具有 C1 级评估等级，那么该组合 DI 部件的评估等级为 C1 级。

给定一个如上所述的组合部件，并且 I 部件具有 C2 级评估等级，那么该组合 DI 部件的评估等级与 D 部件的评估等级相同。

A2.7 DA(D－Only 和 A－Only)组合规则

下面介绍的规则基于新部件由已评估的部件组合而成的概念。本条介绍的规则尤其适用于网络负责 DAC 策略和网络审计策略的部件组合。组合 DA 部件要求仔细考虑工程及系统

结构。

当 A 部件和 D 部件组合成 DA 部件时，该 DA 部件必须保留 D 部件的网络 DAC 策略。这意味着根据 DAC 策略，每个 DAC 接口可能需要一种可以接收 DAC 信息并返回数据的协议。该协议必须能够支持网络 DAC 策略。（注意，如果网络 DAC 策略的定义要求访问决策依赖于用户是“网络组成员”，也就是说是另一个部件的合法用户，那么该 DAC 接口可能不要求任何传送给 DI 部件的标识。）

DA 部件可能向其它部件提供审计支持。此时，必须定义该 DA 部件的审计接口，且必须为该接口建立一个使其能支持网络审计策略的协议。此时，该 DA 部件可以与其它 D－Only 部件进一步组合成新的 DA 部件，所用的规则如上所述。

然而，DI 部件不必为其它部件提供审计服务。此时，该 DI 部件可能仅与其它能满足自身审计服务的部件（也就是 DA 部件、MIAD 部件、MA 部件等）组合。

A2.7.1　DA 部件组合分级

给定一个如上所述的组合部件，且 D 部件至少具有 C2 级评估等级，那么该组合 DA 部件的评估等级是该组合部件的两个部件中最低级。

A2.8　IA（I－Only 和 A－Only）组合规则

下面介绍的规则基于新部件由已评估的部件组合而成的概念。本条介绍的规则尤其适用于网络负责身份鉴别与验证策略和网络审计策略的组合。组合 IA 部件要求仔细考虑工程及系统结构。

当 IA 部件由 I 部件与 A 部件连接而成时，该 IA 部件必须同时保留 A 部件的网络审计接口和协议以及 I 部件的网络身份鉴别与验证接口和协议。

这意味着组合 IA 部件时必须同时提供审计接口和身份鉴别与验证接口。对每个审计接口必须定义一种接收审计数据协议。另外，必须为每个身份鉴别接口定义一种用以接收身份鉴别与验证数据并返回被证实的用户标识的协议。该协议必须能够支持网络 I/A 策略。

A2.8.1　IA 部件组合分级

给定一个如上所述的组合部件，且 I 部件至少具有 C2 级评估等级，那么该组合 IA 部件的评估等级是 A 部件的级别。

A2.9　MD（M－Only 和 D－Only）组合规则

下面介绍的规则基于新部件由已评估的部件组合而成的概念。本条介绍的规则尤其适用于网络负责 MAC 策略和 DAC 策略的部件组合。组合 MD 部件要求仔细考虑工程及系统结构。

当 MD 部件由 M 部件直接与 D 部件连接组合而成时，MAC 策略的组合规则是：M 部件必须通过一个单级设备唯一连接到 D 部件，并且该设备的安全级必须与 D 部件处理的最大数据安全级相同。由直接连接于 D 部件的 MD 部件提供的任何网络接口必须处于 D 部件所在的级别上。

组合 DAC 策略的规则是：由 MD 部件（包括直接连接到 M 部件的 MD 部件）提供的任何网络接口必须支持 D 部件使用的身份标识传递协议。（注意，如果网络 DAC 策略的定义要求访问决策依赖于用户是“网络组成员”，也就是说是另一个部件的合法用户，那么该 DAC 接口

可能不要求任何将被传送给 DI 部件的标识。)

此外,组合 MD 部件必须保证组合部件控制下的任何访问数据的外部请求都同时属于原始 M 和 D 部件的 MAC 和 DAC 策略。

A2.9.1 MD 部件组合分级

给定一个如上所述的组合部件,并且 D 部件至少具有 C2 级评估等级,那么该组合 MD 部件的评估等级将或者是 B1(如果 M 部件的评估等级是 B1)或者是 B2(如果 M 部件的评估等级大于 B1)。

给定一个如上所述的组合部件,并且 D 部件至少具有 C2＋级评估等级,那么指定给该组合 MD 部件的评估等级将与 M 部件的评估等级相同。

A2.10 MI(M－Only 和 I－Only)组合规则

下面介绍的规则基于新部件由已评估的部件组合而成的概念。本条介绍的规则尤其适用于网络负责 MAC 策略和身份鉴别与验证策略的部件组合。组合 MI 部件要求仔细考虑工程及系统结构。

当 MI 部件由 M 部件与 I 部件直接连接组合而成时,MAC 策略的组合规则是:M 部件必须通过一个单级设备唯一连接到 I 部件,并且该设备的安全级必须与 I 部件处理的最大数据安全级相同。直接连接到 I 部件的 MI 部件提供的任何网络接口必须处于 I 部件所在的级别上。

此外,组合 MI 部件必须保留审计接口,以便输出来自 M 部件和 I 部件的审计信息。这意味着 MI 部件必须提供一种手段来输出由于其内部各个部件动作而产生的审计信息。

MI 部件可能向其它部件提供身份鉴别与验证支持服务。时此必须定义 MI 部件的身份标识接口,并且为该接口建立一种使其能够支持网络 I/A 策略的协议,此时,MI 部件可能与其它 M－Only 部件进一步组合形成新的 MI 部件,所使用的规则如上所述。

然而,MI 部件不必要为其它部件提供身份鉴别与验证服务,此时,该 MI 部件可能仅与其它能满足自身的身份鉴别与验证服务的部件(即 MI 部件、MIAD 部件、DI 部件等)组合。

组合 MI 部件必须保证 MI 部件的任何直接用户连接都能支持 MAC 策略和网络身份鉴别与验证策略。这意味着如果 M 部件支持直接用户连接,那么该 M 部件必须支持在这些连接上的用于交换身份鉴别与验证信息(与 I 部件)的协议,这完全支持网络 I/A 策略。

A2.10.1 MI 部件组合分级

给定一个如上所述的组合部件,且 A 部件至少具有 C2 级评估等级,那么该组合 MA 部件的评估等级与 M 部件的评估等级相同。

A2.11 MA(M－Only 和 A－Only)组合规则

下面介绍的规则基于新部件由已评估的部件组合而成的概念。本条介绍的规则尤其适用于网络负责 MAC 策略和审计策略的部件组合。组合 MA 部件要求仔细考虑工程与系统结构。

当 MA 部件由 M 部件与 A 部件直接连接组合而成时,MAC 策略的组合规则是:M 部件必须通过一个单级设备唯一连接到 A 部件,并且该设备的安全级必须与 A 部件处理的最大数据安全级相同。直接连接到 A 部件的 MA 部件提供的任何网络接口必须处于 A 部件所在的

级别上。

MA 部件可能向其它部件提供审计支持服务。此时必须定义 MA 部件的审计接口，并且为该接口建立一种使其能够支持网络审计策略的协议，此时，MA 部件可能与其它 M－Only 部件进一步组合形成新的 MI 部件，所使用的规则如上所述。

然而，MA 部件不必要为其它部件提供审计服务，此时，该 MA 部件可能仅与其它能满足自身的审计服务的部件(即 MA 部件、MIAD 部件、DA 部件等)组合。

A2.11.1 MA 部件组合分级

给定一个如上所述的组合部件，且 A 部件至少具有 C2 级评估等级，那么该组合 MA 部件的评估等级将是 B1(如果 M 部件的评估等级是 B1)或者是 B2(如果 M 部件的评估等级大于 B1)。

给定一个如上所述的组合部件，且 A 部件至少具有 C2＋级评估等级，组合 MA 部件的评估等级与 M 部件的评估等级相同。

A2.12 IAD 组合规则

下面介绍的规则基于新部件由已评估的部件组合而成的概念。本条介绍的规则尤其适用于网络负责 DAC 策略、身份鉴别与验证策略、审计策略的部件组合。组合 IAD 部件要求仔细考虑工程及系统结构。

当 IAD 部件由直接连接的部件组合而成，该 IAD 部件必须与作用于 DI 部件、DA 部件和 IA 部件的组合规则一致。如果 IAD 部件支持直接连接用户，那么该 IAD 部件必须至少满足一个 C2 级网络系统的所有要求。

A2.12.1 IAD 部件组合分级

给定一个如上所述的组合部件，并且 I 部件和 D 部件各自具有 C2 级评估等级，那么该组合 IAD 部件的评估等级是 A 部件的评估等级。

给定一个如上所述的组合部件，并且 I 部件具有 C2 级评估等级，D 部件具有 C2＋级评估等级，那么该组合 IAD 部件的评估等级将是 A 部件的评估等级。

A2.13 MDA 组合规则

下面介绍的规则基于新部件由已评估的部件组合而成的概念。本条介绍的规则尤其适用于网络负责 MAC 策略、DAC 策略和审计策略的部件组合。组合 MDA 部件要求仔细考虑工程及系统结构。

当 MDA 部件由直接连接的部件组合而成时，则 MDA 部件必须与 MD 部件、MA 部件及 DA 部件的组合规则相一致。

A2.13.1 MDA 部件组合分级

给定一个如上所述的组合部件，并且 A 部件具有 C2 级评估等级，D 部件具有 C2 级或更高的评估等级，那么该组合 MDA 部件的评估等级将或者为 B1 级(如果 M 部件的评估等级为 B1)或者为 B2 级(如果 M 部件的评估等级大于 B1 级)。

给定一个如上所述的组合部件，并且 D 部件和 A 部件各自具有 C2＋级评估等级，那么该组合 MDA 部件的评估等级将与 M 部件的评估等级相同。

A2.14 MDI 组合规则

下面介绍的规则基于新部件由已评估的部件组合而成的概念。本条介绍的规则尤其适用于网络负责 MAC 策略、DAC 策略和身份鉴别与验证策略的部件组合。组合 MDA 部件要求仔细考虑工程及系统结构。

当 MDI 部件由直接连接的部件组合而成时，该 MDI 部件必须与 MD 部件、MI 部件及 DI 部件的组合规则相一致。

A2.14.1 MDI 部件组合分级

给定一个如上所述的组合部件，且 I 部件和 D 部件各自具有 C2 级评估等级，那么该组合 MDI 部件的评估等级将是 B1 级(如果 M 部件的评估等级为 B1)或 B2 级(如果 M 部件的评估等级大于 B1 级)。

给定一个如上所述的组合部件，且 I 部件具有 C2 级评估等级，D 部件具有 C2＋级评估等级，那么该组合 MDI 部件的评估等级将与 M 部件的评估等级相同。

A2.15 MIA 组合规则

下面介绍的规则基于新部件由已评估的部件组合而成的概念。本条介绍的规则尤其适用于网络负责 MAC 策略、身份鉴别与验证策略及审计策略的部件组合。组合 MIA 部件要求仔细考虑工程及系统结构。

当 MIA 部件由直接连接的部件组合而成时，该 MIA 部件必须与 MI 部件、MA 部件及 IA 部件的组合规则相一致。

A2.15.1 MIA 部件组合分级

给定一个如上所述的组合部件，并且 I 部件和 A 部件各自具有 C2 级评估等级，那么该组合 MIA 部件的评估等级将为 B1 级(如果 M 部件的评估等级为 B1)或为 B2 级(如果 M 部件的评估等级大于 B1 级)。

给定一个如上所述的组合部件，且 I 部件具有 C2 级评估等级，A 部件具有 C2＋级评估等级，那么该组合 MIA 部件的评估等级将与 M 部件的评估等级相同。

A2.16 MIAD 组合规则

下面介绍的规则基于新部件由已评估的部件组合而成的概念。本条介绍的规则尤其适用于网络负责 MAC 策略、DAC 策略和身份鉴别与验证策略及审计策略的部件组合。组合 MIAD 部件要求仔细考虑工程及系统结构。

当 MIAD 部件由直接连接的部件组合而成时，该 MIAD 部件必须与 MIA 部件、MDA 部件、MDI 部件及 IAD 部件的组合规则相一致。如果 MIAD 部件支持直接连接的用户，则该 MIAD 部件必须至少满足 B1 级网络系统的所有要求。

