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, 55108, United States

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.

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

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

*Corresponding author
Email addresses: huxxx221@umn.edu (Bin Hu), seile017@umn.edu (Peter Seiler)

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, 13, 14]. There exist different approaches to design fault tolerant controllers for actuation systems [15, 16, 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, 19, 20]. The FTC handles any detected actuator failure by switching to a pre-specified backup controller. For example, a 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 $P[T_X \leq N]$.

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

$$P[T_X \leq N] = \sum_{j:\phi(M_j)=0} P\left[\mathbf{x}(N) = M_j\right] = 1 - \sum_{j:\phi(M_j)=1} P\left[\mathbf{x}(N) = M_j\right] \tag{1}$$

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 Figure 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 1.92m, mass of 7.41kg, nominal cruise speed of 25m/s, and endurance of 15 to 20min. The flight control computer runs at 50 Hz. Additional details on this research infrastructure can be found in survey papers [23, 24, 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.

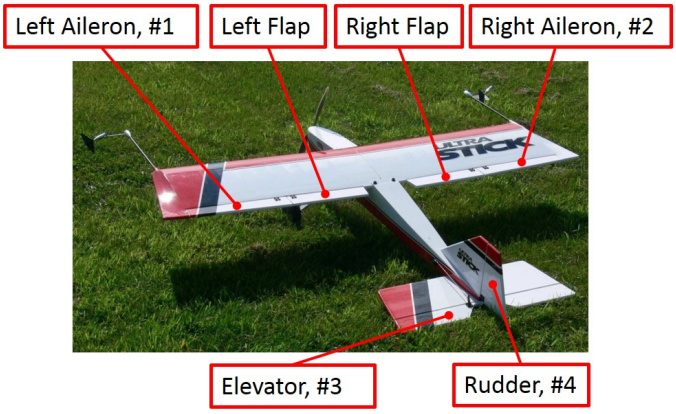

Figure 1: University of Minnesota Ultra Stick 120 UAV (Faser).

Consider the baseline actuation system with four actuator components numbered as shown in Figure 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 interested in reliability during this mission time, and we assume

perfect maintenance between different missions. Hence, the goal is to compute $P[T_X \leq N]$ with time window N corresponding to one hour. Specifically, the flight computer runs at 50Hz sample rate, and hence $N = 1.8 \times 10^5$ corresponds to the number of time steps at this specified sample rate. The computation of the per-hour system failure probability $P[T_X \leq N]$ requires knowledge of the component failure probabilities $P[T_{X,i} \leq N]$. This information has been estimated as $P[T_{X,i} \leq N] \approx 2.5 \times 10^{-3}$ for the four actuators used on Faser [26]. In addition, all actuator components are assumed to be statistically independent.

The intended function of the actuation system is to safely fly the UAV. This includes straight and level flight as well as coordinated turns with zero sideslip. The structure function of the actuation system is determined by considering the baseline controller described in [23]. The baseline controller is a classical design that coordinates the four actuators to achieve safe flight. Based on nonlinear simulations, we determined that the actuation system fails to function properly in the event of a single actuator failure. Thus this design is a series architecture, and the structure function is defined as $\phi(M_0) := 1$ and $\phi(\mathbf{x}) := 0$ otherwise. Now (1) can be applied to compute the system failure probability per hour:

$$P[T_X \leq N] = 1 - \prod_{i=1}^{4} P[T_{X,i} > N] \approx 1.0 \times 10^{-2} \tag{2}$$

All actuator components have equivalent reliability in this example and $P[T_X \leq N] \approx \sum_{i=1}^{4} P[\mathbf{x}(N) = M_i]$. Increasing the system reliability would require additional fault tolerance for all four component failure modes in $\mathcal{M}_1$. There are several methods to introduce fault tolerance for one specific component failure mode. For example, to handle the critical elevator failure mode M_3, we can replace the current single elevator actuator by a triplex actuation subsystem. An alternative strategy is to design the baseline controller so that the aircraft continues safe flight in the event of an elevator failure, $\phi(M_3) = 1$ (passive FTC). The problem formulation in Section 2.3 focuses on another possible design: active FTC. This approach requires a method to detect the elevator actuator failure $\{\mathbf{x}(k) = M_3\}$ and switch to a backup controller with a new structure function ϕ_3 such that $\phi_3(M_3) = 1$. A reliable design of low-cost UAVs tolerates each component failure mode in $\mathcal{M}_1$ by one of the above three methods while using minimum number of actuators. Section 2.3 formulates a general FTC structure model based on this principle.

2.3. Problem Formulation: FTC Structure

This section formulates the reliability structure for a FTC system. The FTC system consists of a primary controller K_0, a FDI scheme, and a set of backup controllers $\{K_i\}$. The primary controller is initially used and the system switches to one of the backup controllers if the FDI scheme detects a component failure.

The notation $\mathcal{M}_i$ was introduced to denote events with exactly i actuator failures. Let $\mathcal{C} \subset \mathcal{M}_1$ denote the single actuator failure modes that are passively tolerated by the primary controller K_0. The system with the primary controller K_0 has a structure function ϕ_0 satisfying $\phi_0(\mathbf{x}) = 1$ for $\mathbf{x} \in \mathcal{M}_0 \cup \mathcal{C}$ and $\phi_0(\mathbf{x}) = 0$

otherwise. Let $\mathcal{D} \subset \mathcal{M}_1$ denote the single actuator failure modes that are handled by active FTC. For each event $M_i \in \mathcal{D}$, there is a backup controller K_i such that the actuation system has a structure function $\phi_i(\mathbf{x}) = 1$ for $\mathbf{x} \in \{M_0, M_i\}$ and $\phi_i(\mathbf{x}) = 0$ otherwise. This structure function is compactly expressed as $\phi_i(\mathbf{x}) = \prod_{j \neq i} x_j$. In other words, the backup controller K_i uses the control authority in the remaining unfailed components to tolerate a failure in component i. The structure function ϕ_i is non-decreasing and the system fails after its first failure that occurs after switching to controller K_i. In practice the use of backup controller K_i in the presence of the component failure mode M_i leads to a loss of aircraft performance but, if properly designed, ensures continued safe flight. Aerospace systems typically have a requirement to tolerate all single component failures. Hence we assume $\mathcal{C} \cup \mathcal{D} = \mathcal{M}_1$. This assumption can be relaxed with minor notational changes for systems with low probability, single component failures leading to system failure. We further assume that the actuator failure time distributions do not change before and after the control reconfiguration. The load on each actuator may be increased when the FTC system continues operation with part of its actuators under a backup controller. However, it is reasonable to assume that the increased load will not significantly change the actuator failure time distributions since the mission time is typically much shorter than the mean value of the actuator failure time. Based on this assumption the backup controller can be viewed as a "hot standby" of the primary controller.

The active FTC requires a FDI scheme to monitor component i for each component failure mode $M_i \in \mathcal{D}$. The monitoring channel for component i generates a logic signal $d_i(k)$ at time k defined by $d_i(k) := 1$ if the FDI scheme determines that component i is operational at time k and $d_i(k) := 0$ otherwise. We assume $d_i(k)$ remains equal to zero after the first time that the FDI scheme flags component i as failed. Thus the detection time for component i, denoted $T_{D,i}$, is uniquely defined by $T_{D,i} := \min\{k > 0 : d_i(k) = 0\}$. The subscript "$D$" indicates that this is a detection time. The FTC system switches to the appropriate backup controller at the first detection time $T_{D,i}$ of an actuator failure $M_i \in \mathcal{D}$. The FTC structure is assumed to handle only the first component failure, and there are no further reconfigurations after the first switch to a backup controller. Therefore, the system switching time can be uniquely defined as $T_D := \min_{\{i:M_i \in \mathcal{D}\}} T_{D,i}$. If two or more component failures are detected simultaneously then any of the appropriate back-up controllers may be selected. The choice is irrelevant as the FTC structure is assumed to tolerate at most one component failure. The probability of multiple alarms at one time step given single or no component failures is neglected.

The proposed FTC structure is summarized as follows. The FTC system initially uses the primary controller K_0. Under this controller, the FTC structure has a structure function satisfying $\phi_0(\mathrm{x}) = 1$ for $\mathrm{x} \in \mathcal{M}_0 \cup \mathcal{C}$. Several FDI channels are used to monitor the remaining single component failures $M_i \in \mathcal{D}$ that lead to system failure under K_0. The first failure detected in a certain component i causes a switch at time $T_D = T_{D,i}$ to backup controller K_i. Under K_i, the FTC structure has a structure function with $\phi_i(\mathrm{x}) = 1$ for $\mathrm{x} \in \{M_0, M_i\}$. Proper design of the FTC system ensures continued operation after this first detected component failure. This FTC structure model captures the essential features of a real FTC system.

Next we define a generalized, time-varying structure function $\phi(\mathbf{x}, k)$ to model the jumps in the FTC structure from ϕ_0 to ϕ_i. Specifically, we define the generalized structure function as $\phi(\mathbf{x}, k) := \phi_i(\mathbf{x})$ if the FTC structure is using controller K_i at time k. This generalized function indicates the state of the FTC structure: $\phi(\mathbf{x}(k), k) := 1$ if the FTC structure is operational at time k and $\phi(\mathbf{x}(k), k) := 0$ if the FTC structure is in a failed mode. A standard architecture with a fixed controller and non-repairable components will fail after the first actuator failure. The FTC structure, on the other hand, is designed to tolerate specific first component failures. This requires the component failure to be quickly detected so that the system does not continue using a failed component. For example, the aircraft may tolerate an elevator actuator failure as long as it switches in time to a backup controller that has been designed to handle this component failure. Formally we require that a component failure $M_j \in \mathcal{D}$ be detected within a pre-specified maximum delay, also referred to as a hard deadline [27] or hard time limit [28]. The maximum detection delay for different component failure modes can be different. The maximum detection delay for the mode $M_j \in \mathcal{D}$ is denoted as N_j. High fidelity simulations can be used to determine the maximum detection delay before the backup controller is no longer able to recover the system. The FTC system failure is formally defined as follows.

Definition 1. The FTC structure fails at time $T \leq N$ if one of the following events occurs:

(a) There exists $k_0 \leq N$ such that $\phi(\mathbf{x}(k_0), k_0) = 0$ for some $\mathbf{x}(k_0) \notin \mathcal{D}$.

(b) There exist j and $k_0 \leq N$ such that for each $k \in \{k_0, k_0 + 1, \ldots, k_0 + N_j - 1\}$ we have $\mathbf{x}(k) = M_j \in \mathcal{D}$ and $\phi(\mathbf{x}(k), k) = 0$.

