2011 American Control Conference
on O'Farrell Street, San Francisco, CA, USA
June 29 - July 01, 2011

Performance Analysis of Fault Detection Systems Based on Analytically Redundant Linear Time-Invariant Dynamics

Timothy J. Wheeler, Peter Seiler, Andrew K. Packard, and Gary J. Balas

Abstract— **In the aircraft industry, it is common to use physically redundant components to ensure that the overall system meets the necessary safety requirements. For systems where physical redundancy is impractical (e.g, Unmanned Aerial Vehicles), analytical redundancy can be used to reduce the number of components needed. However, it is more difficult to certify the safety of an analytically redundant system. This paper presents a performance analysis framework that applies to both physically and analytically redundant sensor systems with linear time-invariant dynamics and additive faults. The framework is used to compare and certify the performance of two air-data sensor examples—one with physically redundant altitude sensors, and another that exploits the analytical relationship between altitude, airspeed, and flight path angle. In both examples, a threshold fault detection scheme is used.**

I. Introduction

The aircraft industry has many years of experience designing systems driven by extremely stringent safety requirements. The system availability and integrity requirements for commercial flight control electronics are typically on the order of no more than 10^{-9} catastrophic failures per flight hour [1], [2]. The industry has converged to a design solution that is based almost exclusively on physical redundancy at all levels of the design. For example, the Boeing 777 control law software is implemented on three primary flight computing modules. Each computing module contains three dissimilar processors with control law software compiled using dissimilar compilers. The inertial and air data sensors have a similar level of redundancy [3], [4].

The designs used in the aircraft industry achieve extraordinarily high levels of availability and integrity. However, the use of physical redundancy dramatically increases system size, complexity, weight, and power consumption. Moreover, such systems are extremely expensive in terms of design and development costs, as well as the unit production costs. There is an increasing demand for high-integrity, but at the same time low cost, fault tolerant aerospace systems, e.g., Unmanned Aerial Vehicles and fly-by-wire in lower end business/general aviation aircraft. In such applications, analytical redundancy may be used to limit the number of sensors needed, but the ability to detect sensor failures may also be diminished. The use of analytical fault detection algorithms would represent a major shift away from the current design approach used by the aerospace industry. One critical aspect preventing this shift is the need to certify the airworthiness of safety-critical systems. In particular, there is a lack of tools to rigorously analyze the reliability for systems that use analytical redundancy.

This paper presents a framework for the rigorous performance analysis of fault detection schemes based on analytically redundant sensors with linear time-invariant (LTI) dynamics. It is shown that this framework also applies to physically redundant sensor systems with LTI dynamics. The performance analysis is carried out for a particular sensor example with little justification for the choice of numerical parameter values. The emphasis is on the method of analysis rather than the design of the particular sensor systems analyzed.

The outline of the paper is as follows: Section II demonstrates that both types of sensor systems have the same basic structure if the sensor dynamics are LTI. Using a thresholding fault detection scheme [5], [6], [7], probabilistic performance metrics for are defined for this common LTI system structure. Relevant results from reliability theory are presented in Section III. Section IV introduces an air-data sensor example, and the numerical performance analysis of the air-data example is presented in Section IV-C. Finally, conclusions and possible avenues of future research are discussed in Section V.

II. Problem Formulation

We begin by presenting a unified framework for analyzing physically and analytically redundant sensor systems with LTI sensor dynamics. Consider the physically redundant sensor system in Fig. 1. The two identical sensors have the same discrete-time LTI sensor dynamics S. Sensor 1 uses S to measure a quantity u and produce $\hat{m}$, while Sensor 2 uses the same S to measure u and produce $\tilde{m}$. Both sensors are affected by an i.i.d. Gaussian random process $\{v_{i,k}\}$ and a random fault signal $\{f_{i,k}\}$, such that the event $\{f_{i,k} = 0\}$ indicates that the Sensor i is in the nominal mode (i.e., no fault) at time k. The residual $\{r_k\}$ is defined as $r_k := \hat{m} - \tilde{m}$, for all k. In the absence of noises v_1 and v_2 and faults f_1 and f_2 the residual would be zero. Since the dynamics of S are LTI and the noises and faults enter additively, the overall system represented by Fig. 1 is also LTI.

Consider the analytically redundant sensor system in Fig. 2. As in the physically redundant case, the sensor dynamics S and T are discrete-time LTI systems; however, in this case, S and T are different. Again, for $i = 1, 2$, $\{v_{i,k}\}$ is an i.i.d. Gaussian noise and $\{f_{i,k}\}$ is a random fault signal. Sensor 1 uses S to measure some quantity u and produce

T. J. Wheeler and A. K. Packard are with Department of Mechanical Engineering, University of California, Berkeley. Email: twheeler@berkeley.edu and pack@me.berkeley.edu.

P. Seiler and G. J. Balas are with the Aerospace and Engineering Mechanics Department, University of Minnesota, Twin Cities. Email: seiler@aem.umn.edu and balas@umn.edu.

