ATNP/WG3
WP/12-__

<u>AERONAUTICAL TELECOMMUNICATION NETWORK (ATN)</u>

<u>WG3 - ATN Applications and Upper Layers</u>

Rio de Janeiro (Brazil), 16-20 March 1998

System Management Requirements for Air-Ground CNS/ATM-1 Package Applications

Prepared by F. Picard

Summary

ICAO is in the process of standardising the requirements for ATN System Management. This will allow public and private ATN operators to develop applications to monitor and control remotely some of the resources managed by the ATN systems installed in the aircraft and in the ground facilities.

The Application Service Elements (ASE) provide application-users with the communication functions suitable to each ATN application. They are candidate for being remotely managed by airline or ATC system managers.

This document identifies the main management functions the ASEs may require in the five usual system management functional areas ("FCAPS"): <u>F</u>ault management, <u>C</u>onfiguration management, <u>A</u>ccounting, <u>P</u>erformance monitoring and <u>S</u>ecurity management. The analysis of these requirements lead to the identification of the ASE resources which have to be visible from the system managers, i.e. to define the minimum set of ASE managed objects to be included in the ATN MIB to cover the management of the ASEs.

1. INTRODUCTION

The objective of this document is to analyse the system management requirements of the CNS/ATM-1 Package air-ground applications.

Chapter 2 lists the assumptions made in this document on the system management environment.

Chapter 3 identifies for each system management domain (fault, configuration, accounting, performance and security management) what are the system management requirements of the ATN air-ground application in terms of communications resources required to be made visible to the SM applications and actions on the communication resources.

This analysis was used to define the contents of the system management data base (MIB) related to the application components (Document ATNP/WG3/SG3: "Elements of Management Information related to the ATN Application Layer").

2. ASSUMPTIONS ON THE SYSTEM MANAGEMENT ENVIRONMENT

2.1 Administrative Authorities

Management operations are usually performed by Administrative Authority (AA). An AA is an administrative unit responsible for the correct functioning of a set of systems and resources involved in the ATN data link operations.

As far as the application resources management is concerned, two types of AAs are of interest: the **airline AA** and the **ATC AA** respectively responsible for the management of the applications on-board and of the ground-based applications.

The Management Domain assigned to these AAs considered is limited **-** in the scope of this document **-** to communication resources implemented by the ATS CNS/ATM-1 air-ground applications, although other Management Domains could be defined for other types of applications (e.g. AOC). It is assumed in this document that the scope of the AAs is limited to the resources related to the applications hosted in the air and ground ATN ESs. The management of resources controlled by the lower layers (1-4) of both ESs and ISs and by the upper layers (5, 6 and part of 7 up to the dialogue service) of the ESs is outside the scope of this document.

2.2 SM Managers

An airline AA monitors and controls the operation of the airborne part of the air-ground applications. An airline AA operates several distributed SM managers or a centralised SM manager on the ground. As the distribution of the management centres on the ground does not impact the application SM requirements, the assumption is made that **there is a single Airline SM Centre per airline from which all SM data related to the aircraft is sent and processed**.

The assumption is taken here that **there is no SM manager installed in the aircraft**. If there is one, the communications between the air manager and the air agents is a local matter.

The ATC AA may have distributed SM managers or a centralised SM manager on the ground. An ATC AA monitors and controls the operation of the ground part of the air-ground applications. The assumption is made here that **there is a single Management ATC SM Centre per ATC Authority**. ATC AAs do not communicate directly with airborne SM agents.

Airline and ATC SM Centres may need to exchange SM information. This will be done through exchanges between SM Managers based on bilateral agreements defining the nature of the exchanges (types of information, triggering events, frequency, etc…). The SM information exchanged between SM Centres shall be covered by an ICAO standard.

This document focuses on the exchange of management information between agent and managers belonging to the same AA. In theory, this contents of this information is to be defined by each AA, independently of the other AAs. Actually it is not required to standardise this information nor the communication protocols needed to exchange this information on a world-wide basis. Only communications between managers of different AAs are required to be normalised. These communications are not covered by this document.

2.3 SM Agents

Each airborne ES implements a SM agent. The airborne SM Application Entity has a direct visibility of the Managed Objects (MOs) which have been defined in order to model the application resources implemented in the ES.

Each ground ES implements a SM agent. The ground SM Application Entity has a direct visibility of the Managed Objects (MOs) which have been defined in order to model the application resources implemented in the ES.

3. SYSTEM MANAGEMENT REQUIREMENTS OF ATN UPPER LAYERS AND ATN APPLICATIONS

System Management activities are usually grouped into the five following areas:

a) Fault management,
b) Configuration management,
c) Accounting management,
d) Performance management, and
e) Security management.

The SM Application provides services supporting one or several areas. This section aims at identifying precisely the nature of these services, limiting the scope of the managed objects to the air-ground ASEs.