A2.16.1 MIAD 部件组合分级

给定一个如上所述的组合部件，且 I 部件和 D 部件各自具有 C2 级评估等级，那么该组合 MIAD 部件的评估等级将或者为 B1 级(如果 M 部件的评估等级为 B1)或为 B2 级(如果 M 部件的评估等级大于 B1 级)。

给定一个如上所述的组合部件，且 I 部件具有 C2 级评估等级，D 部件和 A 部件各具有 C2＋级评估等级，那么该组合 MIAD 部件的评估等级与 M 部件的评估等级相同。

A3 特殊部件评估指南

A3.1　M－Only 部件(M 部件)

M－Only 部件是对 MAC 策略提供网络支持的部件，该策略在 GJB 2646 中说明。该 M 部件不包括必要的、用来充分支持在本标准中定义的任何 3 种其它网络策略(即 DAC、身份鉴别与验证、审计)的机制。

M 部件属于 B1、B2、B3、A1 四种等级之一。

M 部件根据满足某等级的所有要求的最高级别进行分级。

A3.1.1　概述

在参考要求中，TCB 意为 M 部件上的 NTCB 分部。同时，M 部件的审计意为“M 部件将产生由 M 部件完成的任何可审计动作的审计数据”。另外，该 M 部件将包括使审计收集部件可以得到审计数据的机制。

A3.1.2　一般性条件

如本标准 5.1～5.4 条所示，表 A2 中列出的要求可以直接应用于 M 部件。

表 A2　无须进一步说明便可应用的 M 部件要求

	B1 级章条号	B2 级章条号	B3 级章条号	A1 级章条号
配置管理		5.3.2.3.2.3	5.3.3.3.2.3	5.4.1.3.2.3
设计文档	5.3.1.4.4	5.3.2.4.4	5.3.3.4.4	5.4.1.4.4
设备标号		5.3.2.1.3.4	5.3.3.1.3.4	5.4.1.1.3.4
向多级设备的输出	5.3.1.1.3.2.1	5.3.2.1.3.2.1	5.3.3.1.3.2.1	5.4.1.1.3.2.1
标 号	5.3.1.1.3	5.3.2.1.3	5.3.3.1.3	5.4.1.1.3
人可读的输出标号	5.3.1.1.3.2.3	5.3.2.1.3.2.3	5.3.3.1.3.2.3	5.4.1.1.3.2.3
标号完整性	5.3.1.1.3.1	5.3.2.1.3.1	5.3.3.1.3.1	5.4.1.1.3.1
强制访问控制	5.3.1.1.4	5.3.2.1.4	5.3.3.1.4	5.4.1.1.4
客体重用	5.3.1.1.2	5.3.2.1.2	5.3.3.1.2	5.4.1.1.2
安全特性用户指南	5.3.1.4.1	5.3.2.4.1	5.3.3.4.1	5.4.1.4.1
系统完整性	5.3.1.3.1.2	5.3.2.3.1.2	5.3.3.3.1.2	5.4.1.3.1.2
测试文档	5.3.1.4.3	5.3.2.4.3	5.3.3.4.3	5.4.1.4.3
可信分布				5.4.1.3.2.4
可信设备管理		5.3.2.3.1.4	5.3.3.3.1.4	5.4.1.3.1.4
可信恢复			5.3.3.3.1.5	5.4.1.3.1.5

A3.1.3 特殊性要求

下述要求需要附加说明。

3.1.3.1 主体敏感标号

a. 准则

(B2 级 5.3.2.1.3.3;B3 级 5.3.3.1.3.3;A1 级 5.4.1.1.3.3)

b. 解释

本要求不适用于不支持直接终端输入的 M 部件,此时该要求无法满足。任何支持直接终端输入的 M 部件必须满足规定的要求。

c. 原理

某用户只有直接连接到一个支持 MAC 策略的部件上时,才能改变对话的当前级。如果用户直接连接到不支持 MAC 策略的部件上,该用户永远在它所直接附属的部件所在的级别上操作。如果用户直接连接到一个 M 部件上,则该 M 部件必须满足规定的所有要求。如果 M 部件不直接与用户进行通信,则不需要支持这个要求,该要求由直接与用户通信的 M 部件满足。

A3.1.3.2 可信路径

a. 准则

(B2 级 5.3.2.2.1.1;B3 级 5.3.3.2.1.1;A1 级 5.4.1.2.1.1)

b. 解释

本要求不适用于不支持直接终端输入的 M 部件(例如,该 M 部件可能不连接到任何终端用户 I/O 设备)。任何支持直接与用户通信的 M 部件必须满足规定的要求。另外,一个带有直接连接用户的 M 部件必须提供可以建立用户的许可证以及与用户当前会话联系起来的机制。

c. 原理

为了保证发生涉及安全的活动时(例如用户鉴别、设置当前会话安全等级),用户仅与 TCB 进行通信,可信路径是必要条件。然而,可信路径并不涉及 TCB 内部的通信,仅涉及用户和 TCB 之间进行通信。因此,如果一个 M 部件不支持任何直接用户通信,则该 M 部件不需要包含保证 TCB 与用户直接通信的机制。

当 M 部件不支持直接用户通信时,用户的许可证必须由 M 部件建立。有三种手段提供此支持:

第一,通过单级信道连接所有直接用户,信道的最大级别等于信道最小级别,对信道的物理访问隐含着该信道此级别上的许可证;此时,可能不存在任何涉及安全的活动,这样,可用的可信路径要求可能仅由设备标号提供;

第二,通过单级信道连接一些直接用户,其中信道的最大级别与它的最小级别不等,对该信道的物理访问隐含该信道在最大级别上的许可证。

第三,通过单级信道连接一些直接用户,其中信道的最大级别与它的最小级别不等,且该 M 部件包含一些内部机制将用户许可证映射到信道的域上。

前两种机制通过外部手段将用户的许可证映射到该用户的动作上。第三种机制要求一些

内部机制。这样的机制可能是一个由 M 部件维护的用户的身份、口令或许可证数据库。另一种可行的机制可能是 M 部件内部的协议及接口定义，用来通过多级信道保存从其它 M 部件中获取的信息(该信道是多级的是因为信道传递标号，即用户许可证)。

A3.1.3.3 系统体系结构

a. 准则

(B1 级 5.3.1.3.1.1；B2 级 5.3.2.3.1.1；B3 级 5.3.3.3.1.1；A1 级 5.4.1.3.1.1)

b. 解释

一个 M 部件必须满足所有的规定要求。在本标准中，“完备定义 TCB 的用户接口”意为完备定义 M 部件的参考监视器与参考监视器外部主体之间的接口。

c. 原理

该 M 部件可能不具有直接用户接口，但期望它能支持非 TCB 的主体。完备定义 TCB 及 TCB 外部主体之间的接口是很重要的。(注意，此时主体总是在部件内部，即“内部主体”)

A3.1.3.4 隐蔽信道分析

a. 准则

(B2 级 5.3.2.3.1.3；B3 级 5.3.3.3.1.3；A1 级 5.4.1.3.1.3)

b. 解释

一个 M 部件必须满足规定的条件。另外，如果存在需要被审计的信道，则该 M 部件应包含一种机制使审计数据可在 M 部件外部获得(例如，传递数据给一个审计收集部件)。

c. 原理

如果一个 M 部件包含需要被审计的隐蔽信道，则该 M 部件必须生成审计数据使审计得以进行。因为网络中所有的隐蔽信道存在于一个 M 部件上，所以 M 部件必定是记录隐蔽信道可能的使用情况的审计记录的源。

A3.1.3.5 安全测试

a. 准则

(B1 级 5.3.1.3.2.1；B2 级 5.3.2.3.2.1；B3 级 5.3.3.3.2.1；A1 级 5.4.1.3.2.1)

b. 解释

M 部件必须满足规定的所有要求，除非明确指明“在自主安全策略下，一般被否定，”，此时该要求对 M 部件来说不适用。

c. 原理

M 部件不支持自主安全策略，因此，测试这样的策略毫无价值。

A3.1.3.6 设计规格说明和验证

a. 准则

(B1 级 5.3.1.3.2.2；B2 级 5.3.2.3.2.2；B3 级 5.3.3.3.2.2；A1 级 5.4.1.3.2.2)

b. 解释

M 部件必须满足规定的要求。

安全策略可解释为被部件支持的 MAC 策略。模型可解释为被部件所支持的 MAC 策略的参考监视器的某部分(例如，当前访问集的表示、主体和客体的敏感标号、Bell-LaPadula 模型

的简单的安全和约束特性)。

A3.1.3.7 可信设备手册

(B1 级 5.3.1.4.2;B2 级 5.3.2.4.2;B3 级 5.3.3.4.2;A1 级 5.4.1.4.2)

b. 解释

M 部件必须满足规定的要求,除非明确指明"用以检查和维护审计文件的过程",这段文字意为"必须定义与审计数据输出相关的机制和协议。",同样若指明"包括改变一个用户的安全特征"时,该要求对 M 部件不适用。

c. 原理

M 部件既不维护审计文件,也不提供检查它们的机制。然而,它必须提供输出审计文件的机制,并且在可信设备手册中定义这些机制。M 部件也不维护用户信息。

A3.1.4 M 部件的典型应用

以通过验证安全内核提供 MAC 的 MLS 包交换作为 M 部件的例子,如图 A1 所示。该部件支持非自主访问集的 16 种等级和 64 类。MLS 包交换是作为 M 部件针对上述要求进行分级的。

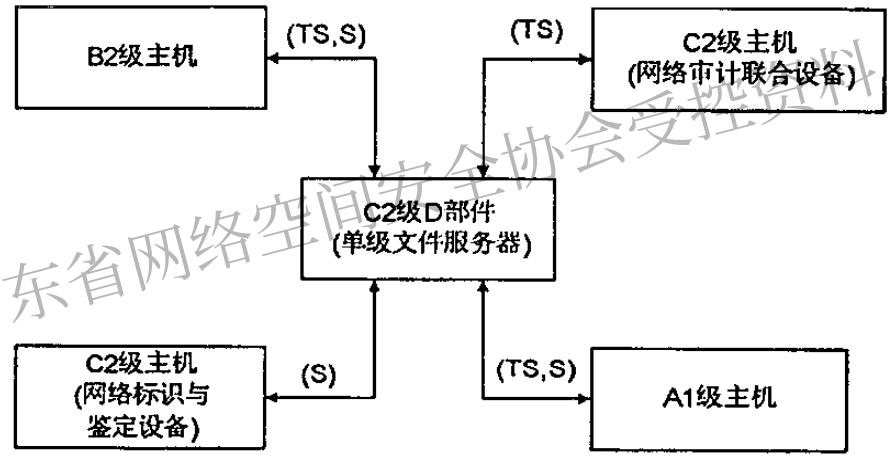


图 A1 M 部件的典型应用

上例中的 A1 级 M 部件可以作为一个多级包交换用在网络中。该 M 部件可以配置成具有几个单级信道和一定数目的多级信道。本例中假定每个多级信道有绝密和机密两级。同样假设这些单级信道具有绝密级或机密级多级信道直接与 B2 主机连接,每个信道各具有一个系统高绝密和系统低机密。直接连接到 C2 主机的单级信道也各具有一个系统高绝密和系统低机密级。单级信道直接与 C2 主机连接,它们中一些运行在专用的机密级上,另一些运行在专用的绝密级上。这些专用绝密主机中的一台以及专用机密主机中的一台将负责收集发生在

M 部件的审计信息。在这种方式下，可建立一种允许多级主机之间以及多级主机和单级主机之间安全地进行通信的网络。由作为多级安全包交换的 M 部件对这样的通信进行必要的分隔。注意，第 A3.2 条中的分组规则导致全局 NTCB 的 B2 级评估等级。

A3.2　D－Only 部件(D 部件)

D－Only 部件对 DAC 策略提供网络支持，该策略在 GJB 2646 中已说明。D 部件不包括必要的、用来充分支持在本标准中定义的任何 3 种其它网络策略(即 MAC、身份鉴别与验证、审计)的机制。

