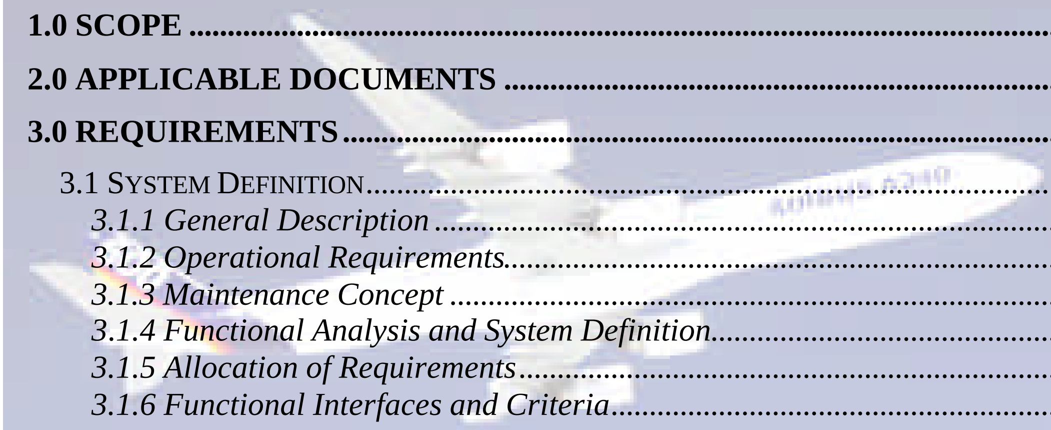
# System Specification

***Type-A Document***

# Airbus A330/A340 Flight Control System



## Contents

## 1.0 Scope

This document is made in the scope of the Systems Engineering Class at the University of Twente. It is a Type-A document describing the design of *The Airbus A330/A340 Primary Flight Control System*. The emphasis in our design is on the fault tolerance of the control of the plane, because this control system is mission critical.

## 2.0 Applicable documents

This document assumes you are familiar with the general Airbus design information presented in *Case2001AirbusA330.pdf.* This description is taken from the book "*Safety Critical Systems*" by Niel Story (1996) Addison Wesley, ISBN 0 201 42787 7 and is available at http://www.rt.el.utwente.nl/syseng/Exercises/Case2001AirbusA330.pdf.

Information on pilot interfaces is taken from the Dutch magazine "*Piloot & Vliegtuig*", number 9/2000 Uitgeverij P&V, ISSN 1381 1827 (See also http://www.pilootenvliegtuig.nl).

General information about Airbus can be found at http://www.airbus.com/.

During the design extensive use was made of the book "*Systems Engineering and Analysis*" by B.S. Blanchard and W.J. Fabrycky (1997) Prentice-Hall, Inc. ISBN 0 13 135047 1.

# 3.0 Requirements

## *3.1 System Definition*

This type-A document describes the specifications for the design of a flight control system for the Airbus A330/A340.

In the Airbus A320, which was introduced in 1988, digital techniques were used for the primary flight controls. Although this aircraft can be flown using mechanical backup systems, under normal circumstances it adopts a complete fly-by-wire approach, where crew commands are transmitted to the control surfaces through computers rather than by mechanical linkages. In the mid-1990s Airbus introduced the A330/A340 family of aircraft. This also incorporates fly-by-wire techniques and makes extensive use of advanced computer systems. The A330 is a twin-engined aircraft, whereas the A340 has four engines. Due to the Fly-by-Wire concept, the ‘user interface’ for the pilot is the same for all A3xx types, which saves a considerable amount of flight training hours.

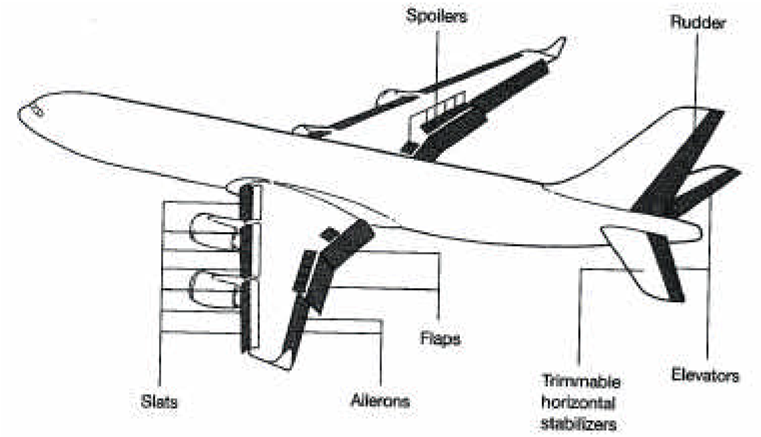


*Figure 1 Flight Control Surfaces of an A340*

Although the A330 and A340 aircraft can be flown without the use of their electronic flight control system (EFCS), failure of this system would represent a considerable reduction in overall safety levels. The EFCS therefore requires a very high level of integrity and is designed and produced to the stringent standards appropriate for such a system. Because the aircraft relies heavily on its computer system to operate its various control surfaces, it is imperative that the control system remains operational at all times. Fault detection is therefore not sufficient to provide safety and the system must also provide effective fault tolerance to allow the unit to continue safe operation, perhaps for several hours, in the presence of faults. In this case, we will concentrate on the architectural features to achieve a high level of fault tolerance, which is absolutely needed for this kind of mission-critical systems.