978-1-4577-0079-8/11/$26.00 ©2011 AACC

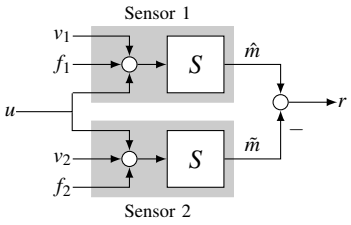

Fig. 1. Physically redundant sensor system with LTI sensor dynamics S, subject to noises v_1 and v_2 and random fault signals f_1 and f_2.

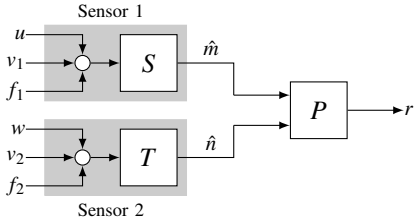

Fig. 2. Analytically redundant sensor system with LTI sensor dynamics S and T, subject to noises v_1 and v_2 and random fault signals f_1 and f_2. The LTI system P represents a dynamic analytical relationship between the quantities $\hat{m}$ and $\hat{n}$.

$\hat{m}$. Sensor 2 uses T to measure some other quantity w and produce $\hat{n}$. The block labeled P is an LTI system that represents the analytical relationship between $\hat{m}$ and $\hat{n}$. In the absence of noises and faults, the residual r produced by P acting on the inputs $\hat{m}$ and $\hat{n}$ is zero. Because S, T, and P are LTI and the noises and faults enter additively, the overall system represented by Fig. 2 is also LTI.

A. Performance Metrics

Since the physically redundant sensor system (Fig. 1) and the analytically redundant sensor system (Fig. 2) are both represented by discrete-time LTI dynamics, it suffices to consider the general case:

$$\begin{aligned} x_{k+1} &= Ax_k + B_u u_k + B_v v_k + B_f f_k, \\ r_k &= Cx_k + D_u u_k + D_v v_k + D_f f_k, \end{aligned} \tag{1}$$

where $\{u_k\}$ is a known sequence of physical quantities, $\{v_k\}$ is an i.i.d. Gaussian sequence with $v_k \sim \mathcal{N}(0,I)$, for all k, and $\{f_k\}$ is a random fault sequence. Assume that if $v_k = 0$ and $f_k = 0$, for all k, then the residual is zero (i.e., $r_k = 0$, for all k).

The performance metrics are defined with respect to a residual thresholding scheme. That is, a fault is declared if the magnitude of the residual exceeds some threshold. Applications of fixed thresholding [5], [6] and time-varying thresholding [7] have appeared in the literature. More concretely, the threshold function is defined as

$$\delta(r) := \mathbb{I}(|r| > \varepsilon),$$

where $\mathbb{I}$ is the indicator function and $\varepsilon > 0$ is the threshold. In this paper, we assume that a fixed threshold is used for all time.

At each time $k \geq 0$, define $H_{0,k} := \{f_k = 0\}$ to be the event that no fault is occurring and $H_{1,k} := \{f_k \neq 0\}$ to be the event that some fault is occurring. Similarly, define $R_{0,k} := \{\delta(r_k) = 0\}$ to be the event that the fault detector decides that no fault is occurring and $R_{1,k} := \{\delta(r_k) = 1\}$ to be the event that the fault detector decides that some fault is occurring. The performance of the threshold fault detector δ, with respect to system (1), is quantified by the probability of a *true negative*

$$p_k^{\mathrm{TN}} := \mathbb{P}(R_{0,k} \cap H_{0,k}), \tag{2}$$

the probability of a *false positive*

$$p_k^{\mathrm{FP}} := \mathbb{P}(R_{1,k} \cap H_{0,k}), \tag{3}$$

the probability of a *false negative*

$$p_k^{\mathrm{FN}} := \mathbb{P}(R_{0,k} \cap H_{1,k}), \tag{4}$$

and the probability of a *true positive*

$$p_k^{\mathrm{TP}} := \mathbb{P}(R_{1,k} \cap H_{1,k}), \tag{5}$$

where the names of these probabilities are taken from the statistical hypothesis testing literature [8], [9]. Collectively, we refer to these quantities as the *performance metrics* for the fault detector.

Although the probabilities (2)–(5) provide all the necessary information, their numerical values can be difficult to interpret. For example, suppose that $\mathbb{P}(H_{1,k}) \approx 0$ for $k = 0,1,\ldots,T$. This implies that

$$\mathbb{P}(H_{1,k}) = p_k^{\mathrm{FN}} + p_k^{\mathrm{TP}} \approx 0.$$

Since both p_k^{FN} and p_k^{TP} are small, it is difficult to get a sense of how well the fault detection scheme will perform in the presence of a fault at times $k \in \{0,1,\ldots,T\}$. In this case, it is beneficial to consider the relative magnitudes of p_k^{FN} and p_k^{TP}. This approach gives rise to two conditional probabilities: the probability of *detection*

$$p_k^{\mathrm{D}} := \mathbb{P}(R_{1,k} \,|\, H_{1,k}) = \frac{p_k^{\mathrm{TP}}}{p_k^{\mathrm{TP}} + p_k^{\mathrm{FN}}}, \tag{6}$$

and the probability of a *false alarm*

$$p_k^{\mathrm{F}} := \mathbb{P}(R_{1,k} \,|\, H_{0,k}) = \frac{p_k^{\mathrm{FP}}}{p_k^{\mathrm{FP}} + p_k^{\mathrm{TN}}}. \tag{7}$$

Note that, by rearranging equations (6) and (7), the performance metrics can be computed from p_k^{D}, p_k^{F} and $\mathbb{P}(H_{1,k})$.

