12

Electrical Flight Controls, From Airbus A320/330/340 to Future Military Transport Aircraft: A Family of Fault-Tolerant Systems

Dominique Briere
Aerospatiale

Christian Favre
Aerospatiale

Pascal Traverse
Aerospatiale

12.1 Introduction

The first electrical flight control system for a civil aircraft was designed by Aerospatiale and installed on the Concorde. This is an analog, full-authority system for all control surfaces. The commanded control surface positions are directly proportional to the stick inputs. A mechanical back-up system is provided on the three axes.

The first generation of electrical flight control systems with digital technology appeared on several civil aircraft at the start of the 1980s with the Airbus A310 program. These systems control the slats, flaps, and spoilers. These systems were designed with very stringent safety requirements (control surface runaway must be extremely improbable). As the loss of these functions results in a supportable increase in the crew's workload, it is possible to lose the system in some circumstances.

TABLE 12.1 Incremental Introduction of New Technologies

First Flight In:	1955	1969	1972	1978–1983	1983	1987
Servo-Controls, and Artificial Feel	x	x	x	x	x	--> x
Electro-Hydraulic Actuators		x	x	x	x	--> x
Command and Monitoring Computers		x	x	x	x	--> x
Digital Computers				x	x	--> x
Trim, Yaw Damper, Protection	x	x	x	x	x	--> x
Electrical Flight Controls		x		x	x	-->x
Side-Stick, Control Laws				x		--> x
Servoed Aircraft (Auto-pilot)	x	x	x	x	x	--> x
Formal System Safety Assessment		x	x	x	x	--> x
System Integration Testing	x	x	x	x	x	--> x
	Carevelle	Concorde	A300	Flight test Concorde A300	A310, A300–600	A320

The Airbus A320 (certified in early 1988) is the first example of a second generation of civil electrical flight control aircraft, rapidly followed by the A340 aircraft (certified at the end of 1992). These aircraft benefit from the significant experience gained by Aérospatiale in the technologies used for a fly-by-wire system (see Table 12.1). The distinctive feature of these aircraft is that all control surfaces are electrically controlled and that the system is designed to be available under all circumstances.

This system was built to very stringent dependability requirements both in terms of safety (the system may generate no erroneous signals) and availability (the complete loss of the system is extremely improbable).

The overall dependability of the aircraft fly-by-wire system relies in particular on the computer arrangement (the so-called control/monitor architecture), the system tolerance to both hardware and software failures, the servo-control and power supply arrangement, the failure monitoring, and the system protection against external aggressions. It does this without forgetting the flight control laws which minimize the crew workload, the flight envelope protections which allow fast reactions while keeping the aircraft in the safe part of the flight envelope, and finally the system design and validation methods.

The aircraft safety is demonstrated by using both qualitative and quantitative assessments; this approach is consistent with the airworthiness regulation. Qualitative assessment is used to deal with design faults, interaction (maintenance, crew) faults, and external environmental hazard. For physical ("hardware") faults, both qualitative and quantitative assessments are used. The quantitative assessment covers the FAR/JAR 25.1309 requirement, and links the failure condition classification (minor to catastrophic) to its probability target.

The aim of this chapter is to describe the Airbus fly-by-wire systems from a fault-tolerant standpoint. The fly-by-wire basic principles are presented first, followed by the description of the main system features common to A320 and A340 aircraft, the failure detection and reconfiguration procedures, the A340 particularities, and the design, development, and validation procedures. Future trends in terms of fly-by-wire fault-tolerance conclude this overview.

12.2 Fly-by-Wire Principles

On aircraft of the A300 and A310 type, the pilot orders are transmitted to the servo-controls by an arrangement of mechanical components (rods, cables, pulleys, etc.). In addition, specific computers and actuators driving the mechanical linkages restore the pilot feels on the controls and transmit the autopilot commands (see Figure 12.1).

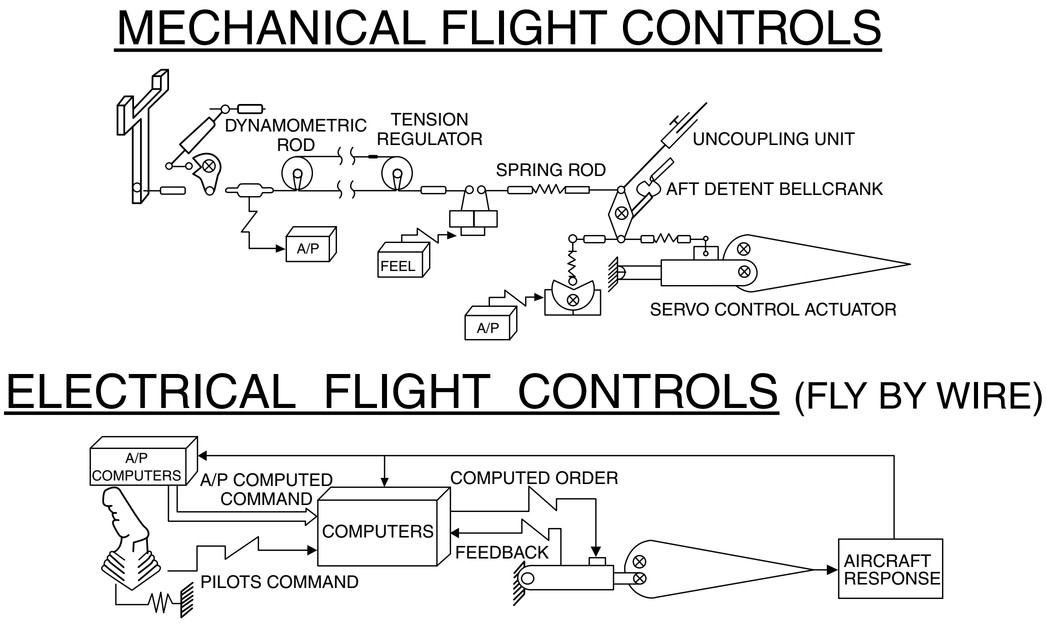

FIGURE 12.1 Mechanical and electrical flight control.

