ICS 03.220.50
V 54
备案号：

MH

中华人民共和国民用航空行业标准

MH/T 4018.2—2004

民用航空空中交通管理管理信息系统技术规范 第2部分：系统与网络安全

Technical standards for air traffic management of civil aviation management information system— Part 2: System and network security

2004－12－20 发布　　2005－04－01 实施

中国民用航空总局　发布

目　　次

前　言

MH/T 4018《民用航空空中交通管理管理信息系统技术规范》分为三个部分：

——第1部分：系统数据与接口；

——第2部分：系统与网络安全；

——第3部分：系统网络与接入。

本部分为MH/T 4018的第2部分。

本部分由中国民用航空总局空中交通管理局提出并负责解释。

本部分由中国民用航空总局航空安全技术中心归口。

本部分由中国民用航总局空中交通管理局负责起草，中国民用航空东北地区管理局空中交通管理局参加起草。

本部分主要起草人：吕小平、李朝阳、齐鸣、李作明、赵凡、闫鹏、郑雪松、唐朝达、邱镭。

民用航空空中交通管理管理信息系统技术规范
第2部分：系统与网络安全

1 范围

MH/T 4018的本部分规定了民用航空空中交通管理（以下简称空管）管理信息系统与网络安全的技术规范。

本部分适用于空管管理信息系统的设计与建设。

2 规范性引用文件

下列文件中的条款通过MH/T 4018的本部分的引用而成为本部分的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本部分，然而，鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注明日期的引用文件，其最新版本适用于本部分。

GB/T 2887—2000 电子计算机场地通用规范

GB/T 9387.2—1995 信息处理系统 开放系统互连 基本参考模型 第2部分：安全体系结构(idt ISO 7498-2：1989)

