Reliability Engineering and System Safety 94 (2009) 456–462

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Operational reliability assessment of an aircraft environmental control system

K. Jenab *, K. Rashidi

Department of Mechanical and Industrial Engineering, Ryerson University, Toronto, Ontario, Canada M5B 2K3

ARTICLE INFO

Article history:
Received 29 August 2007
Received in revised form
14 February 2008
Accepted 9 May 2008
Available online 17 May 2008

Keywords:
Hybrid warm–cold standby system
Human errors
Flow-graph
Maintenance optimization

ABSTRACT

The aircraft environmental control system (ECS) is composed of several non-identical and non-dedicated subsystems working as warm–cold standby subsystems. Also, their state transition times are arbitrary distributed. This paper presents a flow-graph-based method to calculate time-to-failure data and failure probability of the ECS. The obtained data from the model may be used for maintenance optimization that employs the failure limit strategy for ECS. The model incorporates detectable failures such as hardware failures, critical human errors, common-cause failures, maintenance categories, and switch activation methods. A numerical example is also presented to demonstrate the application of the model.

1. Introduction

In [1], authors developed probabilistic reliability models taking into account common-cause failure, human errors, and partially energized standby subsystems. In [2], Using Markovian method, author developed formula for the availability of the standby system composed of identical units that are preventively maintained. In [3], authors developed a closed-form equation for a k-out-of-n warm standby system with dormant failure. In [4], authors presented a human errors analysis model with arbitrarily distributed repair times for a system composed of two working units and one standby unit. In [5], using exact distribution of the sum of two independent beta variables, the reliability of the standby system composed of units with beta-distributed lifetime was calculated. In [6], a two-unit standby system was investigated wherein the standby unit is put in cold state for a certain amount of time before it is allowed to become warm. In [7], using Markovian model, authors analyzed a standby system made up of n units in parallel start operating and remaining m units are in standby mode. In [8], considering the constant failure rate, the availability of a standby system with n+1 identical units and one standby unit was studied. In [9], several measures of reliability for a two-unit warm standby system with slow switch considering hardware and human error failures were assessed by Markovian method. In [10], using the regenerative point technique in Markov renewal processes, the reliability measures for a two-unit warm standby system with a slow switch subject to hardware and human error failures were studied. In [11], assuming imperfect repair, an optimal geometric model for a cold standby repairable system with only two identical units was developed. In [12], a system composed of m operating units, w warm standby units and R repairmen was studied. In [13], using reliability techniques, a statistical method was proposed for preventive maintenance of a standby relays in power system. In [14], authors developed imprecise reliability models of a cold standby system because of unavailability of precise probability distribution of the unit times to failure. In [15], considering a minimal repair with negligible repair time, a standby system lifetime was studied. In [16], a warm standby system composed of units with different failure and repair rates was studied. In [17], a cold standby system made up of non-repairable units with Erlang distribution lifetimes was investigated. Table 1 classifies the published literature dealt with standby systems subject to human errors, common cause (CC), and hardware failures (HFs). This classification shows that the published papers overlooked a warm–cold standby system defined as hybrid standby system with arbitrary failure distributions. Therefore, the aim of this study is to investigate such a standby system, and calculate time-to-failure data and the system failure probability by using a flow-graph-based method. The results are required for maintenance optimization employing the failure limit strategy [18].

2. Problem description

One of the major functions of the aircraft environmental control system (ECS) is to maintain the temperature of the cabin at passenger comfort level. This hybrid standby system is made up

* Corresponding author. Tel.: +1 416 979 5000x6424; fax: +1 416 979 5265.
E-mail address: jenab@ryerson.ca (K. Jenab).

0951-8320/$ - see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ress.2008.05.003