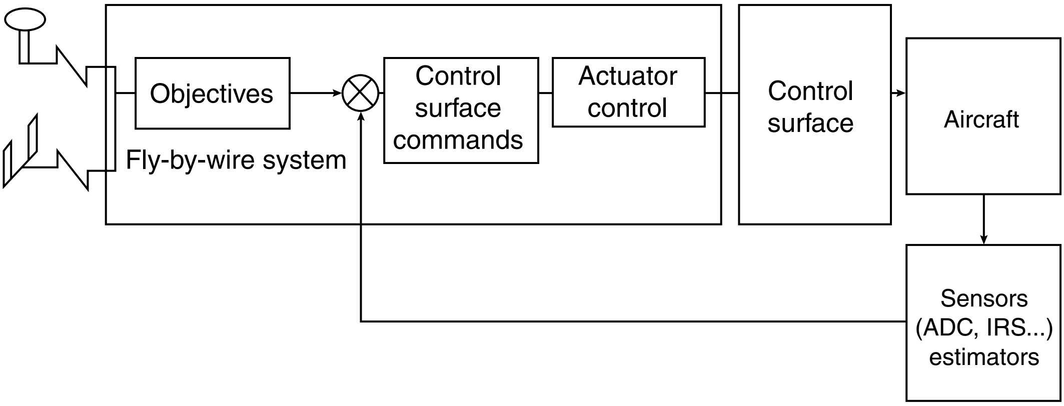

FIGURE 12.2 Flight control laws.

The term fly-by-wire has been adopted to describe the use of electrical rather than mechanical signalling of the pilot's commands to the flying control actuators. One can imagine a basic form of fly-by-wire in which an airplane retained conventional pilot's control columns and wheels, hydraulic actuators (but electrically controlled), and artificial feel as experienced in the 1970s with the Concorde program. The fly-by-wire system would simply provide electrical signals to the control actuators that were directly proportional to the angular displacement of the pilot's controls, without any form of enhancement.

In fact, the design of the A320, A321, A330, and A340 flight control systems takes advantage of the potential of fly-by-wire for the incorporation of control laws that provide extensive stability augmentation and flight envelope limiting [Favre, 1993]. The positioning of the control surfaces is no longer a simple reflection of the pilot's control inputs and conversely, the natural aerodynamic characteristics of the aircraft are not fed back directly to the pilot (see Figure 12.2).

The sidesticks, now part of a modern cockpit design with a large visual access to instrument panels, can be considered as the natural issue of fly-by-wire, since the mechanical transmissions with pulleys, cables, and linkages can be suppressed with their associated backlash and friction.

The induced roll characteristics of the rudder provide sufficient roll maneuverability of design a mechanical back-up on the rudder alone for lateral control. This permitted the retention of the advantages of the sidestick design, now rid of the higher efforts required to drive mechanical linkages to the roll surfaces.

Looking for minimum drag leads us to minimize the negative lift of the horizontal tail plane and consequently diminishes the aircraft longitudinal stability. It was estimated for the Airbus family that no significant gain could be expected with rear center-of-gravity positions beyond a certain limit. This allowed us to design a system with a mechanical back-up requiring no additional artificial stabilization.

These choices were obviously fundamental to establish the now-classical architecture of the Airbus fly-by-wire systems (Figures 12.3 and 12.4), namely a set of five full-authority digital computers controlling the three pitch, yaw, and roll axes and completed by a mechanical back-up on the trimmable horizontal stabilizer and on the rudder. (Two additional computers as part of the auto pilot system are in charge of rudder control in the case of A320 and A321 aircraft.)

Of course, a fly-by-wire system relies on the power systems energizing the actuators to move the control surfaces and on the computer system to transmit the pilot controls. The energy used to pressurize the servo-controls is provided by a set of three hydraulic circuits, one of which is sufficient to control the aircraft. One of the three circuits can be pressurized by a Ram air turbine, which automatically extends in case of an all-engine flame-out.

The electrical power is normally supplied by two segregated networks, each driven by one or two generators, depending on the number of engines. In case of loss of the normal electrical generation, an emergency generator supplies power to a limited number of fly-by-wire computers (among others). These computers can also be powered by the two batteries.

