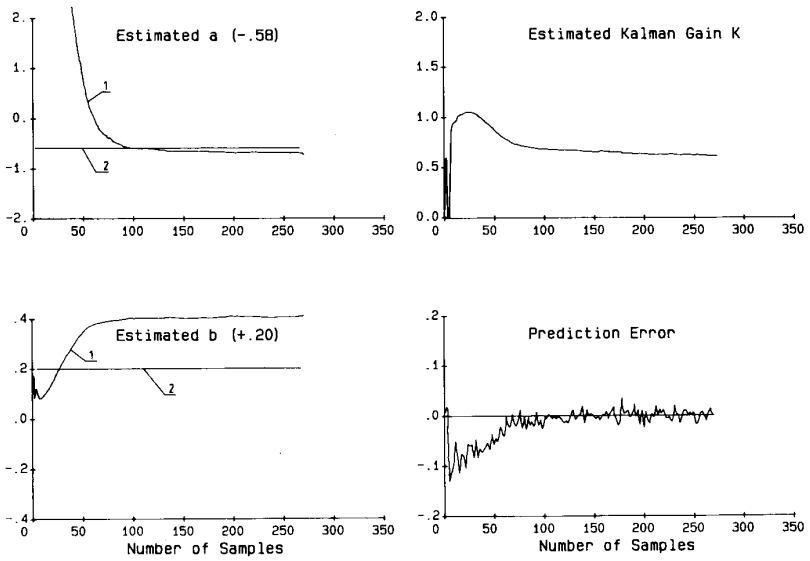

Fig. 4. Same example as Fig. 2 with the linear filter, but measurement corrupted with noise. (1) is estimate, (2) is true value.

discrete state-space system model. Both versions are treated using a linear discrete measurement equation. These algorithms were investigated with reference to the theory of linear RPE methods and the theory of nonlinear filtering. The innovations model formulation was found to be attractive, and the algorithms were implemented and tested against computer simulations showing excellent convergence and bias properties that by far exceed those of a linear continuous/discrete filter.

REFERENCES

[1] M. Blanke, "Propulsion losses related to automatic steering and prime mover control," Ph.D. dissertation, Tech. Univ. Denmark, Dec. 1981.

[2] ——, "Cross-bispectrum technique identification of nonlinear ship speed dynamics," *Int. J. Comput. Contr.*, vol. 2, pp. 54–62, 1986.

[3] M. Blanke and L. B. Sørensen, "The Ljung innovations filter used for identification of nonlinear ship speed dynamics," presented at the 7th Ship Contr. Syst. Symp., Bath, U.K., 1984.

[4] D. T. Gavel and S. G. Azevedo, "Identification of continuous time systems—An application of Ljung's corrected extended Kalman filter," presented at the Sixth. IFAC Symp. on Identification and Syst. Parameter Estimation, USA, June 1982.

[5] A. Gelb, Applied Optimal Estimation. New York: M.I.T. Press, 1974.

[6] G. C. Goodwin and R. L. Payne, *Dynamic System Identification: Experiment Design and Data Analysis.* New York: Academic, 1977.

[7] A. H. Jazwinski, *Stochastic Processes and Filtering Theory.* New York: Academic, 1970.

[8] L. Ljung, *System Identification—Theory for the User.* (Lecture Notes). Linköping, Sweden: University of Linköping, 1984.

[9] L. Ljung and T. Söderström, *Theory and Practice of Recursive Identification.* Cambridge, MA: M.I.T. Press, 1983.

[10] L. Ljung, "Analysis of a general recursive prediction error identification algorithm," *Automatica,* vol. 17, no. 1, pp. 89–99, 1981.

[11] ——, "Identification methods, model validation recursive identification methods for off-line identification problems," presented at the Sixth IFAC Symp. Identification Syst. Parameter Estimation, USA, June 1982.

[12] L. Ljung, "Asymptotic behavior of the extended Kalman filter as a parameter estimator for linear systems," *IEEE Trans. Automat. Contr.,* vol. AC-24, no. 1, 1979.

[13] P. S. Maybeck, *Stochastic Models, Estimation, and Control. Volume 1.* New York: Academic, 1979, Volume 2, New York: Academic, 1982.

[14] P. Young, *Recursive Estimation and Time-Series Analysis.* New York: Springer-Verlag, 1984.

[15] W.-W. Zhou, "Filtering and recursive identification," Servolaboraty, Technical Univ. Denmark, Rep. 85-A-582, Oct. 1985.

[16] ——, "Identification of nonlinear marine systems," Ph.D. dissertation. Servolaboratory, Tech. Univ. Denmark, Lyngby, Denmark, Rep. ISBN 87-87950-467-4, June 1987.

Failure Detection and Identification

MOHAMMAD-ALI MASSOUMNIA, GEORGE C. VERGHESE, AND ALAN S. WILLSKY

Abstract—**Using the geometric concept of an unobservability subspace, a solution is given to the problem of detecting and identifying control system component failures in linear, time-invariant systems. Conditions are developed for the existence of a causal, linear, time-invariant processor that can detect and uniquely identify a component failure, first for the case where components can fail simultaneously, and second for the case where they fail only one at a time. Explicit design algorithms are provided when these conditions are satisfied. In addition to time domain solvability conditions, frequency domain interpretations of the results are given, and connections are drawn with results already available in the literature.**

I. INTRODUCTION

Failure detection and identification (FDI) is currently the subject of extensive research, and is being used in the design of highly reliable control systems. An FDI process essentially comprises two stages: residual generation and decision making. In this note we concentrate on residual generation, and refer the reader to the extensive literature on the decision-making phase of FDI (see [21], [10], and [19] for comprehensive surveys). All our discussion will be for finite-dimensional, linear, time-invariant (LTI) systems.

The output of a residual generator is, by definition, a function of time

Manuscript received July 18, 1986; revised February 29, 1988. Paper recommended by Past Associate Editor, J. B. Pearson. The work of the first author was supported by NASA Langley Research Center under Grant NAG1-126. The work of the other authors was supported in part by the Air Force Office of Scientific Research under Grant AFOSR-82-0258 and in part by the Army Research Office under Grant DAAG-29-84-K-005.