D 部件属于 C1、C2、C2＋三种等级之一(由下面所述要求定义)。

D 部件是根据满足一个某等级的所有要求的最高级别进行分级的。

A3.3　概述

在参考要求中，TCB 意为参照 D 部件的 NTCB 分部。同时，对 D 部件审计的任何参照都意为“D 部件将产生由 D 部件完成的任何可审计动作的审计数据”。另外，D 部件将包括使审计部件可以得到这些审计数据的机制。

A3.3.1　一般性条件

在表 A3 中列出的要求直接应用于 M 部件，如在本标准 5.1～5.4 条所示。

表 A3　无须进一步说明便可应用的 D 部件要求

要　求	C1 章条号	C2 章条号	C2＋章条号
自主访问控制	5.2.1.1.1	5.2.2.1.1	5.3.3.1.1
客体重用		5.2.2.1.2	5.2.2.1.2
安全特性用户指南	5.2.1.4.1	5.2.2.4.1	5.2.2.4.1
安全测试	5.2.1.3.2.1	5.2.2.3.2.1	5.2.2.3.2.1
系统体系结构	5.2.1.3.1.1	5.2.2.3.1.1	5.2.2.3.1.1
系统完整性	5.2.1.3.1.2	5.2.2.3.1.2	5.2.2.3.1.2
测试文档	5.2.1.4.3	5.2.2.4.3	5.2.2.4.3

A3.3.2　特殊要求

下面列出的要求需要附加说明。

A3.3.2.1　可信设备手册

a. 准则

(C1 级 5.2.1.4.2；C2 级 5.2.2.4.2；C2＋级 5.2.2.4.2；)

b. 解释

D 部件必须满足规定的要求，除非明确指明“用以检查和维护审计文件的过程”，这段文字意为“必须定义与审计数据输出相关联的机制和协议。”。

c. 原理

M部件既不维护审计文件，也不提供检查它们的机制。然而，它必须提供将审计文件输出到审计部件的机制，这些机制在可信设备手册中定义。

A3.3.2.2 设计文档

a. 准则

(C1级5.2.1.4.4;C2级5.2.2.4.4;C2+级5.2.2.4.4;)

b. 解释

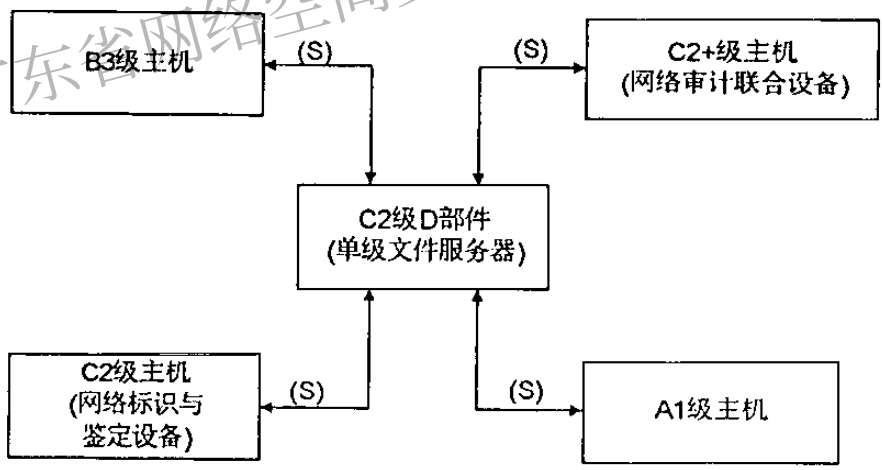
D部件必须满足规定的条件。另外，设计文档必须描述D部件在可用的主体许可证(也就是用户标识)与其它部件之间进行通信的协议。

c. 原理

D部件不维护用户身份鉴别与验证信息。然而，它可能使用某种已鉴定的用户标识作为DAC决策的基础。这样的信息必须通过身份鉴别协议提供给D部件。D部件使用的协议可能会变化，但它必须表明足以能支持D部件所支持的DAC策略。例如一个简单DAC策略：在每个主机基础上，访问被授权或被拒绝。此时所用的协议可能静态地赋予每个端口一个主机号。来自一个给定端口的所有请求与主机的访问许可证有关。这个协议不足以在每个主机上支持访问授权或拒绝的DAC策略。

A3.3.3 D部件的典型应用

以一个通过文件访问控制表提供DAC的系统为D部件的例子，如图A2所示。该系统是作为一个C2+级D部件针对上述要求进行分级的。



图A2 D部件的典型应用

上例中的C2+级D部件可以作为一个单级文件服务器用在网络中。该D部件可以配置成具有几个通信信道(每个信道将被连到一个具有同等访问级别的单级设备上)。例中的所有

文件将是保密的，并且假定系统连接到其它单级部件的所有信道为保密部件；或者在多级部件的情况下，连接到单级设备的信道为保密设备。与 D 部件相关的文档必须指明传递用户标识和文件名的协议。必须在每个部件的连接上遵守该协议。另外，文档必须指定用来输出审计信息的协议。该审计协议必须与它所附属的审计节点的协议完全相同。注意，A2 中的组合规则导致一个对全局 NTCB 的 B3 级评估等级。

A3.4 I－Only 部件（I 部件）

I－Only 部件是对身份鉴别与验证策略提供网络支持的部件，该策略在 GJB 2646 中说明。该 I 部件不包括必要的、用来充分支持在本标准中定义的任何 3 种其它网络策略（即 MAC、DAC、审计）的机制。

I 部件属于 C1、C2 两种等级之一（由下面所述要求定义）。

I 部件是根据满足某等级的所有要求的最高级别进行分级的。

A3.4.1 概述

在参考要求中，TCB 意为参照 I 部件的 NTCB 分部。同时，对一个 I 部件审计的任何参照意为“I 部件将产生由 I 部件完成的任何可审计动作的审计数据”。另外，I 部件将包括使审计收集部件可以得到审计数据的机制。

A3.4.2 一般条件

在表 A4 中列出的要求直接应用于 I 部件，如在本标准 5.1～5.4 条所示。

A3.4.3 特殊条件

下面列出的要求需要附加说明。

表 A4 无须进一步说明便可应用的 I 部件条件

要 求	C1 级章条号	C2 级章条号
标识与鉴定	5.2.1.2.1	5.2.2.2.1
客体重用		5.2.2.1.2
安全特性用户指南	5.2.1.4.1	5.2.2.4.1
安全测试	5.2.1.3.2.1	5.2.2.3.2.1
系统体系结构	5.2.1.3.1.1	5.2.2.3.1.1
系统完整性	5.2.1.3.1.2	5.2.2.3.1.2
测试文档	5.2.1.4.3	5.2.2.4.3

A3.4.3.1 可信设备手册

a. 准则

（C1 级 5.2.1.4.2；C2 级 5.2.2.4.2；C2＋级 5.2.2.4.2；）

b. 解释

I 部件必须满足规定的要求，除非明确指明“用以检查和维护审计文件的过程”，这段文字意为“必须定义与审计数据输出相关的机制和协议。”。

c. 原理

I 部件既不维护审计文件，也不提供检查它们的机制。然而，它必须提供将审计文件输出到审计部件的机制，这些机制需要定义在可信设备手册中。

A3.4.3.2 设计文档

a. 准则

(C1 级 5.2.1.4.4；C2 级 5.2.2.4.4；C2＋级 5.2.2.4.4；)

b. 解释

I 部件必须满足规定的要求。另外，设计文档必描述 I 部件将鉴别的主体标识输出到其它部件的协议。

c. 原理

I 部件提供的鉴别标识并不主要用于 I 部件自身，而是被其它执行网络 DAC 策略的部件使用。因此，对 I 部件来说，必须定义将已鉴别的用户标识传递给其它部件的协议。

A3.4.4 I 部件的典型应用

以下述系统为 I 部件的例子，该系统提供身份鉴别与验证工具，如带有命名服务器的 TAC，如图 A3 所示。该系统是作为 C2 级 I 部件针对上述要求进行分级的。I 部件可配置若干通信信道(每个信道将被连接到一个具有相同访问级别的单级设备上)。本例中的 TAC 为一个未分类的 TAC(即没有任何加密支持，可直接的通过电话访问)，系统连接单级设备的所有信道为未分类设备；多级部件连接的单级设备也是未分类部件。TAC 完成所有的鉴定，并将已鉴定的标识传递给网络的其它节点，作为 DAC 决策和审计入口的基础。与 I 部件相关的文档必须指明传递用户身份到连接部件的协议。每个到此部件的连接必须支持该协议。另外，该文档必须指定输出审计信息的协议。该审计协议必须与它所附属的审计部件的协议完全相同。注意，A3 条中的组合规则导致全局 NTCB 的 B3 级评估等级。

A3.5 A－Only 部件(A 部件)

A－Only 部件是对审计策略提供网络支持的部件，该策略在 GJB 2646 中说明。该 A 部件不包括必要的、用来充分支持本标准中定义的任何 3 种其它网络策略(即 MAC、DAC、身份鉴别与验证)的机制。

A 部件属于 C1、C2＋两种等级之一(由下面所述要求定义)。(C2 级 A 部件和 C2＋级 A 部件的区别在于对 B3 级审计要求的实时警铃支持。)

A 部件是根据满足某等级的所有要求的最高级别进行分级的。

A3.5.1 概述

在所参照的要求中，TCB 意为参照 A 部件的 NTCB 分部。

A3.5.2 一般性条件

在表 A5 中列出的要求直接应用于 A 部件，如在本标准 5.1～5.4 条所示。

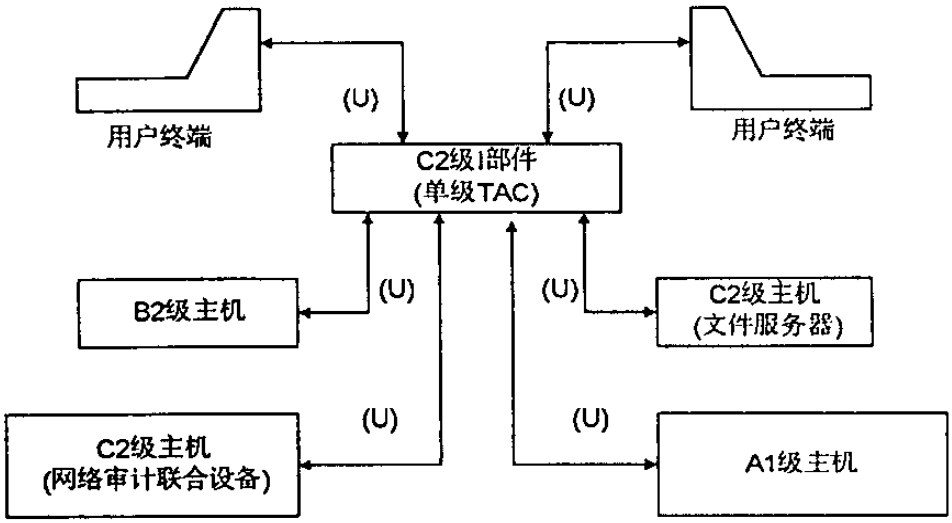


图 A3　I 部件的典型应用

表 A5　无须进一步说明便可应用的 A 部件要求

要　　求	C2 级章条号	C2＋级章条号
审 计	5.2.2.2.2	5.3.3.2.2
客体重用	5.2.2.1.2	5.2.2.1.2
安全特性用户指南	5.2.2.4.1	5.2.2.4.1
安全测试	5.2.2.3.2.1	5.2.2.3.2.1
系统体系结构	5.2.2.3.1.1	5.2.2.3.1.1
体系完整性	5.2.2.3.1.2	5.2.2.3.1.2
测试文档	5.2.2.4.3	5.2.2.4.3
可信设备手册	5.2.2.4.2	5.2.2.4.2

A3.5.3　特殊要求

下面列出的要求需要附加说明。

A3.5.3.1　设计文档

a. 准则

(C2 级 5.2.2.4.4;C2＋级 5.2.2.4.4;)

b. 解释

D 部件必须满足规定的要求。另外,设计文档必须描述 A 部件从其它节点输入审计信息

的协议。

c. 原理

A 部件可用于收集在多个不同部件上生成的审计数据。每一个这样的部件必须能够以允许 A 部件建立审计记录的形式向 A 部件传输信息。由审计部件使用的协议定义可接受的信息形式的机制。

