Reliability Analysis of a Single-Engine Aircraft FADEC

Inlämningsuppgift

SUMMARY

The task is to analyse two options to a fault-tolerant Full Authority Digital Electronic Control system (FADEC) intended for control of an aircraft gas turbine engine. The study concentrates on an application for an aircraft equipped with a single engine, such as the JAS 39 Gripen.

1. INTRODUCTION

The evolution of aircraft gas turbine engines has led to ever increasing demands on engine control systems to increase thrust and improve fuel consumption. These demands have resulted in a widespread use of electronic control systems. The earlier generations of such systems, which used the supervisory concept, were introduced in the 1970s and can be found in a number of aircraft in operation today. It is used in the version of JAS that is in operation today. The supervisory concept does not fully meet the requirements of the most modern engines, however, and this led in the 1980s to the Full Authority Digital Electronic Control (FADEC) concept. A FADEC system controls all the functions required of the engine and introduces a number of improvements, such as: (i) the possibility of implementing sophisticated techniques from modern control theory, techniques that can both increase the performance and the reliability, (ii) a reduction in weight owing to the limited use of hydro mechanics, and (iii) the possibility of implementing built-in support for maintenance, which lowers the cost of maintenance and improves the reliability of the system. As these examples indicate, FADEC supports endeavours toward increasing performance and reliability and reductions in overall cost. FADEC systems are currently in operation in a number of aircraft, of which examples are: the new military aircraft F-18E/F and Eurofighter and the civil aircraft Airbus 320, 321 and Boeing 777.

In aircraft equipped with more than one engine, a single failure in one of the engines does not alone lead to a catastrophic situation. The aircraft can still operate with one engine only, although with degraded performance. However, in a single-engine aircraft, the consequence of such a failure is indeed catastrophic. Thus, to introduce FADEC in a single-engine aircraft puts very hard constraints on the reliability of the FADEC. The reliability of the single components are of the order 10^{-3} h^{-1}. This figure is not good enough for the aircraft and implies that the system must be made **fault tolerant**. Each and every component failure can not be allowed to cause a system failure.

The analysis is restricted to faults in electronic parts, i.e. sensors, computation units and the electronic part of actuator servo valves. Hence, the unavoidable hydro mechanical parts of a FADEC system are not considered. Furthermore, only the components that are safety-critical are taken into account in the analysis. Faults occurring in these components are assumed to be permanent and independent.

ACRONYMS AND EXPLANATIONS

FADEC	-	Full Authority Digital Electronic Control
CU	-	Computation Unit
IU	-	Input Unit
OU	-	Output Unit
CM	-	Control Module (consists of CU, IU and OU)
FVG	-	Fan Variable Geometry
CVG	-	Compressor Variable Geometry
PS3	-	Pressure measurement
WFM	-	Fuel measurement (and control)
A8	-	Exhaust nozzle, variable geometry
H/M	-	Hydromechanical control unit

2. DESCRIPTION OF THE FADEC PROTOTYPES

The two fault-tolerant designs that you are supposed to model are presented in Figure 1 and Figure 2. The basic hardware of a single channel, in the following also called a Control Module (CM), does not differ between the two systems modeled. It consists of an Input Unit (IU), a Computation Unit (CU), and an Output Unit (OU). Input to the CMs is produced by redundant sensors measuring the parameters needed for control. The control laws are calculated in the CUs, and the results are converted, amplified and given as output to the actuator servo valves. To achieve a high level of fault tolerance, the systems are designed to enable each of the CMs to access each of the redundant sensors, as well as to access each actuator servo valve. The control parameters that are measured and controlled and that are safety-critical for the engine (JAS-Gripen RM12) are shown in Table 1. The difference between the systems is that in the one-channel system (also called the mixed system) one electronic channel is replaced by a hydromechanical backup.

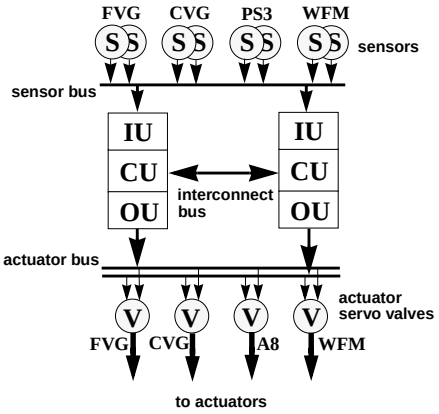

FIGURE 1. Two-channel FADEC

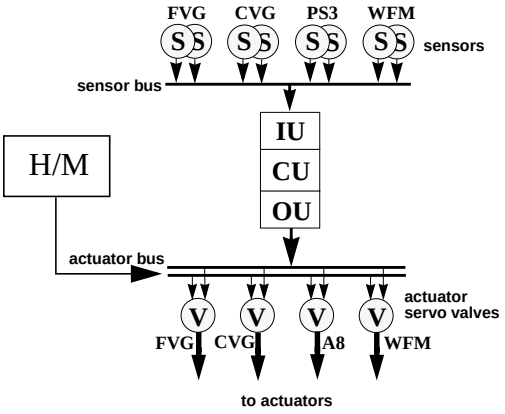

FIGURE 2. FADEC with H/M backup

TABLE 1. Safety critical parameters for the RM12 gas turbine engine

Parameters measured by sensors	Parameters controlled by actuators
Variable geometry of fan - FVG	Variable geometry of fan - FVG
Variable geometry of compressor - CVG	Variable geometry of compressor - CVG
Compressor discharge static pressure - PS3	Variable exhaust nozzle - A8
Main fuel - WFM	Main fuel - WFM

The necessary fault tolerance is achieved by (i) the addition of extra hardware and (ii) the implementation of concurrent error detection mechanisms (CEDM) and self-tests. Both the two-channel and the one-channel approach rely on CEDMs and self-tests that are implemented in software and run in the CUs of each CM.