B. Computational Procedure

For $k \geq 0$, define the notation $f_{0:k} := \{f_0, f_1, \ldots, f_k\}$. Assume that $\{f_k\}$ takes values in some finite set $\mathscr{F}$, so that $f_{0:k} \in \mathscr{F}^{k+1}$ can take only finitely many different values. Also, assume that $\mathbb{P}(f_{0:k} = \hat{f}_{0:k})$ is known (or easily computable), for all $\hat{f}_{0:k} \in \mathscr{F}^{k+1}$ and all $k \geq 0$. Fix a final time T. Note that, conditional on the event $\{f_{0:T} = \hat{f}_{0:T}\}$, the system (1) is linear-Gaussian. Thus, the conditional

distribution of the residual r_k given $\{f_{0:T} = \hat{f}_{0:T}\}$ is Gaussian, where the conditional mean is given by the recurrence

$$\begin{aligned} \hat{x}_{k+1} &:= \mathbb{E}(x_{k+1} \,|\, \{f_{0:T} = \hat{f}_{0:T}\}), \\ &= A\hat{x}_k + B_u u_k + B_f \hat{f}_k, \\ \hat{r}_k &:= \mathbb{E}(r_k \,|\, \{f_{0:T} = \hat{f}_{0:T}\}), \\ &= C\hat{x}_k + D_u u_k + D_f \hat{f}_k, \end{aligned} \tag{8}$$

and the conditional variance is given by

$$\begin{aligned} \Sigma_{k+1} &:= \mathbb{E}((x_{k+1} - \hat{x}_{k+1})(x_{k+1} - \hat{x}_{k+1})^T \,|\, \{f_{0:T} = \hat{f}_{0:T}\}), \\ &= A\Sigma_k A^T + B_v B_v^T, \\ \Lambda_k &:= \mathbb{E}((r_k - \hat{r}_k)^2 \,|\, \{f_{0:T} = \hat{f}_{0:T}\}), \\ &= C\Sigma_k C^T + D_v D_v^T. \end{aligned} \tag{9}$$

We assume that $\hat{x}_0$ and Σ_0 are known.

Since $f_{0:T}$ can only take finitely many discrete values, the performance metric p_k^{TN} can be written as

$$\begin{aligned} p_k^{\mathrm{TN}} &= \mathbb{P}(R_{0,k} \,|\, H_{0,k}) \mathbb{P}(H_{0,k}) \\ &= \sum_{\hat{f}_{0:k} \in \mathscr{G}^{k+1}} \left(\int_{-\varepsilon_k}^{\varepsilon_k} p(r_k \,|\, \hat{f}_{0:k}) \, \mathrm{d}r_k \right) \mathbb{P}(f_{0:k} = \hat{f}_{0:k}), \end{aligned}$$

where $\mathscr{G}^{k+1} := \{f_{0:k} \in \mathscr{F}^{k+1} : f_k = 0\}$ is the set of all fault signals that do not put the system in a fault mode at time k. The Gaussian conditional density $p(r_k \,|\, \hat{f}_{0:k})$, which is $\mathscr{N}(\hat{r}_k, \Lambda_k)$, is obtained by simulating (8) and (9) with the appropriate $\hat{f}_{0:k}$. Similarly, p_k^{FN} can be written as

$$p_k^{\mathrm{FN}} = \sum_{\hat{f}_{0:k} \in \mathscr{H}^{k+1}} \left(\int_{-\varepsilon_k}^{\varepsilon_k} p(r_k \,|\, \hat{f}_{0:k}) \, \mathrm{d}r_k \right) \mathbb{P}(f_{0:k} = \hat{f}_{0:k}),$$

where $\mathscr{H}^{k+1} = \{f_{0:k} \in \mathscr{F}^{k+1} : f_k \neq 0\}$ is the set of fault signals that put the system in a fault mode at time k. Since $\mathbb{P}(R_{1,k} \,|\, H_{0,k}) = 1 - \mathbb{P}(R_{0,k} \,|\, H_{0,k})$, p_k^{FP} can be written as

$$p_k^{\mathrm{FP}} = \sum_{\hat{f}_{0:k} \in \mathscr{G}^{k+1}} \left(1 - \int_{-\varepsilon_k}^{\varepsilon_k} p(r_k \,|\, \hat{f}_{0:k}) \, \mathrm{d}r_k \right) \mathbb{P}(f_{0:k} = \hat{f}_{0:k}).$$

Finally, p_k^{TP} is determined by

$$p_k^{\mathrm{TP}} = 1 - (p_k^{\mathrm{TN}} + p_k^{\mathrm{FP}} + p_k^{\mathrm{FN}}),$$

for all k. Thus, each performance metric is computed as a weighted sum of terms of the form $\int_{-\varepsilon}^{\varepsilon} p(r) \, \mathrm{d}r$, where $p(r)$ is a Gaussian density. Such terms are easily evaluated using the error function, which can be implemented accurately and efficiently as a rational approximation [10].