M.-A. Massoumnia was with the Space Systems Laboratory, Massachusetts Institute of Technology, Cambridge, MA 02139. He is now with Sharif University of Technology, Teheran, Iran.

G. C. Verghese is with the Laboratory for Electromagnetic and Electronic Systems, Massachusetts Institute of Technology, Cambridge, MA 02139.

A. S. Willsky is with the Laboratory for Information and Decision Systems, Massachusetts Institute of Technology, Cambridge, MA 02139.

IEEE Log Number 8824285.

0018-9286/89/0300-0316$01.00 © 1989 IEEE

that is nominally zero or close to zero when no failure is present, and that is distinguishably different from zero when a component of the system fails. Residuals are obtained by exploiting the dynamic relationships among the sensor outputs and actuator inputs [6]–[8]. There are two residual generation approaches that are not only applicable to both sensor and actuator FDI but that also avoid assumptions about how the failed component behaves. These are the methods of *generalized parity relations*, first studied by Chow [4], [5], and later extended by Lou *et al.* [12], [13] and Massoumnia and Vander Velde [16], and the *failure detection filter* introduced by Beard [2], then amplified by Jones [11] and recently revisited by Massoumnia [14] and White and Speyer [23].

Each of these two approaches involves the design of a linear processor with a particular restricted structure. For generalized parity checks, residuals are generated from linear combinations of sensor outputs and applied inputs, taken over a *finite* window. The combinations are chosen to yield residuals that are zero when the components are functioning perfectly, but that have a subset deviating from zero when a particular system component fails. The class of linear processors considered in this design procedure is evidently restricted and does not, for example, allow much freedom to optimize noise rejection.

In Beard's failure detection filter, the linear processor is a full-order observer, with the residuals taken to be the innovations of the observer. The design procedure consists of choosing the observer gain so that failures of different system components affect the residuals in linearly independent directions, thus greatly simplifying the subsequent decision-making process. The restriction to full-order observers is, as we shall see, a rather severe constraint. It not only limits significantly the classes of problems that have solutions—because the set of possible failure modes must satisfy a strong mutual detectability condition [14]—but it also makes the FDI problem and the design process appear more complicated than necessary.

In this note we remove the structural constraints imposed in these previous studies. We only require that our residual generation mechanisms be finite-dimensional, causal, LTI systems, and that they produce residuals with the same desirable properties as in previous studies, i.e., residuals that are sensitive only to particular failure modes. As we shall see, it is possible to construct such processors to detect and uniquely identify failures under less restrictive conditions than those previously reported. This is reflected in the fact that we now obtain necessary and sufficient conditions for solution of each of the FDI problems posed in this note, whereas [14] was largely limited to obtaining sufficient conditions for solvability of a more restricted class of problems.

We begin in Section II by formulating the FDI filter problem, and show how sensor failures and changes in the system parameters can be modeled as pseudoactuator failures. In Section III, the fundamental problem of residual generation (FPRG) is defined. In this problem, it is assumed that there are only two possible failure modes, and that we desire a residual that is affected by the first failure mode but not by the second. Section IV considers the extension of the fundamental problem of residual generation (EFPRG) to the case of multiple failures occurring simultaneously. The solvability condition for this problem is that the failure events satisfy a certain *strongly identifiability* condition. In Section V, the most general form of the FDI problem (within the framework of Section II) is solved. The requisite condition is now that the failure events be *identifiable*, in a sense defined in that section.

This note relies heavily on a few geometric concepts. Most of these are dual to ones already developed in the control literature. The notation and terminology here are those of [1], [22], and [14], and are now quite standard. We recall a few items. The range of L is $\mathfrak{L}$. $\mathfrak{V}(\mathfrak{L})$ denotes the set of all (C, A)-invariant subspaces containing the subspace $\mathfrak{L}$, and $\mathfrak{S}(\mathfrak{L})$ denotes the set of all (C, A)-unobservability subspaces (u.o.s.) containing $\mathfrak{L}$. Given a (C, A)-invariant subspace $\mathfrak{W}$, $\mathfrak{D}(\mathfrak{W})$ denotes the set of all D such that $(A + DC)\mathfrak{W} \subseteq \mathfrak{W}$. For an A-invariant subspace $\mathfrak{S}$, we denote by $A:\mathfrak{X}/\mathfrak{S}$ the map induced by A on the factor space $\mathfrak{X}/\mathfrak{S}$. The symbol $d(\mathfrak{X})$ denotes the dimension of the vector space $\mathfrak{X}$; $\sigma(A)$ is the spectrum of A; $\boldsymbol{k}$ denotes the finite set $\{1, 2, \cdots, k\}$; and $m(s)$ is the Laplace transform of the function $m(t)$—a common abuse of notation, but unlikely to cause confusion if the use of s as an argument is reserved for Laplace transforms.

We emphasize that even though many of the geometric concepts used in this note are familiar in control theory, or are the duals of familiar concepts, the problems posed and solved are *not* simply obtained from familiar control problems. For instance, a reader acquainted with the disturbance decoupled estimation problem (DDEP) [20], [3], will readily recognize a relationship to FPRG. These two problems, however, have subtle but important differences that completely distinguish them from each other. In DDEP, the state to be estimated is given as part of the problem statement, while in FPRG we have to find that part of the state space that can be estimated even in the presence of an unknown input.

Similarly, a reader who knows of the control decoupling problem, [9], [22], will recognize a dual relationship between that problem and EFPRG. Despite this duality, the structure of the residual generator proposed in Theorem 4 is quite different from that of the extended decoupling controllers given in [22], since there is no compatibility (cf. [22]) issue in EFPRG. As a final illustration, note that the filter suggested in the proof of Theorem 8, when multiplied by the plant transfer matrix, results in a transfer matrix with zeros on the diagonal and nonzero elements everywhere else—a structure that is complementary (and certainly not identical or dual) to the structure considered in the familiar decoupling problem of control theory.