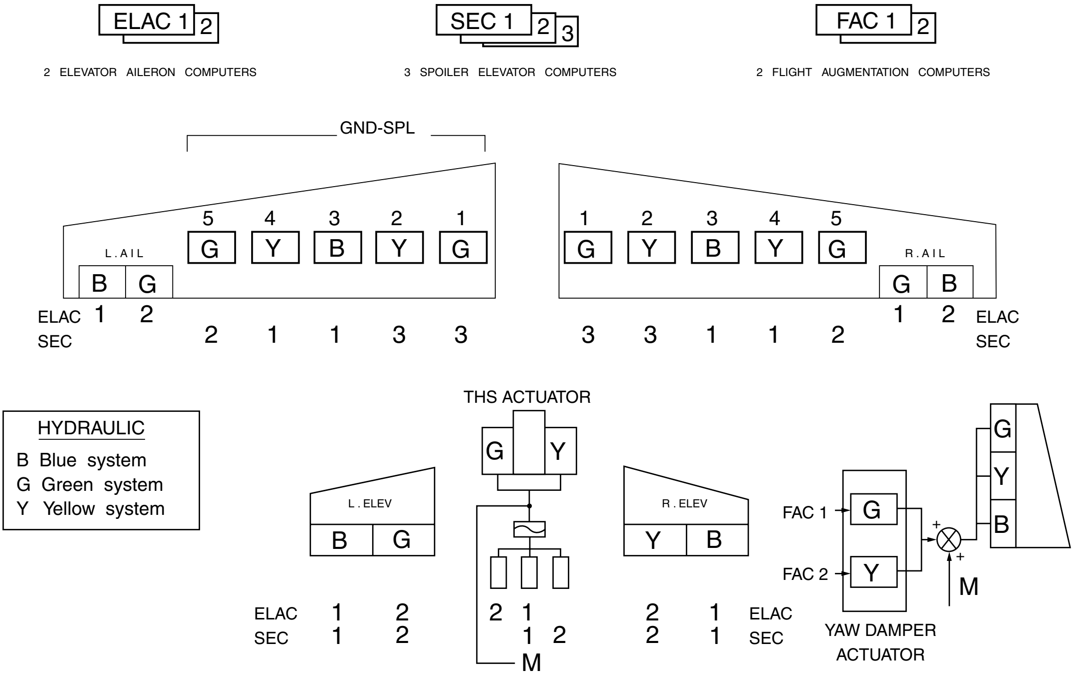

FIGURE 12.3 A320/A321 flight control system architecture.

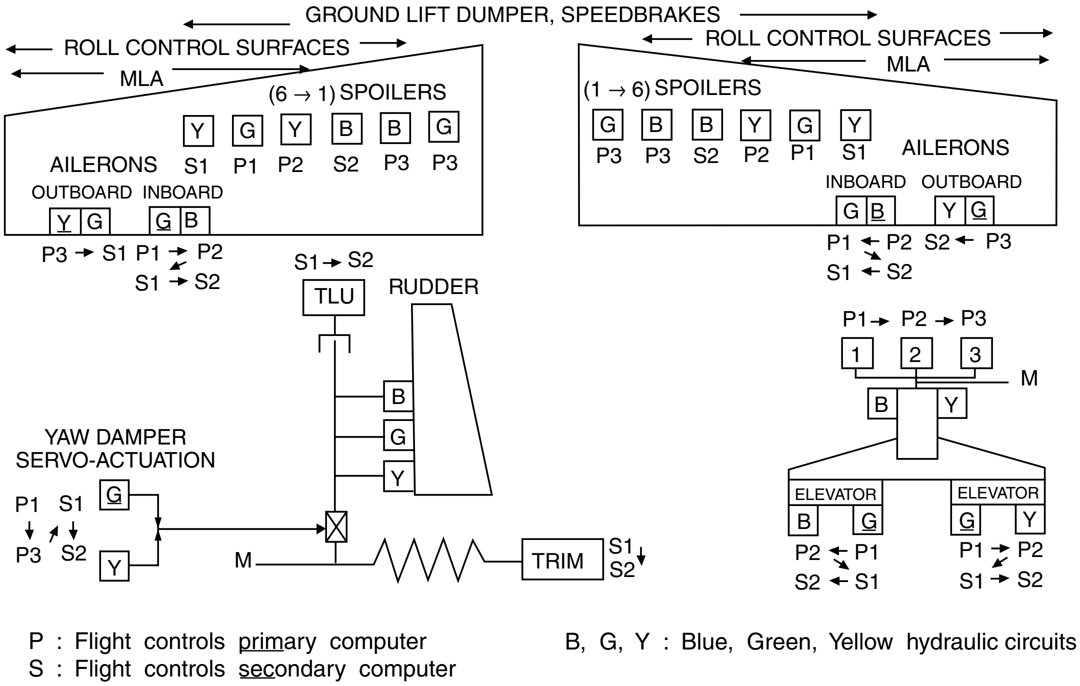

FIGURE 12.4 A330/A340 flight control system architecture.

12.3 Main System Features

12.3.1 Computer Arrangement

12.3.1.1 Redundancy

The five fly-by-wire computers are simultaneously active. They are in charge of control law computation as a function of the pilot inputs as well as individual actuator control, thus avoiding specific actuator control electronics. The system incorporates sufficient redundancies to provide the nominal performance and safety levels with one failed computer, while it is still possible to fly the aircraft safely with one single computer active.

As a control surface runaway may affect the aircraft safety (elevators in particular), each computer is divided into two physically separated channels (Figure 12.5). The first one, the control channel, is permanently monitored by the second one, the monitor channel. In case of disagreement between control and monitor, the computer affected by the failure is passivated, while the computer with the next highest priority takes control. The repartition of computers, servo-controls, hydraulic circuit, and electrical bus bars and priorities between the computers are dictated by the safety analysis including the engine burst analysis.

12.3.1.2 Dissimilarity

Despite the nonrecurring costs induced by dissimilarity, it is fundamental that the five computers all be of different natures to avoid common mode failures. These failures could lead to the total loss of the electrical flight control system.

Consequently, two types of computers may be distinguished:

2 ELAC (elevator and aileron computers) and 3 SEC (spoiler and elevator computers) on A320/A321 and,

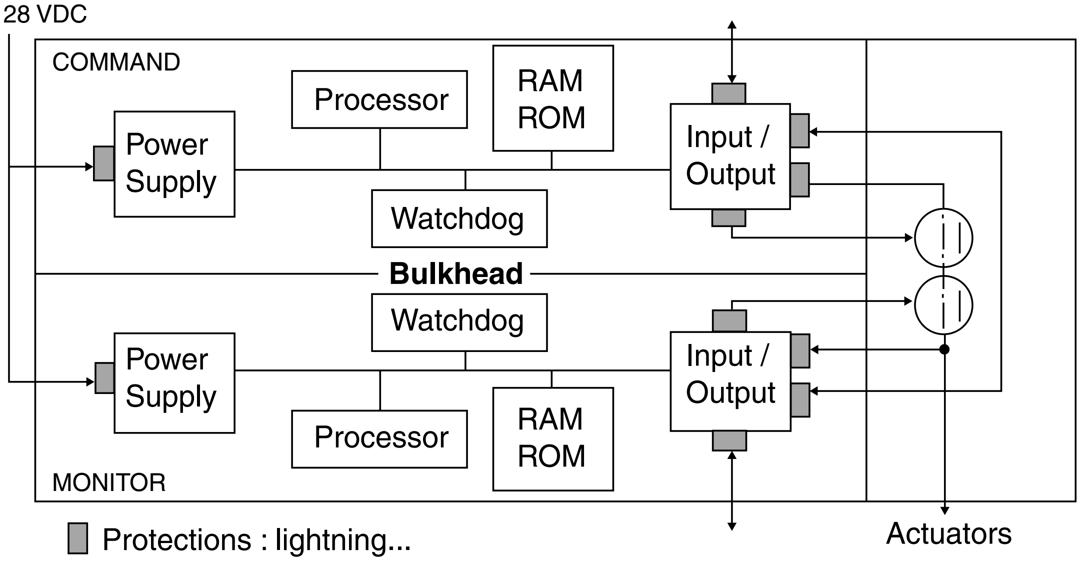

FIGURE 12.5 Command and monitoring computer architecture.

3 FCPC (flight control primary computers) and 2 FCSC (flight control secondary computers) on A330/A340.

Taking the 320 as an example, the ELACs are produced by Thomson-CSF around 68010 microprocessors and the SECs are produced in cooperation by SFENA/Aerospatiale with a hardware based on the 80186 microprocessor. We therefore have two different design and manufacturing teams with different microprocessors (and associated circuits), different computer architectures, and different functional specifications. At the software level, the architecture of the system leads to the use of four software packages (ELAC control channel, ELAC monitor channel, SEC control channel, and SEC monitor channel) when, functionally, one would suffice.

12.3.1.3 Serve-Control Arrangement

Ailerons and elevators can be positioned by two servo-controls in parallel. As it is possible to lose control of one surface, a damping mode was integrated into each servo-control to prevent flutter in this failure case. Generally, one servo-control is active and the other one is damped. In case of loss of electrical control, the elevator actuators are centered by a mechanical feedback to increase the horizontal stabilizer efficiency.

Rudder and horizontal stabilizer controls are designed to receive both mechanical and electrical inputs. One servo-control per spoiler surface is sufficient. The spoiler servo-controls are pressurized in the retracted position in case of loss of electrical control.

12.3.1.4 Flight Control Laws

The general objective of the flight control laws integrated in a fly-by-wire system is to improve the natural flying qualities of the aircraft, in particular in the fields of stability, control, and flight domain protections. In a fly-by-wire system, the computers can easily process the anemometric and inertial information as well as any information describing the aircraft state. Consequently, control laws corresponding to simple control objectives could be designed. The stick inputs are transformed by the computers into pilot control objectives which are compared to the aircraft actual state

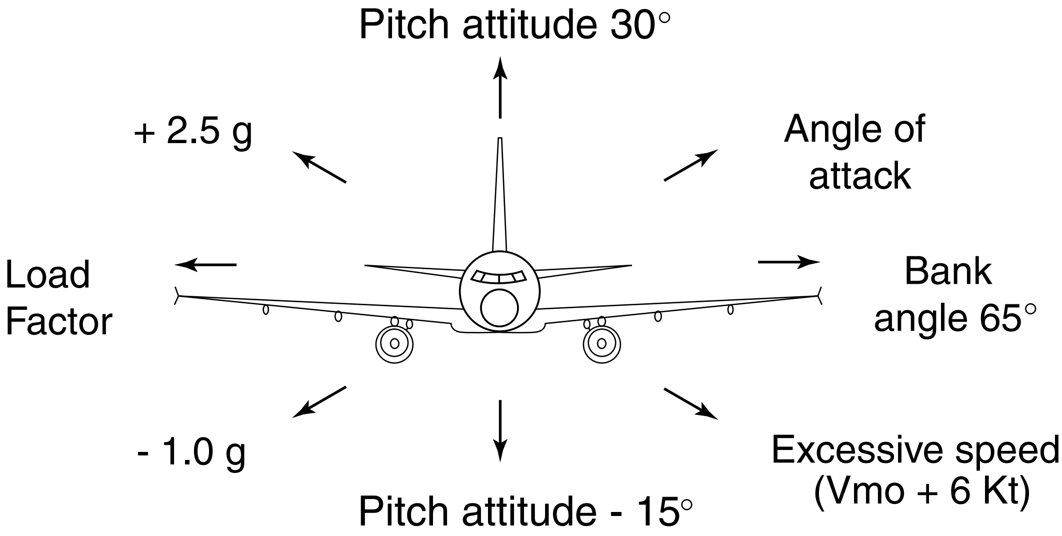

FIGURE 12.6 A320 flight envelope protections.

measured by the inertial and anemometric sensors. Thus, as far as longitudinal control is concerned, the sidestick position is translated into vertical load factor demands, while lateral control is achieved through roll rate, sideslip, and bank angle objectives.

The stability augmentation provided by the flight control laws improves the aircraft flying qualities and contributes to aircraft safety. As a matter of fact, the aircraft remains stable in case of perturbations such as gusts or engine failure due to a very strong spin stability, unlike conventional aircraft. Aircraft control through objectives significantly reduces the crew workload; the fly-by-wire system acts as the inner loop of an autopilot system, while the pilot represents the outer loop in charge of objective management.

Finally, protections forbidding potentially dangerous excursions out of the normal flight domain can be integrated in the system (Figure 12.6). The main advantage of such protections is to allow the pilot to react rapidly without hesitation, since he knows that this action will not result in a critical situation.

12.3.1.5 Computer Architecture

Each computer can be considered as being two different and independent computers placed side by side (see Figure 12.5). These two (sub)computers have different functions and are placed adjacent to each other to make aircraft maintenance easier. Both command and monitoring channels of the computer are simultaneously active or simultaneously passive, ready to take control.