It is important to emphasize that $\phi(\mathbf{x}(k), k) = 0$ does not necessarily imply failure of the FTC structure. In particular, the FTC structure is designed to essentially self-repair in the event of a component failure mode $M_j \in \mathcal{D}$ via transition to a backup controller. This self-repair is only successful if the component failure M_j is detected within the maximum delay N_j. Event (b) in the definition above corresponds to the case where the component failure M_j is not detected in time leading to failure of the FTC structure. Finally, a minor point is that any system failure caused by a component failure initiated at time $k_0 \leq N$ is counted in this N-step window. Different boundary assumptions can be handled with minor notational changes.

We want to compute the probability of system failure within the N-step window, i.e. $P[T \leq N]$. To compute this metric, we need to know the component failure models $P[\mathbf{x}(k) = M_j]$, the structure functions $\phi_j(\mathbf{x}(k))$ corresponding to the different controllers K_j, the maximum detection delay N_j, and various FDI performance metrics. The first three pieces of information have already been discussed. Now we will briefly introduce the FDI performance metrics required for the analysis in Section 3:

1. **FDI False Alarm**, $P\left[T_D \leq N \;\middle|\; \mathbf{x}(N) = M_j\right]$ for $M_j \in \mathcal{C}$:
   This is the conditional probability that the FDI logic switches to a backup controller at time T_D in the N-step window given that the occurred component failure mode can be handled by the primary controller. This is a false alarm probability over the N-step window.

2. **FDI Missed Detection**, $P\left[\{T_{D,j} \geq k + N_j\} \;\middle|\; \{T_{X,j} = k, \min_{i \neq j} T_{X,i} > N\}\right]$:
   This is defined for $k = 1, \ldots, N$ and $\{j \;:\; M_j \in \mathcal{D}\}$. This is the conditional probability that the FDI logic $d_j(k)$ does not detect the failure of actuator j at time k within the maximum delay N_j. This is the probability of a missed detection conditioned on a component failure at time k.
3. **FDI Bad Interaction**, $P\left[\{T_D < T_{D,j} < k + N_j\} \;\middle|\; \{T_{X,j} = k, \min_{i \neq j} T_{X,i} > N\}\right]$:
   This is defined for $k = 1, \ldots, N$ and $\{j \;:\; M_j \in \mathcal{D}\}$. This is the conditional probability that the FDI channel $d_j(k)$ successfully triggers an alarm within the maximum delay N_j given a failure in actuator j at time k. However the FTC structure fails to switch to the proper backup controller due to an alarm in another channel of the FDI scheme. This metric accounts for bad interactions between different FDI channels.

We will explain how to estimate these FDI performance metrics in Section 4.2.

The switching mechanism of FTC systems can be designed in many different ways. It is difficult to seek a general formulation covering all FTC designs. For the sake of conciseness, this paper focuses on the proposed FTC structure which is suitable for low-cost UAV applications. In this case, the required FDI performance metrics will provide straightforward insights on how FDI performance interacts with hardware failures (as further explained in Section 3). In principle, our analysis can be extended to more complex FTC systems given proper modifications of FDI performance metrics. However, most extensions require additional mathematical notations, and the resultant modified FDI performance metrics will be less intuitive than the current FDI performance metrics. The details of these extensions are beyond the scope of this paper.

2.4. Literature Review of Related Dynamic Reliability Analysis Tools

The FTC structure formulated in Section 2.3 introduces two key issues. First, the FTC structure switches between different controllers based on the FDI monitoring signals. As a result, the order of the component failures and the FDI alarms has to be considered in the reliability analysis. Second, the FTC structure depends on the FDI performance, and proper FDI performance metrics are required in the FTC reliability analysis. There exist dynamic reliability analysis tools which can address the first issue. However, these existing dynamic tools are not easily adapted to the FTC analysis problem mainly due to the second issue.

Markov and semi-Markov modeling techniques are flexible, and have strong modeling power in addressing the ordering issue of the reliability analysis [29]. They have been extensively used to analyze the dynamic behavior of reconfigurable systems. However, Markov models can experience state space explosion and become computationally intractable [30]. Under certain circumstances, more computationally efficient techniques such as dynamic fault trees [31], coverage modeling [32, 33], discrete-time Bayesian network modeling [34], sequential decision diagrams [35], and Petri nets [36] can be applied to solve dynamic reliability problems.

Incorporating FDI performance into FTC reliability is another main issue in the FTC reliability analysis problem. Markov (or semi-Markov) models have been successfully applied to the FTC reliability analysis

when the FDI models are governed by constant transition matrices [37, 27]. In more general cases, coverage modeling has been used to quantify the FDI performance [28, 38, 39]. However, it is not easy to get the coverage parameter in applications. One can estimate this parameter by experimental data generated from a full-scale simulator [28], but the time-varying and non-exponential nature poses difficulty for the accurate estimate of this parameter based on limited data. Moreover, the coverage parameter mostly models short term behaviors, such as FDI missed detections. Long term FDI behaviors, e.g. false alarms, are typically not included in the coverage modeling.

Single-frame false alarm rates and missed detection rates have also been used as fault detection performance metrics [40, 41, 42, 43]. These metrics can be integrated into system reliability analysis by an extended fault tree [40], or stochastic activity networks [41, 42]. The continuous time counterparts of these single-frame probabilities have also been used to model the diagnosis reliability [44]. False alarm rates and missed detection rates can be directly computed from the stochastic model of the FDI residuals [40], or indirectly estimated from Monte Carlo simulations of stochastic activity networks [45]. To further model the maximum detection delay and the time correlations in the FDI residuals, new false alarm metrics and missed detection metrics are proposed by incorporating time scales into the single-frame false alarm and missed detection probabilities [46]. These fault detection performance metrics can be directly computed from the stochastic model of the fault detection algorithm and aggregated to the system failure probability per hour by the law of total probability. However, these metrics only apply for a dual redundant system (consisting of only two hardware components) with one fault detection channel. A FTC system typically has more than two components, and includes multiple FDI channels. In this case, more general FDI performance metrics are required to model the interactions between different FDI channels.

In this paper, we generalize the results in [46] to a large class of FTC systems via a structure function approach. Our method relies on the FDI performance metrics proposed in Section 2.3. These metrics can also be computed from the stochastic model of the FDI algorithm. Correlations in FDI decision signals are embedded in the proposed FDI metrics. Our proposed approach does not require the generation of Markov or semi-Markov models. Moreover, our approach is computationally efficient and scales linearly with the number of the components in the FTC system. The main limitation of our new analysis method is that it is mainly developed for low-cost UAV FTC systems. Thus our proposed approach and existing techniques (Markov approach, coverage modeling, stochastic activity networks, etc) provide complementary benefits.

3. FTC structure Reliability Analysis

This section gives a direct formula to compute the failure probability per hour $P[T \leq N]$ for the FTC structure. The analysis relies on pivotal decomposition which is a special application of the law of total probability [4]. The law of total probability states: Let the events $\{\Omega_n : n = 0, 1, 2, \ldots\}$ form a disjoint

partition of the sample space. Then for any other event $\mathcal{A}$, the following is true:

$$P[\mathcal{A}] = \sum_n P[\mathcal{A} \cap \Omega_n] = \sum_n P[\mathcal{A} \mid \Omega_n] P[\Omega_n] \tag{3}$$

3.1. General Approach

Since $\{\mathbf{x}(N) = M_j : j = 0, 1, \ldots, 2^n - 1\}$ form a disjoint partition of the sample space, we can directly apply the law of total probability to express $P[T \leq N]$ as:

$$P\left[T \leq N\right] = \sum_{j=0}^{2^n-1} P[\{T \leq N\} \cap \{\mathbf{x}(N) = M_j\}] \tag{4}$$

Equation (4) is also referred to as pivotal decomposition. The basic idea is to determine how the 2^n mutually exclusive modes $\{M_j\}_{j=0}^{2^n-1}$ can lead to FTC structure failure. The probability $P[\{T \leq N\} \cap \{\mathbf{x}(N) = M_j\}]$ can be efficiently computed for any given M_j. Then we can compute the system failure probability per hour by aggregating all 2^n terms using Equation (4). Next we classify the component failure modes M_j into three mutually exclusive categories:

1. $M_j \in \mathcal{C}$: Component failure modes that can be tolerated by the primary controller.
2. $M_j \in \mathcal{D}$: Component failure modes that can not be tolerated by the primary controller but can be tolerated by a backup controller K_j.
3. $M_j \in \mathcal{C}^c \cap \mathcal{D}^c$: All remaining component failure modes consisting of no failures M_0 as well as all modes with two or more component failures $(\mathcal{M}_2, \mathcal{M}_3, \ldots)$. The case with two or more component failures is tolerated by no controllers.

M_j belongs to one and only one of the above three categories. Thus Equation (4) can be rewritten as a sum of three terms:

$$\begin{aligned} P\left[T \leq N\right] = & \sum_{j:M_j \in \mathcal{C}^c \cap \mathcal{D}^c} P[\{T \leq N\} \cap \{\mathbf{x}(N) = M_j\}] \\ & + \sum_{j:M_j \in \mathcal{C}} P[\{T \leq N\} \cap \{\mathbf{x}(N) = M_j\}] + \sum_{j:M_j \in \mathcal{D}} P[\{T \leq N\} \cap \{\mathbf{x}(N) = M_j\}] \end{aligned} \tag{5}$$

Three technical lemmas are presented next and used to compute the various terms in this sum. Proofs of all lemmas are presented in the appendix. First, Lemma 1 is used to compute the term associated with $M_j \in \mathcal{C}^c \cap \mathcal{D}^c$ (category 3).

Lemma 1. *If $M_j \in \mathcal{C}^c \cap \mathcal{D}^c \cap \mathcal{M}_0^c$, then $P[\{T \leq N\} \cap \{\mathbf{x}(N) = M_j\}] = P[\{\mathbf{x}(N) = M_j\}]$.*

Lemma 1 states that the component failure modes $(\mathbf{x}(N) = M_j)$ directly lead to the system failure $(T \leq N)$ if none of the controllers (primary or backup) can tolerate these modes. It is clear that $P[\{T \leq$

$N\} \cap \{\mathbf{x}(N) = M_0\}] = 0$ since all controllers function properly in the presence of no actuator failures. The probability of the system failure caused by component failure modes in Category 3 can be computed as

$$\begin{aligned}\sum_{j:M_j \in \mathcal{C}^c \cap \mathcal{D}^c} P[\{T \leq N\} \cap \{\mathbf{x}(N) = M_j\}] &= \sum_{j:M_j \in \mathcal{C}^c \cap \mathcal{D}^c \cap \mathcal{M}_0^c} P[\{\mathbf{x}(N) = M_j\}] \\ &= 1 - \sum_{j:M_j \in \mathcal{C} \cup \mathcal{D} \cup \mathcal{M}_0} P[\{\mathbf{x}(N) = M_j\}]\end{aligned} \tag{6}$$

This term only involves hardware failure models and is unaffected by the FDI performance. We need only $n+1$ calculations to compute this term since the set $\mathcal{C} \cup \mathcal{D}$ contains all n possible single actuator failures. This term scales linearly with the number of the components in the FTC system.

