ICS 35.020
L 07

MH

中华人民共和国民用航空行业标准

MH/T 0073—2020

民用航空跨网数据交换安全技术要求

Security technical requirement for data exchanging across regional networks of civil aviation

2020-07-20发布　　2020-10-01实施

中国民用航空局　发布

前　言

本标准按照GB/T 1.1-2009《标准化工作导则 第1部分：标准的结构和编写》给出的规则起草。

本标准由中国民用航空局人事科教司提出。

本标准由中国民航科学技术研究院归口。

本标准起草单位：中国民航大学、中国民用航空局空中交通管理局。

本标准主要起草人：钟安明、周景贤、王双、杨锐、唐屹、顾兆军、张礼哲、刘春波、隋嚞、刘超、吕宗平、陈宝刚。

民用航空跨网数据交换安全技术要求

1 范围

本标准规定了民用航空（以下简称民航）跨网数据交换区技术框架和安全技术要求。

本标准适用于民航不同单位、不同安全等级网络之间的跨网数据安全交换系统的设计、建设和运行。

2 术语和定义

下列术语和定义适用于本标准。

2.1

跨网数据交换区 Across Regional Networks Exchange Area

采取逻辑隔离或物理隔离的不同网络之间进行数据交换时，对各类交换业务进行注册、接入认证、操作监控与审计的区域。

3 跨网数据交换区技术框架要求

3.1 通则

跨网数据交换业务应采用跨网数据交换区作为统一的出入口，应采取设备认证、格式检查等安全措施实现两个不同网络之间的数据交换，保证数据交换的保密性、完整性、可用性。

3.2 数据分类和交换方式

交换数据包括数据库数据、文件数据、流媒体数据、请求命令与响应数据等。交换方式包括单向数据传输、双向数据传输。

3.3 跨网数据交换区组成

跨网数据交换区位于交换网络之间，由网络接入区、边界保护区、应用服务区、安全隔离区和安全监测区五部分组成，整体架构见图 1。

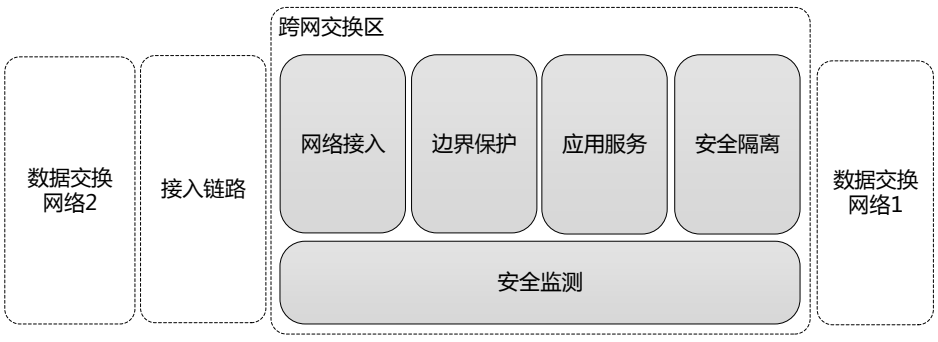

图1 跨网数据交换区架构图

图1中各区域功能要求如下：

a) 网络接入区：实现不同网络与数据交换系统的连接、路由访问控制，安全策略设置；
b) 边界防护区：实现对数据交换系统的安全保护，包括网络级的身份认证、访问控制、权限管理、恶意代码防范等；
c) 应用服务区：处理各类不同网络之间传输和数据，实现应用级的身份认证、访问控制等功能，防止非法访问；
d) 安全隔离区：实现不同网络之间的安全隔离与信息交换，根据安全策略实现网络之间的安全数据摆渡；
e) 安全监测区：对各种应用和操作进行监测、统计分析及安全审计，实现整个数据交换的安全监测和审计。

4 安全技术要求

4.1 网络接入

应支持接入访问控制，并对交换数据来源进行识别和控制。

4.2 边界保护

4.2.1 应支持接入应用的身份认证，并采用安全的双向认证协议。

4.2.2 应支持接入应用的安全访问控制，并将接入应用的访问权限限定于跨网交换区内，且只能访问指定应用和数据。

4.2.3 应支持及时发现入侵行为、病毒、恶意代码传播行为和报警，并能防止重放、篡改和伪造等攻击。

4.3 应用服务

4.3.1 业务操作方式如为“数据交换”类型，在进行数据交换之前，跨网交换区必须对交换业务的数据流量实现通信协议的剥离。并按照业务预先注册的数据格式要求，对数据的类型，格式进行严格检查，对数据内容进行过滤，限制所有不符合要求的数据传入跨网交换区。

4.3.2 业务操作方式如为“授权访问”类型，应实现应用系统的身份认证，细粒度访问控制和授权管理。

4.3.3 应支持应用级日志记录，并按照集中监控与审计要求进行报送。

4.4 安全隔离

4.4.1 应采用光闸或网闸作为数据传输连接通道；应通过协议转换，以信息摆渡的方式实现数据交换，单向数据传输必须确保数据无反向传输。

4.4.2 数据库数据、文件数据交换时，交换服务应具备设备认证、数据抽取、数据装载、格式检查、内容过滤等功能。

4.4.3 流媒体数据、请求命令与响应数据交换时，交换服务应具备设备认证、格式检查、内容过滤等功能。

4.5 安全监测

4.5.1 应支持实时监测跨网数据安全交换业务状态、设备运行状态。

4.5.2 应支持对跨网数据安全交换业务的行为、安全事件和交换内容进行审计。

4.5.3 应支持对系统管理和运维人员的管理行为进行审计

4.5.4 应支持对安全事件进行报警。

4.5.5 应支持配置文件、审计日志的备份功能，并提供备份数据的导入、到处、查询功能。

4.5.6 应支持设备日志、网络日志、审计日志等数据留存不少于六个月。

5 可用性要求

5.1 单向数据传输系统支持线路冗余，应在一条线路故障时保证单向数据的传输。

5.2 双向数据交换系统支持热备，应在故障时自动切换交换任务到其他运行的双向数据交换系统。

5.3 双向数据交换系统支持负载均衡，应根据负载自动切换交换任务到其他运行的双向数据交换系统。

5.4 网络设备、主机服务器、安全设备支持热备，应在故障时自动切换到其他运行的设备

5.5 应用系统支持低耦合性、易扩展性，以及系统的故障处理机制，应在系统的运行故障时快速回滚以保障业务连续性。

参 考 文 献

[1] GB/T 20273-2019 信息安全技术 数据库管理系统安全技术要求
[2] GB/T 20279-2006 信息安全技术 网络和终端设备隔离部件安全技术要求
[3] GW 0205-2014 国家电子政务外网 跨网数据安全交换技术要求与实施指南