Each channel includes one or more processors, their associated memories, input/output circuits, a power supply unit, and specific software. When the results of these two channels diverge significantly, the links between the computer and the exterior world are cut by the channel or channels which detected the failure. The system is designed so that the computer outputs are then in a dependable state (signal interrupt via relays). Failure detection is mainly achieved by comparing the difference between the control and monitoring commands with a predetermined threshold. As a result, all consequences of a single computer fault are detected and passivated, which prevents the resulting error from propagating outside of the computer. This detection method is completed by permanently monitoring the program sequencing and the program correct execution.

Flight control computers must be robust. In particular, they must be especially protected against overvoltages and undervoltages, electromagnetic aggressions, and indirect effects of lightning. They are cooled by a ventilation system but must operate correctly even if ventilation is lost.

12.3.1.6 Installation

The electrical installation, in particular the many electrical connections, also comprises a common-point risk. This is avoided by extensive segregation. In normal operation, two electrical generation systems exist without a single common point. The links between computers are limited, the links used for monitoring are not routed with those used for control. The destruction of a part of the aircraft is also taken into account; the computers are placed at three different locations, certain links to the actuators run under the floor, others overhead, and others in the cargo compartment.

12.4 Failure Detection and Reconfiguration

12.4.1 Flight Control Laws

The control laws implemented in the flight control system computers have full authority and must be elaborated as a function of consolidated information provided by at least two independent sources in agreement.

Consequently, the availability of control laws using aircraft feedback (the so-called normal laws) is closely related to the availability of the sensors. The Airbus aircraft fly-by-wire systems use the information of three air data and inertial reference units (ADIRUs), as well as specific accelerometers and rate gyros. Moreover, in the case of the longitudinal normal law, analytical redundancy is used to validate the pitch rate information when provided by a single inertial reference unit. The load factor is estimated through the pitch rate information and compared to the available accelerometric measurements in order to validate the IRS data.

After double or triple failures, when it becomes impossible to compare the data of independent sources, the normal control laws are reconfigured into laws of the direct type where the control surface deflection is proportional to the stick input. To enhance the dissimilarity, the more sophisticated control laws with aircraft feedback (the normal laws) are integrated in one type of computer, while the other type of computer incorporates the direct laws only.

12.4.2 Actuator Control and Monitor

The general idea is to compare the actual surface position to the theoretical surface position computed by the monitoring channel. When needed, the control and monitor channels use dedicated sensors to perform these comparisons. Specific sensors are installed on the servovalve spools to provide an early detection capability for the elevators. Both channels can make the actuator passive. A detected runaway will result in the servo-control deactivation or computer passivation, depending on the failure source.

12.4.3 Comparison and Robustness

Specific variables are permanently compared in the two channels. The difference between the results of the control and monitoring channels are compared with a threshold. This must be confirmed before the computer is disconnected. The confirmation consists of checking that the detected failure lasts for a sufficiently long period of time. The detection parameters (threshold, temporization) must be sufficiently "wide" to avoid unwanted disconnections and sufficiently "tight" so that undetected failures are tolerated by the computer's environment (the aircraft). More precisely, all systems tolerance (most notably sensor inaccuracy, rigging tolerances, computer asynchronism) are taken into account to prevent undue failure detection, and errors which are not detectable (within the signal and timing thresholds) are assessed in respect to their handling quality and structural loads effect.

12.4.4 Latent Failures

Certain failures may remain masked a long time after their occurrence. A typical case is a monitoring channel affected by a failure resulting in a passive state and detected only when the monitored channel itself fails. Tests are conducted periodically so that the probability of the occurrence of an undesirable event remains sufficiently low (i.e., to fulfill [FAR/JAR 25] § 25.1309 quantitative requirement). Typically, a computer runs its self-test and tests its peripherals during the energization of the aircraft, and therefore at least once a day.

12.4.5 Reconfiguration

As soon as the active computer interrupts its operation relative to any function (control law or actuator control), one of the standby computers almost instantly changes to active mode with no or limited jerk on the control surfaces. Typically, duplex computers are designed so that they permanently transmit healthy signals which are interrupted as soon as the "functional" outputs (to an actuator, for example) are lost.

12.4.6 System Safety Assessment

The aircraft safety is demonstrated using qualitative and quantitative assessments. Qualitative assessment is used to deal with design faults, interaction (maintenance, crew) faults, and external environmental hazard. For physical ("hardware") faults, both a qualitative and a quantitative assessments are done. In particular, this quantitative assessment covers the link between failure condition classification (Minor to Catastrophic) and probability target.

12.4.7 Warning and Caution

It is deemed useful for a limited number of failure cases to advise the crew of the situation, and possibly that the crew act as a consequence of the failure. Nevertheless, attention has to be paid to keep the level of crew workload acceptable. The basic rule is to get the crews attention only when an action is necessary to cope with a failure or to cope with a possible future failure. On the other hand, maintenance personnel must get all the failure information.

The warnings and cautions for the pilots are in one of the following three categories:

- Red warning with continuous sound when an immediate action is necessary (for example, to reduce airplane speed).
- Amber caution with a simple sound, such that the pilot be informed although no immediate action is needed (for example, in case of loss of flight envelope protections an airplane speed should not be exceeded).
- Simple caution (no sound), such that no action is needed (for example, a loss of redundancy).

Priority rules among these warnings and cautions are defined to present the most important message first (see also [Traverse, 1994]).

12.5 A340 Particularities

The general design objective relative to the A340 fly-by-wire system was to reproduce the architecture and principles chosen for the A320 as much as possible for the sake of commonality and efficiency, taking account of the A340 particularities (long-range four-engine aircraft).

12.5.1 System

As is now common for each new program, the computer functional density was increased between the A320 and A330/A340 programs: The number of computers was reduced to perform more functions and control an increased number of control surfaces (Figure 12.3).