A3.5.4 A 部件的典型应用

以下述系统为 A 部件的例子，该系统提供对网络环境的审计收集和检查工具，如图 A4 所示。该系统是作为 C2＋级 I 部件针对上述要求进行分级的。

本例中的 A 部件将操作在系统高层(绝密)，通过绝密信道从若干部件中收集信息。A 部件作为一个整体向网络提供审计功能。它定义每个部件传递信息给 A 部件的审计协议，结果是建立审计记录。本例中的审计者(即负责检查审计文件的人)通过连接 A 部件的操作台访问 A 部件。在其它情况下，审计者通过另一部件访问 A 部件，此时，A 部件负责执行哪些用户(即审计者)能够查看审计数据的访问控制策略。这要求 A 部件建立一种用户标识传递协议，这很类似 D 部件。注意，A3 条的组合规则导致全局 NTCB 的 B3 级评估等级。

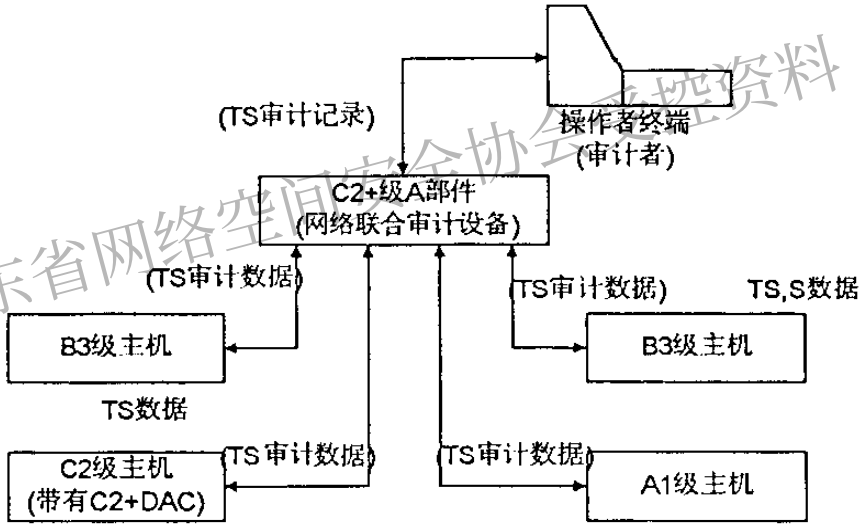


图 A4 A 部件的典型应用

附 录 B
NTCB 的原理
（补充件）

B1 目的

本标准的 5.1～5.4 条阐述了军用计算机安全评估准则(GJB 2646)。它是评估由计算机和通信设备组成的具有独立可信计算基(TCB)的单独计算机系统，在网络系统中称 TCB 为网络可信计算基，即 NTCB，它可物理或逻辑地分布在网络各部件之上。这种观点的默认情况是：被评估的网络(包括互连主机)是单独计算机系统的模拟，因此可利用 GJB 2646 的有关说明进行评估。本附录的目的是给上述观点提供主要的技术原理和图示说明。此处所示的原理将有助于网络和网络部件的负责人和评估者理解网络分部成部件的方式，由此可得到最终评估和认可的结果。本附录理论性和条理性很强，对于只关心 GJB 2646，而不欲获知其推导过程的读者可不必参阅。

可独立成章的附录 A 讨论了网络部件评估说明，阐述了下述观点：特殊网络部件评估是最终评估整体网络的首要步骤，该观点以网络的整体安全策略可以清晰地分割为单独部件上的安全策略为前提。一旦单独部件评估完成，整体体系结构与设计将支持最终网络评估，并将其视为多个可信部件的组合，每一部件完成分配于其上的安全策略，所有部件合作完成整体网络安全策略。将不同网络策略分布到部件之上的特殊指南见附录 A(补充件)的相关章条，针对每一分部策略的一般原理将在本附录中阐述。

本附录所描述的“网络是什么”的观点以及网络的 NTCB 完全分部成单独网络部件上的 NTCB 分部的观点与下述目标一致：满足 GJB 2646 的指定评估类别后，向网络颁发单独许可证。这一目标可能并不适于每一个应用环境，也可能不满足网络负责人欲互连已存在系统的要求。评定及认可这类网络的风险是一个既重要又有趣的问题，此处不考虑这种情况，也就是说，默认情况是评估支持网络安全策略的整体网络。

B2 背景与概述

B2.1 本附录组成

本附录由以下章条组成：B3 讨论如何正确组织网络 NTCB 所完成的策略及其在各网络部件上的分布；B4 讨论支持分部的 NTCB 观点的充分性及针对整体网络的参考监视器可由局部自治的参考监视器组成；B5 在 B4 真实通信信道的情况下，讨论部件间通信信道互连的理想情况，并深入讨论可提供通信安全技术和安全系统技术的情况；B6 讨论了其余支持分部的 NTCB 观点的原理。

B3 安全策略

GJB 2646 中的“安全策略”的含义为“用以规范组织结构管理，保护和分配敏感信息方式的一系列法律、规则和实例。”。此处的“安全策略”与“形式化安全策略模型”和“安全策略模型”不同。某组织机构的“安全策略”的最终目的是控制人员对信息的访问。

由该含义可知安全策略相关人员对敏感信息的访问包括保密性与完整性，只有独立而规

范的网络安全策略被某个组织机构所接受时(该机构欲在网络及其部件上存储、传送和处理信息),才可能进行最终的网络评估。网络安全策略是以利用本附录评估网络及其部件为先决条件。如果某网络欲允许多个机构共享信息,并成功地认可此项功能,必须在网络设计时,将多方接受的安全策略定义做为早期目标。

B3.1 强制访问控制策略

在通常被定义为"强制访问控制"的访问控制中,其多方接受的策略应尽量向前兼容,因为此类控制基于标号比较,标号将指定信息库中拥有用户许可证的信息的安全级,而用户许可证将指定用户访问该信息的正式授权。多方接受的策略的定义包括:将多种级别和许可证的多个系统合并成一个规范的系统,实际上,如果某组织机构使用的系统尚未被标识,在每个机构中负责信息的人员必须决定哪个外部用户许可证可做为访问某级信息的基础。

对某些特殊的机构,可能不存在 GJB 2646 中所定义的显式的强制访问策略(尤其是一些商用研究所可能会如此)。不过此类机构可以组成一个试验性的强制访问策略,即拥有单独访问类和许可证级别,如每一从属于某研究所的用户会有一个访问该所全部信息的许可证,这样,所有在网络上共享信息的研究所,在策略一级,可以用相对向前兼容的方式解决系统级的强制访问控制,这样做至少可以易于理解特殊决定的策略问题和影响。

B3.2 自主访问控制策略

某机构在自主访问控制的策略种类上,有更大的选择余地。如 GJB 2646 所定义的"自主访问控制"包括基于用户和用户组成员标识的用户对信息的访问控制,也包括已授权访问某客体的用户将该授权直接或间接传递至另一用户的能力(可使用拷贝授权或提供拷贝授权的方式)。在这些限制中,可以允许策略在很大范围内随用户分组方式、可能形成访问控制基础的已命名信息库的分类、可能形成访问控制基础的访问模式、用户用来定义限制或传播信息访问许可的机制的不同而不同。因此,在设计网络时,一系列机构可能在策略生成阶段形成系统和策略,而且,这样形成的全局策略,可能在很大程度上依赖于网络能力及功能的完成。

B3.3 支持策略

除 GJB 2646 所示的基础访问策略(强制和自主)以外,还有与个体安全操作的责任有关的其它功能。这些功能通常统称为"支持"策略,它们所提供的环境可允许基础访问策略有效地工作并完成监视功能。

责任需求由两部分主要的策略子集组成:标识与鉴定策略及审计策略,前者可支持强制和自主访问控制策略,并且在允许个体访问前指定和标识许可证的鉴定;在强制访问控制时,它是决定个体许可证的基础;在自主访问控制时,它是决定个体用户组的基础;而且,它还是记录发生或引起可审计事件的个体的标识符的基础。

审计策略可提供与个体用户唯一相关的安全事件的记录,这样,对敏感信息负责任的人员可掌握引起安全事件的用户信息。

不同机构采用的支持策略,其相异程度甚至可能超过自主访问控制。对于网络负责人而言,形成一个多方接受的全局支持策略,是一件比完成自主访问控制还困难的事。

B3.4 形式化安全策略模型

如 GJB 2646 所定义,形式化安全策略模型应具备数学化的精确的安全策略说明。安全策

略的目标是反映外部授权施加于系统之上的要求，形式化安全策略模型的目的是做为理论链的精确起点，以获得更高评估级别所要求的保证级别。这样，要求与原理相关的形式化安全策略模型，是 B2 级的要求；因为较低级别的理论链不需要数学化的精确度，故无需引入形式化安全策略模型。因此，形式化安全策略模型不是无关紧要的需求，它的目的是组成高级系统所需的理论链。

目前的形式化安全策略模型仅仅为访问控制策略而设。这种模型是指定级别系统中参考监视器的表征，选择模型表征，在很大程度上受系统的工艺特性的影响，如建造支持 B2 或更高级系统的理论链的可行性和经济性主要因使用模型(该模型与主体、客体及目标系统的访问特性有直观上的相似性)而显著增长。

如前所述，已分部 NTCB 的参考监视器是由一系列单独部件上的安全核心组成的。为保证每一安全核心可正常工作，每一部件都应具备形式化安全策略模型。然而，要求每一安全核心的形式化模型均相同，或要求网络具备全局的安全模型，而且每一子模型都正确反映分配于该部件之上的全局安全策略，是过分严格的。因为形式化模型的唯一功能是支持安全核心的评估，所以网络部件的负责人和设计者可以自由选择最有效达到该目的的、与部件的工艺特性相关的模型；按照需求，模型是安全策略的精确表示，而主体将由部件完成。

B3.5　网络策略要求的总结

综上所述，评估计算机网络系统的先决条件是具备全局的强制(如已具备)，自主和支持性策略，且上述策略被多个管理机构所接受并以人可访问的信息方式说明(如对计算机和网络系统可行)。在强制策略中，应具备一全局策略，它包括相对向前兼容的事件，如一个机构所使用的用户许可证如何与另一机构所使用的信息访问级别相关联；受特殊网络体系结构的影响，形成适当的自主或支持性策略将更具有挑战性。

B4　分部的 NTCB 观点的推导

B4.1　分部的 NTCB 简介

利用上述定义，可得以下结论。

假设：某主体在生命期内隶属于单独部件；该主体只能访问该部件上的客体。部件的通信链路不会威胁其上信息的安全。

则可得结论如下：所有部件参考监视器之总和形成网络的参考监视器。

该结论可成立，因为：

a. 所有网络访问是有中介的(因为不是局部的访问)；

b. 网络参考监视器不能被篡改(因为部件参考监视器不能被篡改)并易于合法化。(由上述推论可知，如果部件参考监视器可保证操作正确，网络参考监视器也可保证操作正确，不访问交叉部件的结构减小了附加的复杂度)。

在将上述基本理论扩展到非理想的网络系统之前，应检查使结论合法的每一先决条件，并简要说明每一项可达到当前网络工艺水平的原因。一般情况下，指定网络的负责人和网络设计师在评估之前要执行的关键的一步是，合法地将部件和通信信道分部以便于评估者验证其原理的合法性。

第 1 个原理是主体对单独部件的约束。传统的主体表示法〈过程，域〉可充分满足这一原

理，只要将主体对客体的访问限制在一个部件上，就可保证不会有包含一个以上部件客体的域。因此，即使允许“远程进程”存在(时常会发生这种情况)，也不存在从一个部件迁移到另一部件的主体。一旦远程部件上有事件发生，也就引进了新的主体(因为保护域发生了变化)。

第2个原理要求某主体只能在与其相关的部件内直接访问某客体。此处主要的理论是了解信息怎样在部件间传递而无须客体共享(详见B5)。从逻辑上讲，理想的通信信道上的部件连接，可视为信息从一个设备到另一个设备的直接发送(无须中介客体)，例如：“运动中”的信息不被视为客体——只要在它到达目的部件“停下来”前没有主体访问该客体即可，然后该信息便处于某客体之中了。

