6th INTERNATIONAL MULTIDISCIPLINARY CONFERENCE

AIRCREAFT CONTROL LAWS MODIFICATION AS A CONSEQUENCE OF FAILURES APPEARANCE

Boguslaw Dolega, Rzeszow University of Technology, ul.W.Pola 2, 35-959 Rzeszow, Poland

Abstract: *Failures of aircraft control and navigation systems are critical, because their presence can dramatically decrease flight safety. To make the flight safe, the failures, which can occur in its subsystems, must be considered during designing process. This paper presents the architecture of control system which makes possible to achieve its highest safety. Changing the way of using their subsystems, redesigning its own structure and updating its parameters to adapt to the new situation can be named as reconfiguration. The necessary information for reconfiguration process is generated by the fault detection and isolation systems. Good cooperation of these systems makes aircraft control and navigation systems fault-tolerant. These problems which respect the conference motto: "**Unity in diversity**" will also be presented.*
Key words*: Fault Tolerant Control, Reconfiguration, Fly-By-Wire Control System Architecture*

1. INTRODUCTION

The aircraft control process is usually taken by the pilot or automat. The main goal of this process is generating some inputs which drive the aircraft from one state to another (required) in some finite time. This process is based on the knowledge of aircraft behaviours. During the flight mode of the pilot, control and navigation system and aircraft cooperate using different interconnections and can be interpreted as a system. The behaviours of the system can be changed when some faults appear because the faults are identified as an unpermitted deviation of characteristic property of the system from the acceptable behaviour. Because losing of aircraft controllability can be the cause of the accidents and other danger, this situation is especially considered by the designers of control systems. They take fault prevention by passive or active ways. The passive ways are realized by using the special parts, with higher reliability. Unfortunately this way cannot preclude all failures (e.g. some of these are caused by pilot's behaviour). For last decades the designers haven't forgotten about the passive way of taking fault prevention, but they have also started using the active way [4, 5]. In this way the deviation from faultless state should be detected and evoke counteracting fault appearance. These counteracting are mainly connected with control actions (taken by autopilot or pilot). In this paper we present the basic assumptions taken during designing the

Fly-By-Wire control system for a small aircraft. In Control and Avionics Department of Rzeszow University of Technology such control system has been made and tested and results of this research will be also presented.

2. THE BASIC ASSUMPTIONS

The diagnostic analysis and conclusions about the cause of an observed behaviour are of the type [7]: "The system is working normally" or "The system operates with a certain fault". To deduce (from observed variables of the process), if any component is faulty we must be able to take decision if extracted behaviour is normal or non-normal. We need the model of normal behaviour and non-normal behaviour of the system. The process of behaviour extraction (as extraction of the symptoms) can be taken with the usage of different methods because we observe different elements of the system [3]. For us the most important are methods based on control quality index. The control quality can be identified with verification of realization of the flight goal. If the flight goals are realized the actual faults are not catastrophic. The most of the control quality indexes are based on information about some controller output signals and some state variables. This information cannot be distorted but it is not always possible. In such cases the role of a fault detector can take the other element of our system, especially the pilot.

If we assume set of possible faults we are able to make analysis which provides the designer with necessary information to start the synthesis of fault tolerant system. We know that the redundancy is necessary to achieve fault tolerance. Redundancy can be achieved by various means. The straightforward way is multiplication of airborne equipment, but it can also be accomplished by the usage of different components which have identical functions. Hardware multiplication can complicate the system and make it more expensive. In our architecture the possibility of triplet hardware redundancy will be allowed.

When the fault has been identified, different corrective actions can be taken in order to attain a normal functioning mode. This action relies on structural or parametric changes and will be called a reconfiguration. In the classic approach the reconfiguration ought to restore the system to a normal functioning mode after fault detection and localization the components affected by faults. It would seem that if the reconfiguration perfectly compensates for the effects of the fault, then the presence of the fault might be hidden from the pilot. Therefore a lot of approaches are based on automated solutions of reconfiguration. In this case, the pilot has been reintroduced into the reconfiguration process. The reconfiguration caused by fault appearing which is a fully automated process is not prepared to new diagnostic situations. Such situations are not taken into consideration during synthesis process. It could generate dangerous situations and they can become the reason of decrease safety. Sometimes some human factors as: human memory limitations [2], mental workload and trust [6], have to be taken into account of reconfiguration to succeed. Of course, making the reconfiguration based only on operator's activity is not a good solution. Humans have troubles in managing a number of alternatives and also human errors can occur in reasoning process [8]. Because both, human and machine have their own restrictions, the diagnostic and reconfiguration problem can be only partially resolved. Therefore cooperation between them is the best alternative. We must build the system with a structure and functions based on human-centered automation concepts that should aim to reduce human errors in providing a cooperative work organization [9]. The consequence of this approach are Billings [1] principles of human-centred automation in aircraft pilotage:

1. the pilot bears the responsibility for safety of flight,
2. pilots must remain in command of their flights.

