

# The AFTN Message Switch Case Study

Copyright © 2003 David Bush  
Email: david.bush@iee.org

## ***Important***

*The intent of this document is to provide a Case Study for the illustration of Requirements Engineering approaches in a COTS scenario.*  
***Obviously, this document should NOT be used for any procurement action!***

## **Background**

AFTN messaging performs an essential role in the provision of an ATC Service. Some of the equipment providing the AFTN service is of 1970s vintage. Not only are these going to become unsupported, but they will become unable to handle the increasing traffic volumes, particularly during the summer, when AFTN traffic peaks (it is roughly proportional to the aircraft traffic volumes). It is estimated that there is a 75% chance that the system will fail to cope with traffic next summer (11 months away), and so to ensure that the high integrity of the messaging service is maintained, the existing switch needs replacing before then.

## ***General Requirement***

Two new message switches are required. Firstly, a main operational switch at one site, and additionally, a fully functional message switch to be provided for contingency operation at the system management site. A support facility (TAD) to provide for the testing and development of the operational systems is also required.

Opinions differ as to whether the TAD should be co-located with the main switch (where it is closer to the main operational system and supports the case for the continuation of a significant engineering support capability at the site), or at the contingency site (where the responsible business area has the policy of centralising maintenance and support at the management centre).

## ***Performance Requirements***

The system needs to support a message rate of 50 AFTN, CIDIN, and TELEX messages per second. There can be no accumulation of messages.

For a sustained message input rate of 40 messages a second, the system needs to support a peak output rate of 300 messages per second for at least 1 minute. (Assuming a mean Input/Output ratio of 1:6).

In addition to this, the system needs to provide a CIDIN relay function at a minimum of 12 packets per second, and a peak CIDIN relay function rate of 50 packets per second. The relay time should not exceed 3 seconds.

In the event of a sudden surge of incoming messages the system shall exhibit "graceful degradation" rather than system shutdown. During "graceful degradation", the system must be able to respond immediately to operator commands that will alleviate the overload situation.

Key sizing/capacity needs are:

- 1900 channels, 1750 circuits and more than 40 direct asynchronous connections; for either CIDIN or AFTN use;
- 6 telex lines;
- 6500 routes.

### ***Safety & Security Requirements***

The switches must not contribute to an unacceptable level of risk to safety of operations, either by commission or omission.

It must not be possible to perform any sort of change, maintenance or interference with the operation of the switches except from the TSF or operational consoles, to ensure that unauthorised changes are not made to the system.

Messages passed through the switch must remain secure.

The fulfilment of these requirements must be adequately demonstrated in a safety case.

### ***Customisation***

The system needs to be able to cope with the customer's specific variations on the ICAO AFTN standard.

### ***Dependencies***

The connectivity between the switches and the system users will be provided by the customer, using its own X25 and ground communications networks, which provide high availability point to point data and voice circuits.

Connectivity between the message switches and their associated user terminals will be the responsibility of the supplier.

### ***Procurement Requirements - Design Data Availability***

Shortly after the start of the contract, the customer will need to see a detailed system design showing all hardware and software functionality and performance, so that a view can be taken on Safety Case development.

### ***Procurement Requirements - HCI Prototyping***

A prototype should be used to develop and test the HCI functionality, and to determine the detailed requirements. But the key requirement is for a highly usable system, particularly in terms of time to learn, ease of access to information, appropriate feedback to the user based on their actions, meaningful error handling, and so on. The HCI should present information consistently with related systems that users are currently operating and in a way that allows rapid and accurate assimilation.

### ***Procurement Requirements - Testing***

The main system test will be carried out on each system in its installed final location. This will need to exercise the full functionality of the system and will

demonstrate its safe and reliable performance in the operational environment. It will include a transitional operations period, where there must be no failure in providing the operational messaging service.

### ***Transition to Operations***

The customer will need on-site assistance from staff familiar with the system, to assist in the transition to operational service.

The transition to operations should ideally take place during the less busy winter months (a window between 7 and 8 months hence) so that the chance of adverse impact on service delivery is minimised.

## Supplementary Notes

### Technical Background

The Aeronautical Fixed Telecommunications Network (AFTN) is a global messaging network. It provides for the exchange of messages to improve the safety, regularity and efficiency of international air navigation. Messages exchanged through the AFTN include Flight Plans, NOTAMs, meteorological messages, distress messages, flight regularity messages, administrative and service messages.

Message switching systems provide the switches that route messages around the AFTN to their required destination. (For example, aircraft using the UK airspace will have a flight plan request filed by their Operations Centre. For all European flights, these requests must then be routed to the Central Flow Management Unit (CFMU) in Brussels (which calculates routes for all known traffic). The resulting flight plans then need to be routed to European ATC agencies, and so on to ATC Centres and Airports. )

CIDIN: The Common ICAO Data Interchange Network is a data transport service that underpins the current AFTN network.

AMHS: The Aeronautical Message Handling Service is a modern protocol equivalent of the AFTN/CIDIN service.

### Commercial Message Switch Information

The following sites provide some information about COTS AFTN Message Switches. #

<http://www.digres.com/aftn/MMS.htm>

<http://www.corobor.com/aftn.html>

<http://www.sw.nec.co.jp/english/AFTN/>

<http://www.gwdi.com/prodserv/AFTN.html>

[http://www.cnd.co.nz/cnd\\_QSS.htm](http://www.cnd.co.nz/cnd_QSS.htm)

<http://www.copperchase.co.uk/products/afswitch.htm>

### Safety Assurance

Most organisations working in the safety related/safety critical arena in UK assure the safety of their operations through the production of a 'Safety Case'.

Suppliers sometimes do not have regulated safety systems, and may not have the capability to construct the system safety case, in these cases the customer might take on this responsibility, and would then need access to

---

# These examples have been selected purely on the basis of being the first ones listed during an Internet search!

detailed design and performance data. For general information, a Safety Case might address the following objectives:\*

***Requirements Validity***

- To ensure that arguments and evidence are available which show that the Safety Requirements correctly state what is necessary and sufficient to achieve tolerable safety, in the operational context.

***Requirements Satisfaction***

- To ensure that arguments and evidence are available which shows that the solution satisfies its Safety Requirements.

***Requirements Traceability***

- To ensure that arguments and evidence are available which shows that all Safety Requirements can be traced to the same level of design at which their satisfaction is demonstrated

***Un-Required Functionality***

- To ensure that functions implemented as a result of Safety Requirements are not interfered with by other functions implemented in the software.

***Configuration Consistency***

- To ensure that the arguments and evidence for the safety of the system in it operational context, are derived from a known set of products, data and descriptions which have been used in the production of that version.

---

\* These are 'system level' generalisations of the Objectives stated in CAP670, SW01 - Regulatory Objectives for Software Safety Assurance in ATS Equipment