III. Fault Models & Reliability Theory

Let τ be a random variable that represents the failure time of some physical component, and let f and F be the probability density function (PDF) and cumulative density function (CDF) of τ, respectively. The *failure rate* is defined as the expected number of failures in some interval of time given that no failure has occurred yet. More precisely, the failure rate is defined as

$$\begin{aligned} \rho_{\Delta_t}(t) &:= \frac{\mathbb{P}(t < \tau \leq t + \Delta_t \,|\, \tau > t)}{\Delta_t} \\ &= \frac{F(t + \Delta_t) - F(t)}{\Delta_t (1 - F(t))}, \end{aligned}$$

for each t and Δ_t. Taking the limit as $\Delta_t \to 0$ yields the *hazard rate* at time t:

$$h(t) := \frac{f(t)}{1 - F(t)}.$$

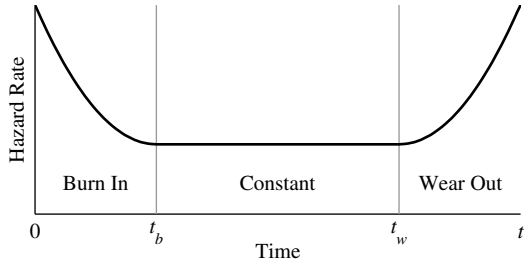

Fig. 3. The "bathtub curve" describes the hazard rate function of many real-world systems that have a burn-in phase (time 0 to t_b) and a wear-out phase (after time t_w).

In many applications, the hazard rate takes the shape of the "bathtub curve" shown in Fig. 3. Initially, the probability of a failure is high as the component is "burned in". Then, for a period of time, say t_b to t_w, the hazard rate is constant. Finally, after time t_w, the component begins to wear out and failures become more likely. Because failures may be rare, the empirically estimated failure rate for a long time interval may be the only available statistic for the component. Hence, it is common to assume that the component is in the middle of the bathtub curve where $h(t)$ is constant. See [11] for a more thorough discussion of reliability theory.

Suppose that the failure time of some component is modeled by an exponentially distributed random variable τ_c with parameter λ, which we write as $\tau_c \sim \mathrm{Exp}(\lambda)$. The PDF and CDF of τ_c are

$$f_c(t) := \lambda e^{-\lambda t}, \qquad F_c(t) := 1 - e^{-\lambda t},$$

respectively. Therefore, the hazard rate of τ_c is

$$h_c(t) = \frac{\lambda e^{-\lambda t}}{1 - (1 - e^{-\lambda t})} = \lambda.$$

Since the hazard rate of τ_c is constant, the exponential distribution is a useful model for the constant portion of the bathtub curve (t_b to t_w in Fig. 3). However, τ_c only applies to continuous-time models.

The discrete analog of the exponential distribution is the geometric distribution. Let Δ_t be the discrete sample time such that $k = t/\Delta_t$, and let τ_d be a geometric random variable with parameter q, which we write as $\tau_d \sim \mathrm{Geo}(q)$. The probability mass function (PMF) and CDF of τ_d are

$$f_d(k) := (1 - q)^{k-1} q, \qquad F_d(k) := 1 - (1 - q)^k,$$

respectively, for $k \geq 1$. Although the hazard rate is not well-defined in discrete time, the failure rate of τ_d at time $t = k\Delta_t$ is

$$\rho_{d,\Delta_t}(k) = \frac{q}{\Delta_t}.$$

Note that $\rho_{d,\Delta_t}(k)$ does not depend on k. To see the connection between τ_c and τ_d, consider the parameter value $\hat{q} = 1 - e^{-\lambda\Delta_t}$. The CDF of $\tau_d \sim \text{Geo}(\hat{q})$ is

$$F_d(k) = 1 - (e^{-\lambda\Delta_t})^k = 1 - e^{-\lambda k\Delta_t} = F_c(k\Delta_t),$$

and the failure rate is

$$\rho_{d,\Delta_t}(k) = \frac{\hat{q}}{\Delta_t} = \frac{1 - e^{-\lambda\Delta_t}}{\Delta_t} \approx \lambda - \frac{\lambda^2\Delta_t}{2} + \mathcal{O}(\Delta_t^2),$$

which converges to $h_c(t) = \lambda$ as $\Delta_t \to 0$. Hence, $\tau_d \sim \text{Geo}(\hat{q})$ is an accurate discrete representation of $\tau_c \sim \text{Exp}(\lambda)$, for small Δ_t. The following application utilizes this connection between the exponential and geometric distributions to model component failures.

IV. Application: Air-Data Probes

Nearly all aircraft flying today utilize air data probes to measure total and static pressure in order to determine airspeed and altitude. For proper operation, the probes must be free of any blockages, e.g. due to icing or dirt. Failures of these probes have resulted in numerous fatal accidents of commercial, military, and general aviation aircraft (e.g., Air France Flight 447 [12], [13]). To combat these failures, sensor hardware redundancy is typically combined with voting systems such that erroneous measurements can be detected and discarded. This section considers the problem of fault detection in two air-data sensor systems—one based on physical redundancy and the other based on analytical redundancy.