这种观点与GJB 2646中的定义一致，该定义称访问某客体即隐含访问该客体包含的信息。符合安全的通信信道中(在B6.2讨论)，不会有主体访问正在传输的信息，因此这类信道不必视为客体。上述论点也适用于包含内部主体的复杂信道，因此这类信道应继续分部。

第3个原理要求每个部件包含一个部件参考监视器，它完成该部件内与主体客体有关的网络访问控制策略。为验证这一原理，每一个部件内包含一个简化的部件参考监视器。例如，某指定部件内的主体和客体分别拥有相同的授权和安全级，因此按照控制策略，不会拒绝访问要求。每个参考监视器只需完成与局部访问有关的访问控制策略即可。

第4个原理要求部件间的通信信道不能破坏敏感信息的安全性。该原理的证明较繁琐，详见B6。在B6之前，本原理将做为边界条件允许在网络中作为单独可信部件评估，并允许这类部件合并进整体系统。

B4.2 分部的NTCB观点综述

在说明分部的NTCB概念以及GJB 2646标准如何适用于NTCB之前，假定由松散耦合的NTCB分部构成的网络运行在单机系统上(该计算机系统的TCB可由GJB 2646标准评估)。这一观点说明，将NTCB分部成若干松散耦合的NTCB分部在概念上可行并且不与当前的评估标准冲突。这一原理可以非正式地证明，安全网络可以简单地分部为安全的计算机系统。

B4.3 独立系统目标的特点

假定某个多处理器、多道程序的独立计算机系统，这一系统可达到GJB 2646标准的B2级或更高级别。该系统拥有一个形式化安全策略模型(如Bell或LaPadula模型)，并且与模型一致。在此系统中，假设TCB的代码和数据可在单总线紧耦合的并行处理器上共享。由于这是一个带有形式化安全策略模型的多道程序操作系统的独立系统，它可在任何处理器上支持上述过程，可以访问所需的内存段，并与其余处理器上的进程共享。另外，每一个进程可通过I/O信道使用设备。特别应假定的是，存在由TCB控制下各级可信进程控制的可用的多级I/O信道。每一多级信道都应符合GJB 2646标准中多级设备的概念。

B4.4 松散耦合的可信网络特点

假定某任意的网络体系结构由若干种结点组成，可处理多级信息并由多级通信信道相连。再假设该网络是安全的，并满足B3.1所述示的原理，即

每个主体驻留在一个单独部件上；

任何主体不能访问其它部件的客体；

每个部件都包含一个局部自律的参考监视器；

通信信道是安全的，不会破坏信息的安全性，主机由多级通信信道子网相连（该子网可能由部件和简单的通信信道组成）。每一部件内的主体可保证信息在部件间安全地交换。

端对端连接可以抽象为由通信介质相连的一对设备。广播信道可以抽象为由共享的通信介质相连的一组设备。预想的网络可能包含单级和多级连接。

B4.5 单独系统内网络的模拟

预想的网络可以自然方式模拟为单机系统。

网络中的每一个部件主体可模拟为单独目标系统中的单独主体。在一个部件上的所有网络主体可分配至单独系统的一个处理器上，并假定每个网络部件上存在一个可用的处理器。

计算机系统中的通信设备可视应用所需分为多级或单级的 I/O 设备。对每一设备，假定存在服务器主体，它可正确完成通信信道协议，对于多级设备，则拥有可信主体要求的可信特征。由于每个设备局部适用于网络系统的处理节点，所以它就局部适用于单独计算机系统，例如只能被该处理器访问。

最后，I/O 设备由系统外部的物理介质连接，对于端对端信道是成对的，对于广播信道是成组的。

上述模拟可以达到预想网络的精确表示。由于这是一个已评估的单独系统，因此它的安全性可以达到单独系统所要求的保证级别，并满足不同通信信道的通信安全级。在本标准 5.1～5.4 条中所描述的标准说明了模拟网络的方式。

B4.6 从单独模拟转化为分布式系统

不同处理器上的主体不能共享内存段。这是因为将单独网络部件内的所有主体分配到单独系统的单独处理器上，而主体不能访问不同部件的客体。

而且，不同处理器上处理的主体不能使用由 TCB 提供的进程通信机制，所有处理器通信机制由驻留在 I/O 设备驱动器上的 I/O 设备协议提供。由于这些协议在被模拟的网络中可用，所以它们的正确实现不依赖于内存共享，因此，可通过共享的物理资源提供远程设备合作。

这样，在安全核心之外，不含有任何两个不同处理器上的进程共享内存段。假设每一处理器拥有局部内存，所有应用段可以转移到合适的处理器局部内存地址空间，假如 TCB 的代码是“无瑕的”（如可重入），TCB 代码的全部拷贝也可以移到每个处理器局部的内存地址空间，而不会引起任何不良后果。同理，由单独处理器可访问的元素组成的 TCB 内部数据结构也可以转移到上述处理器的局部内存。

TCB 中必须与其它处理器共享的数据结构表示不同处理器上运行的进程所共享的资源。然而，在被描述的模型中，不存在这样的资源。网络中的设备对于网络部件而言是局部的，因此只能被计算机系统内一个处理器上运行的主体访问。处理器之间不会发生进程间通信，所需共享的全局内存是分配给主体的全局内存控制表。

这样，在网络的模拟环境里，不会出现共享资源的情况。代码和数据的分部可以允许 TCB 进行内部的再重构，因此 TCB 可以分部并转移到处理器局部的资源里，而不会有全局内存驻留的代码和数据。这种内部的可重构不会影响系统的运行，也不会影响与 GJB 2646 标准的一致性。

上述分部和 TCB 局域化的另一结果是不存在通过系统总线的通信，即：所有的 TCB 表都是局部锁定的，因此不需要 TCB 内的处理器间通信。再重构中的任一步骤都不会改变处理器总和构成单独 TCB 这一事实，也正因为如此，单独 TCB 可以看做是 TCB 分部的总和。

已分部的 TCB 是一系列 I/O 设备驱动器，每一个针对一个 I/O 设备。某特定设备只能由单独处理器上运行的主体使用。如果该设备不是局部的，设备主体的代码和数据也可以从 TCB 分部移到其它处理器上。此时，系统仍是模型的合法解释，并与标准一致。

系统中仍然只有一个 TCB，它分部于不同的异步处理器上，在需要支持局部设备的 TCB 分部内，其代码和数据支持不同的设备。物理处理器间唯一的联系是单级或多级通信信道。这些通信信道由通信安全技术保证其安全级别。

每个处理器及其相关设备可以分成单独的物理包。假定的单独系统与假定的网络系统中有些许差别，已分部的单独系统中的单独 TCB 可依然是单独 TCB，它可以转化成一系列 TCB 分部的总和，每个 TCB 分部负责完成局部或部件内的访问控制策略。

某特殊包内的 TCB 可由一个相同的 TCB(拥有相同的顶层说明和相同的保证级别)来替代而不会影响系统整体的安全或与 GJB 2646 的一致性。实际上，分部内所有的硬件或软件的 TCB 基础都可以替换，只要他们拥有相同的评估级别并且可以满足与其它部件相连的接口协议。

最后，基于每个包内 TCB 所建立的特殊形式化安全策略模型可以互有区别，只要每个模型都是网络安全策略的合法表示即可。

B4.7　有关模拟论点的结论

上述非形式化论点表明，处理节点的网络可以模拟成可评估的、带有安全核心的单独系统，而且系统可以分部成部件的总和，每个部件拥有一个 TCB 分部。模拟后的系统与原始系统在主要特点上相同，并与标准高度一致。这一论点可以为本标准的 5.1～5.4 条提供启发式基础。也可以这样认为，NTCB 分部的集合构成一个 NTCB，因为网络中只有一个安全策略，所以只应存在一个 NTCB，它由各 NTCB 在局部主体和客体上完成。

网络的设计与评估如欲达到较高的级别，一定要定义网络整体安全策略，并保证部件间的通信信道可以正常工作，无须一定要求每个处理节点都完成一样的安全策略模型。

B5　分部间的合作

本章主要考虑安全核心之外的 NTCB，例如完成支持策略并由可信主体携带的那一部分 NTCB。一些非核心的 NTCB 功能与那些不是网络的可信计算机系统相同，如局部用户的注册鉴定。这些 NTCB 功能可以看成是网络部件上完成的功能。

其它非核心 NTCB 功能提供不同的与网络有关的服务，我们称之为可信网络服务。通常，这些功能的主要任务是完成不同部件上可信主体间安全紧要信息传递所用的协议。可信协议是协调 NTCB 分部间合作的服务方式，例如它可能改变单级通信信道的安全级别。由于每个部件都可以在内部将与其相连的 I/O 设备重新标号，因此，就需要一个可信协议协调这种改变。

本章主要讨论两个例子以说明网络体系结构及相关可信网络服务间的关系。例 1 中的网络使用可信网络接口单元并保护线路分布，例 2 使用端对端加密方式，例子之后，讨论可信网

络服务的设计规格与验证。

B5.1 可信接口单元例子

某网络的不可信主体在不同的单安全级上通信，其网络接口单元(TIU)通过受保护的通信子网发送和接收有标号的信息。TIU 的功能是将信息敏感标号置于输出信息上并检查输入信息的标号，这样主机只能接收与其认证级别相符的信息。

由于通信子网可以携带各级信息，与任何 TIU 和子网相连的 I/O 设备应为较高级的单级设备。TIU 和主机之间的连接取决于主机的级别。这样，低级主机的 TIU 必须包含一个可以读高级信息写低级信息的可信主体。

B5.2 端对端加密例子

某网络内的主机可以通过可信的前端处理器(TFE)在不同的安全级别上通信，并可以通过公共通信子网接收和发送加密信息。假设 TFE 包含来自密钥发配中心(KDC)的被保护的信息级别的密钥，支持网络不同的安全级别并以主机方式与网络相连，KDC 在 TFE 的请求下发送密钥，并使用正确认可的协议来鉴别请求者和新的密钥。

计算机系统内完成参考监视器的硬件和软件部件称为“安全核心”，在 GJB 2646 中定义为：“可信计算基的硬件、固件和软件元素，构成参考监视器。它可以协调所有访问，可以防修改并可验证正确性”。

从定义可知，“安全核心”永远是计算机系统内 TCB 的一部分，是“计算机系统内保护机制的总和，包括硬件、固件和软件，它们一起负责执行安全策略。TCB 正确执行安全策略的能力依赖于系统管理者针对安全策略的正确输入”。尤其是 TCB 包括完成支持性策略的机制，而只有执行访问控制策略时才引用安全核心。

B5.3 设计规格说明与验证

为达到 A1 级要求的保证级别，需要 NTCB 形式化顶层规格说明(FTLS)，包括每个 NTCB 分部的部件 FTLS。正如在独立计算机系统中所述，尽管 NTCB 非核心部分所支持的策略不属于形式化安全策略模型所表示的访问控制策略，它们也应被说明。尤其应该说明在每一部件内支持可信网络服务的软件。

可信网络服务在何处支持强制策略取决于网络部件的 FTLS 中所包含的协议。最起码，每一 NTCB 分部内的可信主体规则应包含于每个部件 FTLS 中。为达到文档要求，应为每个可信协议提供说明以显示分部间的互连关系以及这些表示和部件 FTLS 相关部分的对应关系。

独立 TCB 中的 FTLS 包括操作系统内的虚拟实体，如进程、设备、内存段和访问表的表示，NTCB 的 FTLS 包括协议实体和虚拟实体的表示。

在端对端加密例子中，FTLS 与可信网络服务支持策略之间的对应关系包括在通信子网上传送的所有数据应以正确的密钥加密，KDC 只允许在访问控制范围内共享密钥。在可信接口单元例子中，对应关系应显示每一个 TIU 应在给定的主机标号上检查消息并给消息打标志。

B5.4 总结

网络中某些非核心的 NTCB 功能可视为可信网络服务。他们提供可信的协议以便不同

NTCB 分部上的可信主体可以完成安全相关的合作。这些服务的 FTLS 及其支持策略之间的对应性显示了特殊的优点，他们以网络专用的概念表达，显示了网络安全体系结构的关键。

B6　部件间的通信信道

本章详细讨论连接各部件的通信信道，旨在了解与系统安全性相关的特殊信道的特点，以及这些信道的评估方式与网络整体评估的关系，在认可过程以前，也应说明网络支持某应用的充分性。