3.1 Fault Management

3.1.1 High Level Requirements for Fault Management

Fault management concerns the detection of a problem, fault isolation and correction to normal operation. Although fault management can to a certain extent be achieved by polling the managed objects, and searching for error conditions, fault management deals most commonly with notifications as they occur. Data reporting mechanisms to report alarms or alerts is the best way to accomplish health checks of specific managed object's performance without having to double the amount of polling being accomplished. ISO has defined a specific notification (communicationAlarm) for reporting alarm conditions.

The ATN SARPs shall cover the management of faults which affect the ATN communication between organisations and between the air and the ground.

Faults detected and notified to SM managers reflect communication errors that occurred in the communication part of the ATN applications, i.e. the Application Entities. Faults indicate the abnormal behaviour of the ASE. It should be clear that operational fault detection and management are under the responsibility of the application service users and are therefore outside the scope of the ATN SM application (e.g. user actions not conforming to the SARPs user requirements (SARPs chapter 7).

Faults identified shall reflect a failure of the communication system. 'Operational' faults are not relevant for the SM managers.

ASE communication faults shall be tracked in the following conditions:
– inability of an application entity to establish communications with a peer application entity,
– loss of end-to-end communication between peer application entities, and
– inability of the application entity to provide correctly the application service.

When the fault can be detected before it becomes serious, an alarm should be produced. This alarm is needed only if the application user or the SM manager is able to react in such a way that the fault is avoided. Otherwise, the alarm is useless.

An alarm should be sent when the fault occurrence is detectable.

Likewise, a detected fault shall be notified on-line to a SM manager if and only if this SM manager is able to react to the fault and improve the fault situation. Otherwise, a log of the fault notification (via SM log procedures) or a local log of the event (via local trace procedures) is sufficient.

A fault notification shall be sent only to managers that can correct the fault situation immediately. Otherwise a trace in a log is sufficient.

3.1.2 Faults in the CNS/ATM-1 ASEs

This section identifies amongst the faults occurring in the CNS/ATM-1 applications (CM, ADS, CPDLC and FIS(ATIS)) the ones which have to be tracked by the SM application. Basically, they are three types of errors affecting the ASEs: faults generated by the application-users, by the ASE and by the dialogue service provider.

3.1.2.1 Application-user faults

Local faults initiated by the application-users (e.g. invalid primitive or primitive parameter, primitive out of sequence) are detected locally by the ASE. The peer ASE is not informed of the fault. The fault is indicated via a local means to the application-user which should log the fault notification and take the appropriate corrective action (redo or user-abort). A remote SM manager would be unable to intervene, so there is no need to inform him on-line.

User-generated abort reflect the detection by the user of a serious error. Such abort causes the brutal termination of the pending application communications.

The failure of an instance of communication due to a user abort shall be logged.Dialogue Service Provider faults

When a fault occurs in the dialogue service provider, a provider abort primitive is indicated to the application-users. Such abort causes the brutal termination of the pending application communications. Very likely the fault has been also detected in the communication layer where it occurred and notified to the SM manager according to its severity. There is no need to send at the application level a fault notification to the SM manager.

The failure of an instance of communication due to a failure of the communication service provider shall be logged.

3.1.2.3 ASE-generated faults

These faults are identified in the application SARPs under the heading "Exception Handling". They identify either an error in the local ASE (e.g. an unrecoverable error) or in the peer ASE (e.g. reception of an invalid or not permitted PDU, time-out, etc.).

It is assumed that ATC AAs are interested in being informed of these kind of errors as soon as possible. The ASEs constitute the critical path of the operational data link information. On the ground, they provide communication services to a wide range of users: controllers, surveillance systems, safety-related systems, meteorological systems, etc… Switch to a backup system could be a corrective action when such an error is experienced.

The airline AAs are less interested to get the fault notification on-line since a ground controlled action would be difficult to implement.

The failure of an instance of communication due to an error within the application shall be
- logged when detected in the aircraft,
- notified to the SM manager when detected on the ground.

In most cases, ASE level faults detected at one side are indicated to the other side via the exchange of an ABORT PDU. In other words, a resource in the air ES and a resource in the ground ES are able to detect the same ASE fault. By looking at the abort reason, both ESs are aware of the nature of the fault, except when the transmission of the ABORT PDU is not possible (e.g. when an unrecoverable error is detected, it is likely that the system can not communicate any more). The only exception to this rule is when the application-association can not be established due to a problem of the peer ASE not detectable in the peer ASE (e.g. invalid TSEL, unrecoverable error in the Transport, Session, Presentation, the ACSE or the CF). However, this error is detected in the transport or in the upper layers of the peer ES.

Based on the fact that both sides are aware of the ASE-generated fault, there is no need to downlink fault notification in real-time to the airline SM manager. The ATC SM manager can forward the notification to the airline SM manager.

The fault notifications issued by airborne agent are logged locally. The fault notifications issued by ground agents are sent to the ground ATC managers which can forward these notifications to the airline managers, based on bilateral agreements between the airline AA and the ATC AA.

3.2 Configuration Management

3.1.3 General Requirements

Some configuration parameters inherent to the ASEs may have to be known and/or modified by the SM manager. Two types of parameters exist:

- configuration parameters defined in the SARPs.

