Reliability Engineering and System Safety 140 (2015) 130–141

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

# Pivotal decomposition for reliability analysis of fault tolerant control systems on unmanned aerial vehicles

Bin Hu*, Peter Seiler

*Department of Aerospace Engineering and Mechanics, University of Minnesota, Minneapolis, MN 55455, United States*

ARTICLE INFO

*Article history:*
Received 15 December 2014
Received in revised form
27 March 2015
Accepted 3 April 2015
Available online 13 April 2015

*Keywords:*
Certification
Fault tolerant control
Fault detection and isolation
Unmanned aerial vehicles

ABSTRACT

In this paper, we describe a framework to efficiently assess the reliability of fault tolerant control systems on low-cost unmanned aerial vehicles. The analysis is developed for a system consisting of a fixed number of actuators. In addition, the system includes a scheme to detect failures in individual actuators and, as a consequence, switch between different control algorithms for automatic operation of the actuators. Existing dynamic reliability analysis methods are insufficient for this class of systems because the coverage parameters for different actuator failures can be time-varying, correlated, and difficult to obtain in practice. We address these issues by combining new fault detection performance metrics with pivotal decomposition. These new metrics capture the interactions in different fault detection channels, and can be computed from stochastic models of fault detection algorithms. Our approach also decouples the high dimensional analysis problem into low dimensional sub-problems, yielding a computationally efficient analysis. Finally, we demonstrate the proposed method on a numerical example. The analysis results are also verified by Monte Carlo simulations.



## 1. Introduction

Commercial flight control electronics must not only be highly reliable but their reliability must also be certified by aviation authorities. The system reliability requirements for civil aircraft are typically on the order of no more than $10^{-9}$ catastrophic failures per flight hour [1,2]. The aviation industry meets these requirements by using fault tolerant designs that are based almost exclusively on physical redundancy. For example, the Boeing 777 flight control electronics is implemented with multiply redundant flight computing modules, sensors, and actuators [3]. The widely used triplex or quadruplex redundant designs can be viewed as special cases of the "*k*-out-of- *n*: good" structure [4,5], and the overall system reliability can be effectively computed via static reliability analysis tools, e.g. a fault tree analysis [6,7]. Hence, the existing design and analysis techniques provide a mature approach to build reliable but expensive aircraft.

Low-cost unmanned aerial vehicles (UAVs) also have numerous applications, e.g. for use in precision agriculture [8]. These small UAVs cannot afford the full payload associated with physically redundant architectures due to their more restrictive cost, size, power, and weight requirements. In fact, most low-cost UAVs on the market are currently based on a two-actuator design without introducing fault tolerance [9,10]. However, the Modernization and Reform Act of 2012 requires the Federal Aviation Administration to integrate UAVs into the national airspace in a reliable and safe way [11]. This creates new design challenges in order to introduce fault tolerance into the UAV while maintaining low cost.

Fault tolerant control (FTC) provides an alternative design solution that is not exclusively reliant on physical redundancy [12–14]. There exist different approaches to design fault tolerant controllers for actuation systems [15–17]. The basic operation of a traditional physically redundant system and a FTC system is summarized in the context of a conventional aircraft with three surfaces (aileron, rudder, elevator). A traditional physically redundant design relies on a triplex actuation subsystem on each surface for a total of nine actuators. Under nominal conditions a single (baseline) control algorithm coordinates all the actuators to maneuver the aircraft. Any failed actuator is compensated by the other unfailed components in the triplex actuation subsystem, and the aircraft continues with the baseline controller. A FTC system can, in principal, be designed with a single actuator per surface for a total of only three actuators. The FTC system consists of two key parts: a fault detection and isolation (FDI) scheme and a set of backup controllers. The FDI scheme monitors the actuators using real-time measurements, dynamic models, and/or data mining techniques [18–20]. The FTC handles any detected actuator failure by switching to a pre-specified backup controller. For example, a

* Corresponding author.
*E-mail addresses:* huxxx221@umn.edu (B. Hu), seile017@umn.edu (P. Seiler).

http://dx.doi.org/10.1016/j.ress.2015.04.005
0951-8320/

failure in the rudder actuator would cause a switch to a backup controller designed to maneuver the aircraft using only the remaining surfaces (elevator and aileron).

The reliability of a FTC system depends on the performance of its FDI algorithm. Integration of FDI techniques and reliability analysis is an issue which has received increasing attention [21]. Proper FDI reliability metrics are required when integrating the component reliabilities to the system reliability. The existing tools quantify the FDI performance by coverage parameters, which can be time-varying, correlated, and difficult to determine in practice. Single-frame detection and false alarm probabilities can also be used as FDI metrics, but they do not model the time and space interactions in FDI residuals. A literature review on related analysis tools will be presented in Section 2.4 after the FTC analysis problem is formulated.

The objective of this paper is to assess the impact of FTC on the overall system reliability. There are two main contributions. First, we define a new reliability structure model, termed the FTC structure, in Section 2. The FTC structure generalizes the existing structure function approach and captures the switching nature of the active FTC system. This is a useful abstract reliability model for FTC systems designed for low-cost UAVs. Second, we develop an approach to efficiently compute system failure probability per hour of the proposed FTC structure based on several new FDI performance metrics (Section 3). This approach only requires information that can be easily obtained in practice. The proposed FDI performance metrics capture the interactions in different FDI channels, and can be directly computed from the stochastic models of FDI algorithms. The analysis is based on pivotal decomposition [4,5] which allows the FTC reliability analysis to be decoupled into low dimensional sub-problems. This simplifies the computation. Section 4 demonstrates the proposed approach on a numerical example and highlights the design trade-offs. The results are also verified by Monte Carlo simulations.