Next, the term in (5) associated with $M_j \in \mathcal{C}$ (category 1) is computed via the next lemma.

Lemma 2. *If $M_j \in \mathcal{C}$, then $P[\{T \leq N\} \cap \{\mathbf{x}(N) = M_j\}] = P[\{T_D \leq N\} \cap \{\mathbf{x}(N) = M_j\}]$.*

Lemma 2 describes the case where the primary controller is working properly, the FDI logic triggers a false alarm and then the backup controller fails. Lemma 2 directly gives:

$$\sum_{j:M_j \in \mathcal{C}} P[\{T \leq N\} \cap \{\mathbf{x}(N) = M_j\}] = \sum_{j:M_j \in \mathcal{C}} P\left[T_D \leq N \;\middle|\; \mathbf{x}(N) = M_j\right] P[\{\mathbf{x}(N) = M_j\}] \tag{7}$$

This term involves the FDI false alarm metric and scales linearly with the number of the elements in $\mathcal{C}$.

The next lemma is used to compute the term associated with $M_j \in \mathcal{D}$ (category 2).

Lemma 3. *The following statement holds:*

$$\begin{aligned}&\sum_{j:M_j \in \mathcal{D}} P[\{T \leq N\} \cap \{\mathbf{x}(N) = M_j\}] = \\ &\sum_{j:M_j \in \mathcal{D}} \sum_{k=1}^{N} P\left[\{T_{D,j} \geq k + N_j\} \;\middle|\; \{T_{X,j} = k, \min_{i \neq j} T_{X,i} > N\}\right] P[T_{X,j} = k, \min_{i \neq j} T_{X,i} > N] + \\ &\sum_{j:M_j \in \mathcal{D}} \sum_{k=1}^{N} P\left[\{T_D < T_{D,j} < k + N_j\} \;\middle|\; \{T_{X,j} = k, \min_{i \neq j} T_{X,i} > N\}\right] P[T_{X,j} = k, \min_{i \neq j} T_{X,i} > N]\end{aligned} \tag{8}$$

where $P[T_{X,j} = k, \min_{i \neq j} T_{X,i} > N]$ depends only on hardware component failure models.

Lemma 3 can be understood as follows. For $M_j \in \mathcal{D}$, the component failure mode $\{\mathbf{x}(N) = M_j\}$ leads to a system failure in two ways. Since $M_j \in \mathcal{D}$, component j is monitored by the FDI decision logic $d_j(k)$. If the FDI decision logic misses the detection of the failure in component j ($T_{D,j} \geq T_{X,j} + N_j$) then the FTC system fails. The probability of this event corresponds to the first term on the right hand side of (8)

in Lemma 3, which is affected by the FDI missed detection metric. Even if the FDI channel on component j works properly ($T_{D,j} < T_{X,j} + N_j$), the FTC system can fail because of a wrong switch to an improper backup controller either due to an early false alarm ($T_D < T_{X,j}$ and $T_D < T_{D,j}$) in other FDI channels or a missed isolation in the FDI scheme ($T_{X,j} \leq T_D < T_{D,j}$). This event is described by the second term on the right hand side of (8), which is affected by the FDI bad interaction metric. Notice that (8) scales with the number of the elements in $\mathcal{D}$, and can be efficiently evaluated.

Lastly, substitute (6), (7), and (8) into (5), and the final result becomes:

$$
\begin{aligned}
&P[T \leq N] = \\
&\sum_{j:M_j \in \mathcal{C}^c \cap \mathcal{D}^c \cap \mathcal{M}_0^c} P[\{\mathbf{x}(N) = M_j\}] + \sum_{j:M_j \in \mathcal{C}} P\left[T_D \leq N \;\middle|\; \mathbf{x}(N) = M_j\right] P[\{\mathbf{x}(N) = M_j\}] + \\
&\sum_{j:M_j \in \mathcal{D}} \sum_{k=1}^{N} P\left[\{T_{D,j} \geq k + N_j\} \;\middle|\; \{T_{X,j} = k, \min_{i \neq j} T_{X,i} > N\}\right] P[T_{X,j} = k, \min_{i \neq j} T_{X,i} > N] + \\
&\sum_{j:M_j \in \mathcal{D}} \sum_{k=1}^{N} P\left[\{T_D < T_{D,j} < k + N_j\} \;\middle|\; \{T_{X,j} = k, \min_{i \neq j} T_{X,i} > N\}\right] P[T_{X,j} = k, \min_{i \neq j} T_{X,i} > N]
\end{aligned}
\tag{9}
$$

This equation provides an intuition for the basic causes of the FTC structure failure. The first term is due to the hardware component failures which cannot be covered by FTC designs. The second term refers to the component failure modes, which can be covered by the primary controller, but the FDI scheme triggers a false alarm that leads to a system failure when a backup controller is improperly used. The third term refers to the case where the FDI scheme fails to detect the actuator failures that should be covered by the backup controller. The last term accounts for the improper interactions between different FDI channels and refers to the case where the FTC system is switched to a wrong controller based on an early false alarm or a missed isolation of the FDI scheme. Equation (9) decouples the causes of the system failure based on hardware component failures and the FDI performance. This allows the effect of the FDI performance on the total system reliability to be fully separated from the reliability of the hardware components. Section 4.2 will present an example to demonstrate the computation of the FDI performance metrics used in (9).

3.2. Example: Dual Redundant Systems

This section connects the general approach presented in Section 3.1 to a previous result for dual redundant systems with a fault detection scheme [46]. The existing result was originally derived from an exhaustive approach enumerating all failure possibilities. The structure function approach was not used since it is straightforward to define the system failure for a dual system. The approach presented in Section 3.1 generalizes the old result to FTC systems via pivotal decomposition of structure functions. This demonstrates the generality of the new approach and provides a concrete example to clarify the notation.

The dual redundant system consists of one actuator as a primary component and another actuator as

a standby. A fault detection scheme is used to monitor the primary actuator. When there is no failure detected, the primary actuator is in active mode and the backup actuator is in passive mode. When a failure on the primary actuator is detected, the primary actuator will become passive, and the backup actuator will become active. The primary actuator is the only actuator being monitored, i.e. $T_{D,1} = T_D$. This dual redundant system can be viewed as a special case of the FTC structure proposed in Section 2.3. In this case, $n = 2$. The primary controller K_0 sends control commands to the first component, and sends zero signals to the second component. The component failure mode $\{M_2 = (1, 0)\}$ is tolerated by K_0. The component failure mode $\{M_1 = (0, 1)\}$ is designed to be handled by the backup controller K_1. We have $\mathcal{M}_0 = \{(1, 1)\}$, $\mathcal{C} = \{(1, 0)\}$, $\mathcal{D} = \{(0, 1)\}$.

For $M_j \in \mathcal{C}^c \cap \mathcal{D}^c$ (category 3), (6) becomes:

$$\sum_{j:M_j \in \mathcal{C}^c \cap \mathcal{D}^c \cap \mathcal{M}_0^c} P\left[\mathbf{x}(N) = M_j\right] = P[\mathbf{x}(N) = (0, 0)] = P[T_{X,1} \leq N, T_{X,2} \leq N] \tag{10}$$

For $M_j \in \mathcal{C}$ (category 1), we need one computation since $\mathcal{C}$ has one element $(1, 0)$. Controller K_0 sends zero signals to the backup actuator before switching. Hence this actuator does not affect the switching time T_D, and T_D is statistically independent from $T_{X,2}$. From (7) we get:

$$P[T_D \leq N, T_{X,1} > N, T_{X,2} \leq N] = P[T_{D,1} \leq N \mid T_{X,1} > N] P[T_{X,1} > N, T_{X,2} \leq N] \tag{11}$$

For $M_j \in \mathcal{D}$ (category 2), we will use (8). $\mathcal{D}$ has one element $(0, 1)$. The first term in (8) is $\sum_{k=1}^{N} P[T_{D,1} \geq k + N_1, T_{X,1} = k, T_{X,2} > N]$. $T_{D,1}$ is statistically independent of $T_{X,2}$. Hence:

$$\begin{aligned} &\sum_{k=1}^{N} P[T_{D,1} \geq k + N_1, T_{X,1} = k, T_{X,2} > N] = \\ &\qquad \sum_{k=1}^{N} P[T_{D,1} \geq k + N_1 | T_{X,1} = k] P[T_{X,1} = k, T_{X,2} > N] \end{aligned} \tag{12}$$

Finally since $T_{D,1} = T_D$, the probability that $T_D < T_{D,1}$ is always 0. Hence the second term in (8) is 0. Therefore we sum all the terms to get:

$$\begin{aligned} P[T \leq N] =& P[T_{X,1} \leq N, T_{X,2} \leq N] + P[T_{D,1} \leq N \mid T_{X,1} > N] P[T_{X,1} > N, T_{X,2} \leq N] \\ &+ \sum_{k=1}^{N} P[T_{D,1} \geq k + N_1 | T_{X,1} = k] P[T_{X,1} = k, T_{X,2} > N] \end{aligned} \tag{13}$$

which is the exact result presented in previous work [46].

3.3. Simplifying Approximations: Guidelines for FDI Design

This section discusses a simplifying approximation for the FTC reliability formula (9). The simplifications are based on approximations of the FDI performance metrics as detailed by supporting derivations in the appendix. The simplifying approximation provides insights useful for FDI design.

We consider simplifying approximations for the system failure probability under different component failure modes. For $M_j \in \mathcal{C}^c \cap \mathcal{D}^c$, only hardware component failure models are required. For $M_j \in \mathcal{C}$, the FDI false alarm metric $P\left[T_D \leq N \;\middle|\; \mathbf{x}(N) = M_j\right]$ is involved, and requires one computation.

