ICS 03.220.50
V 54

MH

中华人民共和国民用航空行业标准

MH/T 4018.7—2012

民用航空空中交通管理管理信息系统技术规范 第7部分：数据安全

Technical standards for air traffic management of civil aviation management information system — Part 7: Data Security

2012-01-19 发布　　2012-05-01 实施

中国民用航空局　发布

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》分为以下部分：
--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；
--第4部分 GNSS完好性监测数据接口；
--第5部分 电子公文交换接口；
--第6部分 人事数据交换；
--第7部分 数据安全。
本部分为MH/T 4018的第7部分。
本部分按照GB/T 1.1－2009给出的规则起草。
本部分由中国民用航空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局航空器适航审定司批准立项。
本部分由中国民航科学技术研究院归口。
本部分起草单位：中国民用航空局空中交通管理局、成都民航空管科技发展有限公司。
本部分主要起草人：齐鸣、陈朝勇、李锋、肖颖、唐屹、段培超、王强。

民用航空空中交通管理管理信息系统技术规范
第 7 部分：数据安全

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）管理信息系统数据在传输、存储和使用中数据安全定级和保护措施。

本部分适用于空管管理信息系统数据在传输、存储和使用中的安全管理。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 22081—2008 信息技术 安全技术 信息安全管理实用规则

GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求

3 术语和定义

GB/T 22239—2008、GB/T 22081—2008界定的以及下列术语和定义适用于本文件。

3.1

数据安全 data security

针对数据传输、存储和使用过程的安全控制，包括数据安全存储、数据加密传输、数据备份和恢复等机制。

3.2

客体 object

数据受到破坏时所侵害的对象。

4 数据安全定级

4.1 定级要素

4.1.1 数据安全等级由两个定级要素决定：数据受到破坏时所侵害的客体和对客体造成侵害的程度。

4.1.2 数据受到破坏时所侵害的客体包括：

a) 公民、法人和其他组织的合法权益；

b) 空管单位的合法权益；

c) 社会秩序、公共利益。

4.1.3 对客体的侵害程度由客观方面的不同外在表现综合决定，侵害程度包括：

a) 特别严重侵害；
b) 严重侵害；
c) 一般侵害。

侵害程度的界定见4.2.4.3。

4.2 定级方法

4.2.1 定级流程

数据安全等级定级流程为：

a) 确定定级对象；
b) 确定数据受到破坏时所侵害的客体；
c) 根据不同的受侵害客体，从多方面评定数据安全受到破坏对客体的侵害程度；
d) 确定数据安全等级。

4.2.2 定级对象的确定

定级对象为需要进行定级的空管管理信息系统涉及的数据。

4.2.3 受侵害的客体的确定

定级对象受到破坏时所侵害的客体为：

a) 侵害社会秩序、公共利益包括：
   1) 影响公众在法律约束和道德规范下的正常生活秩序；
   2) 影响空管管理和服务的工作秩序；
   3) 影响公众获取空管管理系统公开的数据；
   4) 影响公众接受航空服务；
   5) 影响其他社会秩序、公共利益的事项。
b) 侵害空管单位的利益包括：
   1) 影响空管单位正常的业务运行；
   2) 影响空管单位的声誉；
   3) 其他影响空管单位利益的事项。
c) 侵害公民、法人和其他组织的合法权益。

4.2.4 侵害程度的确定

4.2.4.1 应根据不同的受侵害客体、侵害后果确定侵害程度。

4.2.4.2 判断侵害程度时：

a) 如果受侵害客体是公民、法人或其他组织的合法权益，应以本人或本单位的总体利益作为判断基准；
b) 如果受到侵害的客体是空管单位的利益，应以空管单位或空管行业的总体利益作为判断基准；
c) 如果受到侵害的客体是社会秩序、公共利益时，应以空管行业或国家的总体利益作为判断基准。

4.2.4.3 侵害程度的界定如下：

a) 特别严重侵害：空管行政管理、安全管理、空管业务以及运行能力受到致命影响或侵害，导致空管业务能力和运行能力严重下降，公民、法人和其他组织的合法权益受到严重的影响或侵害，社会影响较大；

b) 严重侵害：严重影响或侵害空管行政管理、安全管理、空管业务以及运行能力，导致空管业务能力和运行能力显著下降，公民、法人和其他组织的合法权益受到影响或侵害，社会影响较小；

c) 一般侵害：影响或侵害空管行政管理、安全管理、空管业务以及运行能力，导致业务能力和运行能力轻微降低，公民、法人和其他组织的合法权益受到较低的侵害。

4.2.4.4 数据安全等级的确定

根据数据在遭到破坏后对客体的侵害程度，数据安全等级包括：

a) 3 级：数据受到破坏后，公民、法人和其他组织的合法权益或空管单位的业务和工作职能受到特别严重侵害，或者对社会秩序和公共利益造成严重侵害或特别严重侵害；

b) 2 级：数据受到破坏后，公民、法人和其他组织的合法权益或空管单位的业务和工作职能受到严重侵害，或者对社会秩序和公共利益造成一般侵害；

c) 1 级：数据受到破坏后，公民、法人和其他组织的合法权益或空管单位的业务和工作职能受到一般侵害，但不侵害社会秩序和公共利益。

详见表1。

表1 数据安全等级

数据安全被破坏时所侵害的客体	对相应客体的侵害程度		
	一般侵害	严重侵害	特别严重侵害
公民、法人和其他组织的合法权益	1 级	2 级	3 级
空管单位的合法权益	1 级	2 级	3 级
社会秩序、公共利益	2 级	3 级	3 级