本章结构如下所示：B6.1 讨论在 GJB 2646 中通信信道的概念，B6.2 定义符合安全的通信信道，其余部分讨论单级或多级信道例子。

B6.1　通信信道的基本概念

为达到 GJB 2646 的目的，网络被视为由部件及部件间连接所组成的系统。“通信信道”一词是“信道”的延伸，在 GJB 2646 中，“信道”指“系统中信息传送的路径”，这一术语也可指路径的运行机制。

先讨论“端对端”通信信道。“通信信道”和“I/O 设备”是不同的概念，通信信道是由通信介质耦合在一起的 I/O 设备。从部件的角度看，信息是以充分无错且物理安全的方式在设备上发送和接收，并满足与设备相关的标号要求。负责人和评估人都应按照信道的安全策略要求来确定上述条件是否已达到保证要求。这一需求是 NTCB 分部评估时的边界条件，它主要同错误检测与恢复机制、加密机制及其它通信安全机制一道完成。

图 B1　端对端通信信道

如图 B1 所示，两个处理节点由一条信道相连，处理部件 P1 利用 I/O 设备 D1 通过 I/O 设备 D2 与处理部件 P2 通信。假设 D1 和 D2 以某物理介质 M 相连。部件 P1 中的主体 S1 以下述方式与部件 P2 中主体 S2 传递信息，每个主体都包含某级别的客体，称为缓冲区，并与局部可用的设备相连，P1 中的 S1 将缓冲区中的信息传入 D1，P2 中的 S2 通过 D2 将信息写入缓冲区。此处无须指明共享客体或共享设备，当然通信细节依赖于共享的通信协议。

广播通信信道稍有区别。不是一对 I/O 设备通过物理介质相连，而是一组设备。每个设备都有接收和发送装置。每个发送装置传送的信息可由任何接收装置接收。

B6.2　评估基础——符合安全的信道

可信网络体系结构中的通信信道必须是符合安全的。如果在评估时，或在安装手册和可信设备手册中说明网络策略的完成依赖于信道的特性，那么该信道即为可信的。按第一种方法产生的已评估网络系统，其安全特性不受安装和配置的影响，第二种方法则深受其影响。当然，评估时的条件与限制应严格说明。

整体网络安全策略可以通过验证 NTCB 分部的正确性以及安装时是否达到所有通信信

道的环境要求而获得。本条将显示不符合安全的信道应该再生为符合安全的，以便于网络评估。有三种常用方法可用于再生符合安全的信道，

a. 在与信道相连部件的 NTCB 分部内控制使用负责安全紧要传输的信道；

b. 采用端到端通信技术并做为相连 NTCB 分部的一部分被评估，以减少信道物理环境对信道安全特性的影响；

c. 信道的固有特性应在可信设备手册中说明。

最后一种方法保留了特殊信道对认证者的充分性，正确的评估以通信信道为基础，此时假设通信信道具备所要求的特性。

评估工作集中在采用技术的正确性上，机制的充分性也是认证的一个方面。

利用上述技术可以得到符合安全的信道，例如密码术可以防止未授权的修改并可检测错误。在评估每一个信道时，以下外部环境因素的脆弱性和一个内部因素应予以考虑：

a. 通信安全性——传输过程中敏感信息的未授权的泄露或修改；

b. 通信可靠性——信息的不可靠发布，信息发布应由 NTCB 的正确操作完成；

c. 通信保真度——由于噪音引起的安全紧要数据(如传输中的安全标号)的改变；

d. 隐蔽记号——信道机制给信息隐蔽地标记；

如果要求信道驱动器的隐蔽信道分析，那么信道的隐蔽记号机制将做为正常的事件进行评估。

第一种脆弱性，即敏感信息传送时的安全性应由以下机制提供：

a. 可信设备手册中应明显标明已安装的信道完全符合安全范围；

b. 适合于端对端通信安全技术的信道应做为 NTCB 分部的一部分予以归档和评估；

c. 利用 NTCB 分部的内部控制，限制信道传送非敏感信息。

信道对敏感信息的不可靠发布的脆弱性可由以下三种技术解决：

a. 在可信设备手册中明文规定信道由高度可靠的介质和设备构成；

b. 为信道提供合适的端对端协议，使得与信道耦合的 NTCB 分部内信息能有效地传送并可以评估其正确性；

c. 限制 NTCB 分部内非紧要功能的分布并评估其正确性。

信道对噪音的脆弱性，可能会影响安全相关数据的正确性，可由以下技术解决：

a. 在可信设备手册中明文规定，信道由严格防噪音的介质和设备构成；

b. 为信道在 NTCB 分部内提供合适的端对端减少噪音技术，并评估其正确性；

c. 限制信道对 NTCB 非紧要功能的无噪音分布，并评估其正确性。

下面三个例子说明如何使用上述机制。

例 1，两个松散耦合的可信的合作处理器，一个处于活动使用态，另一个处于热就绪态，相连于指定的通信信道上。该信道将交换大量动态的安全相关数据，该信道必须可信地保护标号完整性并可靠而且无噪音地发布安全相关数据。噪音并不是设计问题。信道应该驻存在物理上安全的环境中。

最简单的评估策略是在可信设备手册中明文规定所需要的环境限制，信道必须安置在系统高安全范围中，必须由高度可靠和无噪音的介质和设备构成。在评估时，应验证上述限制的

有关文档。物理安装时所选信道的一致性较易被评估。这种评估方法的好处是版本升级时，可以无须再评估。

例 2，若干单级主机通过多级包交换机制相连以模拟单独级别主机构成的网络。主机与包交换之间的通信以包内部硬通信端口所决定的标号进行。通信信道必须是安全的，但无须可靠和无噪音。

有两种不同的方法可以评估上述体系结构。第一种方法较自然，将体系重构，将包交换机制视为网络部件，通过单级别信道与每一主机相连。网络文档中说明每一新信道都限制在系统安全范围内，安全相关信息在传输中不要求可靠性和保真性。第二个原理在评估中验证，第一个在认可中验证。

第二种方法较极端，它要求包交换是通信信道的一部分。这种情况下很难在评估时显示包交换机制符合安全性。负责人将在文档中说明主机的互连限制而且每一信道应限制在安全范围内，这样评估时可以包含包交换，但这与网络评估说明抵触。在端对端虚信道中使用多级包交换机制以达到文档所需的安全范围是认可人员针对单独系统的责任。在将上述策略应用于指定系统时，应运用附录 C 的技术。

例 3，两个可信多级系统通过信道传送文件，该信道不防噪音、不可靠也不安全。数据全加密，由非 NTCB 软件完成可靠的传输。

通信安全和密码树技术应包含在已评估的 NTCB 分部中。他们的正确性是评估的一部分，他们的充分性和基于传输信息的真实敏感级是认可的一部分。为实现信道可靠性，应归档并评估 NTCB 内部控制机制，该机制可以阻止所传输的信息使用信道。

B6.3　多级通信信道的 GJB 2646 标准

本条从预防内部危胁的角度讨论与网络中使用通信信道有关的 GJB 2646 标准。由于 A1 级准则是最严格的而且是所有级别中需求的全集，所以从 A1 级开始讨论。

在 A1 级标准中要求："TCB 支持将最小最大的安全级别分配到所有相连的物理设备"。如果网络由部件通过通信信道连接而成，物理环境应包括设备及连接设备的介质。为信道分配访问级别时，必须考虑介质所具备的物理安全性、应用于介质上传送安全信息的通信安全技术、信道上设备的物理可访问性、节点在网络的结构中所处的角度，以及信道的预定用途。由于这些限制，标准要求正确地为信道上的设备作标号。例如某信道可能被分配为只支持从"未分类"到"秘密"范围。这种标号由 NTCB 分部的网络安全策略要求。

除了为耦合网络处理部件与通信信道的设备标号外，GJB 2646 还要求标号输入和输出信息的多级信道："当 TCB 输出时，敏感标号应准确而无二义性地表示内部标号并与输出信息相关"，而且，"当 TCB 通过信道向某客体输入或输出时，信道使用的协议应该在敏感标号和相关信息之间提供无二义性的连接"。该标准从网络通信信道角度要求信息在输出时正确地被标号，并在输入和输出设备之间共享协议，而且可以无二义性和正确地保持标号信息的相关性，输入标号由接收方 NTCB 分部负责。此处，无须再度强调与标号信息相关的完整性。

B6.4　单级通信信道

标准要求"TCB 应把最大和最小敏感级别分配到所有相连的物理设备上"并且"执行由设备所处的物理环境施加的限制。"此处的设备包括所有单级和多级设备。单级设备与信道的特

点在5.1～5.4条说明，“不要求单级I/O设备和信道维持所处理信息的敏感标号。”因此，不能支持所传送信息标号的设备和(或)信道毫无疑问是单级的。

耦合信道和处理节点的设备的最大安全级和最小安全级可能相同也可能不同。

所有设备的最大和最小安全级都相同的情况是正常情况，此时信道上传送安全级不变的单级信息。

与单级设备相连的不同设备也可能其最大和最小安全级不相同。此时，信道可能携带未标号信息，但一次只携带一个安全级的信息。与信道耦合的NTCB分部负责阻止与当前信道上安全级不同的信息的传送，这一点与“TCB应提供一种机制，TCB和某授权用户可以通过该机制指定通过单级通信信道或I/O设备输入或输出的信息的唯一敏感级”相符。在NTCB分部，这意味着某一级别的未标号信息可以从一个授权用户那里人工转移到另一个授权用户。上述标准要求每个NTCB分部内应有一个可靠协议控制对信道的访问，并且信息在信道上传送之前，级别的改变应有序地进行。

B7　其它考虑

B7.1　参考监视器，安全核心和可信计算基

“参考监视器”是初级抽象概念，允许有序地评估单独计算机系统是否执行强制和自主性访问控制。

GJB 2646中“参考监视器”概念是“一种访问控制概念，是联系主体访问客体的抽象机制”。虽然参考监视器包含保护的概念，但该功能本身独立于任何访问控制策略。该功能假设系统由一系列活跃的实体(即主体)和一系列被动实体(即客体)组成。主体与客体间的控制关系(如主体访问客体)，按照参考监视器要求，只有在访问控制策略允许的情况下，访问才合法。因此参考监视器也可视为系统资源的管理者，特殊点是该功能在与其控制下的主体和客体之间有一个定义良好的接口。为有效地提供保护，参考监视器的实现应该：

a. 防止冲击；

b. 允许访问；

c. 简单，以便于支持高级保证的分析。

简明地讲，网络体系结构应具备以下显著特点：

a. 在多级部件内的主体和客体应符合GJB 2646说明；

b. 主体和客体应限制在单独部件内，即主体不能访问不同部件上客体；

c. 部件内表示主体与客体访问相关状态的信息，应由该部件上NTCB分部局部维护。

依照上述规则连接处理器与外设的网络可粗略地被认为具备松散耦合的安全核心的网络。由于访问的局部性，每个安全核心都是自治的。一个部件上主体可在两个安全核心的控制下将信息传送到另一主体。然而，由于所有的访问都是局部的，所以所有的访问都是安全核心在部件内进行协调的。因此，系统内所有安全核心的总和可以充分协调系统内的所有访问；

B7.2　网络可信计算基与参考监视器

在较高级别的系统中，TCB、安全核心和参考监视器可以不加明显修改直接应用于可信网络评估。特别是NTCB可定义为在网络中执行所有安全策略保护机制的总和。该定义隐含表明被评估的系统有单独的NTCB，而NTCB是完成预定策略机制的总和。

GJB 2646 要求在较高评估级别系统中，参考监视器是 TCB 的一部分。这种技术虽然在理论上不能保证高保证度的系统，然而却是当前具有已被证实的记录的技术，而且也是当前能较经济地实现的最好技术。

基于上述原因，本标准 5.1～5.4 条应该从实效的角度定义安全网络，而且 GJB 2646 中“参考监视器”和“安全核心”应尽量少改动以应用于较高评估级别的系统。因此要求 B2 级可信的网络及更高级网络应包含参考监视器的物理实现，协调网络内主体对客体的访问，而且它应是防冲击的还应足够小以便于验证合法性。