II. Failure Representation and Problem Formulation

Assume our nominal LTI system is described by the state-space model

$$\dot{x}(t) = Ax(t) + Bu(t) + \sum_{i=1}^{k} L_i m_i(t) \tag{1a}$$

$$y(t) = Cx(t) + \sum_{i=1}^{q} J_i n_i(t). \tag{1b}$$

Here $x(t) \in \mathfrak{X}$, $u(t) \in \mathfrak{U}$, and $y(t) \in \mathfrak{Y}$, with the dimensions of $\mathfrak{X}$, $\mathfrak{U}$, and $\mathfrak{Y}$ being n, m, and l, respectively. The nominal input $u(t)$ and the output $y(t)$ are assumed to be known and will be referred to as the *observables* of the system. The functions $m_i(t) \in \mathfrak{M}_i$ (with $d(\mathfrak{M}_i) = k_i$) and $n_i(t) \in \mathfrak{N}_i$ (with $d(\mathfrak{N}_i) = q_i$) are arbitrary and unknown functions of time. We refer to the function $m_i(t)$ as the ith *actuator failure mode* and to $n_i(t)$ as the ith *sensor failure mode*. When no failure is present, the $m_i(t)$ and $n_i(t)$ are all equal to zero, by definition. They become nonzero precisely when the corresponding failure mode occurs. From now on we shall refer to the maps $L_i:\mathfrak{M}_i \to \mathfrak{X}$ and $J_i:\mathfrak{N}_i \to \mathfrak{Y}$ as *actuator failure signatures* and *sensor failure signatures*, respectively.

Because we do not constrain $m_i(t)$ and $n_i(t)$ to any special function class, a wide variety of actuator and sensor failures fits this representation. To model the failure of the jth sensor, for instance, simply set J_1 equal to the jth column of the $l \times l$ identity matrix. If the sensor fails completely, i.e., gives a zero output, then $n_1(t) = -c_j x(t)$, where c_j is the jth row of the output matrix C. Note that we can also model a change in the dynamics of the plant, i.e., a change in A, by choosing L_i appropriately.

The fact that we do not assume any prior mode of component failure, i.e., that $m_i(t)$ and $n_i(t)$ in (1) can be arbitrary, is a major distinction between our approach to failure modeling and the majority of approaches in the literature. Note that the same approach to failure modeling is used in [2], [11], [14], and [23]. Since the $m_i(t)$ and $n_i(t)$ are arbitrary, there is no loss of generality in assuming, as we shall from now on, that the failure signatures are one-to-one (monic).

We shall also find it more convenient to represent sensor failures by pseudoactuator failures. For this, consider the unknown function $n_i(t)$ to be the output of some invertible, finite-dimensional LTI system driven by an appropriate input. The only restriction that we impose on the LTI system is that it be strictly causal, i.e., have no direct feedthrough term. If the dynamics of the systems generating the sensor failure modes are now added to the dynamics of the system (1), the sensor failures can be represented as actuator failures. Hence, all the analysis that follows uses

the model

$$\dot{x}(t) = Ax(t) + Bu(t) + \sum_{i=1}^{k} L_i m_i(t) \tag{2a}$$

$$y(t) = Cx(t) \tag{2b}$$

where it is assumed that A, B, L_i, and C have already been appropriately modified so that the sensor failures are properly represented as pseudoactuator failures.

Considering the system in (2) now, the *FDI filter problem* (FDIFP) is to design an LTI dynamic residual generator that takes the observables $u(t)$ and $y(t)$ as inputs and generates a set of residual vectors $r_i(t)$, $i \in p$, with the following properties.

1) When no failure is present, all the residuals $r_i(t)$ decay asymptotically to zero. Hence, the net transmission from $u(t)$ to the residuals is zero, and the modes observable from the residuals are asymptotically stable.

2) In the jth failure mode (i.e., when $m_j(t) \neq 0$), the residuals $r_i(t)$ for $i \in \Omega_j$ are nonzero, and the other residuals $r_\alpha(t)$ for $\alpha \in p - \Omega_j$ decay asymptotically to zero. Here the prespecified family of *coding* sets $\Omega_j \subseteq p, j \in k$, is chosen such that, by knowing which of the $r_i(t)$ are (or decay to) zero and which are not, we can uniquely identify the failure.

Note that in the general problem there is no constraint on the number p of residual vectors. We shall say more about the coding sets Ω_j below and also in Section V. If a set of residuals with the above properties can be generated, then the identification task is trivial. We need only to determine the residual patterns and identify the failure by referring to the table of coding sets.

One important design consideration is how to choose the coding sets Ω_j. The simplest code is just to take $p = k$ and $\Omega_i = \{i\}$, i.e., to let precisely one of the residuals be nonzero for any one failure. This coding scheme enables us to correctly identify simultaneous failures. At the other extreme, if we know that simultaneous failures do not occur, then the smallest possible number of residuals is obtained via a so-called binary coding [15] in which case p equals the smallest integer above $\log_2 (k + 1)$. The practical danger with picking the smallest allowable number is that, if one of the residuals does not cross the threshold, then a completely erroneous identification of the error may be made. Section V pursues the question of coding sets further. It is shown there, in the course of obtaining the solvability condition for FDIFP, that FDIFP will not have a solution for certain families of failure events, no matter what coding sets are used.

In the next section, we solve a restricted version of FDIFP. The solution to this restricted problem will then be used to tackle more general problems in the sections that follow.

III. The Fundamental Problem of Residual Generation (FPRG)

In this section, we assume that only *two* failure events are present, and examine when a residual generator can be designed to be sensitive to the first failure but insensitive to the second. This restricted version of FDIFP will be called the *fundamental problem in residual generation* (FPRG).