12.5.2 Control Laws

The general concept of the A320 flight control laws was maintained, adapted to the aircraft characteristics, and used to optimize the aircraft performance, as follows:

- The angle of attack protection was reinforced to better cope with the aerodynamic characteristics of the aircraft.
- The dutch roll damping system was designed to survive against rudder command blocking, thanks to an additional damping term through the ailerons, and to survive against an extremely improbable complete electrical failure thanks to an additional autonomous damper. The outcome of this was that the existing A300 fin could be used on the A330 and A340 aircraft with the associated industrial benefits.
- The take-off performance could be optimized by designing a specific law that controls the aircraft pitch attitude during the rotation.
- The flexibility of fly-by-wire was used to optimize the minimum control speed on the ground (VMCG). In fact, the rudder efficiency was increased on the ground by fully and asymmetrically deploying the inner and outer ailerons on the side of the pedal action as a function of the rudder travel: the inner aileron is commanded downwards, and the outer aileron (complemented by one spoiler) is commanded upwards.
- A first step in the direction of structural mode control through fly-by-wire was made on the A340 program through the so-called "turbulence damping function" destined to improve passenger comfort by damping the structural modes excited by turbulence.

12.6 Design, Development, and Validation Procedures

12.6.1 Fly-by-Wire System Certification Background

An airline can fly an airplane only if this airplane has a type certificate issued by the aviation authorities of the airline country. For a given country, this type certificate is granted when the demonstration has been made and accepted by the appropriate organization (Federal Aviation Administration in the U.S, Joint Aviation Authorities in several European countries, etc.) that the airplane meets the country's aviation rules and consequently a high level of safety. Each country has its own set of regulatory materials although the common core is very large. They are basically composed of two parts: the requirements on one part, and a set of interpretations and acceptable means of compliance in a second part. An example of requirement is "The aeroplane systems must be designed so that the occurrence of any failure condition which would prevent the continued safe flight and landing of the aeroplane is extremely improbable" (in Federal and Joint Aviation Requirements 25.1309, [FAR/JAR 25]). An associated part of the regulation (Advisary Circular from FAA, Advisory Material — Joint from JAA 25.1309) gives the meaning and discuss such terms as "failure condition," and "extremely improbable." In addition, guidance is given on how to demonstrate compliance.

The aviation regulatory materials are evolving to be able to cover new technologies (such as the use of fly-by-wire systems). This is done through special conditions targeting specific issue of a given airplane, and later on by modifying the general regulatory materials. With respect to A320/A330/A340 fly-by-wire airplane, the following innovative topics were addressed for certification (note: some of these topics were also addressing other airplane systems):

- Flight envelope protections
- Side-stick controller
- Static stability
- Interaction of systems and structure
- System safety assessment

- Lightning indirect effect and electromagnetic interference
- Integrity of control signal transmission
- Electrical power
- Software verification and documentation, automatic code generation
- System validation
- Application-specific integrated circuit

It is noteworthy that an integration of regulatory materials is underway which is resulting in a set of four documents:

- A document on system design, verification and validation, configuration management, quality assurance [ARP 4754, 1994]
- A document on software design, verification, configuration management, quality assurance [DO178B, 1992]
- A document on hardware design, verification, configuration management, quality assurance [DO254, 2000]
- A document on the system safety assessment process [ARP 4761, 1994]

12.6.2 The A320 Experience

12.6.2.1 Design

The basic element developed on the occasion of the A320 program is the so-called SAO specification (Spécification Assistée par Ordinateur), the Aerospatiale graphic language defined to clearly specify control laws and system logics. One of the benefits of this method is that each symbol used has a formal definition with strict rules governing its interconnections. The specification is under the control of a configuration management tool and its syntax is partially checked automatically.

12.6.2.2 Software

The software is produced with the essential constraint that it must be verified and validated. Also, it must meet the world's most severe civil aviation standards (level 1 software to [D0178A, 1985]–see also [Barbaste, 1988]). The functional specification acts as the interface between the aircraft manufacturer's world and the software designer's world. The major part of the A320 flight control software specification is a copy of the functional specification. This avoids creating errors when translating the functional specification into the software specification. For this "functional" part of the software, validation is not required as it is covered by the work carried out on the functional specification. The only part of the software specification to be validated concerns the interface between the hardware and the software (task sequencer, management of self-test software inputs/outputs). This part is only slightly modified during aircraft development.

To make software validation easier, the various tasks are sequenced in a predetermined order with periodic scanning of the inputs. Only the clock can generate interrupts used to control task sequencing. This sequencing is deterministic. A part of the task sequencer validation consists in methodically evaluating the margin between the maximum execution time for each task (worst case) and the time allocated to this task. An important task is to check the conformity of the software with its specification. This is performed by means of tests and inspections. The result of each step in the development process is checked against its specification. For example, a code module is tested according to its specification. This test is, first of all, functional (black box), then structural (white box).

Adequate coverage must be obtained for the internal structure and input range. The term "adequate" does not mean that the tests are assumed as being exhaustive. For example, for the structural test of a module, the equivalence classes are defined for each input. The tests must cover the module input range taking these equivalence classes and all module branches (among other things) as a basis. These equivalence classes and a possible additional test effort have the approval of the various parties involved (aircraft manufacturer, equipment manufacturer, airworthiness authorities, designer, and quality control).

The software of the control channel is different from that of the monitoring channel. Likewise, the software of the ELAC computer is different from that of the SEC computer (the same applies to the FCPC and FCSC on the A340). The aim of this is to minimize the risk of a common error which could cause control surface runaway (control/monitoring dissimilarity) or complete shutdown of all computers (ELAC/SEC dissimilarity).

The basic rule to be retained is that the software is made in the best possible way. This has been recognized by several experts in the software field both from industry and from the airworthiness authorities. Dissimilarity is an additional precaution which is not used to reduce the required software quality effort.

12.6.2.3 System Validation

Simulation codes, full-scale simulators and flight tests were extensively used in a complementary way to design, develop, and validate the A320 flight control system (see also [Chatrenet, 1989]), in addition to analysis and peer review.