Table 1
Classification of published literature on standby systems

Failure distribution	Ref.	Configuration of standby	Model
With human errors			
Exponential	[1]	Cold with common cause failure	Markov
Exponential	[4]	Cold	Markov
Exponential	[7]	Warm	Markov
Exponential	[9]	Warm	Mathematical expansion
Exponential	[10]	Warm	Mathematical expansion
Without human errors			
Exponential	[2]	Cold	Markov/simulation
Exponential	[3]	Warm	Mathematical expansion
Beta	[5]	Cold	Mathematical expansion
Exponential	[6]	Hot/warm/cold	Mathematical expansion
Exponential	[8]	Cold	Markov
Exponential	[11]	Cold	Mathematical expansion
Exponential	[12]	Warm	Mathematical expansion
Exponential	[13]	Cold	Mathematical expansion
Exponential	[14]	Cold	Mathematical expansion
Weibull	[15]	Cold	Simulation
Exponential	[16]	Warm	Markov
Erlang	[17]	Cold	Mathematical expansion

of two dedicated cooling packs, and a non-dedicated RAM air as shown in Fig. 1. The non-dedicated subsystem can be manually activated only in the certain flight altitude by the flight crew. In the normal operation, both cooling packs are automatically operating. In case of one pack failure, the remaining pack will automatically take over the load and an appropriate message will be posted on the crew alert system display (CAS) in the aircraft cockpit.

The system state would be reversible if the cooling pack fails due to overheat. Up to this stage, we have the two-unit warm standby system with automatic switch subject to HFs. In case of both packs failure, crews are instructed to switch manually to RAM air in accordance with the aircraft flight manual. This stage is a cold standby with slow switch subject to hardware and crew error failures. The crew errors may result from poor control panel design, poor work environment, poor task assignment, inadequate training, poorly written flight manual, operating procedures, and deficiency of master minimum equipment list. Therefore, the required maintenance activities performed by the flight crews during the flight (Category I) or by maintenance crews in the bases (Category II) may be associated with human errors.

To calculate time-to-failure data and the failure probability of such a system, we define a warm–cold standby system (hybrid) with related terms and conditions in the remaining part of this section. The warm–cold standby system comprises of several non-identical and non-dedicated subsystems, which are independently functioning; however, they can be manually or automatically activated subject to

(1) manual override option,
(2) subsystem availability if it is non-dedicated, and
(3) meeting certain flight operational requirements such as flight altitude.

The dedicated subsystems work in a warm standby configuration with automatic switch activation. On the other hand, the non-dedicated subsystems work in cold standby configuration with manual activation in accordance with the flight manual. As a maintenance point of view, the subsystems may be repaired during the flight by the flight crews or at the base by the maintenance crews based on maintenance procedures. The maintenance task may be subjected to critical human errors (CHEs) resulting from poor design, poor work environment, poor task assignment, inadequate training, poorly written manuals, operating procedures, and maintenance procedures. Also, there exist CC failures that may be caused by a common design or material deficiency, a common installation error, a common maintenance error, or a common harsh environment. This type of failure leads to total system failure. Third type of failure is HF (i.e., subsystem failure and switch failure) that can be classified to detectable and non-detectable HFs. Occurrence of the detectable failure will be announced by warning, caution, or advisory message to the CAS display in the aircraft cockpit for taking appropriate action in accordance with the flight and maintenance manuals. In fact, the occurrence of the non-detectable failure will remain dormant until next maintenance inspection.

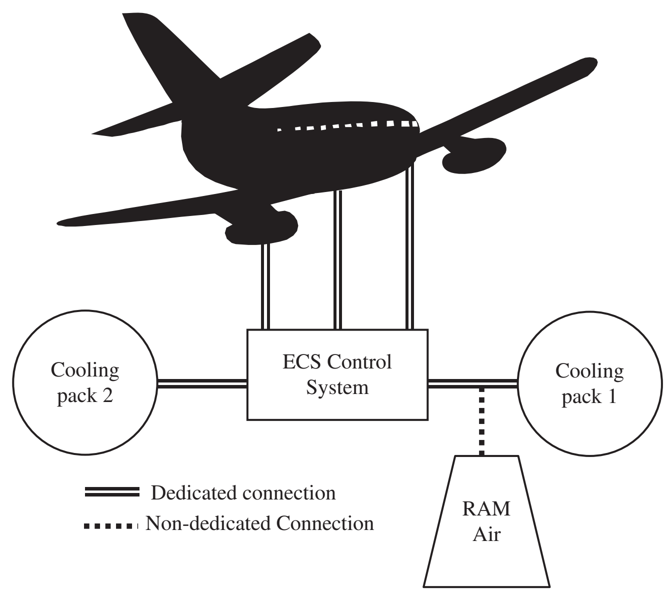

Fig. 1. Environmental control system block diagram.

To develop an analytical model for computing time-to-failure data and failure probability of such a system, the following assumptions are taken into account:

- Dedicated subsystems only serve the warm–cold standby system.