2.1 Functional Description of the Two-Channel Hot Standby Configuration

In the two-channel concept, one of the CMs (the master) is in charge, i.e. it controls the actuators. In case of an error in the master module, the control is passed to the other CM, and the erroneous module disconnects. An error in the standby module results only in a disconnection. There is of course a small probability that the module does not detect an error in itself even though there is one. Here, we will assume that the coverage probability for the master channel is 0.99. The coverage probability is the probability to detect, locate and properly handle a component failure. (To handle a component failure properly means to switch in a standby component)

Here are the main reasons for a critical system failure in the two-channel case. The intensities are given in the end.

- Two sensors or actuators of the same kind fail during the same mission
- The two electronic channels fail during the same mission
- The master channel fails and the backup channel is not switched in.

- Engine extinction.
  If the exciter fails and after that there is an engine flame-out.

2.2 Functional Description of the Mixed-Channel system

The fault tolerance of this system is based on the single module's ability to detect an error in itself and to disconnect in a controlled fashion. In case of an error in the electronic channel, the control is passed to the hydromechanical unit, and the erroneous module disconnects. The coverage probability for the electronic channel is also assumed to be 0.99.

The hydromechanical backup (H/M) is a hot standby. It is inspected every tenth mission. This means that if the unit breaks down in the first mission after an inspection, the pilot will, unknowingly, fly the next nine mission without a backup.

The main reasons for the one-channel system to fail are:

- Engine extinction
  If the exciter fails and after that there is an engine flame-out.

- Two sensors of the same kind fail during the same mission
- The electronic channel fail and the H/M backup is broken - or breaks down during the same mission
- The master channel fails and the H/M backup channel is not switched in

3. GENERAL ASSUMPTIONS AND FAILURE INTENSITIES

To be able to model the system and obtain results from these models, some assumptions are necessary

- Every component is assumed to fail independently of every other component. Thus, the various subsystems - control modules (including the electronic parts of the servo valves) and sensors (CVGs, FVGs, PS3s and WFMs) - fail independently of one another.
- Each flight mission is supposed to be two hours.
- Constant failure rates. The assumption of constant failure rates means that we neglect the possibility that the failure probabilities are higher during certain phases of the flight mission. It further means that the distribution for the time to failure of a component is exponential and that any type of wear out problem is neglected.
- Perfect repair of the electronic parts. This means that the system is as good as new after every flight mission, that is we assume that at the inspection after every mission all faults are successfully repaired. Note that this is not the case for the H/M backup.
- The hydromechanical backup (H/M) is a hot standby. It is inspected every tenth mission, and is then repaired if necessary.

- Permanent hardware faults. All faults are assumed to be permanent without possibility of repair until after the mission, when all faults are repaired.
- The coverage factor are assumed to be 0.99 for the master channel of the two-channel system. The coverage probability for the electronic channel of the mixed system is also assumed to be 0.99.
- Sensor coverage. If one sensor fails the control module might receive the wrong signal. However, there are detection mechanisms and with a very high probability (0.999) we assume that it is possible to cover a sensor failure, i.e. to choose the correct value. This high probability is also explained by the fact that it is often only critical if there is a large deviation from the correct value.
- The secondary sensors and actuactors may be assumed to be on hot standby, but these are checked before every mission.
- The actuator coverage probability is assumed to be 1.00. This implies that both actuators of one type have to fail to cause a system failure.
- Engine flame-out. The engine is assumed to become extinct (flame-out) once in a hundred missions and these instances are assumed to appear independent of each other and with constant intensity.
- The following failure rates shall be used in the modelling:

TABLE 2. Intensities

Component	Rate[a] given /hour
CVG and FVG sensors	0.002
PS3 and WFM sensors	0.005
all actuators have the same rate	0.0005
Input unit	0.002
Computation unit	0.002
Output unit	0.001
Hydromechanical backup	0.0001
Engine Exciter	0.002

a. Rates are only of the right magnitude

EXERCISES

Please give all answers with three significant digits. Use λ_i for intensities.

1. What is the probability of having a critical system failure during a mission, due to loss of the value from the CVG sensors? Loss of the value means that either both CVG sensors are broken or that we use the value from the erroneous one.

Assume that all other components have failure rates zero. This means that we can neglect the probability that the mission ends in advance due to some other failure.

2. What is the probability of having a critical system failure during a mission, due to loss of the value from any of the sensors?

In the following exercises assume that sensors and actuators never fail.

3. Model the two different systems using only Markov Chain Modelling.

To solve the following exercises, you may use either set up a system of differential equations based on the models and solve them, or you may simulate the models with a computer program.

4. What is the probability of failure during ten missions of the two-channel system?

5. What is the probability of failure during ten missions of the one-channel system? You may assume that the 10 missions start with a newly inspected H/M unit.

6. Compare the reliability of the two systems. How would you improve the system?