For $M_j \in \mathcal{D}$, both the FDI missed detection metric and the FDI bad interaction metric depend on the time step k. For any fixed j, both these metrics require N computations. When the probability $P\left[T_D \leq N \;\middle|\; \mathbf{x}(N) = M_0\right]$ is significantly smaller than 1 (e.g. < 0.1), the following approximation can be used for $k = 1, 2, \ldots, N$:

$$P\left[\{T_{D,j} \geq k + N_j\} \;\middle|\; \{T_{X,j} = k, \min_{i \neq l} T_{X,i} > N\}\right] \approx P\left[\{T_{D,j} \geq 1 + N_j\} \;\middle|\; \{T_{X,j} = 1, \min_{i \neq l} T_{X,i} > N\}\right] \quad (14)$$

The detailed derivation of (14) can be found in the appendix. Based on (14), the FDI missed detection metric can be evaluated for all $k = 1, 2, \ldots, N$ using one calculation of the conditional probability that $d_j(k) = 1$ for all $k = 1, 2, \ldots, N_j$ given that actuator j fails at the first time step ($T_{X,j} = 1$). This probability can be viewed as a missed detection probability in FDI channel j over a detection window with size N_j.

Similarly, the FDI bad interaction metric can be decoupled as:

$$\begin{aligned}
&P\left[\{T_D < T_{D,j} < k + N_j\} \;\middle|\; \{T_{X,j} = k, \min_{i \neq j} T_{X,i} > N\}\right] \\
=& \sum_{l=1}^{k+N_j-2} P\left[\{T_D = l, l < T_{D,j} < k + N_j\} \;\middle|\; \{T_{X,j} = k, \min_{i \neq j} T_{X,i} > N\}\right] \\
=& \sum_{l=1}^{k-1} P\left[\{T_D = l, l < T_{D,j} < k + N_j\} \;\middle|\; \{T_{X,j} = k, \min_{i \neq j} T_{X,i} > N\}\right] \\
+& \sum_{l=k}^{k+N_j-2} P\left[\{T_D = l, l < T_{D,j} < k + N_j\} \;\middle|\; \{T_{X,j} = k, \min_{i \neq j} T_{X,i} > N\}\right]
\end{aligned} \quad (15)$$

The first term accounts for the case where the FDI channel j sends an alarm before its maximum detection delay, but the system switches to another wrong controller due to an early false alarm in other FDI channels. This term can be approximated by a FDI false alarm metric on mode M_0, which is $P\left[T_D \leq N \;\middle|\; \mathbf{x}(N) = M_0\right]$. The second term refers to the case where the FDI scheme detects a failure after its occurrence but makes a mistake in isolating the failure position. This metric can also be approximated from one term which does not depend on k: $P\left[\{T_D < T_{D,j} < 1 + N_j\} \;\middle|\; \{T_{X,j} = 1, \min_{i \neq j} T_{X,i} > N\}\right]$. This term can be viewed as a missed isolation probability over a time window of size N_j.

Now we can simplify the formula for the system failure probability $P[T \leq N]$ by an approximation. For simplicity, the following are defined as:

$$\hat{q}_j := P[\mathrm{x}(N) = M_j] \tag{16}$$

$$\hat{P}_{F,j} := P\left[T_D \leq N \;\middle|\; \mathbf{x}(N) = M_j\right] \tag{17}$$

$$\hat{P}_{MD,j} := P\left[\{T_{D,j} \geq 1 + N_j\} \;\middle|\; \{T_{X,j} = 1, \min_{i \neq l} T_{X,i} > N\}\right] \tag{18}$$

$$\hat{P}_{MI,j} := P\left[\{T_D < T_{D,j} < 1 + N_j\} \;\middle|\; \{T_{X,j} = 1, \min_{i \neq j} T_{X,i} > N\}\right] \tag{19}$$

$$\hat{P}_{B,j} := \hat{P}_{MD,j} + \hat{P}_{F,0} + \hat{P}_{MI,j} \tag{20}$$

Each of these definitions has a clear meaning. $\hat{q}_j$ is the hardware failure probability per hour due to mode M_j. $\hat{P}_{F,j}$ is the false alarm probability per hour under mode M_j. $\hat{P}_{MD,j}$ is the missed detection probability within the N_j-step detection window conditioned on the j-th component failure occurring at $k = 1$. $\hat{P}_{MI,j}$ is the missed isolation probability within the N_j-step detection window conditioned on the j-th component failure occurring at $k = 1$. $\hat{P}_{B,j}$ is the sum of probabilities that FDI channel j is doing bad work. The "hat" denotes that these probabilities are valid over multiple steps, i.e. they are not single-frame probabilities.

With this notation, the system failure probability (9) is approximated as:

$$P[T \leq N] \approx \sum_{j:M_j \in \mathcal{C}^c \cap \mathcal{D}^c \cap \mathcal{M}_0^c} \hat{q}_j + \sum_{j:M_j \in \mathcal{C}} \hat{q}_j \hat{P}_{F,j} + \sum_{j:M_j \in \mathcal{D}} \hat{q}_j \hat{P}_{B,j} \tag{21}$$

(21) is an approximation of (9). It provides insights for FTC design. The first term on the right side of (21) can be expressed as $1 - \sum_{j:M_j \in \mathcal{C} \cup \mathcal{D} \cup \mathcal{M}_0} \hat{q}_j$. This provides a lower bound on the system failure probability and only depends on the hardware model. No matter how well the FDI algorithm performs, the FTC system failure probability will not be lower than this bound. To achieve this lower bound, roughly we require that the second and third terms on the right side of (21) are significantly smaller than the first term. The number of the elements in $\mathcal{C} \cup \mathcal{D}$ is n. Hence, a design requirement can be:

$$\begin{aligned} \hat{P}_{F,j} &\ll (1 - \sum_{j:M_j \in \mathcal{C} \cup \mathcal{D} \cup \mathcal{M}_0} \hat{q}_j)/(n\hat{q}_j) \\ \hat{P}_{B,j} &\ll (1 - \sum_{j:M_j \in \mathcal{C} \cup \mathcal{D} \cup \mathcal{M}_0} \hat{q}_j)/(n\hat{q}_j) \end{aligned} \tag{22}$$

There is a design trade-off between these two requirements. When both requirements are satisfied, the FTC design will significantly improve the system reliability. Notice the approximation holds when $\hat{P}_{F,j}$ is small. If the FDI system satisfies (22), the approximation automatically holds.

4. Case Study: Reliability Analysis of a UAV FTC System

4.1. UAV FTC Structure

Linear system analysis can be used to study whether a FTC system can be designed given a certain number of control surfaces [47]. A trim analysis can be performed to show that the minimum number of actuators required to cover all single actuator failures is six. As shown in Figure 2, the rudder is split into two pieces, each actuated by its own servo. A similar split rudder design can be found in [48]. The elevator is split in a similar manner. The detailed design of the split rudder and elevator is documented in [49]. This design adds two servos to the system. We will perform a numerical study on this six-actuator FTC design.

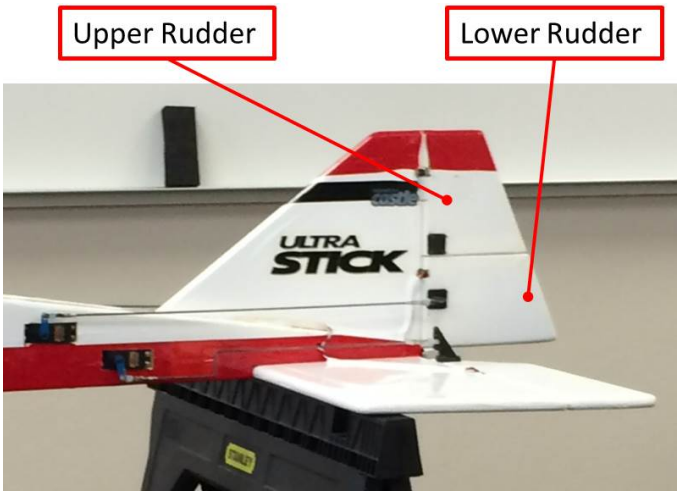

Figure 2: The split surfaces design of the Ultra Stick 120 UAV.

The components of this new design are numbered in Table 1. The primary controller K_0 can be designed to handle a single failure in either the upper or lower rudder servo [49]. Hence, we have $\mathcal{C} = \{M_5, M_6\}$ and $\mathcal{D} = \{M_1, M_2, M_3, M_4\}$. Four backup controllers are designed to cover all the single component failures in $\mathcal{D}$. Under controller K_i $(i = 1, 2, 3, 4)$, the FTC system has a structure function $\phi_i = \prod_{j \neq i} x_j$, and hence $\phi_i(M_i) = 1$. Components 1-4 are monitored by a FDI scheme. Each component is monitored by one FDI channel. The FTC system will switch to a backup controller in case of the first alarm in FDI channels.

	Left Aileron	Right Aileron	Left Elevator	Right Elevator	Upper Rudder	Lower Rudder
i	1	2	3	4	5	6

Table 1: Numbering Components for the Redesigned Actuation System

The FDI scheme monitoring the actuation system is assumed to be a model-based algorithm. A FDI channel on component i is compromised of two parts: a filter that generates a residual $r_i(k)$ and a decision function which determines the logic signal $d_i(k)$ that indicates the status of actuator i. The filter output,

$r_i(k)$, is a random variable which is designed to achieve a decoupling property: $r_i(k)$ has a zero mean when the primary actuator is operational ($x_i(k) = 1$) and a non-zero mean when a failure occurs ($x_i(k) = 0$). The decision logic generates the status signal $d_i(k)$ based on $r_i(k)$. There are many different approaches to design the FDI algorithm [19, 20]. The FDI channel on component i used in the current FTC design is shown in Figure 3. At each sample time k, actuator i moves the control surface based on a control input $u_i(k)$, which is a pulse-width modulation signal. The real control surface position $s_i(k)$ is directly measured. Suppose the actuator dynamics are perfectly known. An estimated control surface position can be computed based on the control input $u_i(k)$ and the actuator model Act_{model}. The residual $r_i(k)$ is generated from the difference between the measured and estimated control surface positions. Assume any disturbances on the primary actuator are negligible. Moreover, the noise affecting the measurement $s_i(k)$ is assumed to be the same for all i, and is modeled by an independent and identically distributed (i.i.d.) Gaussian process $v(k)$ with zero mean and variance σ^2. Finally, the failure on actuator i that occurs when $x_i(k) = 0$ is modeled by an additive bias f_i subject to $s_i(k)$. Given these assumptions, the FDI residual $r_i(k)$ is modeled as:

$$r_i(k) = v(k) + (1 - x_i(k))\, f_i \tag{23}$$

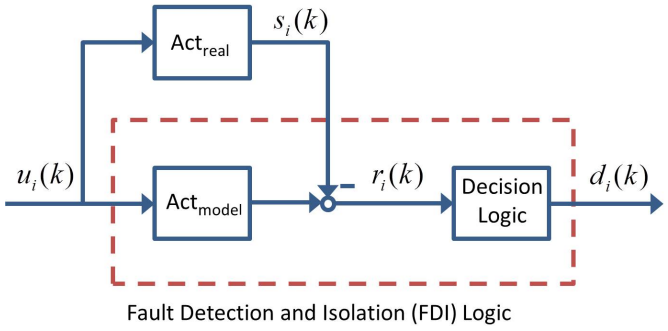

Figure 3: Fault Detection and Isolation (FDI) logic monitoring component i

The decision logic uses a constant thresholding:

$$d_i(k) := \begin{cases} 0 & \text{if } |r_i(k_0)| > H_i \text{ for some } k_0 \leq k \\ 1 & \text{else} \end{cases} \tag{24}$$

A failure is declared in actuator i when the residual magnitude exceeds the threshold H_i. After that, $d_i(k)$ remains at 0. This fault detection logic is i.i.d. in time before its first detection.