Consider the model given in (2), with $k = 2$:

$$\dot{x}(t) = Ax(t) + Bu(t) + L_1 m_1(t) + L_2 m_2(t) \tag{3a}$$

$$y(t) = Cx(t). \tag{3b}$$

The dimensions of the matrices in (3) are the same as in (1). It is desired that a nonzero $m_1(t)$ should show up in the output $r(t)$ of the residual generator, while a nonzero $m_2(t)$ should not affect $r(t)$. As usual, our observables are the known actuation signal $u(t)$ and the output $y(t)$.

The most general form for a realizable LTI processor that takes the observables $y(t)$ and $u(t)$ as inputs and generates a residual $r(t)$ is

$$\dot{w}(t) = Fw(t) - Ey(t) + Gu(t) \tag{4a}$$

$$r(t) = Mw(t) - Hy(t) + Ku(t) \tag{4b}$$

where $w(t) \in \mathfrak{W}$. Combining (3) and (4), we get

$$\begin{pmatrix} \dot{x}(t) \\ \dot{w}(t) \end{pmatrix} = \begin{pmatrix} A & 0 \\ -EC & F \end{pmatrix} \begin{pmatrix} x(t) \\ w(t) \end{pmatrix} + \begin{pmatrix} B & L_2 \\ G & 0 \end{pmatrix} \begin{pmatrix} u(t) \\ m_2(t) \end{pmatrix} + \begin{pmatrix} L_1 \\ 0 \end{pmatrix} m_1(t) \tag{5a}$$

$$r(t) = (-HC \; M) \begin{pmatrix} x(t) \\ w(t) \end{pmatrix} + (K \; 0) \begin{pmatrix} u(t) \\ m_2(t) \end{pmatrix}. \tag{5b}$$

Define the extended spaces $\mathfrak{X}^e = \mathfrak{X} \oplus \mathfrak{W}$ and $\mathfrak{U}^e = \mathfrak{U} \oplus \mathfrak{M}_2$. With $x^e(t) \in \mathfrak{X}^e$ and $u^e(t) \in \mathfrak{U}^e$, (5) can be rewritten as

$$\dot{x}^e(t) = A^e x^e(t) + B^e u^e(t) + L^e m_1(t) \tag{6a}$$

$$r(t) = H^e x^e(t) + K^e u^e(t) \tag{6b}$$

where the definitions of the matrices in (6) are evident from (5).

Now we can explore different criteria for deciding whether the first failure mode will show up in the residual, i.e., whether a nonzero $m_1(t)$ will affect $r(t)$. The most natural approach is to require that the transfer matrix $T(s)$ from $m_1(s)$ to $r(s)$ be *left invertible*, so that *any* nonzero $m_1(t)$ results in a nonzero $r(t)$. Another approach is to only ask that the system relating $m_1(t)$ to $r(t)$ be *input observable*. Recall that a system (C, A, B) is input observable if B is monic and the image of B does not intersect the unobservable subspace of (C, A). In terms of transfer matrices, left invertibility is equivalent to the columns of $C(sI - A)^{-1}B$ being linearly independent over the field of rationals in s, while input observability is equivalent to independence over the field of real numbers.

Even if the system relating $m_1(t)$ to $r(t)$ is only input observable and not left invertible, *almost any* nonzero $m_1(t)$ will produce a nonzero residual $r(t)$. This is because it is extremely unlikely that an arbitrary nonzero $m_1(t)$ will hide itself for all t in the nullspace of the mapping from $m_1(t)$ to $r(t)$. It may therefore be argued that the requirement of left invertibility is too stringent for FDI purposes. In any case, the transfer matrix $T(s)$ is often (or even usually) a column vector, and in this case input observability is equivalent to left invertibility.

Based on these arguments, we define FPRG as the problem of finding all the matrices in (4) such that the following maps satisfy the indicated constraints:

$$u^e \mapsto r = 0 \tag{7}$$

$$m_1 \mapsto r \text{ is input observable.} \tag{8}$$

In addition, we shall require that the observable modes of the pair (H^e, A^e) be asymptotically stable, so that the contribution to $r(t)$ of initial conditions in (5) dies out asymptotically.

We need a few preliminaries in order to derive the solvability condition for FPRG. First, with $x \in \mathfrak{X}$, define the embedding map $Q: \mathfrak{X} \to \mathfrak{X}^e$ by

$$Qx := \begin{pmatrix} x \\ 0 \end{pmatrix}. \tag{9}$$

Note that if $\mathfrak{V} \subseteq \mathfrak{X}^e$, then

$$Q^{-1}\mathfrak{V} = \{x : x \in \mathfrak{X} \text{ and } \begin{pmatrix} x \\ 0 \end{pmatrix} \in \mathfrak{V}\}. \tag{10}$$

Using this definition, it is relatively simple to relate the unobservability subspaces of the systems in (6) and (3). The following fundamental result, which exactly accomplishes this task, is crucial to the solvability condition of FPRG.

Proposition 1: Let $\mathfrak{S}^e$ be the unobservable subspace of (H^e, A^e). Then $Q^{-1}\mathfrak{S}^e$ is a (C, A)-unobservability subspace; see [20], [18], and [17]. ●●

With this result at our disposal, the solvability condition can be obtained.

Theorem 2: FPRG has a solution if and only if

$$\mathfrak{S}^* \cap \mathfrak{L}_1 = 0 \tag{11}$$

where $\mathcal{S}^* = \inf \underline{\mathcal{S}}(\mathcal{L}_2)$. Also, if (11) holds, then the dynamics of the residual generator can be assigned arbitrarily.