## 2. Problem formulation

We first introduce the notation (Section 2.1). In Section 2.2, we pose a minimum redundancy design problem, which motivates the FTC reliability analysis problem formulated in Section 2.3. Section 2.4 reviews related analysis tools and explains how our approach and existing tools can provide complementary benefits.

### 2.1. Notation

Our objective is to compute the failure probability of the FTC system within a time window. A FDI scheme is typically implemented on a computer with a specified sampling frequency. One can either approximate the discrete-time FDI performance with a continuous-time process or discretize the hardware failure time based on the computer sampling frequency. Since the flight computer samples fast, both approaches should lead to similar results. In this paper, we adopt a discrete-time approach with the specified period of time denoted by $N$. One thing worth noting is that the discretized time step is determined by the computer sampling rate. Hence the discretized time step is not a parameter which can be changed in the analysis.

Now consider a static system consisting of $n$ components. The state of component $i$ ($i=1,\ldots,n$) at time $k$ is described by a binary random variable $x_i(k)$: $x_i(k)$:=1 if component $i$ is operational at time $k$ and $x_i(k)$:=0 if the component has failed. The failure time of component $i$ is defined by $T_{X,i}$:=$\min\{k>0 : x_i(k)=0\}$. The subscript "$X$" indicates that the failure time is defined for a non-repairable hardware component. Denote the vector of component states as $\mathbf{x}(k)=(x_1(k),\ldots,x_n(k))\in\{0,1\}^n$ which has $2^n$ realizations. The system state at time $k$ is described by the structure function $\phi : \{0,1\}^n \to \{0,1\}$ defined by $\phi(\mathbf{x}(k))$:=1 if the system is operational at time $k$ and $\phi(\mathbf{x}(k))$:=0 if the system has failed. The system failure time is defined as $T_X$:=$\min\{k>0 : \phi(\mathbf{x}(k))=0\}$. The system failure probability is $P[T_X \le N]$.

Now we introduce the notation for different component failure modes. Let $M_0$ denote the $n$-dimensional vector whose entries are all 1. The event $\{\mathbf{x}(N)=M_0\}$ denotes the mode with zero component failures in the $N$-step window. Let $M_i$ denote the $n$-dimensional vector whose entries are all 1 except the $i$-th entry which is 0. The event $\{\mathbf{x}(N)=M_i\}$ denotes the case where only component $i$ fails within the $N$-step window. Define $\mathcal{M}_i$ to be the set of $n$-dimensional vectors with $i$ entries equal to 0 and $n-i$ entries equal to 1. The event $\{\mathbf{x}(N)\in\mathcal{M}_i\}$ corresponds to $i$ component failures in the $N$-step window. In particular, $\mathcal{M}_0=\{M_0\}$ and $\mathcal{M}_1=\{M_1,\ldots,M_n\}$. The $2^n$ different realizations of $\mathbf{x}(N)$ are denoted by $M_j$ where $j=0,\ldots,2^n-1$. The events $\{\mathbf{x}(N)=M_j\}$ $(j=0,\ldots,2^n-1)$ form a disjoint partition of the sample space. Failures can be viewed as severe faults, but some faults are not failures [6]. Therefore, $M_i$ $(i\neq 0)$ can be referred to as either a component failure mode or a system fault mode. Then pivotal decomposition can be expressed as

$$P[T_X \le N] = \sum_{j:\phi(M_j)=0} P[\mathbf{x}(N)=M_j] = 1 - \sum_{j:\phi(M_j)=1} P[\mathbf{x}(N)=M_j]. \quad (1)$$

### 2.2. Motivating study: UAV actuation system

This section applies pivotal decomposition to study the reliability of an actuation system on a UAV. This will motivate the FTC structure introduced in Section 2.3. The study focuses on the Ultra Stick 120 UAV shown in Fig. 1. This UAV, referred to as Faser, is one of the primary flight test vehicles used by the University of Minnesota (UMN) UAV Research Group [22]. Faser is a commercially available, fixed-wing, radio-controlled aircraft. It has a wing span of 1.92 m, mass of 7.41 kg, nominal cruise speed of 25 m/s, and endurance of 15–20 min. The flight control computer runs at 50 Hz. Additional details on this research infrastructure can be found in survey papers [23–25]. The standard configuration for Faser includes six control surfaces: two ailerons, two flaps, one elevator, and one rudder. Flaps are not used since we will consider a minimum redundancy design problem. Hence, the actuation system only includes the remaining four control surfaces. Each surface has an independent actuator for a total of four actuators.

Consider the baseline actuation system with four actuator components numbered as shown in Fig. 1. As defined previously, the failure time of component $i$ is denoted by $T_{X,i}$ $(i=1,\ldots,4)$ and the failure time of the actuation system is denoted by $T_X$. Typical aerospace requirements are specified per hour because flight times are approximately on this order. For example, a common UAV precision agriculture mission would take about 1 hour. We are

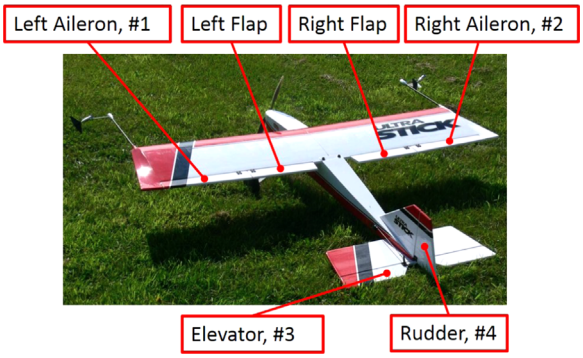


**Fig. 1.** University of Minnesota Ultra Stick 120 UAV (Faser).