A. Sensor Equations

The basic air data relationships are derived in [2]. For compressible air and subsonic speeds, the static and total pressures, P_s and P_t, are related to calibrated (indicated) airspeed V by

$$V = \phi_1(P_t, P_s) := c_0 \left(5 \left(\frac{P_t - P_s}{P_0} + 1 \right)^{\frac{2}{7}} - 5 \right)^{\frac{1}{2}}, \qquad (10)$$

where $c_0 := 340.294\,\text{m/s}$ is the speed of sound at sea level and $P_0 := 101.325\,\text{kPa}$ is the static pressure at sea level. The indicated airspeed model ϕ_1 does not account for changes in density due to changes in altitude. Hence, the indicated airspeed deviates from the true airspeed at altitudes above sea level. A more accurate model would use a measurement of the outside air temperature to determine the changes in density and compute the true airspeed. By restricting our attention to low altitudes, we ignore this complexity and assume that V equals the true airspeed.

For altitudes in the troposphere (up to about 17000 km), the static pressure P_s is related to altitude h by

$$h = \phi_2(P_s) := \frac{T_0}{L} \left(1 - \left(\frac{P_s}{P_0} \right)^{LR/g} \right) \qquad (11)$$

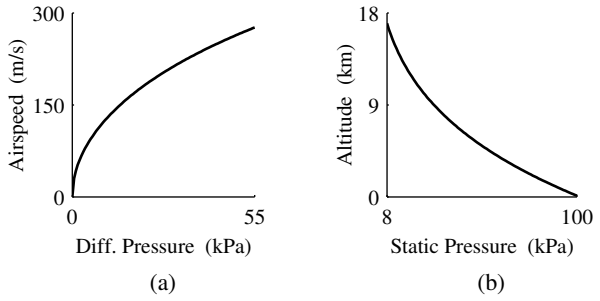

Fig. 4. Plot of (a) the (indicated) airspeed V as a function of differential pressure $P_d := P_t - P_s$ and (b) the altitude h as a function of static pressure P_s. The values plotted here are typical for subsonic flight in the troposphere.

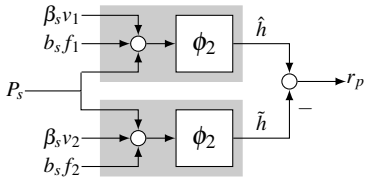

Fig. 5. System of two physically redundant altitude sensors. Both sensors measure the same static pressure P_s, but each sensor is corrupted by independent noise signals v_1 and v_2 and fault signals f_1 and f_2.

where $T_0 := 288.15\,\text{K}$ is the temperature at sea level, $L := 6.49\,\text{K/km}$ is the troposphere lapse rate, $g := 9.80665\,\text{m/s}^2$. is the gravity constant at sea level, and $R := 287.0529\,\text{J/kg·K}$ is the specific gas constant for dry air. These sensor equations are plotted in Fig. 4. Note that ϕ_1 and ϕ_2 are only mildly nonlinear for modest changes in airspeed and altitude.

B. Sensor Systems Considered

Using the air-data sensors as our example, we demonstrate how to apply the framework of Section II. Consider the physically redundant sensor system in Fig. 5 and the analytically redundant sensor system in Fig. 6. The physically redundant system consists of two static pressure ports, modeled by ϕ_2, while the analytically redundant system consists of a static port (ϕ_2), a pitot probe (ϕ_1), and a direct measurement of the flight path angle. In order to apply the methods of Section II, the sensor systems must be LTI. Hence, we assume that aircraft is performing a gentle climb maneuver where the airspeed is constant, the flight path angle is positive but small, and the altitude slowly increases. Since the sensor equations are only mildly nonlinear for small changes in altitude (see Fig. 4), we linearize the sensor equations at the initial altitude and assume that this linearization holds over the entire climb. The maneuver is parameterized by the triple $(\bar{V}, \bar{\gamma}, h_0)$, and the increasing altitude is given by the analytical relationship

$$h(t) = h_0 + \int_0^t \psi(\bar{V}, \bar{\gamma})\,\mathrm{d}s,$$

where $\psi(V, \gamma) := V \sin(\gamma)$. The sensor equations ϕ_1 and ϕ_2 are then inverted to find the corresponding P_t and P_s trajectories. Define $\bar{P}_t$ and $\bar{P}_s$ to be the initial values of these trajectories. Both sensor systems are linearized about the point $(\bar{P}_t, \bar{P}_s)$ and then discretized in time.

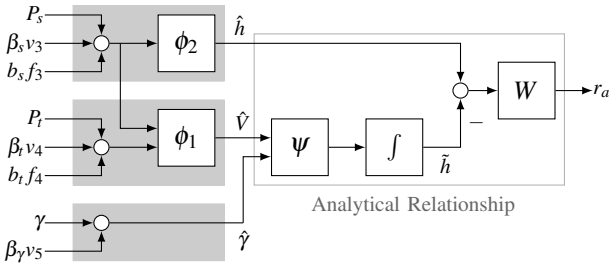

Fig. 6. System of three air data sensors measuring static pressure P_s, total pressure P_t, and flight path angle γ, respectively. The sensors are subject to noises v_3, v_4, and v_5 and random fault signals f_3 and f_4. A dynamic analytical relationship is to generate the residual signal r_a.