Proof:

(Only If): Consider the system given in (5) and (6). For (7) to hold, we should have $K^e = 0$, and

$$\langle A^e | \mathcal{B}^e \rangle \subseteq \mathcal{S}^e := \langle \ker H^e | A^e \rangle. \tag{12}$$

Equation (12) implies $\mathcal{B}^e \subseteq \mathcal{S}^e$, hence $Q^{-1}\mathcal{B}^e \subseteq \mathcal{S} := Q^{-1}\mathcal{S}^e$. Using Proposition 1, $\mathcal{S}$ is a (C, A)-u.o.s. Also $Q^{-1}\mathcal{B}^e \supseteq \mathcal{L}_2$. Therefore

$$\mathcal{S} \in \mathcal{S}(\mathcal{L}_2). \tag{13}$$

For (8) to hold, we should have L^e monic and $\mathcal{L}^e \cap \mathcal{S}^e = 0$. Thus, we should have L_1 monic (which we have assumed) and

$$Q^{-1}(\mathcal{L}^e \cap \mathcal{S}^e) = Q^{-1}\mathcal{L}^e \cap Q^{-1}\mathcal{S}^e = \mathcal{L}_1 \cap \mathcal{S} = 0. \tag{14}$$

Obviously, (13) and (14) hold only if (11) is true.

(If): Let $D_0 \in \underline{D}(\mathcal{S}^*)$, let $P: \mathfrak{X} \to \mathfrak{X}/\mathcal{S}^*$ be the canonical projection, and let $A_0 = A + D_0C: \mathfrak{X}/\mathcal{S}^*$. Also let H denote a solution of $\ker HC = \mathcal{S}^* + \ker C$, and let M be the unique solution of $MP = HC$. By construction, the pair (M, A_0) is observable, so there exists a D_1 such that $\sigma(F) = \Lambda$, where $F = A_0 + D_1M$ and Λ is an arbitrary self-conjugate set. With P^{-r} denoting a right inverse of P, let $D = D_0 + P^{-r}D_1H$, $E = PD$, $G = PB$ and $K = 0$. Define $e(t) = w(t) - Px(t)$; this fixes the order of the residual generator at $n - d(\mathcal{S}^*)$. Then it follows quite simply that

$$\dot{e}(t) = Fe(t) - PL_1m_1(t)$$

$$r(t) = Mw(t) - Hy(t) = Me(t).$$

Thus, $r(s) = T(s)m_1(s)$ with $T(s) = -M(sI - F)^{-1}PL_1$. The requirement in (7) is clearly satisfied. Now, since $\mathcal{S}^* \cap \mathcal{L}_1 = 0$ and L_1 is monic, it follows that PL_1 is monic. Moreover, the pair (M, F) is observable. Hence, from the definition of input observability, it follows that the system relating $m_1(t)$ to $r(t)$ is input observable and (8) is satisfied. ●●

The major step in the design of the filter is to place the image of the second failure signature in the unobservable subspace of the residual $r(t)$, and then to factor out the observable subspace so that the order of the filter is reduced. It was noted that the order of the residual generator given in Theorem 2 is $n - d(\mathcal{S}^*)$, and this order is in general conservative. The reason is that there may be a u.o.s $\mathcal{S} \supset \mathcal{S}^*$ satisfying $\mathcal{S} \cap \mathcal{L}_1 = 0$. Clearly, using this $\mathcal{S}$ further reduces the order of the residual generator. Unfortunately, no systematic way is known for constructing such noninfimal unobservability subspaces.

The reader who is familiar with the disturbance decoupled estimation problem (DDEP) [20], [3], will readily recognize a relationship between DDEP and FPRG. These two problems have subtle differences, however, that completely distinguish them from each other. In DDEP, the state to be estimated is given as part of the problem statement. In FPRG, we have to find that part of the state space that can be estimated even in the presence of the unknown input $m_2(t)$.

We now give an interesting interpretation of the solution to FPRG. Referring to Theorem 2, the residual generator can be rewritten as follows:

$$\dot{w}(t) = A_0w(t) - PD_0y(t) + Gu(t) + D_1r(t) \tag{15a}$$

$$r(t) = Mw(t) - Hy(t). \tag{15b}$$

By choosing D_0 and H appropriately, we change the observability properties of $(HC, A + D_0C)$ in such a way that failure of the second actuator becomes unobservable from the residual. Next, by injecting the residual $r(t)$ back into the filter, the spectrum of the residual generator is modified as desired. The residual generator given in (15) can be thought of as an observer for the hypothetical system

$$\dot{z}(t) = A_0z(t) + u_h(t) \tag{16a}$$

$$y_h(t) = Mz(t) \tag{16b}$$

where $u_h(t) := P[Bu(t) - D_0y(t)]$ is the hypothetical input, and $y_h(t) := Hy(t)$ is the hypothetical measurement. This interpretation of the residual generator can be used to compute the gain D_1 as the solution of an optimal estimation problem [15].

The generic solvability of FPRG is summarized in the following result.

Proposition 3: Let us assume that A, C, L_1, and L_2 are arbitrary matrices with respective dimensions $n \times n$, $l \times n$, $n \times k_1$, and $n \times k_2$. Then FPRG generically has a solution if and only if

$$k_1 + k_2 \leq n \tag{17}$$

and

$$k_2 < l. \tag{18}$$

Proof: The simple proof is given in [15]. ●●

IV. Extension of FPRG to Multiple Failure Events (EFPRG)

In this section we extend FPRG to the case of multiple failures. Let us assume that k failure events are present. Suppose we want to design a processor that generates k residuals, $r_i(t)$, $i \in k$, such that the ith failure mode $m_i(t)$ affects the ith residual and only this residual. More precisely, what we require is that the transfer matrix relating $m_i(s)$ to $r_i(s)$ for each $i \in k$ should be input observable, and the transfer matrix from $m_i(s)$ to all other $r_j(s)$, $j \neq i$, should be zero. The earlier stability requirement for the observable modes is also maintained.

In the notation of Section II, the problem we have just formulated is the same as the FDIFP with the coding sets $\Omega_i = \{i\}$, $i \in k$. This particular version of the FDIFP will be called the *extension* of the fundamental problem in residual generation (EFPRG). If EFPRG has a solution, then it is evidently possible to detect and identify even simultaneous failures. Note that for identifying simultaneous failures, we need at least as many residuals as there are failure events. In this sense, the coding set $\Omega_i = \{i\}$ (or any permutation of it) is minimal.