4.2.5 定级变更

数据安全等级应随应用环境和侵害后果的变化适当变更。

5 保护措施

5.1 保护等级

数据安全保护等级分为3级保护、2级保护和1级保护。不同安全等级的数据应采取不同等级的保护措施。

5.2 3 级保护

5.2.1 技术要求

5.2.1.1 应能够对使用数据的用户进行身份鉴别，身份鉴别安全要求应符合 GB/T 22239－2008 中 7.1.4.1 的规定。

5.2.1.2 应提供访问控制功能，根据访问策略控制对数据的访问。

5.2.1.3 应提供用户授权机制，由授权主体配置访问控制策略，严格限制用户的缺省访问权限。

5.2.1.4 应根据业务需要授予用户最小数据访问权限。

5.2.1.5 应具有对重要信息资源设置敏感标记的功能。

5.2.1.6 应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。

5.2.1.7 数据通信的完整性应符合 GB/T 22239－2008 中 7.1.4.4 的规定。
5.2.1.8 数据通信的保密性应符合 GB/T 22239－2008 中 7.1.4.5 的规定。
5.2.1.9 数据的完整性应符合 GB/T 22239－2008 中 7.1.5.1 的规定。
5.2.1.10 数据的保密性应符合 GB/T 22239－2008 中 7.1.5.2 的规定。
5.2.1.11 应提供本地数据备份与恢复功能，完全数据备份至少每天一次。备份介质应场外存放。
5.2.1.12 应提供异地数据备份功能，利用通信网络将关键数据定时批量传送至备用场地。
5.2.1.13 应能对数据的主要处理和存储设备提供冗余。
5.2.1.14 在数据遭到破坏导致系统不能正常工作时，应能在较快时间内使用备份数据恢复。恢复后的数据应确保系统业务的连续性。
5.2.1.15 备份数据的介质应符合 GB/T 22081－2008 中 10.5.1 f)的规定。
5.2.1.16 备份数据的恢复应符合 GB/T 22081－2008 中 10.5.1 g)的规定。

5.2.2 管理要求

5.2.2.1 系统安全管理规定中应包含数据管理的相关内容。
5.2.2.2 应制定数据管理人员和操作人员数据操作规程。
5.2.2.3 应按 GB/T 22239－2008 中 7.2.5.3 建立介质管理规范。
5.2.2.4 应按 GB/T 22081－2008 中 10.7.2 处理废弃介质。
5.2.2.5 应按 GB/T 22239－2008 中 7.2.5.11 建立备份与恢复管理规范。
5.2.2.6 应按 GB/T 22239－2008 中 7.2.5.13 建立数据安全应急预案。
5.2.2.7 应确保应急预案的执行有足够的资源保障。
5.2.2.8 应每年定期进行数据安全应急预案培训与演练。
5.2.2.9 应每年定期审查并根据实际情况更新应急预案内容。

5.3 2 级保护

5.3.1 技术要求

5.3.1.1 应能够对使用数据的用户进行身份鉴别，身份鉴别安全要求应符合 GB/T 22239－2008 中 6.1.4.1 的规定。
5.3.1.2 应提供访问控制功能，根据访问策略控制对数据的访问。
5.3.1.3 应提供用户授权机制，由授权主体配置访问控制策略，严格限制用户的缺省访问权限。
5.3.1.4 应根据业务需要授予用户最小数据访问权限。
5.3.1.5 数据通信的完整性应符合 GB/T 22239－2008 中 6.1.4.4 的规定。
5.3.1.6 数据通信的保密性应符合 GB/T 22239－2008 中 6.1.4.5 的规定。
5.3.1.7 数据的完整性应符合 GB/T 22239－2008 中 6.1.5.1 的规定。
5.3.1.8 数据的保密性应符合 GB/T 22239－2008 中 6.1.5.2 的规定。
5.3.1.9 应能对重要数据进行备份和恢复。
5.3.1.10 应能对数据的关键处理和存储设备提供冗余。
5.3.1.11 在数据受到破坏导致系统不能正常工作时，备份数据应能恢复系统主要功能。

5.3.2 管理要求

5.3.2.1 系统安全管理规定中应包含数据管理的相关内容。
5.3.2.2 应制定数据管理人员和操作人员数据操作规程。
5.3.2.3 应按 GB/T 22239－2008 中 6.2.5.3 建立介质管理规范。

5.3.2.4 应按 GB/T 22081－2008 中 10.7.2 处理废弃介质。
5.3.2.5 应按 GB/T 22239－2008 中 6.2.5.10 建立备份与恢复管理规范。
5.3.2.6 应按 GB/T 22239－2008 中 6.2.5.12 建立数据安全应急预案。
5.3.2.7 应每年定期进行数据安全应急预案培训。

5.4 1 级保护

5.4.1 技术要求

5.4.1.1 应能够对使用数据的用户进行身份鉴别，身份鉴别安全要求应符合 GB/T 22239－2008 中 5.1.4.1 的规定。
5.4.1.2 应提供访问控制功能，控制用户组和（或）用户对用户数据的访问。
5.4.1.3 应提供用户授权机制，由授权主体配置访问控制策略，严格限制用户的缺省访问权限。
5.4.1.4 数据通信的完整性应符合 GB/T 22239－2008 中 5.1.4.3 的规定。
5.4.1.5 数据的完整性应符合 GB/T 22239－2008 中 5.1.5.1 的规定。
5.4.1.6 应能够对重要数据进行备份和恢复。
5.4.1.7 在数据遭到破坏导致系统不能正常工作时，备份数据应能恢复系统主要功能。

5.4.2 管理要求

5.4.2.1 系统安全管理规定中应包含数据管理的相关内容。
5.4.2.2 应按 GB/T 22239－2008 中 5.2.5.3 建立介质管理规范。
5.4.2.3 应按 GB/T 22239－2008 中 5.2.5.8 建立备份与恢复管理规范。