

ICS 35.020
CCS L 07

MH

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

MH/T 0076-2020

**Basic requirements for civil aviation network security level
protection
(English Translation)**

Issued on: July 20, 2020

Implemented on: October 1, 2020

Issued by: Civil Aviation Administration of China

Table of Contents

Foreword	
Introduction	
1 Scope	
2 Normative references	
3 Terms and definitions	
4 Overview of Civil Aviation Network Security Level Protection	
5 First level safety requirements	
6 Second level safety requirements	
7 Level 3 safety requirements	
8 Level 4 Safety Requirements	
9 Level 5 Safety Requirements	
Appendix A (Normative Appendix) About the selection and use of general safety requirements and extended safety requirements	
Appendix B (Normative Appendix) Requirements for the overall safety protection capability of the graded protection objects	
References	

Foreword

This standard was drafted in accordance with the rules given in GB/T 1.1-2009.

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, Guangdong Airport Baiyun Information Technology Co., Ltd., Nankai University.

Introduction

According to GB/T 1.1-2009 "Guidelines for Standardization Work Part One. Standard Structure and Compilation", "Network of the People's Republic of China" Security Law", "Regulations of the People's Republic of China on the Protection of Computer Information System Security" (Order No. 147 of the State Council), "Information Security Level Protection Management Measures (Gongtongzi [2007] No. 43), GB/T 22239 "Basic

Requirements for Information Security Technology Network Security Level Protection" and "Interim Measures for the Administration of Civil Aviation Network and Information Security" (MD-PE-2013-01), "Regarding Further Strengthening of Civil Aviation Network and Information Security "Notice" (Civil Aviation Renfa [2013] No. 62) requires the formulation of this standard.

This standard is based on GB/T 22239 "Basic Requirements for Information Security Technology Network Security Level Protection", and is based on the system characteristics of the civil aviation industry.

Levy, put forward and stipulate the basic safety protection requirements of different safety protection levels.

This standard is one of a series of standards related to civil aviation network security level protection.

The standards related to this standard include.

--MH/T 0069 Guidelines for the classification of civil aviation network security protection.

In this standard, the parts in bold indicate the increased or enhanced requirements in higher levels.

Basic requirements for civil aviation network security grade protection

1 Scope

This standard specifies the general requirements and safety requirements for the protection objects of the first to fourth levels of civil aviation network security protection.

Expansion requirements.

This standard is applicable to guide the safety construction and supervision and management of hierarchical non-secret civil aviation network security protection objects.

Note: The fifth-level protection object is a very important supervision and management object, which has special management mode and safety requirements, so it is not carried out in this standard.

description.

2 Normative references

The following documents are indispensable for the application of this document. For dated reference documents, only the dated version applies to this document.

For undated references, the latest version (including all amendments) applies to this document.

GB/T 25069 Information Security Technical Terms GB/T 22239 Information Security

Technology Network Security Level Protection Basic Requirements MH/T 0069 Guidelines for the Classification of Civil Aviation Network Security Level Protection

3 Terms and definitions

The following terms and definitions established by GB/T 25069, GB/T 22239 and MH/T 0069 apply to this document. For ease of use, Some terms and definitions in GB/T 22239 are repeated below.

Cybersecurity

By taking necessary measures to prevent attacks, intrusions, interference, sabotage, illegal use and accidents on the network, the network is the state of stable and reliable operation, and the ability to ensure the integrity, confidentiality, and availability of network data.

[GB/T 22239-2019, Terms and Definitions 3.1] 3.2 Security protection ability the degree to which it can resist threats, detect security incidents, and restore the previous state after damage.

[GB/T 22239-2019, Terms and Definitions 3.2] 3.3 (Civil aviation) production network (of civil aviation) Network facilities that carry the production business system of civil aviation transportation.

Office network

Network facilities that carry office automation systems.

4.1 Hierarchical protection objects

Hierarchical protection objects refer to objects in the network security hierarchical protection work, usually referring to computers or other information terminals and related equipment.

A system that collects, stores, transmits, exchanges, and processes information in accordance with certain rules and procedures, mainly including basic information Networks, cloud computing platforms/systems, big data platforms/systems, Internet of Things, industrial control systems, and systems using mobile internet technology.

According to their importance in national security, economic construction, and social life, the objects of hierarchical protection have an impact on national security and social status after being destroyed.

Order, public interest, and the degree of harm to the legitimate rights and interests of citizens, legal persons and other organizations, etc., are divided into five security protections from low to high.

level.

Refer to MH/T 0069 for the method for determining the safety protection level of civil aviation protection objects.

4.2 Different levels of security protection capabilities

The basic security protection capabilities that different levels of protection objects should have are as follows.

The first level of security protection capability. It should be able to protect against malicious attacks from individual threat sources with few resources, general Damage to key resources caused by natural disasters and other threats of considerable damage.

Features.

The second level of security protection capability. It should be able to protect against malicious attacks from small external organizations and threat sources with few resources.

Damage to important resources caused by attacks, general natural disasters, and other threats of a considerable degree of harm, which can discover important security vulnerabilities and to deal with security incidents, after it is damaged, it can restore some functions within a period of time.

The third level of security protection capability. it should be able to protect against organized groups from outside under a unified security strategy, with relatively rich resources the main resource damage caused by malicious attacks, more serious natural disasters, and other threats of considerable damage it can detect and monitor attacks and deal with security incidents in time, and restore most of its functions quickly after it is damaged.

The fourth level of security protection capability. It should be able to protect against national-level, hostile organizations, and rich assets under a unified security strategy.

Resource damage caused by malicious attacks, severe natural disasters, and other threats of a considerable degree of threat to resources can be it can detect and monitor attacks and security incidents in time, and can quickly restore all functions after it is damaged.

The fifth level of security protection capability. omitted.

4.3 Safety general requirements and safety extension requirements

Due to different business goals, different technologies used, and different application scenarios, different levels of protection objects will be different the form appears, and the manifestation may be called basic information network, information system (including systems using mobile Internet and other technologies), cloud computing Platform/system, big data platform/system, Internet of Things, industrial control system, etc. The threats faced by different levels of protection objects are different at the same time, security protection requirements will also vary. In order to facilitate the realization of the commonality and individualization of protection objects of different levels and different forms