GB 17859—1999 计算机信息系统 安全保护等级划分准则

GB 50174—1993 电子计算机机房设计规范

GA/T 387—2002 计算机信息系统安全等级保护网络技术要求

GA/T 388—2002 计算机信息系统安全等级保护操作系统技术要求

GA/T 389—2002 计算机信息系统安全等级保护数据库管理系统技术要求

GA/T 390—2002 计算机信息系统安全等级保护通用技术要求

ISO 9001：1994 质量系统 设计研制、生产、装配和维修的质量认证规范

3 术语和定义

GB 17859—1999、GA/T 387～390—2002、GB/T 2887—2000所确立的术语和定义均适用于MH/T 4018的本部分。

4 物理安全

4.1 环境安全

4.1.1 中心机房的安全保护

4.1.1.1 机房场地的选择应符合GB 50174—1993中2.1的要求。

4.1.1.2 机房内部安全防护应符合GB 50174—1993中4.2的要求。

4.1.1.3 机房防火应符合GB 50174—1993中4.3的要求。

4.1.1.4 机房供电、配电应符合GB 50174—1993中6.1的要求。

4.1.1.5 机房空调、降温应符合GB 50174—1993中第3章的要求。

4.1.1.6 机房防水、防潮应符合GB 50174—1993中第7章的要求。

4.1.1.7 机房防静电应符合GB 50174—1993中6.3的要求。

4.1.1.8 机房接地与防雷击应符合GB 50174—1993中6.4的要求。

4.1.1.9 机房电磁干扰防护应符合GB 50174—1993中3.2的要求。

4.1.2 **通信线路的安全防护**

4.1.2.1 应采用有效措施，预防线路截获，使线路截获设备无法工作。

4.1.2.2 应设置线路截获探测装置，及时发现线路截获事件并报警。

4.1.2.3 应设置线路截获定位装置，及时发现线路截获、窃取设备的准确位置。

4.1.2.4 应定期测试信号强度，检查是否有非法装置接入线路。

4.1.2.5 应定期检查接线盒及其他易被人接近的线路部位。

4.1.2.6 应定期检查传输线路各线段及接点，更换老化变质的电缆。

4.1.2.7 传输线路应采用屏蔽电缆并有露天保护或埋于地下，远离强电线路或强电磁场发射源，以减少由于干扰引起的数据错误。

4.1.2.8 铺设室外电缆应采用金属铠装、屏蔽电缆或加装金属套管，以减少各种监控辐射对线路的干扰。

4.1.2.9 调制解调器应放置在受监视的区域，以防止外来连接的企图。应定期检查调制解调器的连接是否有篡改行为。

4.1.3 **信息传输安全**

4.1.3.1 密级信息到达终点之前，不应呈现明文状态。

4.1.3.2 传输密级信息时应进行网络加密，如链路加密、节点加密和用户加密等。

4.1.3.3 为保证密级数据的安全传递，应有备份的网络节点机。

4.1.3.4 不传送信息时接口应阻断。

4.1.3.5 应具有辨认正当通信伙伴的功能。

4.1.3.6 用拨号线能接触网络时，拨号码应予以保护、同时保密信息不宜存放在节点机内。

4.2 **设备安全**

4.2.1 **设备的防盗和防毁**

4.2.1.1 计算机系统的设备和部件应有明显标记。

4.2.1.2 计算机中心应利用光、电、无源红外等技术设置机房报警系统，并有专人值守。

4.2.1.3 机房应采用特殊门锁。

4.2.1.4 机房外部的网络设备应采取加固防护等措施。

4.2.2 **设备的安全可用**

4.2.2.1 支持计算机信息系统运行的所有设备，包括计算机主机、外部设备、网络设备以及其他辅助设备均应安全可用。

4.2.2.2 应提供可靠的运行支持，并有故障容错和故障恢复能力。

4.3 **记录介质安全**

4.3.1 应采取措施，防止存放有用数据的各类记录介质被盗、被毁和受损。

4.3.2 系统中有很高使用价值或很高机密程度的重要数据，应采取加密等方法进行保护。

4.3.3 应采取措施，防止删除和销毁的数据被非法拷贝。

4.4 **安全管理中心的安全**

4.4.1 安全管理中心应符合 GB/T 2887—2000 中 4.9 的要求。

4.4.2 安全管理中心应设置在中心机房，以各种方式与计算机信息系统的各类安全机制相连接。

4.4.3 安全管理中心除了按照一般的机房建设要求进行建设外，还应设置关卡，必要时可安装闭路摄像监视系统。

5 网络安全

5.1 **网络安全建设**

5.1.1 应确定所设计、实现的网络设备、网络协议、网络软件及网络环境。

5.1.2 应分析网络设备、网络协议、网络软件及网络环境的安全要求，分析其可能存在的薄弱环节以及

这些环节可能造成的危害和由此产生的后果。

5.1.3 应确定网络设备、网络协议、网络软件及网络环境的安全策略，根据安全需求分析的结果，确定应控制的危害因素及控制程度、应保护的资源和保护程度。

5.1.4 应确定网络设备、网络协议、网络软件及网络环境应达到的安全等级。

5.1.5 应根据 GB/T 9387.2—1995 确定网络设备、网络协议、网络软件及网络环境在 ISO/OSI 开放系统互联参考模型中所处的网络层次。

5.1.6 应确定安全等级及网络层次，网络安全等级和网络各层次所对应的安全要素见表 1。

5.1.7 应根据 5.4 的要求，使网络设备、网络协议、网络软件及网络环境达到预期的安全需求、安全等级。

表 1 网络安全等级、安全要素与各层的相互关系

安全等级及网络层次		安全要素										
		自主访问控制	强制访问控制	标记	用户身份鉴别	客体重用	安全审计	数据完整性	隐蔽信道分析	可信路径	可信恢复	抗抵赖
用户自主保护级	物理层							★				
	链路层	★			★			★				
	网络层	★			★			★				
	传输层	★			★			★				
	会话层	★			★			★				
	表示层	★			★			★				
	应用层	★			★			★				
系统审计保护级	物理层							★				
	链路层	★			★	★		★				
	网络层	★			★	★	★	★				
	传输层	★			★	★	★	★				
	会话层	★			★	★	★	★				
	表示层	★			★	★	★	★				
	应用层	★			★	★	★	★				★
安全标记保护级	物理层							★				
	链路层	★	★	★	★	★		★				
	网络层	★	★	★	★	★	★	★				★
	传输层	★	★	★	★	★	★	★				★
	会话层	★	★	★	★	★	★	★				★
	表示层	★	★	★	★	★	★	★				★
	应用层	★	★	★	★	★	★	★				★