In a recent paper, Massoumnia [14] defined the similar problem of designing a residual generator of the form

$$\dot{w}(t) = (A + DC)w(t) - Dy(t) + Bu(t) \tag{19a}$$

$$r_i(t) = H_i[w(t) - y(t)] \tag{19b}$$

such that a nonzero $m_i(t)$ only shows up in the residual $r_i(t)$. This problem is a slight generalization of Beard's failure detection filter problem, and was referred to as the *restricted diagonal detection filter problem* (RDDFP) in [14]. Obviously, RDDFP is a special case of the EFPRG that we have formulated here, since in EFPRG the matrix F is not restricted to be of the form $A + DC$ for some appropriate gain matrix D, nor is w required to be of the same dimension as x.

The solvability condition for EFPRG follows immediately from that of FPRG.

Theorem 4: EFPRG has a solution if and only if

$$\mathcal{S}_i^* \cap \mathcal{L}_i = 0, \qquad i \in k \tag{20}$$

where $\mathcal{S}_i^* := \inf \underline{\mathcal{S}}(\Sigma_{j \neq i}\mathcal{L}_i)$.

Proof:

(Only If): The necessity of (20) follows immediately from the proof of Theorem 2, by replacing $\mathcal{L}_1$ and $\mathcal{L}_2$ in Theorem 2 with $\mathcal{L}_i$ and $\Sigma_{j \neq i}\mathcal{L}_j$, respectively.

(If): For sufficiency, the procedure given in Theorem 2 can be used to design k different residual generators, one generator for each of the residuals $r_i(t)$. This collection of residual generators, taken together, constitutes a solution to EFPRG. ●●

A family of failure signatures satisfying the conditions in (20) will be called a *strongly identifiable* family. Theorem 4 thus shows that it is possible to design an LTI residual generator that identifies simultaneous failures within a family of failure events if and only if the family is strongly identifiable.

The order of the residual generator given in Theorem 4, i.e., the sum of

the orders of the k different residual generators, can be quite large. Nevertheless, the residuals in this filter are generated by k completely decoupled filters, and there is a great deal of freedom in choosing the matrices F_i that govern the dynamics of these individual residual generators. This freedom can be used to simplify the decision-making phase of FDI by enhancing the effect of the failure or suppressing the effect of noise on the residual.

The generic solvability conditions for EFPRG are easily stated.

Proposition 5: With A, C and the L_i being arbitrary matrices of dimensions $n \times n$, $l \times n$, and $n \times k_i$, respectively, let $v := \Sigma_{i=1}^{k} k_i$. Then EFPRG generically has a solution if and only if

$$v \leq n \tag{21}$$

and

$$v - \min \{k_i, i \in k\} < l. \tag{22}$$

Proof: The simple proof is given in [15]. ●●

We now interpret the solvability condition for EFPRG in the frequency domain for the *special case where the failure signatures are simply column vectors*. By taking Laplace transforms in (2), we obtain

$$y(s) = G_u(s)u(s) + G_m(s)m(s) \tag{23a}$$

where

$$G_u(s) := C(sI-A)^{-1}B,\ G_m(s) := C(sI-A)^{-1}(L_1 \cdots L_k) \tag{23b}$$

and $m(s) = (m_1(s) \cdots m_k(s))'$. EFPRG involves generating a k-dimensional residual vector $r(s)$ by passing the observables through a causal LTI system

$$r(s) = (H_y(s)\ H_u(s)) \begin{pmatrix} y(s) \\ u(s) \end{pmatrix} = H(s)z(s) \tag{24}$$

where the definitions of $z(s)$ and $H(s)$ are evident from (24). The requirement in EFPRG is that the net transmission from the input $u(s)$ to the residual vector $r(s)$ be zero, and that the failure mode $m_i(s)$ only affect the ith component of $r(s)$. In other words, the objective is to find a proper post-compensator $H(s)$ such that

$$H(s)G(s) = (T(s)\ 0) \tag{25}$$

where

$$G(s) = \begin{pmatrix} G_m(s) & G_u(s) \\ 0 & I \end{pmatrix}. \tag{26}$$

The 0 in (25) is a $k \times m$ matrix, and $T(s)$ is a $k \times k$ *diagonal* matrix with nonzero diagonal elements $T_i(s)$. A further condition needs to be imposed so that, when no failure is present, the residuals due to initial conditions in the system and in the post-compensator die away. This translates to the requirement

$$H_y(s)C(sI-A)^{-1} \text{ and } H(s) \text{ both stable.} \tag{27}$$

It is shown in [15] (also see [16]) that the above problem has a solution if and only if the transfer matrix $G_m(s)$ is left invertible. In other words, when the failure signatures are column vectors, the condition of strong identifiability given in (20) is equivalent to the left invertibility of

$$C(sI-A)^{-1}(L_1 \cdots L_k). \tag{28}$$

The reader who is familiar with the control decoupling problem [9], [22] should readily recognize the dual relationship between the EFPRG and the decoupling problem. Despite the duality, the structure of the residual generator proposed in Theorem 4 is quite different from that of the extended decoupling controllers given in [22], since there is no compatibility issue (cf. [22]) in EFPRG.

An interesting question now is how to reduce the order of the processor proposed in Theorem 4. This task can be accomplished by either restricting the structure of the residual generator, as was done in [14] by formulating the RDDFP, or by relaxing the requirement that the filter should be capable of detecting and identifying simultaneous failures. We shall follow the latter path in the remainder of this note, by considering more complicated coding schemes than the one dealt with in this section.

V. Failure Detection and Identification Filter Problem (FDIFP)

Our objective in this section is to obtain necessary and sufficient conditions for the existence of a residual generator that can uniquely detect and identify a failure within a family of k possible failure events, *assuming that only one failure is present at a time*. This will lead to the concept of an identifiable family of failure signatures.