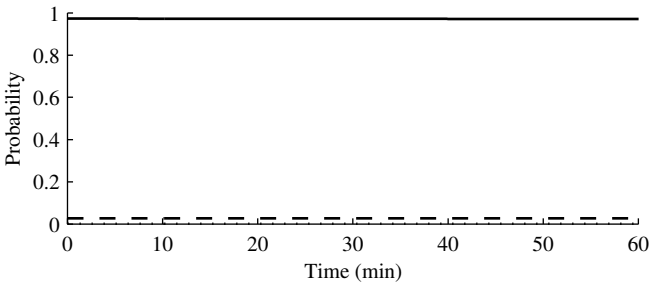

Fig. 7. Performance metrics $\{p_k^{\mathrm{TN}}\}$ (solid line), $\{p_k^{\mathrm{FP}}\}$ (dashed line), and $\{p_k^{\mathrm{FN}}\}$ (dotted line) for the physically redundant sensor system in Fig. 5. The quantity $\{p_k^{\mathrm{TP}}\}$ is omitted for the sake of clarity.

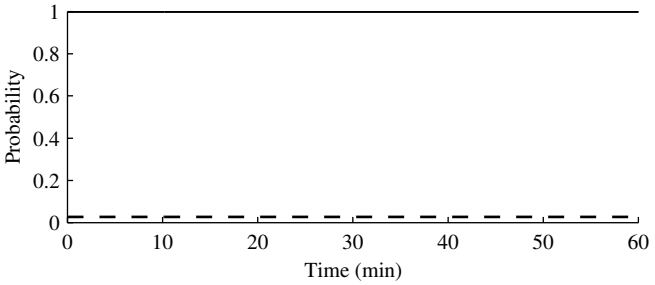

Fig. 8. Conditional probabilities $\{p_k^{\mathrm{D}}\}$ (solid line) and $\{p_k^{\mathrm{F}}\}$ (dashed line) for the physically redundant sensor system in Fig. 5.

In Fig. 5 and 6, the signals $v_1, v_2, \ldots, v_5$ are independent Brownian motions, which are scaled by the positive constants β_s, β_t, and β_γ. The fault signals f_1, f_2, f_3, and f_4 are defined as $f_i(t) := \mathbb{I}(t \geq \tau_i)$, where τ_1, τ_2, τ_3, and τ_4 are independent exponential random variables such that $\tau_1, \tau_2, \tau_3 \sim \mathrm{Exp}(\lambda_s)$ and $\tau_4 \sim \mathrm{Exp}(\lambda_t)$. The constants b_s and b_t determine the magnitudes of these bias faults.

The first-order linearization of ϕ_1 about $(\bar{P}_t, \bar{P}_s)$ is

$$\phi_1(\bar{P}_t + \beta_t v_4 + b_t f_4, \bar{P}_s + \beta_s v_3 + b_s f_3) \approx \phi_1(\bar{P}_t, \bar{P}_s) + \Phi_1 \begin{bmatrix} \beta_t v_4 + b_t f_4 \\ \beta_s v_3 + b_s f_3 \end{bmatrix},$$

and the first-order linearization of ϕ_2 about $\bar{P}_s$ is

$$\phi_2(\bar{P}_s + \beta_s v_j + b_s f_j) \approx \phi_2(\bar{P}_s) + \Phi_2(\beta_s v_j + b_s f_j),$$

where $\Phi_1 := (\nabla \phi_1)^T$, $\Phi_2 := {}^{d\phi_2}/_{dP_s}$. Similarly, ψ is linearized about $(\bar{V}, \bar{\gamma})$ as follows:

$$\psi(\hat{V}, \bar{\gamma} + \beta_\gamma v_5) \approx \Psi_1 \hat{V} + \Psi_2 \beta_\gamma v_5,$$

where $\Psi_1 := \sin(\bar{\gamma})$ and $\Psi_2 := \bar{V}\cos(\bar{\gamma})$. As the noisy signal $\psi(\hat{V}, \hat{\gamma})$ passes through the integrator, the noise accumulates and $\tilde{h}$ diverges from $\hat{h}$. To counteract this effect, a high-pass or "washout" filter with transfer function

$$W(s) = \frac{s}{s+a}, \qquad a > 0,$$

is applied to the difference $\hat{h} - \tilde{h}$. Essentially, this filter cancels the integrator pole at zero and places a stable pole at $-a < 0$. The drawback of using this filter is that it removes the DC component from the signal $\hat{h} - \tilde{h}$, which could mask faults if the bias magnitudes b_t and b_s are small.

The linearized equation for the residual of the physically redundant system (Fig. 5) is

$$r_p = \Phi_2 \beta_s (v_1 - v_2) + \Phi_2 b_s (f_1 - f_2). \tag{12}$$

The residual of the analytically redundant system (Fig. 6) is given by the linearized dynamics

$$\begin{aligned} \dot{\eta} &= -a\eta - [a \;\; \Psi_1]u + B_v v + B_f f, \\ r_a &= \eta + [1 \;\; 0]u + \Phi_2 \beta_s v_3 + \Phi_2 b_s f_3, \end{aligned} \tag{13}$$

where $\eta_0 = -h_0$, $u := [h_0 \; \bar{V}]^T$, $v := [v_3 \; v_4 \; v_5]^T$, $f := [f_3 \; f_4]^T$, and

$$B_v = \begin{bmatrix} -a\Phi_2\beta_s - \Psi_1\Phi_{12}\beta_s & -\Psi_1\Phi_{11}\beta_t & -\Psi_2\beta_\gamma \end{bmatrix},$$
$$B_f = \begin{bmatrix} -a\Phi_2 b_s - \Psi_1\Phi_{12} b_s & -\Psi_1\Phi_{11} b_t \end{bmatrix}.$$