表 1（续）

安全等级及网络层次		安全要素										
		自主访问控制	强制访问控制	标记	用户身份鉴别	客体重用	安全审计	数据完整性	隐蔽信道分析	可信路径	可信恢复	抗抵赖
结构化保护级	物理层							★				
	链路层	★	★	★	★	★		★				
	网络层	★	★	★	★	★	★	★	★	★		★
	传输层	★	★	★	★	★	★	★	★	★		★
	会话层	★	★	★	★	★	★	★	★	★		★
	表示层	★	★	★	★	★	★	★	★	★		★
	应用层	★	★	★	★	★	★	★	★	★		★
访问验证保护级	物理层							★				
	链路层	★	★	★	★	★		★				
	网络层	★	★	★	★	★	★	★	★	★	★	★
	传输层	★	★	★	★	★	★	★	★	★	★	★
	会话层	★	★	★	★	★	★	★	★	★	★	★
	表示层	★	★	★	★	★	★	★	★	★	★	★
	应用层	★	★	★	★	★	★	★	★	★	★	★
注：“★”表示应具有该项技术要求。												

5.2 **网络安全基本要求**

5.2.1 网络应具有对全网网络拓扑、网络配置及网络参数的统一管理、监督与控制功能。

5.2.2 应采取安全措施，确保网络实体的环境安全、防电磁干扰和辐射干扰。

5.2.3 应采取安全措施，确保网络数据传输、交换、存储处理及通信控制的安全。

5.2.4 网络应具有计算机病毒的预防措施。

5.2.5 对灾难性事件应有应急措施。

5.2.6 网络应具有必要的冗余度和降级处理能力。

5.2.7 网络安全设施的接口设备应方便用户并实现透明操作。

5.2.8 网络应具有承受允许的最严重错误的能力。

5.2.9 在确保安全的前提下应充分发挥资源共享的效能。

5.2.10 网络应采取多重安全控制手段。每个安全控制手段均能产生充分的证据，以表明所完成操作的正确性。

5.2.11 网络应记载用户进入网络的各种活动，以提供事后检查。

5.2.12 存取控制应逐级授权。网络在为授权用户提供合法服务的同时，应具有拒绝非法访问的功能。

5.2.13 网络应具有监视和控制网络负载状态的功能，以防止其崩溃和瘫痪。

5.2.14 局域网（LAN）与局域网之间、局域网与广域网（WAN）之间互连，应采用防火墙、入侵检测等安全保护措施。

5.2.15 网络互联网不应影响互联双方原有的安全性。

5.3 **网络基本安全技术**

网络基本安全技术应包括对以下安全要素的保护：

——自主访问控制；

——强制访问控制；

——标记；
——用户身份鉴别；
——客体重用；
——安全审计；
——数据完整性；
——隐蔽信道分析；
——可信路径；
——可信恢复；
——抗抵赖。

5.4 详细技术要求

5.4.1 自主访问控制应符合 GA/T 387—2002 中 6.1 的要求。

5.4.2 强制访问控制应符合 GA/T 387—2002 中 6.2 的要求。

5.4.3 标记应符合 GA/T 387—2002 中 6.3 的要求。

5.4.4 身份鉴别应符合 GA/T 387—2002 中 6.4 的要求。

5.4.5 客体重用应符合 GA/T 387—2002 中 6.5 的要求。

5.4.6 审计应符合 GA/T 387—2002 中 6.6 的要求。

5.4.7 数据完整性应符合 GA/T 387—2002 中 6.7 的要求。

5.4.8 隐蔽信道分析应符合 GA/T 387—2002 中 6.8 的要求。

5.4.9 可信路径应符合 GA/T 387—2002 中 6.9 的要求。

5.4.10 可信恢复应符合 GA/T 387—2002 中 6.10 的要求。

5.4.11 抗抵赖应符合 GA/T 387—2002 中 6.11 的要求。

6 操作系统安全

6.1 技术要求

计算机操作系统应满足表 2 所列出的安全功能技术等级要求。