The first principle is main for the structure and behaviour of our fly-by-wire control system. The pilot always can change modes of aircraft control – from full automatic to direct control surfaces steering modes. The pilot meets the troubles from control system if he wants to change the mode to dangerous mode. For example if one of automatic control modes is impossible to be realized by the control system for the reason of absence or failures in required subsystems. Each of actually realized modes is presented on a special cockpit.

3. THE ARCHITECTURE OF CONTROL SYSTEM

The controlling of the aircraft would be realized with the usage of three levels:

- Level I – normal control, all properties of indirect flight control system are employed,
- Level II – simplified control, only the simple CAS (Control Augmentation System) or forming filters are used,
- Level III – emergency control, displacement of aerodynamic control surfaces depends directly on side-stick displacement.

The change of the method is accomplished automatically by a supervisory subsystem. We also consider a manual switching to Level II in the case of pilot wishes. Level III should be used only in emergency.

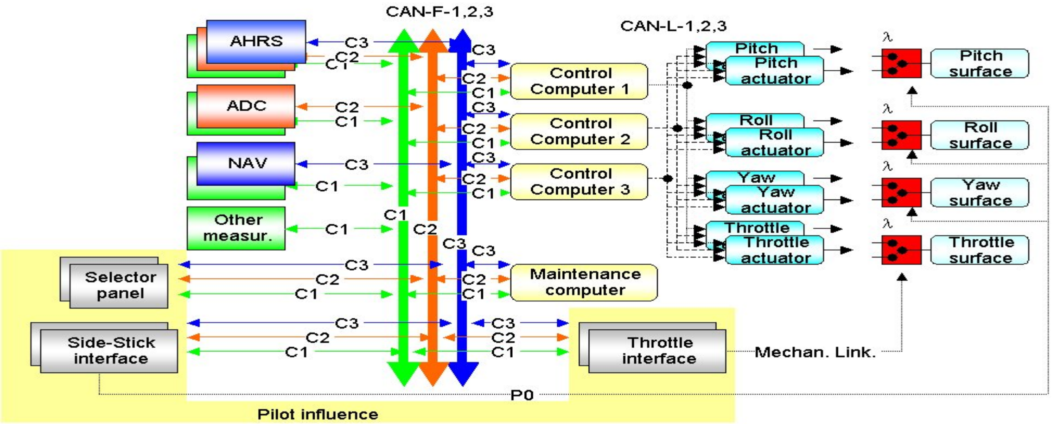

Fig 1. General structure of the fly-by-wire flight control system for PZL-104

Our researches provide us to decentralize the architecture of the system. But it is operating based on hierarchical way of taking conclusions. The general structure of this system is presented in Fig 1. Redundancy as a way of increasing reliability is applied to three independent flight control computers that control double actuators (pitch, roll yaw, and throttle). The pilot selects a control mode using the double control mode selector panels. The throttle level is chosen by the double throttle level interface. The pilot also controls the aircraft by the double Side-Stick interface. Information about movement of the aircraft is provided by:

- three Attitude and Heading Reference Systems (AHRS) – angular orientation,
- two Air Data Computers (ADC) – aircraft movement in relation to air,
- NAV - GNS-530 (GPS, VOR, ILS, comm) and GPS-35 – navigation information,

Triple digital, high speed, bi-directional databus network CAN-2 (CAN-F-1, 2, 3) integrate the Control Computers with pilot interfaces and measurement systems. Those systems are connected to the one databus (C1 or C2 or C3) because that solution is cheaper than others. The actuators are connected to Control Computers through the slow speed version of CAN-2 (CAN-S-1, 2, 3). A lot of databuses and devices connected through these buses led to the adaptation of “CANaerospace” software as the standard of protocol transmission. This provides more fault tolerant transmission. Each message must contain a status bit field to allow continuous integrity monitoring and minimize failure detection time. Each device connected to the network must inform others about detected failures within itself via a dedicated emergency identifier to support system degradation and maintenance actions. Because the message must contain information about the transmitting station and the type of data associated with the particular message, the network becomes opened. At any time we can connect additional devices (e.g. additional sensors or other measurement systems). Creating a system that is open (open architecture) requires applying software procedures that can identify devices and their signals. The information is necessary to generate vector of efficiency. Control computers generate output signals using that vector (for choice of possible and optimum mode, measure signal etc.). As you see, it is a dynamic process. When a subsystem detects fault in another subsystem, it generates signal that includes that information. It is used by the faulty subsystem for self-reconfiguration and by the others subsystems that cooperate with suspected subsystem.