*Figure 2 Pilot interface of the Airbus A330*

### 3.1.1 General Description

The flight control system is the system which controls the plane. This system consists of mechanical and electronic parts, and the pilot. It has to improve safety by means of a high degree of fault tolerance, and also by relieving the tasks of the pilot:

- Reduce the pilot’s workload by providing an intuitive user interface and by performing some functions automatically.
- Prevent the crew from inadvertently exceeding the aircraft’s controllability limits.
- Act to maintain the aircraft within its normal range of operation.
- Prevent the pilot from inadvertently entering a stall condition.

### 3.1.2 Operational Requirements

There are several important requirements to the system.

- Need: An effective fault tolerance to allow the unit to continue safe operation, perhaps for several hours, in the presence of faults. Also reduce the pilot’s workload and prevent the crew from inadvertently exceeding the aircraft’s controllability limits.
- Mission: The flight control system has to be highly unlikely to fail (effectively fault tolerant) so the plane can have safe flights.
- Use profile: The system has to operate during each flight (from takeoff to landing). Flight times range from 1 to about 15 hours.
- Distribution: Each Airbus A330/340 plane has to have one flight control system, consisting of several redundant subsystems.
- Lifecycle: Same as lifecycle of the plane, which is somewhere around 20-30 years.

### 3.1.3 Maintenance Concept

To maintain the flight control system several things are required:

- Modularity so spare parts can be swapped in easily
- Self testing system (and parts) that will indicate faults in an early stage
- Automatic performance logging (so engineers can trace odd behavior in the past)
- Periodic replacement of parts that are subject to wear-out.
- Service engineers, training
- Service documentation, storage and access
- Test and support equipment

### 3.1.4 Functional Analysis and System Definition

From a top-level point of view the flight control system consists of the following parts:

- Electronic Flight Control System (EFCS)
- Actuator control
- Flight control surfaces
- Sensors
- Interface
- Pilot

In figure 3 the relations between these parts are depicted.

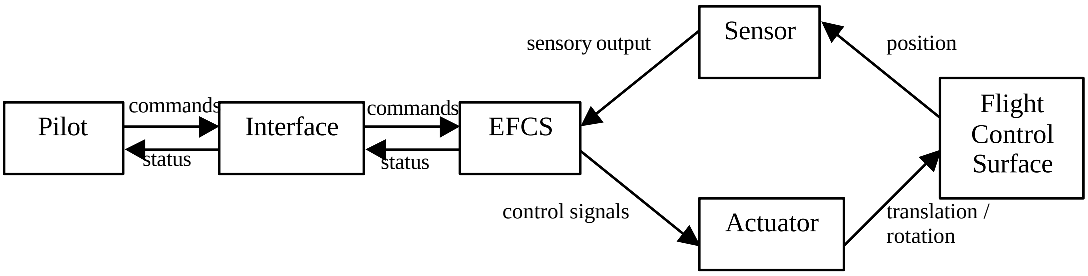


*Figure 3 System top-level functions of the Flight Control System*

Fault tolerance can be implemented by making the entire control system redundant. An example can be seen in figure 4, where there is a mechanical as well as an electronic link to the control surface. The actuators can be mechanical and hydraulic.

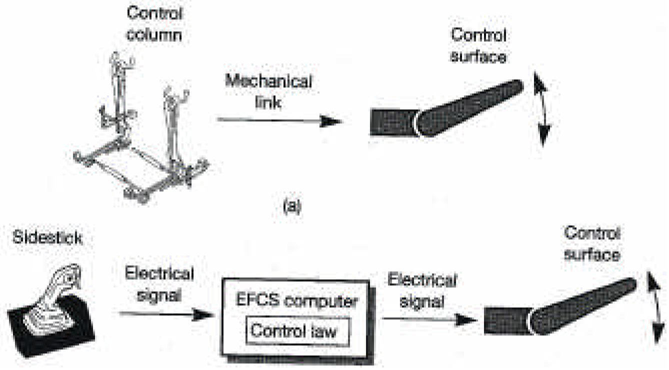


*Figure 4 Mechanical and Electrical control*

This kind of redundancy has to be applied in every subsystem. Suggested is to use multiple pilots, interfaces, computers and (software) algorithms, sensors and actuators, preferably in an arrangement that is designed to provide a high degree of protection against a wide variety of system faults. Triple redundancy will suffice in most emergent cases and will be required for the flight control system.