4.2. Required Information

To analyze the system reliability of the FTC structure presented in Section 4.1, we need to specify hardware failure models and FDI performance metrics. In this paper, the actuator failure time is assumed

to be governed by a continuous-time exponential distribution with a parameter $\lambda = \frac{1}{MTBF}$, where $MTBF$ is the mean time between failures. The exponential distribution is a simple but reasonably realistic model. Moreover, for UAV applications, the mission time is much shorter than the MTBF of components. It may not be necessary to consider aging (Weibull distribution) in this case. The exponential distribution can then be approximated using a discrete-time geometric distribution with a parameter $q := 1 - e^{-\lambda \Delta_t}$ [50] where Δ_t is the flight computer sample time 0.02 sec. Notice that Δ_t is determined by the flight computer sampling frequency. Hence, the discrete failure time $T_{X,i}$ $(i = 1, \ldots, n)$ has the probability mass function:

$$P[T_{X,i} = k] = (1 - q)^{k-1} q \tag{25}$$

Then the component failure probability $P[T_{X,i} \leq N]$ can be computed by:

$$P[T_{X,i} \leq N] = 1 - (1 - q)^N \tag{26}$$

Note that for $q \ll 1$, $P[T_{X,i} \leq N] \approx Nq$. Since all the components have the same reliability, $\hat{q}$ is used to denote the component failure probability per hour. This is similar to the notation introduced in (16). Then the component failure rate q can be estimated from the component failure probability per hour $\hat{q}$.

The FDI channels are statistically independent from each other. Each FDI channel signal $d_j(k)$ is i.i.d. in time before its first detection. For FDI channel j (j corresponds to a component failure mode $M_j \in \mathcal{D}$) , let $P_{F,j} := P[d_j(k) = 0 \mid x_j(k) = 1, d_j(k-1) = 1]$ and $P_{D,j} := P[d_j(k) = 0 \mid x_j(k) = 0, d_j(k-1) = 1]$. The probabilities $P_{F,j}$ and $P_{D,j}$ denote the single-frame probability of false alarm and detection, respectively. The residual is Gaussian at each time:

$$P_{F,j} = 1 - \int_{-H_j}^{H_j} \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{r^2}{2\sigma^2}} dr \tag{27}$$

$$P_{D,j} = 1 - \int_{-H_j}^{H_j} \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(r - f_j)^2}{2\sigma^2}} dr \tag{28}$$

These single-frame probabilities can be accurately and efficiently computed using the error function `erf` in `Matlab`. The multiple-frame FDI performance probabilities can be related to these single-frame probabilities due to the assumption of FDI logic being independent in channel and i.i.d. in time before the first detection. In addition, they are not affected by any actuator failure modes in $\mathcal{C}$. First, we know $\mathcal{C} = \{M_5, M_6\}$. For $M_j \in \mathcal{C}$, $P\left[T_D \leq N \;\middle|\; \mathbf{x}(N) = M_j\right]$ is the conditional probability that at least one FDI channel triggers a false alarm in the N-step window in case of no failures in the actuators monitored by the FDI scheme:

$$P\left[T_D \leq N \;\middle|\; \mathbf{x}(N) = M_j\right] = 1 - \prod_{i: M_i \in \mathcal{D}} (1 - P_{F,i})^N \tag{29}$$

which is the same for $j = 5, 6$ in our example.

Next, consider $M_j \in \mathcal{D}$. We know that $P\left[\{T_{D,j} \geq k + N_j\} \;\middle|\; \{T_{X,j} = k, \min_{i \neq j} T_{X,i} > N\}\right]$ is the conditional probability that a failure is not declared in the FDI channel j in the first $k + N_j - 1$ time steps given that the actuator j failed at time k. This probability is expressed as:

$$P\left[\{T_{D,j} \geq k + N_j\} \;\middle|\; \{T_{X,j} = k, \min_{i \neq j} T_{X,i} > N\}\right] = (1 - P_{F,j})^{k-1}(1 - P_{D,j})^{N_j} \tag{30}$$

Finally, $P\left[\{T_D < T_{D,j} < k + N_j\} \;\middle|\; \{T_{X,j} = k, \min_{i \neq j} T_{X,i} > N\}\right]$ is the probability that the FDI channel j triggers an alarm before time $k + N_j$ given actuator j failed at time k, but other FDI channels triggered at least one alarm before the alarm in channel j so that the FTC structure does not switch to the right backup controller. This probability is quantified by:

$$\begin{aligned}
&P\left[\{T_D < T_{D,j} < k + N_j\} \;\middle|\; \{T_{X,j} = k, \min_{i \neq j} T_{X,i} > N\}\right] \\
=&\sum_{l=1}^{k+N_j-2} P\left[\{T_D = l, l < T_{D,j} < k + N_j\} \;\middle|\; \{T_{X,j} = k, \min_{i \neq j} T_{X,i} > N\}\right] \\
=&\sum_{l=1}^{k-1} \left(\prod_{i:M_i \in \mathcal{D}, i \neq j} (1 - P_{F,i})^{l-1} P_{F,i} \right) (1 - P_{F,j})^{l} \left(1 - (1 - P_{F,j})^{k-l-1}(1 - P_{D,j})^{N_j}\right) \\
+&\sum_{l=k}^{k+N_j-2} \left(\prod_{i:M_i \in \mathcal{D}, i \neq j} (1 - P_{F,i})^{l-1} P_{F,i} \right) (1 - P_{F,j})^{k-1}(1 - P_{D,j})^{l-k+1} \left(1 - (1 - P_{D,j})^{N_j - l + k - 1}\right)
\end{aligned} \tag{31}$$

The first term refers to the early false alarm metric and the second is the missed isolation metric. Finally we can substitute (25)-(31) into (9) to solve the system failure probability $P[T \leq N]$.

4.3. Numerical Results

Two benchmark architectures based only on physical redundancy are presented. In addition to these benchmarks we also analyze a FTC structure using the techniques described in this paper. The reliability of the two physically redundant designs are useful as comparisons for the third, FTC-based design.

The first benchmark is the four-servo actuation system design introduced in Section 2.2. In this case, each of the four control surfaces (left aileron, right aileron, elevator, and rudder) is actuated by its own servo. Hence, four actuators are used. As analyzed in Section 2.2, this four-actuator design has a per-hour failure probability of 10^{-2}. We can replace each actuator in this four-actuator design with a triplex redundant actuation subsystem to improve the reliability. This is the second benchmark we consider. In this case, each of the four control surfaces (left aileron, right aileron, elevator, and rudder) is actuated by three servos. This is a twelve-actuator design. The actuation subsystem for each control surface has a "2-out-of-3: good" structure [4]. As discussed in Section 2.2, the component failure probability per hour was estimated to be

$\hat{q} = 2.5 \times 10^{-3}$ [26]. The triplex actuation subsystem fails if two of the three actuators fail and thus the failure probability per hour for such a triplex subsystem is $3\hat{q}^2(1-\hat{q}) + \hat{q}^3 = 1.875 \times 10^{-5}$. The system failure probability per hour for the twelve-actuator design is $4 \times (1.875 \times 10^{-5}) = 7.5 \times 10^{-5}$.

Next we consider the FTC design with six control surfaces each actuated by its own actuator as described in Section 4.1. The reliability of this six-actuator FTC design is compared to the four-actuator and twelve-actuator benchmarks. Recall the system runs at a 50Hz sample rate and $N = 1.8 \times 10^5$ corresponds to the one hour window. Since the component failure probability per hour is $\hat{q} = 2.5 \times 10^{-3}$, the component failure rate is estimated to be $q \approx 1.39 \times 10^{-8}$. For illustrative purposes, the maximum detection delay is specified as $N_j = 10$ for $j = 1, 2, 3, 4$. In practical applications, the maximum detection delay depends on the specific design of control algorithms. Given a primary controller and a backup controller, one can simulate the reconfiguration process for any specific detection delay. When the detection delay is large enough, the simulated results will show that the aircraft becomes unstable after the failure occurs. In this case, the FTC design cannot reconfigure the aircraft successfully. The largest detection delay which does not lead to such situations is determined from the simulations, and used as the maximum detection delay.

Applying the procedure introduced in Section 4.2, the system failure probability of the six-actuator FTC system can be computed for specific values of the residual variance σ^2, failure bias level f_j, and threshold H_j. First, we assume that the failure bias and FDI thresholds are all the same, i.e. $f_j = f$ and $H_j = H$. Figure 4 shows the six-actuator FTC system failure probability $P[T \leq N]$ as a function of the normalized threshold H/σ for two values of the normalized failure bias level f/σ =1 and 10. The vertical axis is a log-scale to highlight the changes in system performance as a function of the threshold. For f/σ =10, the Monte Carlo verification is performed at several testing points and the results are also plotted in Figure 4. For small thresholds the system will rarely have a missed detection, but will often trigger a false alarm. As a result, for small thresholds, the FTC system will have low reliability. For any $M_j \in \mathcal{C}$, the false alarm directly leads to a system failure because the FTC switches to a back-up controller not designed for these modes. For any $M_j \in \mathcal{D}$, the FTC has a 25% chance to switch to the right controller K_j due to an early false alarm in FDI channel j, and a 75% chance to switch to an incorrect backup controller due to an early false alarm in other FDI channels. Based on this discussion, the system failure probability for small thresholds can be estimated as the sum of $2\hat{q}$ (due to $M_j \in \mathcal{C}$) and $\frac{3}{4} \times 4\hat{q}$ (due to $M_j \in \mathcal{D}$). Hence the system failure probability $P[T \leq N] \approx (2 + \frac{3}{4} \times 4)\hat{q} = 1.25 \times 10^{-2}$. We can see this is even worse than the four-actuator design because now there are two more components that can fail. Notice when H is extremely small, the analysis result is not accurate. Specifically, we assumed that multiple, simultaneous alarms are unlikely and this is no longer valid for extremely small thresholds. This inaccuracy is not of great significance as FDI systems would not be designed with such extremely low thresholds in practice. For large thresholds, the system will rarely have a false alarm but it will also frequently have missed detections when failures occur. Any $M_j \in \mathcal{C}$ will not lead to a system failure in this case. But any $M_j \in \mathcal{D}$ will lead to a system failure.