A "batch" type simulation code called OSMA (Outil de Simulation des Mouvements Avion) was used to initially design the flight control laws and protections, including the nonlinear domains and for general handling quality studies.

A development simulator was then used to test the control laws with a pilot in the loop as soon as possible in the development process. This simulator is fitted with a fixed-base faithful replica of the A320 cockpit and controls and a visual system; it was in service in 1984, as soon as a set of provisional A320 aero data, based on wind tunnel tests, was made available. The development simulator was used to develop and initially tune all flight control laws in a closed-loop cooperation process with flight test pilots.

Three "integration" simulators were put into service in 1986. They include the fixed replica of the A320 cockpit, a visual system for two of them, and actual aircraft equipment including computers, displays, control panels, and warning and maintenance equipment. One simulator can be coupled to the "iron bird" which is a full-scale replica of the hydraulic and electrical supplies and generation, and is fitted with all the actual flight control system components including servojacks. The main purpose of these simulators is to test the operation, integration, and compatibility of all the elements of the system in an environment closely akin to that of an actual aircraft.

Finally, flight testing remains the ultimate and indispensable way of validating a flight control system. Even with the current state of the art in simulation, simulators cannot yet fully take the place of flight testing for handling quality assessment. On this occasion a specific system called SPATIALL (Système Pour Acquisition et Traitement d'Informations Analogiques ARINC et Logiques) was developed to facilitate the flight test. This system allows the flight engineer to:

- Record any computer internal parameter
- Select several preprogrammed configurations to be tested (gains, limits, thresholds, etc.)
- Inject calibrated solicitations to the controls, control surfaces, or any intermediate point.

The integration phase complemented by flight testing can be considered as the final step of the validation side of the now-classical V-shaped development/validation process of the system.

12.6.3 The A340 Experience

12.6.3.1 Design

The definition of the system requires that a certain number of actuators be allocated to each control surface and a power source and computers assigned to each actuator. Such an arrangement implies checking that the system safety objectives are met. A high number of failure combinations must therefore be envisaged. A study has been conducted with the aim of automating this process.

It was seen that a tool which could evaluate a high number of failure cases, allowing the use of capacity functions, would be useful and that the possibility of modeling the static dependencies was not absolutely necessary even though this may sometimes lead to a pessimistic result. This study gave rise to a data processing tool which accepts as input an arrangement of computers, actuators, hydraulic and electrical power sources, and also specific events such as simultaneous shutdown of all engines and, therefore, a high number of power sources. The availability of a control surface depends on the availability of a certain number of these resources. This description was made using a fault tree-type support as input to the tool.

The capacity function used allows the aircraft roll controllability to be defined with regard to the degraded state of the flight control system. This controllability can be approached by a function which measures the roll rate available by a linear function of the roll rate of the available control surfaces. It is then possible to divide the degraded states of the system into success or failure states and thus calculate the probability of failure of the system with regards to the target roll controllability.

The tool automatically creates failure combinations and evaluates the availability of the control surfaces and, therefore, a roll controllability function. It compares the results to the targets. These targets are, on the one hand, the controllability (availability of the pitch control surfaces, available roll rate, etc.) and, on the other hand, the reliability (a controllability target must be met for all failure combinations where probability is greater than a given reliability target). The tool gives the list of failure combinations which do not meet the targets (if any) and gives, for each target controllability, the probability of nonsatisfaction. The tool also takes into account a dispatch with one computer failed.

12.6.3.2 Automatic programming

The use of automatic programming tools is becoming widespread. This tendency appeared on the A320 and is being confirmed on the A340 (in particular, the FCPC is, in part, programmed automatically). Such a tool has SAO sheets as inputs, and uses a library of software packages, one package being allocated to each symbol. The automatic programming tool links together the symbol's packages.

The use of such tools has a positive impact on safety. An automatic tool ensures that a modification to the specification will be coded without stress even if this modification is to be embodied rapidly (situation encountered during the flight test phase for example). Also, automatic programming, through the use of a formal specification language, allows onboard code from one aircraft program to be used on another. Note that the functional specification validation tools (simulators) use an automatic programming tool. This tool has parts in common with the automatic programming tool used to generate codes for the flight control computers. This increases the validation power of the simulations. For dissimilarity reasons, only the FCPC computer is coded automatically (the FCSC being coded manually). The FCPC automatic coding tool has two different code translators, one for the control channel and one for the monitoring channel.

12.6.3.3 System validation

The A320 experience showed the necessity of being capable of detecting errors as early as possible in the design process, to minimize the debugging effort along the development phase. Consequently, it was decided to develop tools that would enable the engineers to actually fly the aircraft in its environment to check that the specification fulfils the performance and safety objectives before the computer code exists.

The basic element of this project is the so-called SAO specification, the Aerospatiale graphic language defined to clearly specify control laws and system logics and developed for A320 program needs. The specification is then automatically coded for engineering simulation purposes in both control law and system areas.

In the control law area, OCAS (Outil de Conception Assistée par Simulation) is a real-time simulation tool that links the SAO definition of the control laws to the already-mentioned aircraft movement simulation (OSMA). Pilot orders are entered through simplified controls including side-stick and engine thrust levels. A simplified PFD (primary flight display) visualizes the outputs of the control law. The