Therefore, both r_p and r_a are governed by continuous-time LTI dynamics. Define a sample time Δ_t, and discretize equations (13) accordingly. (Note that the static map (12) does not need to be discretized.) Because the Brownian motions $v_1, v_2, \ldots, v_5$ have independent increments, the discretized signals $\{v'_{i,k}\}$ are i.i.d. Gaussian random processes with $v'_{i,k} \sim \mathcal{N}(0, \Delta_t)$, for all k. To discretize the fault model, define the parameters $q_s := 1 - e^{-\lambda_s \Delta_t}$ and $q_t := 1 - e^{-\lambda_t \Delta_t}$, the random variables $\tau'_1, \tau'_2, \tau'_3 \sim \mathrm{Geo}(q_s)$ and $\tau'_4 \sim \mathrm{Geo}(q_t)$, and the fault signals $f'_{i,k} = \mathbb{I}(k \geq \tau'_i)$ for all $i = 1, 2, \ldots, 4$ and all k. Then, the discretized linearized dynamics with the noises $\{v'_{i,k}\}$ and fault inputs $\{f'_{i,k}\}$ fit the framework of Section II.

C. Numerical Results

For this analysis, the sample time is $\Delta_t = 0.05\,\mathrm{s}$; the flight path is given by $V = 45\,\mathrm{m/s}$, $\gamma = 0.5^\circ$, and $h_0 = 200\,\mathrm{m}$; the noises are parameterized by $\beta_s = 690\,\mathrm{Pa}$, $\beta_t = 690\,\mathrm{Pa}$, and $\beta_\gamma = 0.2^\circ$; the fault biases are $b_s = 335\,\mathrm{Pa}$ and $b_t = -275\,\mathrm{Pa}$; the fault probabilities are $q_t = q_s = 1.38 \times 10^{-7}$, which corresponds to a mean time-to-failure (MTTF) of about 1000 hrs [11]. For both systems, the threshold is $\varepsilon = 9\,\mathrm{m}$. The pole of the "washout" filter is $a = 0.001$.

The performance metrics for the physically redundant altitude sensors are shown in Fig. 7. Note that the performance metrics are constant in time because the residual dynamics are memoryless. For all k, their values are $p_k^{\mathrm{TN}} = 0.9709$, $p_k^{\mathrm{FP}} = 0.0271$, and $p_k^{\mathrm{FN}} = 1 \times 10^{-6}$. The corresponding joint probabilities $\{p_k^{\mathrm{D}}\}$ and $\{p_k^{\mathrm{F}}\}$ are plotted in Fig. 8. For all k, their values are $p_k^{\mathrm{D}} = 0.9995$ and $p_k^{\mathrm{F}} = 0.0271$.

The performance metrics for the analytically redundant sensor configuration are shown in Fig. 9. Although these

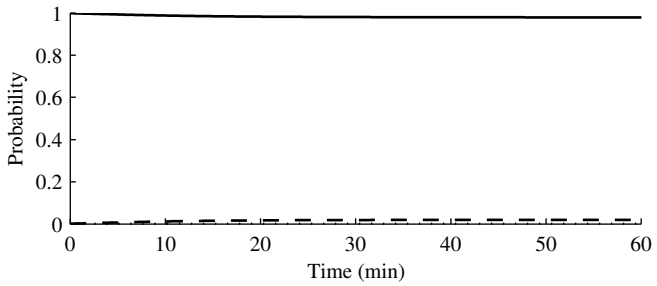

Fig. 9. Performance metrics $\{p_k^{\mathrm{TN}}\}$ (solid line), $\{p_k^{\mathrm{FP}}\}$ (dashed line), and $\{p_k^{\mathrm{FN}}\}$ (dotted line) for the analytically redundant sensor system in Fig. 6. The quantity $\{p_k^{\mathrm{TP}}\}$ is omitted for the sake of clarity.

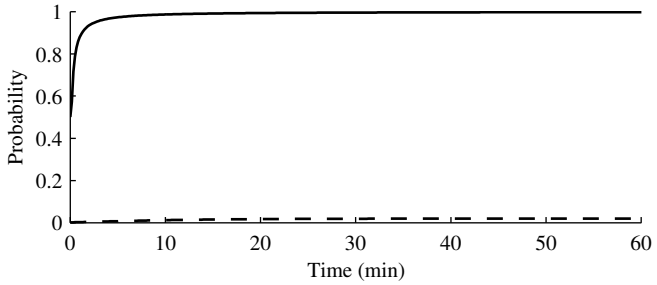

Fig. 10. Conditional probabilities $\{p_k^{\mathrm{D}}\}$ (solid line) and $\{p_k^{\mathrm{F}}\}$ (dashed line) for the analytically redundant sensor system in Fig. 6.