A PWM (Pulse Duration Modulation) signal standard has been used to directly control the actuators (line P0 – Fig 1.). This action will be taken if two of the three Control Computers malfunction or if the CAN networks are necessary for proper transmission failed. This level of control will also take place when the absence of the measurement system is necessary for the mode of flight occurs. The pilot can also switch this level of control as well.

When we talk about the reliability during the flight mod, we ought to note that the aircraft is controlled by four single surfaces. They are not redundant parts. It is easy to prove that the switches (λ - Fig 1) which are responsible for the change of the surface control signals must be the most reliable parts. The switch fulfils arbitration among output signals from control computers. The PWM signal (line P0 – Fig 1) has the highest priority.

As it was shown, the active methods of increasing reliability are based on information generated by the different subsystems. We can make the question – what is the principle of integration of these subsystems. What kind of unity can we find there?

4. UNITY IN DIVERSITY AS CONCLUSION

If we understand "unity in diversity" as aspiration for co-operation, then our control system is an ideal example of this idea. Our system consists of different kinds of redundant relations.

The first type of relations are horizontal relations. We can find them in multiplied parts by hardware or analytical redundancy. When the temporary faults or incorrect action appear the redundant parts which can make the similar function are obligate to be helpful if necessary. This action is possible because individual control elements are connected through CAN buses. The part which is suspected of damage (e.g. control computer by arbiter system) is informed about it and can take special working. It can verify itself if its initial conditions are similar to conditions in parts functioning well. Through exchange of the information, parts suspected of wrong functioning can rebuild themselves to perfect functioning. On the basis of mutual disinterested help, unity relations between equal elements can be built.

The second type of relations are vertical relations. These relations are like teacher-student. In our system we can find them e.g. in the pilot to the control system relations. The pilot is responsible for flight safety and he has casting vote in contentious issues. The control system must be susceptible to pilot orders. Of course, if the pilot’s order is different then a typical one (stored in computer memory and classified as normal for actual state conditions), the control system informs the pilot about this situation. Also we must remember that in the most dangerous situations the pilot reasoning depends on information generating by the control system. Only the control system can take the decision based on a lot of independent information sources in a very short time period. These vertical relations are also the co-operation relations and show as goal unity can be achieved in hierarchical diversity.

5. REFERENCES

1. Billings C.: Aviation automation: the search for a human-centered approach. Erlbaum, Mahwah, NJ, 1997
2. Card S., Moran T., Newell A.: The psychology of human–computer interaction. Erlbaum, Hillsdale, NJ, 1983
3. Dolega B.: Metodyka wykrywania uszkodzen ukladow mechanicznych samolotow w trakcie eksploatacji. *Rozprawa doktorska.* Rzeszow 1994
4. Dołęga B.: Wykrywanie uszkodzen zwielokrotnionych mechanizmow wykonawczych podczas ich dzialania, The 4-th International conference MECHANICS 2004, Scientific Biulletins of Rzeszow University of Technoloogy No 209, Rzeszow 2004
5. Mehra R.K. and Peschon J.: An innovations approach to fault detection and diagnosis in dynamic systems. *Automatica*, Vol.7, 1971, pp.637-640
6. Millot P.: Concepts and limits for human–machine cooperation. IEEE-SMC, CESA’98, Tunisia, 1–4 April 1998
7. Patton R.J., Frank P.M., and Clark R.N.: Issues of Fault Diagnosis for Dynamic Systems. Springer, 2000.
8. Rasmussen J.: Information processing and human–machine interaction. North-Holland, Amsterdam 1986
9. Vanderhaegen F.: Cooperative system organisation and task allocation: illustration of task allocation in air traffic control. Travail Humain 62(3), 1999 pp.192–222

Acknowledgements

This paper was prepared within the framework of the project “Fly-by-wire control system for general aviation aircraft” financed by The Polish State Committee for Scientific Research in the years 2003–2005.