B7.3 NTCB 分部

在本标准中，“网络系统”意味着网络可分割成“部件”，每个部件具有不同的处理和通信功能，因此 NTCB 的功能也必须分配到网络的部件上。

单独网络部件内负责完成网络安全策略的硬件、固件和软件机制的总和称为部件内 NTCB 分部。由于网络部件和信道是周密而不相交的，因此 NTCB 分部所组成的 NTCB 也是不重叠且完整的。

对于强制访问控制而言，有一种较大而有用的网络，它允许 NTCB 分割成 NTCB 分部。可以利用 GJB 2646 中的有关说明评估分部内的强制访问控制，而且也易于证实部件分部后执行强制访问控制的正确性。负责人如欲得到整体网络评估结果，应选择这种网络。

密钥发配的目的是在 TFE 内支持可信局部服务，即通过子网从主机把已分类的消息发送到未分类的适于传输的加密消息中。换句话说，存在可以读高级信息写低级信息的可信主体。

部分可信网络服务在 KDC 内部完成，KDC 为正在传送的信息级别生成密钥，并在访问控制策略的基础上决定哪些 TFE 可以共享密钥；由 KDC 内密钥决定的某级信息的单级主体无须 KDC 核心的特权服务，不过不同级别上的可信网络服务必须正确执行特定策略和协议。

B8 结论

本附录主要讨论如何将 NTCB 分成可合作的、松散耦合的 NTCB 分部的原理。每个 NTCB 分部都可视为局部自治的参考监视器，执行局部主体对局部客体和设备的访问。由于分部可弥补部件间不能共享客体的缺点，因此，NTCB 分部的集合体可充分协调所有主体对客体的访问，因此也可以形成系统参考监视器的基础。在松散耦合的前提下，网络全局安全策略，也可解释为单独的形式化安全策略模型在每个部件中执行访问控制，并且足以证明每个部件都满足安全策略要求。网络体系结构和设计也可以评估其支持策略的能力，并达到预定评估级别。

附录 C
已被认证的 AIS 互连
（补充件）

C1 目标

正如在本标准中所述：许多“网络”因为复杂而无法确切用一个评估等级来反应其可信度，因而不能评估为“单级安全网络”。本附录旨在为强制性安全策略的系统提供互连指南。

C1.1 问题阐述

互连的已被认证的自动信息系统(AIS)是一种操作特性，AIS 认为网络的各部分可独立地创建、管理和认证。互连的已被认证的 AIS 可由多个系统组成(某些系统可能是安全的)，这些系统可具备独立的认证范围，因此系统可同时处理不同安全级的信息。在这种观点下，独立的 AIS 可视为“设备”，可与相邻的系统发送和接收信息。每一 AIS 被认证为可处理单级别的敏感信息。

下例说明何时采用互连的可认证的 AIS 系统，某网络由两个 A1 级系统和两个 B2 级系统构成，均已互连并可被用户局部访问。很明显，如果视该系统为单级安全系统，则其可信度按 5.1～5.4 条的标准，最多为 B2 级。实际上，B2 级不能正确反映两个 A1 级系统及其互连的可信度，因此给该网络定为 B2 级是不确切的。

采用互连的 AIS 观点有助于找到正确的互连策略。

C1.2 部件互连观点与全局网络观点

网络中互连的已认证的 AIS 观点包括两部分内容，部件互连观点和全局网络观点。下面将分别讨论这两点并加以详细分析。

每一个与其他 AIS 连接的 AIS 都应执行“互连规则”，用以限定发送和接收信息的安全级。若使用部件互连观点，每一部件负责分离多级信息并局部确定某信息是否可以被发送和接收，此时该部件无须了解网络中其余部件的认证等级(除了与之相邻的部件之外)。

除了互连规则以外，为防止潜在的安全问题，还可以在网络中增加一些限制。全局网络观点就说明了这些限制。这种观点要求每一部件应获悉网络中其余部件的认证等级。在决定某部件是否可合并进某系统时，将考虑这些等级。这样，信息被泄漏或修改的潜在危险将限制在可接受的范围。

“级连问题”可以说明在网络中加入哪些限制。在可接受级别以上发生未授权的泄漏或修改，就会发生级连问题。网络负责人可以通过限制互连的 AIS 的认证级别来限制这类事件的发生。

C2 认证范围与互连规则

C2.1 认证范围

认证范围反映了网络中的互连部件分离和处理指定敏感信息的能力。可以指定某已被认证的计算机系统等同于一个系统高安全级的单安全级系统。这样的系统不能分离实际处理信息的安全级。所有从该系统输出的信息必须分配高安全级标号，直到某部件被人工赋予一个

较低标号为止。单独的多级 AIS 的认证范围可能等于所处理信息级别的全集。这时，输出信息的标号等于认证范围内所处理信息的实际级别。

在网络中，认证范围将限制输出输入信息的安全级。如果某网络只有专用和系统高级的部件，每一部件将只有单值的认证范围(如认证范围只有一个安全级)。

下例，如图 C1 所示：部件 A 是 B2 级系统，其认证范围为秘密到机密。部件 B 是 A1 级系统，认证范围为秘密到绝密。这样，若部件 A 与部件 B 直接相连，认证范围将限定信息传送的级别不能超过“秘密”。

图 C1　认证范围图示

C2.2　互连规则

多级网络中的一些用户无须了解所处理的全部信息。因此，多级网络可以处理一定范围内的敏感信息并且防止未授权的泄漏和修改。

网络中每一部件必须独立地被认证为可以安全操作，并认证一个指定范围的级别。部件以这些级别合并入网络并唯一保持这些级别。

按照这些定义，多级网络可能由指定系统的高的、多分部的、可控的和多级的部件组成，两个或两个以上的部件分类范畴和(或)分部应该有所区别，而且一些用户无须具有所有正式的认可。

多级网络必须满足以下要求。

C2.2.1　信息传输限制

AIS 通信所使用的每一个 I/O 设备必须有一个与之相对应的设备范围。该范围可以是单级的，也可以是多级的(此时设备应为多级的)，而且它必须包括在 AIS 认可的范围内。

从单级设备输入输出的信息将由该设备的安全级隐式表示，从多级设备输入输出的信息必须由共同认可的协议加以标号，只有当通信链路只携带单级信息时，信息标号可隐含。

从指定的安全级别输出的信息，其接收设备的范围应包含或高于该级别。若输入设备不包含该级别，信息将重新标号为输入设备范围内的较高级别，反之，不能进行重新标号。

C2.2　讨论

设备标号可以反映并限制设备所处的物理环境中可以授权的信息的安全级。

只有具备一个设备到另一设备(该设备范围不包括前一设备标号)的单工无确认传输，并且接收设备的每一标号均低于发送设备的标号范围时，才可以进行信息传输。否则，不允许信息传输。

途经若干 AIS 而发送信息的 AIS 系统可无须了解最终端点系统的认证范围，但这样做有利于网络性能，因为若初始的 AIS 可获知信息不能发送，它将放弃发送请求，因此减少网络资源浪费。

在互连的已认证的 AIS 中，部件的认证范围及网络接口设备的设备范围将由部件管理员和网络管理员共同设置。这些范围一般为静态值，任一改动将视为网络的重新配置。

综上所述，如果遵循互连规则，信息不可能发送到未经认证的不能接收该级别信息的部件上。

C3 全局网络观点

以上规则适合于任何两个或多个已认证的系统之间的通信，但不包括其余的可能存在于网络中的限制。即使所有部件已被评估而且遵循互连规则，也仍有潜在的安全问题。为解决这些问题，应采取全局网络的观点。也就是说，不能在局部决定是否满足某限制。下面讨论两种全局观点，一是局部风险传播，二是级连问题。

C3.1 局部风险传播

建议在指定的环境里使用最小限制的可信系统。应该在最小体系结构要求上具备正式的技术裁决并能够应付指定级别的风险。

在许多情况下，操作需求使系统被认证为多级操作系统因而不能满足推荐级别的要求。从而使某特殊 AIS 用户承受更多的风险，将这样的 AIS 系统合并至网络中，会使所有的 AIS 用户承受附加的风险。

因此，当某未评估的 AIS 或未达到推荐级别的 AIS 欲合并进网络时，应考虑以下限制，如单工联系、传输的人工浏览、密码术隔离，或其他措施以限制它带来的风险。

C3.2 级连问题

另一个互连规则未解决的问题是级连问题。当某穿透者利用网络的连接优势，利用一个高于所有部件上安全级的级别来泄漏信息时，就会发生级连问题。在每一个互连网络中，如果所处理信息的级别高于所有部件可处理的级别，就可能发生级连问题。

下例中有两个系统，每一系统都已认证可以处理两个相邻级别的信息，如图 C2 所示。

图 C2 级连问题示意图

系统 A 处理机密和绝密级信息，所有用户应最小为机密级。系统 B 处理秘密到机密级，所有用户最小为秘密级。

在这两个分系统内部，由于只有两级用户，几乎不存在泄漏风险，而整个系统有三级信息，就增加了泄漏的可能。如果两个系统连接后，可以互传机密信息。这样某穿透者可通过秘密级获知加密信息，从而破坏保护系统。

考虑这样的事件链，

a. 系统 A 的穿透者越过保护机制将绝密信息降至机密；

b. 将降级的信息传送至系统 B；

c. 越过保护机制将同样的信息降级至秘密级。这时就会发生级连问题。

C3.2.1 问题标识

有多种不同复杂度和精确度的方法识别潜在的级连问题。本附录讨论其中两个。第一种方法是利用嵌套情况以保证系统不存在级连问题；另一种在下面章条中讨论，是一种比较不保守而且更具启发性的方法，该方法考虑了网络的互连以及部件 AIS 的评估级别。

如果两个 AIS 系统的认证范围不相斥（无相同级别）或互相嵌套，即一个包含另一个，即可满足嵌套条件，在大多数情况下，利用嵌套条件足以决定是否存在级连问题。不过这是一种较为保守的测试，有时会不满足嵌套条件但也不存在级连问题。

例 1： 图 C1 中部件 A 的认证范围是从秘密到绝密，它完全包含在部件 B 的认证范围秘密到绝密中，因此，不存在级连问题。

例 2：图 C2 中系统 A 与 B 的认证范围不相斥，而又不能完全包含，因此会产生级连问题。

例 3：图 C3 不满足嵌套条件，因为系统 A 与 B 既不相斥也不完全包含，因此可能产生级连问题。实际上，从下文的讨论可以看出，由于使用端对端的加密设备，图 C3 不会发生级连问题。

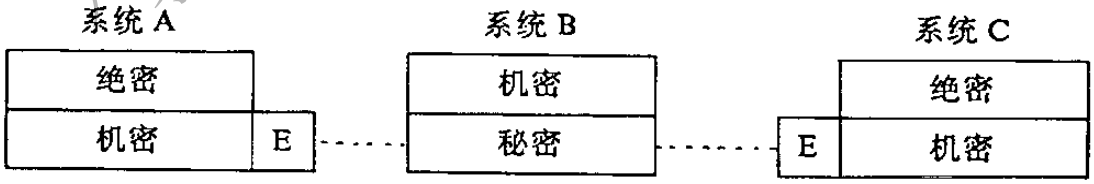


图 C3 级连问题（端对端加密）

C3.2.2 解决方案

可以有若干途径解决级连问题。一是在网络的适当部位使用更加可信的部件，于是穿透者将无法越过保护机制从而避免泄漏。如图 C3 所示，如果系统 A 或 B 中的任一个评估级别为 B3，就足以应付绝密到秘密的认证范围，穿透者将会遇到极大的困难。

另一种可能的解决途径是减少相应的网络连接，或者采用物理上的端对端加密方式。端对端加密只允许欲通信的主机进行加密，从而减少路径上不必要的级连风险。

如图 C3 所示，假设系统 A 欲与系统 C 通信，而 B 仅为中介结点。可能发生的从 A 中绝密

降至 B 中秘密的级连问题可由从 A 到 C 的端对端加密解决，因为从 A 到 C 的加密数据，即使在 B 中降级为秘密也不会引起泄露。

注意：端对端加密方式对图 C2 毫无帮助，因为发生级连问题的部件必须参与通信。

在一些可能发生级连问题的情况下，发生级连问题的风险没有想象中那么大。如上所述利用网络连接的穿透者，一般都要求连接双方的合作，而使用相同的软件及用户，在一般情况下是较少见的。因此，可不予考虑连接上的级连问题。