quantities vary with time, the washout filter W causes steady-state convergence. The steady-state values are $p_k^{\mathrm{TN}} \to 0.9785$, $p_k^{\mathrm{FP}} \to 0.0195$, and $p_k^{\mathrm{FN}} \to 4.5 \times 10^{-6}$. Hence, the overall system reliability, given by p_k^{TN}, is comparable to that of the physically redundant configuration. Because a fault is so unlikely in the time interval considered, the joint probabilities are dominated by the small marginal probability $\mathbb{P}(H_{1,k})$. By definition, the conditional probabilities, shown in Fig. 10, are not multiplied by $\mathbb{P}(H_{1,k})$, so their time-varying nature is much more apparent. Note that these probabilities converge to the steady-state values $p_k^{\mathrm{D}} \to 0.9977$ and $p_k^{\mathrm{F}} \to 0.0196$. Since the performance metric $\{p_k^{\mathrm{TN}}\}$ quantifies the overall system reliability, the values plotted in Fig. 9 certify the reliability of this analytically redundant sensor scheme when the ε-threshold fault detector is used.

V. Conclusions & Future Work

For sensors with linear-time invariant dynamics and additively entering noises and faults, both physically and analytically redundant sensor systems can be written as an LTI system that produces a residual. Applying a threshold fault detector to the residual, we formulated probabilistic performance metrics that apply to any LTI sensor network that generates a residual. These metrics are easily computable if the noises are Gaussian and the faults take finitely many values. This performance analysis was applied to two air-data sensor networks—one consisted of two physically redundant altitude sensors, while the other exploited the analytical relationship between measurements of altitude, airspeed, and flight path angle. The numerical results in Section IV-C illustrate, for particular parameter values, how the performance metrics vary with time, how the same framework can be used to compare the performance of different sensor systems, and how the performance metrics certify the overall reliability of the sensor system.

Future work on this topic will include extensions of the performance analysis framework to more complex sensor systems. For example, the sensor dynamics could be linear time-varying or perhaps even nonlinear. Also, the occurrence of a fault could affect the structure of the sensor dynamics, as well as the structure of the fault signal. Since the analysis performed in Section IV depends on a particular flight path, it would be interesting to determine which flight path yields the worst fault detector performance.

VI. Acknowledgements

This material is based upon work supported by the National Science Foundation under Grant No. 0931931 entitled "CPS: Embedded Fault Detection for Low-Cost, Safety-Critical Systems", the National Aeronautics and Space Administration under Grant No. NNX07AC40A entitled "Reconfigurable Robust Gain-Scheduled Control for Air-Breathing Hypersonic Vehicles", and the Department of Mechanical Engineering at the University of California, Berkeley. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

References

[1] R. J. Bleeg, "Commercial jet transport fly-by-wire architecture considerations," in *Proceedings of the 8th AIAA/IEEE Digital Avionics Systems Conference*. San Jose, CA: AIAA, Oct. 1988, pp. 399–406.

[2] R. Collinson, *Introduction to Avionics Systems*, 2nd ed. Boston: Kluwer Academic, 2003.

[3] Y. C. Yeh, "Triple-triple redundant 777 primary flight computer," in *Proceedings of the 1996 IEEE Aerospace Applications Conference*, Aspen, CO, Feb. 1996, pp. 293–307.

[4] ——, "Design considerations in Boeing 777 fly-by-wire computers," in *Proceedings of the Third IEEE International High-Assurance Systems Engineering Symposium*, Washington, D.C., Nov. 1998, pp. 64–72.

[5] A. Emami-Naeini, M. M. Akhter, and S. M. Rock, "Effect of model uncertainty on failure detection: The threshold selector," *IEEE Transactions on Automatic Control*, vol. 33, no. 12, pp. 1106–1115, 1988.

[6] J. Gertler, *Fault Detection and Diagnosis in Engineering Systems*. New York: Marcel Dekker, 1998.

[7] J. Stoustrup, H. Niemann, and A. la Cour-Harbo, "Optimal threshold functions for fault detection and isolation," in *Proceedings of the 2003 American Control Conference*, Denver, CO, Jun. 2003, pp. 1782–1787.

[8] E. L. Lehmann and J. P. Romano, *Testing Statistical Hypotheses*, 3rd ed. New York: Springer, 2005.

[9] B. C. Levy, *Principles of Signal Detection and Parameter Estimation*. New York: Springer, 2008.

[10] W. J. Cody, "Rational Chebyshev approximations for the error function," *Mathematics of Computation*, vol. 23, no. 107, pp. 631–637, Sep. 1969.

[11] M. S. Hamada, A. G. Wilson, C. S. Reese, and H. F. Martz, *Bayesian Reliability*. New York: Springer, 2008.

[12] *Interim report on the accident on 1st June 2009 to the Airbus A330-203 registered F-GZCP operated by Air France flight AF 447 Rio de Janeiro – Paris*. Bureau d'Enquêtes et d'Analyses pour la sécurité de l'aviation civile, 2009.

[13] *Interim report no. 2 on the accident on 1st June 2009 to the Airbus A330-203 registered F-GZCP operated by Air France flight AF 447 Rio de Janeiro – Paris*. Bureau d'Enquêtes et d'Analyses pour la sécurité de l'aviation civile, 2009.