Assume that p residuals are to be used, and that a corresponding collection of coding sets $\Omega_j \subseteq p, j \in k$, is picked (see Section II). Define the finite set Γ_i as the collection of all those $j \in k$ for which the transfer function from the jth failure mode to the ith residual is required to be 0. The transfer matrices from all other failure modes to this residual are required to be input observable. The sets Γ_i, $i \in p$, evidently contain all the information required for specifying the structure of the transfer matrix relating the vector of failure modes to the vector of residuals. The earlier stability requirements are also maintained. With this definition, we can state the solvability condition for FDIFP.

Theorem 6: For a given family of coding sets, and with the assumption that there is only one failure present at a time, FDIFP has a solution if and only if

$$\mathcal{S}_{\Gamma_i} \cap \mathcal{L}_j = 0,\ j \in k - \Gamma_i,\quad i \in p \tag{29}$$

where

$$\mathcal{S}_{\Gamma_i} := \inf \underline{\mathcal{S}} \left(\sum_{j \in \Gamma_i} \mathcal{L}_j \right), \qquad i \in p. \tag{30}$$

Proof: Using the assumption that there is only one failure present at a time, we can think of FDIFP as p separate FPRG (see Section III) that need to be solved simultaneously. The proof therefore follows from Theorem 2. ●●

Our next objective is to show that FDIFP will not have a solution for certain families of failure events, no matter what coding scheme is used. For this, *assume that the failure signatures are column vectors* in the rest of this section.

The following result is crucial to our derivation.

Lemma 7: Let (C, A) be observable, $d(\mathcal{L}_1) = d(\mathcal{L}_2) = 1$, and $\mathcal{L}_1 \subseteq \mathfrak{I}_2^*$, where $\mathfrak{I}_2^* := \inf \underline{\mathcal{S}}(\mathcal{L}_2)$. Then $\mathfrak{I}_1^* = \mathfrak{I}_2^*$, where $\mathfrak{I}_1^* := \inf \underline{\mathcal{S}}(\mathcal{L}_1)$.

Proof: Since $\mathcal{L}_1 \subseteq \mathfrak{I}_2^*$ and $\mathfrak{I}_2^*$ is a u.o.s., $\mathfrak{I}_2^* \in \underline{\mathcal{S}}(\mathcal{L}_1)$. Thus, the infimality of $\mathfrak{I}_1^*$ implies that $\mathfrak{I}_1^* \subseteq \mathfrak{I}_2^*$, and hence that $C\mathfrak{I}_1^* \subseteq C\mathfrak{I}_2^*$. From the observability of (C, A) and results in [14], we know that $C\mathfrak{I}_1^*$ and $C\mathfrak{I}_2^*$ are both one-dimensional. Thus, $C\mathfrak{I}_1^* = C\mathfrak{I}_2^*$, or equivalently

$$\mathfrak{I}_1^* + \ker C = \mathfrak{I}_2^* + \ker C := \mathcal{V} \tag{31}$$

Also $\mathfrak{I}_2^*$ and $\mathfrak{I}_1^*$ are compatible since $\mathfrak{I}_1^* + \mathfrak{I}_2^* = \mathfrak{I}_2^*$ is (C, A)-invariant (see [14], [15]). Let $D \in \cap_i \underline{D}(\mathfrak{I}_i^*)$. Using (31) and the dual of Proposition 5.3 in [22], we have

$$\mathfrak{I}_2^* = \langle \mathcal{V} | A + DC \rangle = \mathfrak{I}_1^*.$$

●●

Theorem 8: Given an LTI system (C, A, B) with a family of failure signatures $\{L_i, i \in k\}$ and arbitrary failure modes, and assuming that there is only one failure present at a time, it is possible to design a coding set and a residual generator to detect and identify any failure within this family if and only if

$$\mathcal{L}_i \cap \mathfrak{I}_j^* = 0,\ i, j \in k,\ i \neq j \tag{32}$$

where $\mathfrak{I}_j^* = \inf \underline{\mathcal{S}}(\mathcal{L}_j)$.

Proof:

(Only If): Suppose that we have designed a residual generator with an appropriate family of coding sets. It follows that for any two distinct integers $i, j \in k$, there should exist an α such that either

$$i \in \Gamma_\alpha \text{ but } j \notin \Gamma_\alpha \tag{33}$$

or

$$j \in \Gamma_\alpha \text{ but } i \notin \Gamma_\alpha. \tag{34}$$

If (33) holds, then obviously $\mathfrak{I}_i^* \subseteq \mathcal{S}_{\Gamma\alpha}$. Similarly, if (34) holds, then $\mathfrak{I}_j^* \subseteq \mathcal{S}_{\Gamma\alpha}$. Now using the necessary condition given in (29), it follows that

$$\text{either } \mathcal{L}_i \cap \mathfrak{I}_j^* = 0 \text{ or } \mathcal{L}_j \cap \mathfrak{I}_i^* = 0. \tag{35}$$

Using (35) and Lemma 7, we then conclude that (32) necessarily should hold.

(If): We need to show that if a family of failure signatures satisfies the condition given in (32), then there exists a family of coding sets for which the FDIFP has a solution, with the assumption that only one failure is present at a time. For this, just use the coding sets

$$\Omega_i = \{1, \cdots, i-1, i+1, \cdots, k\}, \qquad i \in k \tag{36}$$

to design k different residual generators such that the unobservable subspace of the ith residual is $\mathfrak{I}_i^*$, so that the ith failure mode will not show up in this residual. ●●

A family of scalar failure signatures $\{L_i,\ i \in k\}$ satisfying the condition given in (32) will be called an *identifiable family* of failure signatures. Note that if a family of failure signatures is not identifiable, then there does not exist any processor that can detect and identify the failures in the sense of Section II.

