INTERNATIONAL CIVIL AVIATION ORGANIZATION
ASIA AND PACIFIC OFFICE

ASIA/PAC
AERONAUTICAL TELECOMMUNICATIONS NETWORK
SYSTEM MANAGEMENT POLICY

First Edition – April 2005

AERONAUTICAL TELECOMMUNICATIONS NETWORK
SYSTEM MANAGEMENT POLICY

1. Purpose: This document prescribes the system management policy and associated requirements applicable to the Aeronautical Telecommunications Network (ATN). It applies to ATN implementations and defines the rules governing the management of ATN data, services and resources associated with ATN applications and processes. The design, implementation and operation of the ATN must support the complete and consistent enforcement of this system management policy.

2. Applicability: For the purpose of this policy, the ATN encompasses hardware, software, procedures, standards, facilities, and personnel.

3. Authority: This document is published in accordance with the authority of the International Civil Aviation Organization (ICAO).

4. Implementation and Enforcement: This system management policy defines a minimum set of operational procedures to be followed and technical data, i.e., management information, to be collected and monitored to support the management of ATN data, services, and resources. Local authorities may apply additional procedures and collect/monitor additional technical data to suit local needs, while not degrading the ATN system management posture and maintaining consistency with the minimum essential required system management requirements identified in this ATN System management Policy.

5. System management Services: A comprehensive approach to management of the ATN depends upon the accurate and consistent enforcement of six high level services: fault management, configuration management, accounting management, performance management, and security management.

a. Fault Management - Fault management facilities allow system managers to detect problems in the network and include mechanisms for the detection of and isolation and recovery from abnormal system operation.

b. Accounting Management - Accounting management facilities allow a system manager to determine the usage of system resources and to allocate costs and charges on resources utilization.

c. Configuration and Name Management - Configuration management facilities allow system managers to exercise control over the configuration of the system. Network and system configurations may be changed to alleviate congestion, isolate faults, or otherwise meet changing user needs.

d. Performance Management - Performance management facilities provide the system manager with the ability to monitor and evaluate the performance of the system.

e. Security Management - Security management facilities allow a system manager to manage those services that provide access protection of system resources.

6. System management Policy Statements: The ATN system management policy is intended to result in operational procedures and the collection and monitoring of technical parameters to react to system faults and security events and to adequately provision ATN services and resources. Accordingly, the following functional policy statements are identified in terms of the defined services:

(1) Functional Policy Statements

a. Fault Management

(a) Abnormal system operation impacting ATN services and resources shall be detected, isolated, and recovery measures shall be taken.

b. Accounting Management

(a) The usage of ATN system resources for cost purposes is a local matter.

c. Configuration and Name Management

(a) A record of the changes to the logical and physical configuration of ATN resources shall be maintained.

(b) A record of the assignment and change of AMHS names, NSAP Addresses, subnetwork addresses, and technical parameters affecting interoperability shall be maintained.

d. Performance Management

(a) The usage of ATN resources shall be monitored and analysis performed to determine future resource allocation.

e. Security Management

(a) Security events impacting ATN services and resources shall be monitored and handled through a security incident response capability and contingency planning.

7. Responsible System Manager: Each organization shall designate a System Manager responsible for the system management of their organizational services and resources and responsible for system management coordination with the responsible system managers of other organizations.