Thus the FTC system failure probability for large thresholds is approximately $P[T \leq N] \approx 4\hat{q} = 10^{-2}$.

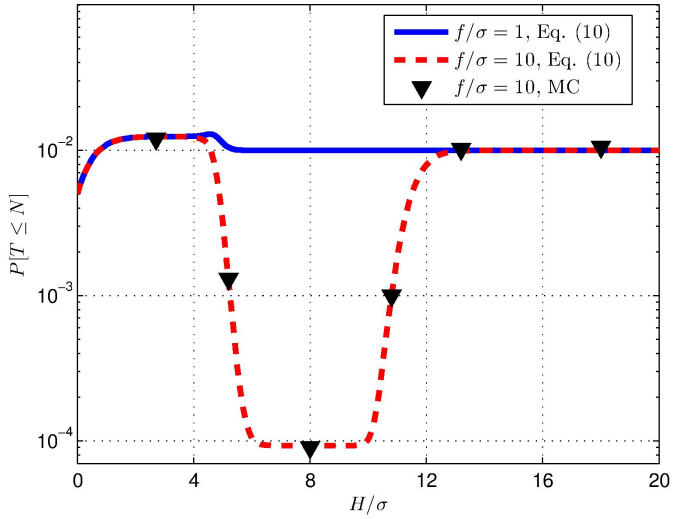

Figure 4: $P[T \leq N]$ vs. H/σ when $H_j = H$ for all j

For intermediate values of the threshold, the system failure probability depends on the ratio of the failure bias to noise level. For large failure bias levels ($f/\sigma = 10$) the threshold can be chosen to achieve a system failure probability near 9.3×10^{-5}. This probabilistic performance is close to the reliability achieved by the twelve-actuator design. This means that the FTC technique can potentially improve the system level reliability if the failure bias size is not small and the FDI scheme is properly designed. Notice that there is an interval of threshold values which will lead to the optimal system reliability in this case. The length of this interval can be potentially used to quantify the robustness of the FDI design.

For f/σ =10, the Monte Carlo simulations are performed at several testing points. Figure 4 shows that the Monte Carlo simulations give almost identical results as the proposed analysis method. While the system failure probability can be computed by our proposed method simultaneously on a standard desktop, the Monte Carlo simulations are time consuming. For example, Monte Carlo simulations require 5×10^4 replications to estimate the system failure probability when $H/\sigma = 2.7$. For each replication, the FDI residuals will be generated on the N-step time window, and this leads to a long computational time since N is quite large in our problem. We implement the Monte Carlo simulations in `Matlab`, and the computational time for 5×10^4 replications is roughly 20 minutes. For $H/\sigma = 5.2$, the system failure probability is smaller, and we roughly require 5×10^5 replications and 4 hours to get an accurate estimate of the system failure probability. Moreover, the Monte Carlo simulations for $H/\sigma = 8$ require 5×10^6 replications which take about 40 hours. Since Figure 4 shows that our proposed analysis method is consistent with the Monte Carlo simulations, we will only apply our proposed method from now on.

Given $f = 10\sigma$, the previous result tells us that high FTC system reliability will be achieved at the

optimal threshold $H = 8.4\sigma$. Now we fix $f_j = 10\sigma$ and $H_j = 8.4\sigma$ for $j = 1, 2, 3$. We want to understand how the system reliability changes if one FDI channel has significantly different levels of performance. Figure 5 shows $P[T \leq N]$ as a function of the normalized threshold H_4/σ for two values of the normalized failure bias level f_4/σ =1 and 10. We can see a similar trend as before. For small thresholds the system will always trigger an alarm in FDI channel 4 and switch to controller K_4. As a result, all $M_j \in \mathcal{M}_1$, except M_4, will lead to a system failure due to the false alarm in FDI channel 4. Hence the system failure probability $P[T \leq N] \approx 5\hat{q} = 1.25 \times 10^{-2}$. Again, this results in a worse system failure probability than the four-actuator design. For large thresholds, the system will rarely have a false alarm in FDI channel 4. However, it will also frequently have missed detections when failures in component 4 occur. M_4 will lead to a system failure in this case. Thus, the FTC system failure probability $P[T \leq N] \approx 2.5 \times 10^{-3}$. For intermediate values of the threshold and relatively large failure bias size, the FDI channel 4 will have good performance and improve the system reliability given proper FDI designs. In this example, we can see the poor performance in any of the FDI channels can severely degrade the system reliability. Hence we need to design a FDI scheme with good performance in all channels so that the system reliability can be improved.

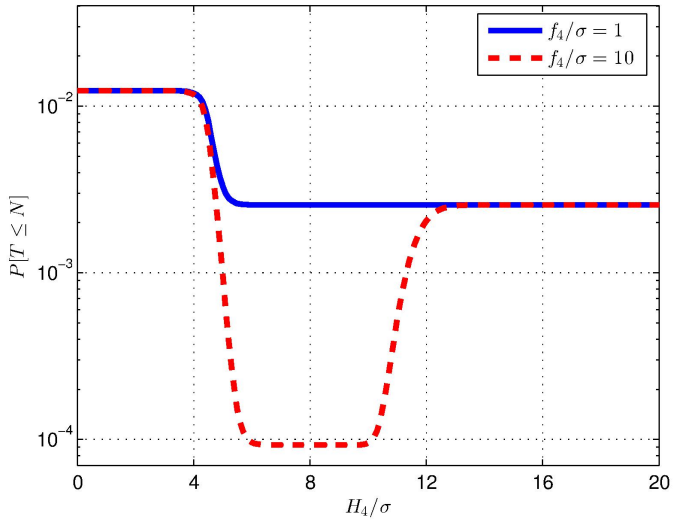

Figure 5: $P[T \leq N]$ vs. H_4/σ when $f_j = 10\sigma$ and $H_j = 8.4\sigma$ for $j = 1, 2, 3$

The results in Figure 5 indicate the importance of proper threshold selection. In addition, Figure 5 shows that for $f_4/\sigma = 10$ the optimal threshold is $H_4^* = 8.4\sigma$ and this yields the optimal performance of $P^*[T \leq N] \approx 9.3 \times 10^{-5}$ for this failure bias level. More generally, let $H_4^*(f_4/\sigma)$ denote the threshold that minimizes $P[T \leq N]$ for a given failure bias level f_4/σ. Since (20) introduced $\hat{P}_{B,4}$ as a measure for the performance of FDI channel 4, now $\hat{P}^*_{B,4}$ denotes the performance metric of FDI channel 4 computed with the optimal threshold. Figure 6 shows the optimal performance $P^*[T \leq N]$, the associated normalized threshold H_4^*/σ and the associated $\hat{P}^*_{B,4}$ as a function of the failure bias level. As expected, the optimal performance

$P^*[T \leq N]$ decreases monotonically with increasing failure bias level. The FDI scheme is able to detect larger failure bias levels (relative to the noise) more easily thus leading to reduced false alarms and missed detections for a properly optimized threshold. Figure 6 also shows the limits of performance for the current model-based FDI scheme. In particular, for small failure bias levels ($f_4/\sigma \leq 3$) the failure probability of the FTC system is 2.5×10^{-3} even if the optimal threshold is chosen. This implies that more advanced filter techniques and decision functions are required if the failure bias level is small relative to the noise. We can also evaluate the performance of the FDI channel 4 based on the simplifying approximations. Recall (22) is a rough requirement for good performance in FDI channel 4. Hence $\hat{P}^*_{B,4} \ll 9.3\times10^{-2}/(6\times2.5) = 6.2\times10^{-3}$ is a rough design requirement. From Figure 6 we roughly see when $f_4 = 6\sigma$, the FTC failure probability approaches its lower bound ($P^*[T \leq N] = 9.8 \times 10^{-5} \approx 9.3 \times 10^{-5}$). The associated $\hat{P}^*_{B,4} = 1.3 \times 10^{-3}$ is shown by the squared locations in Figure 6. We can see $1.3 \times 10^{-3} \ll 6.2 \times 10^{-3}$, and our proposed design requirement is satisfied. As expected, the FDI system failure probability achieves its lower bound when the requirement (22) is satisfied. Furthermore, (22) and (29) show that a very low single-frame probability of false alarm is required for good FDI performance.

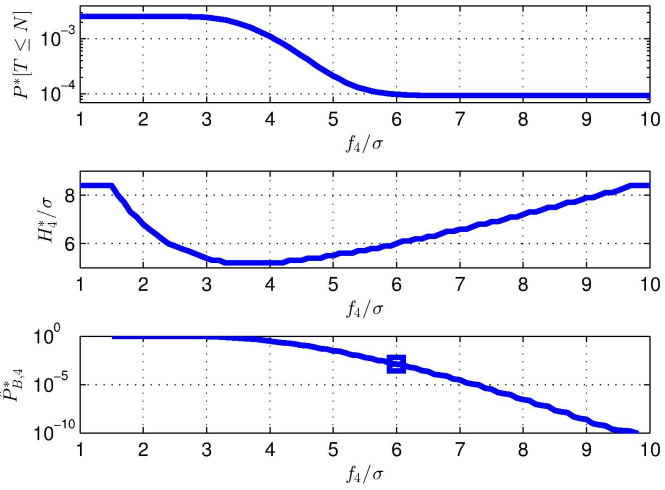

Figure 6: Optimal performance $P^*[T \leq N]$, threshold H_4^*/σ and FDI metric $\hat{P}^*_{B,4}$ vs. f_4/σ

5. Conclusion

This paper analyzes the reliability of a FTC system. Specifically, an actuation system is considered along with a model-based FDI scheme used to monitor the component states. The system failure probability per hour can be exactly computed provided that certain probabilistic information is known for actuator failures and FDI performance. We also derive a simplifying approximation in the case that only restricted hardware and FDI performance information is known. We apply the proposed analysis method to a UAV actuation system. Numerical results are presented to highlight the overall impacts of FTC design on the UAV reliability,

and the FDI design trade-offs. The proposed method is verified by Monte Carlo simulations. Our results show that the FTC technique can significantly improve the system reliability given good FDI performance.