  The static configuration of an ES is determined by the **identification of the applications actually installed** in the ES, the **subsetting rules** of each ASE and the **ASE version number**. These parameters are fixed for a given aircraft or a given ground system. They are defined based on operational requirements and local choices of the airline or the ATC authority.

  There is actually no need to change the ASE static configuration before or during the flight. However, the knowledge of the values taken by these parameters may be very useful to understand the global behaviour of the ASE.

  The SM manager shall be able to assess the data link application capability of an ES and to get the functional configuration of each application.

  Very few parameters are defined in the ASE SARPs as variable configuration parameters. Actually, only the **technical timers** may be configurable in the ASE. Values indicated in the SARPs are only indications of reasonable values. In some operational contexts, the timer values may have to be customised. Some implementations may choose to have fixed values for the timers whereas others will allow to configure them.

- Implementation dependent parameters.

  Each implementation defines its own configuration parameters. The way the value of these parameters can be changed (locally or remotely, via operator commands or command files, etc...) is very dependent of the design of the implementations. Moreover, the configuration parameters are visible only within a management domain. It is unlikely that an AA will allow an other AA to retrieve and modify the configuration of its systems.

  The definition of the configuration parameters and the configuration means are outside the scope of the SARPs.

3.3 Accounting

3.1.4 General Requirements

Accounting management is responsible for collecting and processing data related to resource consumption in the system. The historical record of the usage of the resources may be necessary to understand how a problematic situation occurred.

The usage of the application resources can be measured by the user activity. Two levels of measures may be required. Global statistics should permit to evaluate the amount of activity for a given application and detailed statistics should allow to understand the activity with a particular peer system.

The number of invocations of each application service shall be made available for off-line analysis at application level and instance of communication level.

The amount of resources in use for a given application is also characterised by the number of simultaneous instances of the ASEs, and for each instance the identity of the peer system, the mode of the ASE when modes are defined (e.g. CPDLC/DSC/Forward), the mode of termination of each instance and, when relevant, the way the communication resources are managed by the users (e.g. the maintain dialogue option).

The ES shall notify every creation and deletion of instance of communications with the associated parameters.

3.4 Performance Management

3.1.5 General Requirements

Performance management shall allow monitoring the end-to-end performance of the ATN system provided to the application users. It enables evaluation of the effectiveness of the communication resources during the operational functioning thanks to statistical information and logs of system state histories.

The workload of the applications is already measured - globally or on a connection basis - by the parameters identified in the previous section for the accounting functional area (number and type of service invocations by the users).

The ADSP Manual defines in Part I, Chapter 3 Appendix A three types of communication systems performance requirements related to the ATS data link applications:

- **General Performance Requirements**

  The general performance requirements on the air-ground applications are the following:
  - the probability of non-receipt of a message will be equal to or less than 10^{-6},
  - the probability that non-receipt of a message will fail to be notified to the originator will be equal to or less than 10^{-9}, and
  - the probability that a message will be misdirected will be equal to or less than 10^{-7}.

  These performance requirements can not be monitored at application level. These performance metrics could be evaluated at transport level.

- **Application Specific Performance Requirements**

  The performance requirements specific to each air-ground application is also defined in the ADSP Manual, as shown bellow for the CM application.

APPLICATION	AVAILABILITY	INTEGRITY	RELIABILITY	CONTINUITY
CM	99.9%	10^{-6}	99.9%	99.9%

Table 1 - Application Specific Performance Requirements

It seems difficult to monitor these performance requirements at application level.

- **<u>Transfer Delay Requirements</u>**

PERFORMANCE LEVELS	MEAN END-TO-END TRANSFER DELAY	95% END-TO-END TRANSFER DELAY (SECONDS)	99.996% END-TO-END TRANSFER DELAY (SECONDS)
A	0.5	0.7	1
B	1	1.5	2.5
C	2	2.5	3.5
D	3	5	8
E	5	8	12.5
F	10	15	22
G	12	20	31.5
H	15	30	51
I	30	55	90
J	60	110	180

Table 2 - Transfer Delay Performance Requirements

It is proposed to measure the transit delay at the application level. As the transit delay is indirectly dependant of the requested class of communication service, this parameter should be made available with the transit delay measurements.

As the messages are not timestamped and there is no clock synchronisation mechanisms, the measurement of the transit delay shall be performed on a round trip exchange. The measure includes the transmission time of the request message, the message computation time by the remote system, the human response time and the transmission time of the corresponding response message. If no dialogue was in place, the delay includes the connection establishment delay and the transfer delay for the two messages. Otherwise, the delay includes the data transfer delay for the two messages only.

The mean and max values shall be measured for each confirmed application service.

3.5 Security Management

Security management is responsible for controlling access to the system resources through the use of authentication techniques and authorisation policies. Security functions are performed by the upper layers on behalf of the applications. It is likely that a specific ASE will be designed to handle security mechanisms.

The ASEs themselves will probably not perform security related actions. As a consequence, no resources will be defined at present in the ASE MIB to cover security.