

ICS 35.020
CCS L 07

MH

**INDUSTRY STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

MH/T 0073-2020

**Safety technical requirements for inter-network data exchange
in civil aviation
(English Translation)**

Issued on: July 20, 2020

Implemented on: October 1, 2020

Issued by: Civil Aviation Administration of China

Table of Contents

- Foreword
- 1 Scope
- 2 Terms and definitions
- 3 Technical framework requirements for cross-network data exchange area
 - 3.1 General
 - 3.2 Data classification and exchange methods
 - 3.3 Cross-network data exchange area composition
- 4 Safety technical requirements
 - 4.1 Network access
 - 4.2 Border protection
 - 4.3 Application Service
 - 4.4 Safe isolation
 - 4.5 Safety monitoring
- 5 Availability requirements

Foreword

This standard was drafted in accordance with the rules given in GB/T 1.1-2009 "Guidelines for Standardization Work Part 1: Standard Structure and Compilation".

This standard was proposed by the Department of Personnel, Science and Education, Civil Aviation Administration of China.

This standard is under the jurisdiction of the China Academy of Civil Aviation Science and Technology.

Drafting organizations of this standard. Civil Aviation University of China, Air Traffic Management Bureau of Civil Aviation Administration of China.

1 Scope

This standard specifies the technical framework and safety technical requirements for the cross-network data exchange area of civil aviation (hereinafter referred to as civil aviation).

This standard applies to the design, construction and operation of cross-network data security exchange systems between different civil aviation units and networks of different security levels.

2 Terms and definitions

The following terms and definitions apply to this standard.

Across Regional Networks Exchange Area when data is exchanged between different networks that are logically isolated or physically isolated, the registration, access authentication, Operational monitoring and auditing area.

3.1 General

The cross-network data exchange business should adopt the cross-network data exchange area as a unified entrance and exit, and security measures such as equipment certification and format inspection should be adopted.

Implement data exchange between two different networks to ensure the confidentiality, integrity and availability of data exchange.

3.2 Data classification and exchange methods

Exchange data includes database data, file data, streaming media data, request commands and response data, etc. One-way number Data transmission, two-way data transmission.

3.3 Cross-network data exchange area composition

The cross-network data exchange area is located between the exchange networks. It consists of the network access area, border protection area, application service area, security isolation area and security the monitoring area is composed of five parts, and the overall structure is shown in Figure 1.

- a) Network access area. to realize the connection of different networks and data exchange systems, route access control, and security policy settings;
- b) Border protection zone. to realize the security protection of the data exchange system, including network-level identity authentication, access control, authority management, Malicious code prevention, etc.;
- c) Application service area. processing various types of transmission and data between different networks, realizing application-level identity authentication, access control and other functions, Prevent illegal access;
- d) Security isolation zone. to realize the security isolation and information exchange between different networks, and realize the security data between the networks according to the security strategy.

According to ferry

e) Safety monitoring area. monitoring, statistical analysis and safety auditing of various applications and operations, realizing safety monitoring of the entire data exchange Testing and auditing.

4.1 Network access

Should support access control, and identify and control the source of exchanged data.

4.2 Border protection

4.2.1

Should support the identity authentication of the access application, and adopt a secure two-way authentication protocol.

4.2.2

The security access control of access applications should be supported, and the access permissions of access applications should be limited to the cross-network exchange area, and only Specify the application and data.

4.2.3

It should support timely detection of intrusions, viruses, and malicious code propagation and alarms, and prevent attacks such as replay, tampering, and forgery.
hit.

4.3 Application Service

4.3.1

If the business operation mode is of the "data exchange" type, before data exchange, the cross-network exchange area must the data flow realizes the stripping of the communication protocol. And in accordance with the pre-registered data format requirements of the business, strictly check the type and format of the data, Filter the data content and restrict all data that does not meet the requirements from entering the cross-network exchange area.

4.3.2

If the business operation mode is of the "authorized access" type, the application system's identity authentication, fine-grained access control and authorization management shall be implemented.

Rationale.

4.3.3

Application-level log records shall be supported and submitted in accordance with centralized monitoring and auditing requirements.

4.4 Safe isolation

4.4.1

Optical gates or gatekeepers should be used as data transmission connection channels; data exchange should be realized by means of information ferry through protocol conversion.

One-way data transmission must ensure that there is no reverse transmission of data.

4.4.2

When database data and file data are exchanged, the exchange service shall have equipment authentication, data extraction, data loading, format checking, Content filtering and other functions.

4.4.3

When streaming media data, request commands and response data are exchanged, the exchange service shall have equipment authentication, format checking, content filtering, etc.

Features.

4.5 Safety monitoring

4.5.1

It should support real-time monitoring of the status of cross-network data security exchange business and equipment operation status.

4.5.2

It shall support the auditing of the behavior, security incidents and exchange content of the cross-network data security exchange business.

4.5.3

Should support the audit of the management behavior of system management and operation and maintenance personnel

4.5.4

Alarms for security events should be supported.

4.5.5

The backup function of configuration files and audit logs shall be supported, and the functions of importing, storing and querying backup data shall be provided.

4.5.6

It should support the retention of equipment logs, network logs, audit logs and other data