The results in this paper focus on the analysis of FTC systems. We have not addressed the design and validation of the backup controllers for the UAV considered in the case study. That task is more related to the control design theory, and will also be part of our future work in this area. In the example presented in this paper, the FDI channels are independent from each other. There are also no time correlations in the FDI residuals. In principle, our proposed method can be used to handle the correlations in FDI residuals. However, the computation of FDI performance metrics for complex FDI schemes is worthy of separate research efforts. For many FDI schemes, the FDI performance metrics can be formulated as a first hitting time problem of stochastic processes or rare event analysis problem. Potential solutions for this topic include importance sampling [51], Poisson clumping heuristic [52], and peak over threshold approach [53]. In the future, we will consider applying those candidate solutions to more complex FDI designs. Moreover, phase mission models [54] and multi-state models [55, 56] have received increased attention from reliability engineers. Integration of our approach with these general models will be considered in future work.

Acknowledgments

This work was partially supported by the National Science Foundation under Grant No. NSF-CMMI-1254129 entitled "CAREER: Probabilistic Tools for High Reliability Monitoring and Control of Wind Farms." It was also partially supported by the NASA Langley NRA Cooperative Agreement NNX12AM55A entitled "Analytical Validation Tools for Safety Critical Systems Under Loss-of-Control Conditions", Dr. Christine Belcastro technical monitor. Any opinions, findings, and conclusions or recommendations expressed in this paper are those of the authors and do not necessarily reflect the views of the NSF or NASA.

Appendix A. Proofs of Lemmas

Proof of Lemma 1. We only need to show that $\{\mathbf{x}(N) = M_j\} \subset \{T \leq N\}$ given $M_j \in \mathcal{C}^c \cap \mathcal{D}^c \cap \mathcal{M}_0^c$. We can see this directly from Definition 1. If $M_j \in \mathcal{C}^c \cap \mathcal{D}^c \cap \mathcal{M}_0^c$, then $\phi_i(M_j) = 0$ for all i. We can set $k_0 = N$ and get $\phi(\mathbf{x}(k_0), k_0) = 0$. Hence $T \leq N$. □

Proof of Lemma 2. We will first show that if $T_D \leq N$ and $\mathbf{x}(N) = M_j$, then $T \leq N$. Given $M_j \in \mathcal{C}$, we know $\phi_i(M_j) = 0$ for all $i \neq 0$. Since $T_D \leq N$, $\phi(\mathbf{x}(N), N) = \phi_i(M_j)$ for certain $i \neq 0$. We have $\phi(\mathbf{x}(N), N) = 0$. Set $k_0 = N$. We directly get $T \leq N$.

Now we will show that if $T \leq N$ and $\mathbf{x}(N) = M_j$, then $T_D \leq N$. We will use contradiction. Assume $T_D > N$. Then $\phi(\mathbf{x}(k), k) = \phi_0(\mathbf{x}(k)) = 1$ for all $k \leq N$. Clearly $T > N$ in this case and this contradicts the assumption $T \leq N$. This completes the proof. □

Proof of Lemma 3. First we need to show that if $M_j \in \mathcal{D}$, then:

$$\begin{aligned} P[\{T \le N\} \cap \{\mathbf{x}(N) = M_j\}] = P\left[\{T_{D,j} \ge T_{X,j} + N_j\} \cap \{\mathbf{x}(N) = M_j\}\right] \\ + P\left[\{T_D < T_{D,j} < T_{X,j} + N_j\} \cap \{\mathbf{x}(N) = M_j\}\right] \end{aligned} \tag{A.1}$$

We will show that if $T_{D,j} \ge T_{X,j} + N_j$ and $\mathbf{x}(N) = M_j$, then $T \le N$. $T_{D,j} \ge T_{X,j} + N_j$ implies that $\phi(M_j, k) \ne \phi_j(M_j)$ for all $k \le T_{X,j}+N_j-1$. Set $k_0 = T_{X,j}$, we have $\phi(\mathbf{x}(k), k) = 0$ for all $k_0 \le k \le k_0+N_j-1$ and hence $T \le N$.

Next, we show that if $T_D < T_{D,j} < T_{X,j} + N_j$ and $\mathbf{x}(N) = M_j$, then $T \le N$. Since $T_D < T_{D,j}$, we know $\phi(M_j, k) \ne \phi_j(M_j)$ for all k. Set $k_0 = T_{X,j}$ and $\phi(M_j, k) = 0$ for all $k \ge k_0$. Therefore, $T \le N$.

Finally, we need to show that if $T \le N$ and $\mathbf{x}(N) = M_j$, then $T_{D,j} \ge T_{X,j}+N_j$ or $T_D < T_{D,j} < T_{X,j}+N_j$. We will prove this by contradiction. Suppose $T_{D,j} < T_{X,j} + N_j$ and $T_{D,j} \le T_D$. Since we always have $T_D \le T_{D,j}$, now $T_D = T_{D,j} < T_{X,j} + N_j$. Since the probability of multiple alarms at the same time step given single or no component failures is assumed to be negligible, we have $\phi(\mathbf{x}(k), k) = \phi_0(\mathbf{x}(k))$ for $k < T_D$ and $\phi(\mathbf{x}(k), k) = \phi_j(\mathbf{x}(k))$ for $k \ge T_D$, given that $\mathbf{x}(N) = M_j$. Therefore, $\phi(\mathbf{x}(k), k) = 1$ for all $k < T_{X,j}$ and $k \ge T_D$. Since $T_D < T_{X,j} + N_j$, we have $T_D - T_{X,j} < N_j$. Hence $\phi(\mathbf{x}(k), k) = 0$ for at most $(N_j - 1)$ steps during $k \le N$. Hence $T > N$. This contradicts the condition $T \le N$. We get the desired contradiction.

Now we can connect (A.1) to the FDI performance metrics presented in Section 2.3 using the law of total probability. Notice that $\{T_{X,j} = k : k = 1, 2, \ldots\}$ form a disjoint partition of the sample space, and $P[\mathcal{A} \cap \{T_{X,j} \le N\} \cap \{T_{X,j} = k\}] = 0$ for all $k > N$. Hence the first term on the right hand side of (A.1) is:

$$\begin{aligned} & P\left[\{T_{D,j} \ge T_{X,j} + N_j\} \cap \{\mathbf{x}(N) = M_j\}\right] \\ =& \sum_{k=1}^{N} P\left[\{T_{D,j} \ge k + N_j\} \cap \{T_{X,j} = k\} \cap \{\min_{i \ne j} T_{X,i} > N\}\right] \\ =& \sum_{k=1}^{N} P\left[\{T_{D,j} \ge k + N_j\} \;\middle|\; \{T_{X,j} = k, \min_{i \ne j} T_{X,i} > N\}\right] P[T_{X,j} = k, \min_{i \ne j} T_{X,i} > N] \end{aligned} \tag{A.2}$$

Similarly, the second term on the right hand side of (A.1) can be rewritten as:

$$\begin{aligned} & P\left[\{T_D < T_{D,j} < T_{X,j} + N_j\} \cap \{T_{X,j} \le N, \min_{i \ne j} T_{X,i} > N\}\right] \\ =& \sum_{k=1}^{N} P\left[\{T_D < T_{D,j} < k + N_j\} \cap \{T_{X,j} = k, \min_{i \ne j} T_{X,i} > N\}\right] \\ =& \sum_{k=1}^{N} P\left[\{T_D < T_{D,j} < k + N_j\} \;\middle|\; \{T_{X,j} = k, \min_{i \ne j} T_{X,i} > N\}\right] P[T_{X,j} = k, \min_{i \ne j} T_{X,i} > N] \end{aligned} \tag{A.3}$$

Substitute (A.2) and (A.3) into (A.1), and sum over $\{j : M_j \in \mathcal{D}\}$. This completes the proof. □

Appendix B. Derivation of Simplifying Approximations

We derive simplifying approximations for FDI missed detection metric as follows:

$$
\begin{aligned}
& P\left[\{T_{D,j} \geq k + N_j\} \;\middle|\; \{T_{X,j} = k, \min_{i \neq j} T_{X,i} > N\}\right] \\
& \overset{1}{=} P\left[\min_{1 \leq l \leq k+N_j-1} d_j(l) = 1 \;\middle|\; \{T_{X,j} = k, \min_{i \neq j} T_{X,i} > N\}\right] \\
& \overset{2}{\leq} P\left[\{\min_{k \leq l \leq k+N_j-1} d_j(l) = 1\} \;\middle|\; \{T_{X,j} = k, \min_{i \neq j} T_{X,i} > N\}\right] \\
& \overset{3}{=} P\left[\{\min_{1 \leq l \leq N_j} d_j(l) = 1\} \;\middle|\; \{T_{X,j} = 1, \min_{i \neq j} T_{X,i} > N\}\right] \\
& \overset{4}{=} P\left[\{T_{D,1} \geq 1 + N_j \;\middle|\; \{T_{X,j} = 1, \min_{i \neq j} T_{X,i} > N\}\right] = \hat{P}_{MD,j}
\end{aligned}
\tag{B.1}
$$

The first and fourth steps follow from the definition of $T_{D,j}$. The second step follows from the fact that the probability of any set is always greater than or equal to the probability of its own subset. Notice that $d_j(k)$ can be assumed to be a strong stationary process given no failure, and this leads to the third step. From (B.1), we immediately see that $\hat{P}_{MD,j}$ is an upper bound of the FDI missed detection metrics. To see this is a tight bound, we assume that given the condition $\{T_{X,j} = k, \min_{i \neq j} T_{X,i} > N\}$, we can ignore the dependence between the events $\{\min_{1 \leq l \leq k-1} d_j(l) = 1\}$ and $\{\min_{k \leq l \leq k+N_j-1} d_j(l) = 1\}$. Then we have:

$$
\begin{aligned}
& P\left[\{T_{D,j} \geq k + N_j\} \;\middle|\; \{T_{X,j} = k, \min_{i \neq j} T_{X,i} > N\}\right] \\
& = P\left[\{\min_{1 \leq l \leq k-1} d_j(l) = 1\} \;\middle|\; \{T_{X,j} = k, \min_{i \neq j} T_{X,i} > N\}\right] \hat{P}_{MD,j} \\
& = P\left[\{T_D \geq k \;\middle|\; \mathrm{x}(k-1) = M_0\right] \hat{P}_{MD,j} \geq (1 - \hat{P}_{F,0}) \hat{P}_{MD,j}
\end{aligned}
\tag{B.2}
$$

Since $1 - \hat{P}_{F,0} \approx 1$, we conclude (14) is valid. The derivations for simplifying approximations of the early false alarm case and the missed isolation case are almost identical to the above procedure, and are omitted.