表 2 安全功能技术等级

安全保证技术要求	安全保护等级				
	用户自主保护级	系统审计保护级	安全标记保护级	结构化保护级	访问验证保护级
自主访问控制	★	★	★	★	★
强制访问控制			★	★	★
标记			★	★	★
用户身份鉴别	★	★	★	★	★
客体重用		★	★	★	★
安全审计		★	★	★	★
数据完整性	★		★	★	★
隐蔽信道分析				★	★
可信路径				★	★
可信恢复					★
注：“★”表示应具有该项技术要求。					

6.2 使用

6.2.1 应使用成熟的操作系统（OS）。

6.2.2 在首次使用操作系统时，应对操作系统进行配置管理控制、网络访问控制、口令管理控制以及屏幕加锁控制。

6.2.3 应及时下载操作系统供应商实时发布的OS安全防范补丁，更新系统，减少OS在安全方面的漏洞，对原有的操作系统进行加固。

6.2.4 应及时安装系统和在用程序的补丁包，定期检查帐户和审计文件。

6.3 检查测试

应通过对当前系统配置的分析，查找可能使用户或闯入者获得未认证访问的配置，并对以下内容进行检测：

——配置文件；
——软件版本；
——文件宿主和允许；
——SUID/SGID文件；
——不规则文件；
——用户账户；
——工作组设置；
——口令；
——系统受损；
——系统更改；
——文件基线受损；
——账户设置修改。

7 数据库管理系统安全

7.1 基本要求

数据库管理系统的安全性由可信的IT数据库产品自身来保证，并应具备以下特性：

——保密性：保护存储在数据库中的数据不被泄露和未授权获取；
——完整性：保护存储在数据库中的数据不被破坏和删除；
——一致性：确保存储在数据库中的数据满足实体完整性、参照完整性和拥护定义完整性要求；
——可用性：确保存储在数据库中的数据不因人为的和自然的原因对授权用户不可用。

7.2 身份鉴别

应符合GA/T 389—2002中4.1的要求。

7.3 标记与访问控制

应符合GA/T 389—2002中4.2的要求。

7.4 数据完整性

应符合GA/T 389—2002中4.3的要求。

7.5 数据库安全审计

应符合GA/T 389—2002中4.4的要求。

7.6 客体重用

应符合GA/T 389—2002中4.5的要求。

7.7 数据库可信恢复

应符合GA/T 389—2002中4.6的要求。

7.8 隐蔽信道分析

应符合 GA/T 389—2002 中 4.7 的要求。

7.9 可信路径

应符合 GA/T 389—2002 中 4.8 的要求。

7.10 推理控制

应符合 GA/T 389—2002 中 4.9 的要求。

8 应用系统安全

8.1 输入数据的确认

系统应具备输入数据的确认功能，以确保输入数据的正确性和适用性。

8.2 内部处理控制

系统应具备确认检查功能，以检查数据处理过程中的错误。

8.3 信息验证

在有安全措施要求的地方，应进行应用信息验证以保护信息内容的完整性。

8.4 输出数据的确认

从应用系统中输出的数据应经过确认，以确保存储信息相对于各种情况的处理正确而适当。

8.5 开发和支持过程的安全

系统在开发过程中应遵循 ISO 9001：1994 的要求，在支持过程中应按正式的更改控制程序进行更改控制。

8.6 计算机病毒的预防

系统应配置专用的计算机防病毒软件系统，并定期升级更新。同时应建立有效的防病毒管理机制。

中华人民共和国民用航空
行业标准
民用航空空中交通管理
管理信息系统技术规范
第2部分：系统与网络安全
MH/T 4018.2—2004
*
中国民航出版社出版发行
（北京市朝阳区光熙门北里甲31号楼）
—邮政编码：100028—
北京华正印刷厂印刷

*
开本 880×1230　1/16　印张 0.75　字数 13 千字
2005 年 5 月第 1 版　2005 年 5 月第 1 次印刷　印数 1—500 册
统一书号：1580110·247　定价：10.00 元