Each flight control surface must be driven by multiple independent actuators, which are in turn controlled by different computers. This guarantees that failure of a single actuator or computer will not result in a loss of control of that surface. As movement of the control surfaces is achieved using hydraulic actuators, the hydraulic supply represents a key component within the control system. In common with other commercial aircraft, three separate hydraulic supplies should be used.

## 3.1.5 Allocation of Requirements

The requirements set for the top-level system have to be applied to all subsystems. So if it is required to have threefold redundancy each part (EFCS computers, actuators, sensors, power supplies etc.) has to implement threefold redundancy.

EFCS computers have to interpret pilot commands, combine it with all kinds of sensory input and use it for actuator control and interface display. They also have to monitor (and eventually reconfigure) the entire system, including itself. EFCS computers should operate independently. If one of these computers malfunctions, its tasks should be taken over by the other computers.

Actuators are driven by the EFCS computers and have to position the flight control surfaces. They must be very accurate and show no hysteresis so position is always known.

Sensors are to be used for all flight control surfaces besides for flight status measurements (airspeed, attitude, altitude, horizon, vertical speed, GPS info). The sensors have to be used in high quantities. They must be very accurate and work independently, and stay robust in all weather conditions. They have to be protected against shocks, extreme pressures and temperatures, moisture etc.

The interface has to show sensory measurements, flight status, but also feedback to recent pilot commands. The pilot should be able to request all kinds of information, like system status, air traffic status and weather status. Furthermore it has to show all kinds of calculations, e.g. errors, deviations and also warnings. It should be very reliable and should also be very ergonomically in use. For example primary controls and status displays have to be very clear (colored) in comparison with the rest.

The pilots should be well trained and should be healthy, rest enough, fed enough, have high moral standards, peace with his relatives and never be drunk.

### 3.1.6 Functional Interfaces and Criteria

The interfaces between all components should conform to standardized norms, preferably time-tested and proven industry standards. Interfaces should be clearly labeled for easy service.

## *3.5 Logistics*

### 3.5.1 Maintenance Requirements

For the maintenance of the system, the presence of spare parts and specialized personel at the airport is needed. A detection system in the plane has to provide information for the maintenance crew to check whether all jobs have been carried out. For fast and economic maintenance, all systems and parts must be modular and easily replaceable.

### 3.5.2 Supply Support

All parts that are replaced often, have to be available on (bigger) airports. For all other parts, a file must be kept in which is written where to order spare parts for all locations. For all parts there has to be detailed information about how to transport it. A detailed list with transport specifications is very important. For instance, some parts are very sensitive for vibrations and shocks. If they are placed in the system in the plane, they are constructed in an anti-shock case. So for transport, the same rules of care must be met.

### 3.5.3 Test and Support Equipment

The testing should be done by the plane itself and by the ground crew periodically. The plane should have a testing circuit which is able to test if all sensors are responding correctly and keep track of powerconsumption of all parts. If a part is consuming more power than it's estimated amount, a fault could be present. The ground crew should test all essential parts before every take-off. All other parts should be tested every five flights. A detailed logfile has to be made for all actions. This should be available in the plane as well as in the fabric.

### 3.5.4 Personnel and Training

The pilot must have the feeling that he is actually flying the plane by his own. All parts he has immediate contact with like the *sidestick* should give feedback from the reactions of the plane. Still, he should be aware of the whole flight control system and have knowledge of the way the system works, to react properly if a malfunction occurs.

The testing and maintenance team should know the system in a detailed way although the testing system gives exact information where to test and maintain (this system could malfunction too!). The crew should be informed accurately if new systems are used and should be examined every two years to test if their knowledge is still up to date.

### 3.5.5 Computer Resources (Software)

The computer resources must consist of small subsystems with stable software, which is well tested. It’s better to have more subsystems than one big computer which rules the whole flight control because in case of failure, the other computers immediately take over the tasks of the crashed system, to increase the fault tolerance. Further, the computer system should check all systems on a real-time basis to make sure all parameters are within the fault tolerance limits. If not, a detailed scenario must be present how to react on this particular error notification.

### 3.5.6 Customer Services

For safety reasons, only the basics off the controlsystem will be made public. Detailed information will not be given to third parties. One central cutomer services centre will provide all public information. If all details would be made publically available, it would be easily possible for criminals to (remotely) disable or damage some safety systems.