从更全局的观点来看，可将网络分为若干可能发生级连问题的通信体。如果从一个通信体到另一通信体间不可能发生级连问题，级连分析只须在每一通信体内部进行。

C3.2.3 已评估系统的网络

如果欲互连的系统可评估为某级别，则该级别可用来分析并发现级连问题并测试其解决方法。开发分析过程的第一步是形式化描述级连问题存在与否的必要条件。

下面引入级连条件这一术语。满足级连条件的网络不存在级连问题。该条件以互连系统的评估级别及其连接的方向和安全级的形式给出。

为形式化描述级连条件，仍须引入一些定义。下述各词仅适用于本节。

a. 保护域：(h, s)，h 为某网络部件，s 为其安全级；

b. 步骤：保护域(h1, s1)，(h2, s2)的有序对，其中：

或 s1＝s2　而且 h1 以 s1 的级别向 h2 发送

或 h1＝h2　即：信息在部件内流动

c. 路径：一系列保护域，每一对相邻保护域为一步骤。

步骤是一系列保护域，数据可在其上一步一步地来回移动。数据链上的步骤在以下两种情况下可能发生，一是携带给定级别信息的某部件通过直接通信信道到达另一部件；二是两部件间无直接连接信道，但有端对端加密连接，而且中介节点不可读数据。同一部件上两域之间的步骤可能是一个隐蔽信道。

已知某主机 h，令 L(h)为 h 的用户最小许可证，已知某安全级 s，可得系统所要求的风险率的最小评估级别为 C(s, h)。除非路径上所有系统均闭合，否则均应满足开放系统要求。注意：如果 s 与 L(h)的相关风险系数大于 0，C(s, h)最小为 B1。

根据以上定义可得级连条件为：

对于任一路径(h1, s1)，……，(hn, sn)，其中 sn＝L(hn)且 C(s1, hn)最小为 B1，必存在一(hi, si)，(h(i＋1)，s(i＋1))，其中 hi＝h(i＋1)，hi 的评估级别最小为 C(s1, hn)而 si 不属于 s(i＋1)。

上述条件亦可逆述为：任一路径上的某部件 h 的隐含用户欲在 s1 级泄漏信息，必得超过某 C(s1, hn)级部件上的保护机制。

C4 确定某连接是否可行的启发式过程

可以利用一些方法来决定某系统的风险概率是否远大于其评估等级及其部件评估等级。因为风险率不能大于指定的推荐值，故下述启发式算法可以检验系统并决定是否超出规定的界限。(以正式术语来讲，本算法是级连条件的近似测试)。注意，该算法并不是规定性的，它仅是检查问题的一种途径，还有多种合法的方式。

如同其他启发式算法一样，本算法不能从原理中得到，它主要依靠实验和错误，并可产生合理结果。

本算法不能解决所有的网络安全问题，只能在互连系统时，提供谨慎而有用的指南和建议。

下述算法可决定，由已评估部件组成的某网络是否达到规定的风险范畴。该算法把网络分为若干组，每一组由可交换信息的部件组成，这些部件可在公用安全级上发送和接收信息，评估级别等于或小于指定级别。

某指定值的风险率将与最大可允许的风险率比较，以决定某通信体是否发生不可接受的风险。

a. 创建一网络表，列出网络中所有部件。如表 C1 所示，该表应包括每一部件的以下信息：部件标识符、评估等级、部件向网络发送数据的安全等级范围、部件从网络接收信息的安全等级，部件从网络接收信息及可处理信息的最高级别，可直接访问部件的用户的最小许可证及向网络发送信息的最低级别。

表 C1　例表

部件标识符	评估级别	发送数据的范围	接收数据的范围	最大级别	最小级别
节点 A	B2	TS	S	TS	S
节点 B	A1	S C	S C	TS	FOUO

b. 创建一个网络表评估级别、网络表最大值及网络表最小值。网络表评估等级是表中所列部件的最高评估等级(表 C1)中为 A1。网络表最大值是所有部件向网络发送数据的最高级别(该项由“最大级别”一栏的最大值决定，表 C1 中为 TS)。网络表最小值为部件接收信息的最低级别(该项由“最小级别”一栏的最小值决定，表 C1 中为 FOUO)。

c. 如果网络表评估级别大于 B1(如 A1，B3 或 B2)，则必须建立低于网络表评估级别的小表格，直到 C1 级小表格。应在每一评估级上建立小表格，并首先列出任一评估等级低于或等于该小表评估级别的部件，然后，向表内增加符合下列三个条件的部件：

评估等级等于或低于表格等级的部件；

从表中部件接收数据的部件；

发送数据的级别等于或小于表中节点的部件。

d. 所有的小表都建好后，每一小表的网络表评估级别将按照规则与大表的最大最小值比较。

e. 若所有大表满足要求，则网络满足保证要求。如任一大表的风险率高于允许值，则网络为高风险级，不能按当前设计方式连接。

表 C2　B2 级表 1

部件标识符	评估级别	发送数据的范围	接收数据的范围	最大级别	最小级别
A	B2	S	S	S	S

表 C3　B2 级表 1　扩展表

部件标识符	评估级别	发送数据的范围	接收数据的范围	最大级别	最小级别
节点 A	B2	S	S	S	S
节点 B	B2	S C	S C	S	C

表 C4　B2 级表 1

部件标识符	评估级别	发送数据的范围	接收数据的范围	最大级别	最小级别
节点 A	B2	S	S	S	S
节点 B	B2	S C	S C	S	C

表 C5　B2 级表 2

部件标识符	评估级别	发送数据的范围	接收数据的范围	最大级别	最小级别
节点 A	B2	TS	S, TS	TS	S

C4.1　B2 级表例

表 C2 是在单入口下建立的 B2 级表。如果网络中存在另一节点，评估等级为 B2，并可在 C－S 级收发消息，这一节点将加入到表 C2 中形成表 C3。反之，如果存在 B2 级节点，可在 S－TS 上接收信息而只能在 TS 上发送信息，它将不加入表 C3 而是形成另一个 B2 级表。于是如表 C4 和表 C5 所示，有两个表格。

部件标识符	可允许操作
A	从 TS 级到 C 级接发信息
B	只能在 TS 级接发信息
C	只能接收审计记录，所有记录须在 TS 级
D	从 TS 级到 C 级接发信息
E	只能在 S 级接发信息
F	接发 S 和 TS 级数据

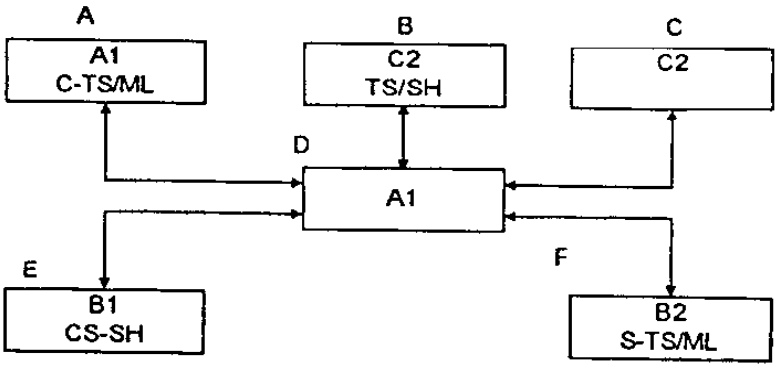


图 C4　例网络

C4.2　例网络与表格

图 C4 说明了一个例网络，由此产生的表格请见表 C6 到表 C11

网络表评估等级＝A1
网络表最大值　＝TS
网络表最小值　＝C
是否符合标准　＝OK

表 C6　网络表格

部件标识符	评估级别	发送数据的范围	接收数据的范围	最大级别	最小级别
A	A1	C－TS	C－TS	TS	C
B	C2	TS	S－TS	TS	S
C	C2		C－TS	TS	C
D	A1	C－TS	C－TS	TS	S
E	B1	S	S	S	S
F	B2	S－TS	S－TS	TS	S

注意：由于没有 B3 级部件，故 B3 级表与 B2 级表相同，此处不再重复。

在 B2 级，网络由 2 个表格表示：表 C7 和表 C8。这是因为部件 C 只能接收数据。这类部件总是以自身为表格的结尾，因为他们永远也不会影响网络中其他节点的安全。唯一要考虑的问题是他们所接收的信息级别是否处在可处理的最大级别内。

在 B1 级，每一部件拥有一个表格(C9，C10，C11)。原因是虽然部件 B 可能从部件 E 接收

数据，但永远不会以低于 E 所发数据的级别向网络发送数据（如 B 只能以 TS 级发送数据，而不会以 C 或 U 级发送）。这样，B 从 E 接收数据不会有附加风险。如果 B 可能以低于或等于 E 的级别发送数据，他们将处于同一表格，因为这将引起附加风险。

表格评估级别　＝B2
表格评估最大值＝TS
表格评估最小值＝S
是否符合标准　＝OK

表 C7　B2 表 1

部件标识符	评估级别	发送数据的范围	接收数据的范围	最大级别	最小级别
F	B2	S－TS	S－TS	TS	S
E	B1	S	S	S	S
B	C2	TS	TS	TS	TS

表格评估级别　＝B2
表格评估最大值＝TS
表格评估最小值＝TS
是否符合标准　＝OK

表 C8　B2 表 2

部件标识符	评估级别	发送数据的范围	接收数据的范围	最大级别	最小级别
C	C2		TS	TS	TS

表格评估级别　＝B1
表格评估最大值＝S
表格评估最小值＝S
是否符合标准　＝OK

表 C9　B2 表 3

部件标识符	评估级别	发送数据的范围	接收数据的范围	最大级别	最小级别
E	B1	S	S	S	S

表格评估级别　＝B1
表格评估最大值＝TS
表格评估最小值＝TS
是否符合标准　＝OK

表 10　B1 表 2

部件标识符	评估级别	发送数据的范围	接收数据的范围	最大级别	最小级别
C	C2		TS	TS	TS

表格评估级别　＝B1
表格评估最大值＝TS
表格评估最小值＝TS
是否符合标准　＝OK

表 C11　B1 表 3

部件标识符	评估级别	发送数据的范围	接收数据的范围	最大级别	最小级别
B	C2	TS	TS	TS	TS

C5　有关环境的事项

由于网络的最基本特性，有必要描述网络链路上的物理与逻辑假设。本标准的 5.5 条适用于单独的安全系统，而不是本附录的网络系统，这一点对于互连的已认证的 AIS 系统同样重要。因此，本章将描述一些重要事项。有兴趣的读者可参见 5.5 条。

本附录的目的并非定义适用于所有环境下的措施，而是标识一些要求和达到预定保护的一般方法。

本附录描述了在未分级网络中控制信息的完整性保护要求以及其他网络控制数据与信息的完整性需求。

C5.1　通信完整性

认证员将定义互连两部件时所需的传输精确性要求。部件互连所涉及的元素都应满足该

要求。因为不可能达到绝对精确，所以应具备检测、发现和报错的能力。可单独或合并使用以下方法限制错误：密码术校验和、被保护线路及可靠分配协议等。

对于两个已认证部件的互连链路上的所有元素，可使用硬件和(或)软件阶段性检查其操作的合法性。应预备网络元素之间的可信通信路径，以备端对端安全通信所需。(初始化、密码术密钥管理、改变主体、改变客体安全级或改变访问所有权等)。

C5.2 拒绝服务

认证员定义拒绝互连部件所提供服务的条件，硬件和(或)软件将阶段性保护互连部件的可访问性。

C5.3 保护数据内容

当逻辑上互连的两部件交换分类信息或未分类但为敏感信息时，每一部件的 DAA 应保证通信内容不受未授权的截获。提供这一保护的方法有密码术、被保护的线路分布式系统(PWDS)。

如果连接的基本结构由服务方为一系列子用户建立，那么服务方应该选择适当的通信保护。不过单独的 DAA 应有责任决定该保护对于所交换的信息是否完备。

附加说明：

本标准由中国航天工业总公司提出。

本标准由中国航天工业总公司七〇八所归口。

本标准由中国航天工业总公司七〇六所起草。

本标准主要起草人：房其敏、王轶昆、卜宗义。

计划项目代号：6HT07。