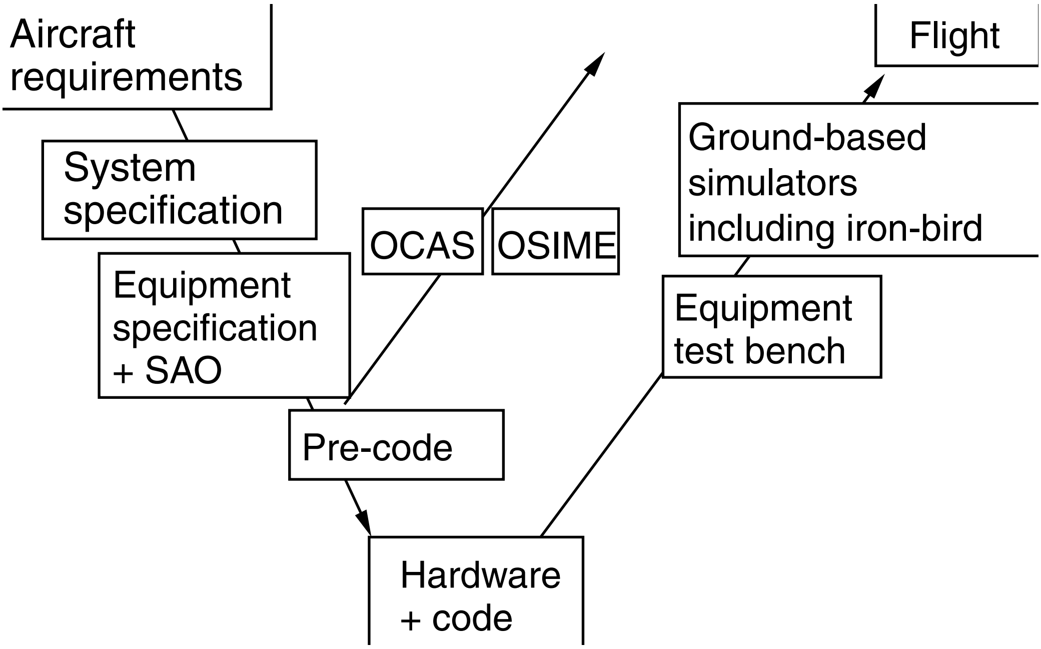

FIGURE 12.7 Validation methodology.

engineer is then in a position to physically judge by himself the quality of the control law that he has just produced, in particular with respect to law transition and nonlinear effects. In the early development phase, this very same simulation was used in the full-scale A340 development simulator with a pilot in the loop.

In the system area, OSIME (Outil de SImulation Multi Equipement) is an expanded time simulation that links the SAO definition of the whole system (control law and system logic) to the complete servo-control modes and to the simulation of aircraft movement (OSMA). The objective was to simulate the whole fly-by-wire system including the three primary computers (FCPC), the two secondary computers (FCSC), and the servo-controls in an aircraft environment.

This tool contributed to the functional definition of the fly-by-wire system, to the system validation, and to the failure analysis. In addition, the behavior of the system at the limit of validity of each parameter, including time delays, could be checked to define robust monitoring algorithms. Non-regression tests have been integrated very early into the design process to check the validity of each new specification standard.

Once validated, both in the control law and system areas using the OCAS and OSIME tools, a new specification standard is considered to be ready to be implemented in the real computers (automatic coding) to be further validated on a test bench, simulator, and on the aircraft (Figure 12.7).

12.7 Future Trends

The fly-by-wire systems developed on the occasion of the A320, A321, A340, and A330 programs now constitute an industrial standard for commercial applications and are well adapted to future military transport aircraft, thanks to the robustness of the system and its reconfiguration capabilities. What are the possible system evolutions? Among others, are the following:

1. New actuator concepts are arising. In particular, systems using both electrical and hydraulic energy within a single actuator were developed and successfully tested on A320 aircraft. This is the so-called electrical back-up hydraulic actuator or EBHA. This actuator can be used to design flight

control systems that survive the total loss of hydraulic power, which is a significant advantage for a military transport aircraft particularly in the case of battle damage.

2. The hardware dissimilarity of the fly-by-wire computer system and the experience with A320 and A340 airline operation will probably ease the suppression of the rudder and trimmable horizontal stabilizer mechanical controls of future aircraft.
3. The integration of new functions, such as structural mode control, may lead to increased dependability requirements, in particular if the loss of these functions is not allowed.
4. Finally, future flight control systems will be influenced by the standardization effort made through the IMA concept (integrated modular avionics) and by the "smart" concept where the electronics destined to control and monitor each actuator are located close to the actuator.

References

ARP 4754, 1994. *System Integration Requirements*. Society of Automotive Engineers (SAE) and European Organization for Civil Aviation electronics (EUROCAE).

ARP 4761, 1994. *Guidelines and tools for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*. Society of Automotive Engineers (SAE) and European Organization for Civil Aviation Electronics (EUROCAE).

Barbaste, L. and Desmons, J. P., 1988. Assurance qualité du logiciel et la certification des aéronefs/ Expérience A320. ler séminaire EOQC sur la qualité des logiciels, April 1988, Brussels, pp. 135–146.

Chatrenet, D., 1989. Simulateurs A320 d'Aérospatiale: leur contribution à la conception, au développement et à la certification. *INFAUTOM 89*, Toulouse.

DO178A. 1985. *Software Considerations in Airborne Systems and Equipment Certification.* Issue A. RTCA and European Organization for Civil Aviation Electronics (EUROCAE).

DO178B, 1992. *Software Considerations in Airborne Systems and Equipment Certification.* Issue B. RTCA and European Organization for Civil Aviation Electronics (EUROCAE).

DOXXX, 1995. *Design Assurance Guidance for Complex Electronic Hardware Used in Airborne Systems.* RTCA and by European Organization for Civil Aviation Electronics (EUROCAE).

FAR/JAR 25. *Airworthiness Standards: Transport Category Airplanes.* Part 25 of "Code of Federal Regulations, Title 14, Aeronautics and Space," for the Federal Aviation Administration, and "Airworthiness Joint Aviation Requirements — large aeroplane" for the Joint Aviation Authorities.

Favre, C., 1993. Fly-by-wire for commercial aircraft — the Airbus experience. *Int. J. Control,* special issue on "Aircraft Flight Control".

Traverse, P., Brière, D., and Frayssignes, J. J., 1994. Architecture des commande de vol électriques Airbus, reconfiguration automatique et information équipage. *INFAUTOM 94*, Toulouse.