References

[1] R. Bleeg, Commercial jet transport fly-by-wire architecture considerations, in: AIAA/IEEE Digital Avionics Systems Conference, 1988, pp. 399–406.

[2] R. Collinson, Introduction to Avionic Systems, 3rd Edition, Springer, 2011.

[3] Y. Yeh, Safety critical avionics for the 777 primary flight controls system, in: 20th Digital Avionics Systems Conference, 2001, pp. 1.C.2.1–1.C.2.11.

[4] M. Rausand, A. Høyland, System Reliability Theory: Models, Statistical Methods, and Applications, Wiley, 2004.

[5] W. Kuo, Optimal Reliability Modeling: Principles and Applications, Wiley, 2002.

[6] W. Vesely, J. Dugan, J. Fragola, Minarick, J. Railsback, Fault Tree Handbook with Aerospace Applications, Tech. rep., National Aeronautics and Space Administration (2002).

[7] W. Lee, D. Grosh, A. Tillman, C. Lie, Fault tree analysis, methods, and applications: a review, IEEE Transactions on Reliability 34 (3) (1985) 194–203.

[8] D. Jerkins, B. Vasign, The Economic Impact of Unmanned Aircraft Systems Integration in the United States, 2013.

[9] Fourthwing Vireo, http://www.fourthwing.com/assets/pdfs/Vireo.pdf (2015).

[10] Sensefly Ebee, https://www.sensefly.com/drones/ebee.html (2015).

[11] FAA Modernization and Reform Act of 2012, H.R. 658, 112th Congress, 2nd Session.

[12] G. Ducard, Fault-tolerant Flight Control and Guidance Systems: Practical Methods for Small Unmanned Aerial Vehicles, Springer, 2009.

[13] H. Alwi, C. Edwards, C. Tan, Fault Detection and Fault-Tolerant Control Using Sliding Modes, Springer-Verlag, 2011.

[14] Y. Zhang, J. Jiang, Bibliographical review on reconfigurable fault-tolerant control systems, Annual Reviews in Control 32 (2008) 229–252.

[15] P. Weber, B. Boussaid, A. Khelassi, D. Theilliol, C. Aubrun, Reconfigurable control design with integration of a reference governor and reliability indicators, Int. J. Appl. Math. Comput. Sci. 22 (1) (2012) 139–148.

[16] W. Sun, H. Pan, J. Yu, H. Gao, Reliability control for uncertain half-car active suspension systems with possible actuator faults, IET Control Theory & Applications 8 (9) (2014) 746–754.

[17] S. Gayaka, B. Yao, Output feedback based adaptive robust fault-tolerant control for a class of uncertain nonlinear systems, Journal of Systems Engineering and Electronics 22 (1) (2011) 38–51.

[18] J. Chen, R. Patton, Robust Model-Based Fault Diagnosis for Dynamic Systems, Kluwer, 1999.

[19] R. Isermann, Fault-Diagnosis Systems: An Introduction from Fault Detection to Fault Tolerance, Springer-Verlag, 2006.

[20] S. Ding, Model-Based Fault Diagnosis Techniques: Design Schemes, Algorithms, and Tools, Springer-Verlag, 2008.

[21] E. Zio, Reliability engineering: Old problems and new challenges, Reliability Engineering & System Safety 94 (2) (2009) 125 – 141.

[22] University of Minnesota UAV research group, http://www.uav.aem.umn.edu/ (2015).

[23] A. Dorobantu, W. Johnson, F. A. Lie, B. Taylor, A. Murch, Y. C. Paw, D. Gebre-Egziabher, G. Balas, An airborne experimental test platform: From theory to flight, in: American Control Conference, 2013, pp. 659–673.

[24] F. A. Lie, A. Dorbantu, B. Taylor, D. Gebre-Egziabher, P. Seiler, G. Balas, An airborne experimental test platform: From theory to flight (part 1), InsideGNSS (2014) 44–58.

[25] F. A. Lie, H. Mokhtarzadeh, P. Freeman, J. Larson, T. Layh, B. Hu, B. Taylor, D. Gebre-Egziabher, P. Seiler, G. Balas, An airborne experimental test platform: From theory to flight (part 2), InsideGNSS (2014) 40–47.

[26] J. Amos, E. Bergquist, J. Cole, J. Phillips, S. Reimann, S. Shuster, UAV for reliability build, `www.aem.umn.edu/∼SeilerControl/SafetyCritical.shtml` (May 2014).

[27] H. Li, Q. Zhao, Z. Yang, Reliability modeling of fault tolerant control systems, Int. J. Appl. Math. Comput. Sci. 17 (4) (2007) 491 – 504.

[28] N. Wu, T. Chen, Reliability prediction for self-repairing flight control systems, in: 35th IEEE Conference on Decision and Control, Vol. 1, 1996, pp. 126–131.

[29] R. Butler, S. Johnson, Techniques for Modeling the Reliability of Fault-Tolerant Systems with the Markov State-Space Approach, Tech. rep., NASA Reference Publication 1348 (1995).

[30] E. Silva, P. Ochoa, State space exploration in Markov models, ACM SIGMETRICS Perf. Eval. Rev. 20 (1) (1992) 152–166.

[31] Y. Mo, A multiple-valued decision-diagram-based approach to solve dynamic fault trees, IEEE Transactions on Reliability 63 (1) (2014) 81–93.

[32] R. Peng, H. Mo, M. Xie, G. Levitin, Optimal structure of multi-state systems with multi-fault coverage, Reliability Engineering & System Safety 119 (0) (2013) 18 – 25.

[33] Q. Zhai, R. Peng, L. Xing, J. Yang, Binary decision diagram-based reliability evaluation of k-out-of-(n+ k) warm standby

systems subject to fault-level coverage, Proc IMechE Part O: J Risk and Reliability 227 (5) (2013) 540–548.

[34] H. Boudali, J. Dugan, A discrete-time Bayesian network reliability modeling and analysis framework, Reliability Engineering & System Safety 87 (2005) 337–349.

[35] L. Xing, O. Tannous, J. Dugan, Reliability analysis of nonrepairable cold-standby systems using sequential binary decision diagrams, IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans 42 (3) (2012) 715–726.

[36] R. Rodríguez, J. Júlvez, J. Merseguer, Quantification and compensation of the impact of faults in system throughput, Proc IMechE Part O: J Risk and Reliability 227 (6) (2013) 614–628.

[37] H. Li, Q. Zhao, Reliability evaluation of fault tolerant control with a semi-Markov fault detection and isolation model, Journal of Systems and Control Engineering 80 (5) (2006) 329 – 338.

[38] N. Wu, Reliability analysis for AFTI-F16 SRFCS using ASSIST and SURE, in: American Control Conference, Vol. 6, 2002, pp. 4795–4800.

[39] N. Wu, Coverage in fault-tolerant control, Automatica 40 (4) (2004) 537 – 548.

[40] J. Åslund, J. Biteus, E. Frisk, M. Krysander, L. Nielsen, Safety analysis of autonomous systems by extended fault tree analysis, International Journal of Adaptive Control and Signal Processing 21 (2-3) (2007) 287–298.

[41] S. Maza, Dynamic modelling and simulation of fault-tolerant systems based on stochastic activity networks, Proc IMechE Part O: J Risk and Reliability 226 (5) (2012) 455–463.

[42] S. Maza, Stochastic activity networks for performance evaluation of fault-tolerant systems, Proc IMechE Part O: J Risk and Reliability 228 (3) (2014) 243–253.

[43] P. Weber, D. Theilliol, C. Aubrun, Component reliability in fault-diagnosis decision making based on dynamic Bayesian networks, Proc IMechE Part O: J Risk and Reliability 222 (2) (2008) 161–172.

[44] C. Bonivento, M. Capiluppi, L. Marconi, A. Paoli, C. Rossi, Reliability evaluation for fault diagnosis in complex systems, in: SafeProcesses, Vol. 6, 2006, pp. 1330–1335.

[45] S. Maza, Diagnosis modelling for dependability assessment of fault-tolerant systems based on stochastic activity networks, Quality and Reliability Engineering International (2014) online.

[46] B. Hu, P. Seiler, A probabilistic method for certification of analytically redundant systems, Int. J. Appl. Math. Comput. Sci. 25 (1) (2015) 103 – 116.

[47] P. Freeman, G. Balas, Actuation failure modes and effects analysis for a small UAV, in: American Control Conference, 2014, pp. 1292–1297.

[48] I. Sadeghzadeh, Y. Zhang, Actuator fault-tolerant control based on gain-scheduled PID with application to fixed-wing unmanned aerial vehicle, in: 2nd International Conference of Control and Fault-Tolerant Systems, 2013, pp. 342–345.

[49] R. Venkataraman, P. Seiler, Certification analysis for a model-based UAV fault detection system, in: AIAA Guidance, Navigation and Control Conference, 2015, pp. AIAA–2015–0857.

[50] T. Wheeler, P. Seiler, A. Packard, G. Balas, Performance analysis of fault detection systems based on analytically redundant linear time-invariant dynamics, in: Proceedings of the American Control Conference, 2011, pp. 214–219.

[51] G. Rubino, B. Tuffin, Rare Event Simulation using Monte Carlo Methods, Wiley, 2009.

[52] D. Aldous, Probability Approximations via the Poisson Clumping Heuristic, Springer-Verlag, 1989.

[53] P. Embrechts, C. Klüppelberg, T. Mikosch, Modelling Extremal Events for Insurance and Finance, Springer, 1997.

[54] J. Andrews, J. Poole, W. Chen, Fast mission reliability prediction for unmanned aerial vehicles, Reliability Engineering & System Safety 120 (0) (2013) 3 – 9.

[55] S. Li, S. Si, H. Dui, Z. Cai, S. Sun, A novel decision diagrams extension method, Reliability Engineering & System Safety 126 (0) (2014) 107 – 115.

[56] S. Li, S. Si, L. Xing, S. Sun, Integrated importance of multi-state fault tree based on multi-state multi-valued decision diagram, Proc IMechE Part O: J Risk and Reliability 228 (2) (2013) 200–208.