It is also possible to state the frequency domain counterpart of the failure identifiability condition given in (32). From (28), we know that the condition

$$\mathcal{L}_i \cap \mathfrak{I}_j^* = 0 \text{ and } \mathcal{L}_j \cap \mathfrak{I}_i^* = 0$$

is equivalent to the statement that the transfer matrix $C(sI - A)^{-1}[L_i, L_j]$ is left invertible. Hence, the condition in (32) is equivalent to the statement that the rational vector subspaces spanned by the $C(sI - A)^{-1}L_i$ are nonintersecting. The necessity of this condition is obvious, since if the image of $C(sI - A)^{-1}L_i$ over the field of rational functions intersects the image of $C(sI - A)^{-1}L_j$, then there exist proper rational functions $m_i(s)$ and $m_j(s)$ such that

$$C(sI-A)^{-1}L_i m_i(s) = C(sI-A)^{-1}L_j m_j(s).$$

This means that the ith and jth failure modes can result in the same output, so it will be impossible to distinguish between these two failures by observing the output of the system.

VI. Conclusion

In this note we have solved the problem of residual generation for FDI by processing the inputs and outputs of an LTI system. We have also developed simple design procedures for generating the residuals when the solvability conditions are satisfied.

Replacing the left-hand side of (2a) by $x(t + 1)$ to obtain a discrete-time model does not change the solvability conditions for any of the problems we have formulated here. In residual generators for discrete-time systems, we can assign the spectrum of the filter to the origin of the complex plane and hence obtain deadbeat behavior. It can be shown that the residuals thus obtained are the same as those produced by generalized parity relations, [4], [5], [12], [13], and [16]. We refer the reader to [16] and [15] for a more complete discussion of the relationship between the generalized parity relations and the residual generators discussed in this note.

A challenging problem for future work is to generate residuals that are robust to modeling errors. The above references on parity relations contain some preliminary results in this direction. The issue in robust residual generation is not simply the stability of the perturbed system—which is what much of the literature on robust control emphasizes—but also the preservation, in some sense, of the coding structure of the transfer matrices.

References

[1] G. Basile and G. Marro, "Controlled and conditioned invariant subspaces in linear system theory," *J. Optimiz. Theory*, vol. 3, pp. 306–315, 1969.

[2] R. V. Beard, "Failure accommodation in linear systems through self-reorganization," Ph.D. dissertation, Dep. Aero. Astro., Mass. Inst. Technol., Cambridge, Feb. 1971.

[3] S. P. Bhattacharya, "Observer design for linear systems with unknown inputs," *IEEE Trans. Automat. Contr.*, vol. AC-23, pp. 483–484, June 1978.

[4] E. Y. Chow, "A failure detection system design methodology," Ph.D. dissertation, Dep. EECS, Mass. Inst. Technol., Cambridge, Oct. 1980.

[5] E. Y. Chow and A. S. Willsky, "Analytical redundancy and the design of robust detection systems," *IEEE Trans. Automat. Contr.*, vol. AC-29, pp. 689–691, July 1984.

[6] J. C. Deckert, M. N. Desai, J. J. Deyst, and A. S. Willsky, "F-8 DFBW sensor failure identification using analytical redundancy," *IEEE Trans. Automat. Contr.*, vol. AC-22, pp. 795–803, Oct. 1977.

[7] F. A. Evans and J. C. Wilcox, "Experimental strapdown redundant sensor inertial navigation systems," *J. Spacecraft Rockets*, vol. 7, pp. 1070–1074, Sept. 1970.

[8] J. P. Gilmore and R. A. McKern, "A redundant strapdown inertial reference unit (SIRU)," *J. Spacecraft Rockets*, vol. 9, pp. 39–47, Jan. 1972.

[9] M. L. J. Hautus and M. Heymann, "Linear feedback decoupling—Transfer function analysis," *IEEE Trans. Automat. Contr.*, vol. AC-28, pp. 823–832, Aug. 1983.

[10] R. Isermann, "Process fault detection based on modeling and estimation methods—A survey," *Automatica*, vol. 20, pp. 387–404, July 1984.

[11] H. L. Jones, "Failure detection in linear systems," Ph.D. dissertation, Dep. Aero. Astro., Mass. Inst. Technol., Cambridge, Aug. 1973.

[12] X. C. Lou, "A system failure detection method: Failure projection," S.M. thesis, Dep. EECS, Mass. Inst. Technol., Cambridge, June 1982.

[13] X. C. Lou, A. S. Willsky, and G. C. Verghese, "Optimally robust redundancy relations," *Automatica*, vol. 22, pp. 333–344, 1986.

[14] M. A. Massoumnia, "A geometric approach to the synthesis of failure detection filters," *IEEE Trans. Automat. Contr.*, vol. AC-31, pp. 839–846, Sept. 1986.

[15] M. A. Massoumnia, "A geometric approach to failure detection and identification in linear systems," Ph.D. dissertation, Dep. Aero. Astro., Mass. Inst. Technol., Cambridge, Feb. 1986.

[16] M. A. Massoumnia and W. E. Vander Velde, "Generating parity relations for detecting and identifying control system component failures," *AIAA J. Guidance Contr.*, to be published.

[17] J. M. Schumacher, "Compensator synthesis using (*C*, *A*, *B*)-pairs," *IEEE Trans. Automat. Contr.*, vol. AC-25, pp. 1133–1138, Dec. 1980.

[18] J. M. Schumacher, "Regulator synthesis using (*C*, *A*, *B*)-pairs," *IEEE Trans. Automat. Contr.*, vol. AC-27, pp. 1211–1221, Dec. 1982.

[19] B. K. Walker, "Recent developments in fault diagnosis and accommodation," presented at the AIAA Guidance Contr. Conf., Aug. 1985.

[20] J. C. Willems and J. Commault, "Disturbance decoupling by measurement feedback with stability or pole placement," *SIAM J. Contr. Optimiz.*, vol. 19, pp. 490–504, July 1981.

[21] A. S. Willsky, "A survey of design methods for failure detection in dynamic systems," *Automatica*, vol. 12, pp. 601–611, Nov. 1976.

[22] W. M. Wonham, *Linear Multivariable Control: A Geometric Approach*. New York: Springer-Verlag, 1985.

[23] J. E. White and J. L. Speyer, "Detection filter design: Spectral theory and algorithms," *IEEE Trans. Automat. Contr.*, vol. AC-321, pp. 593–603, June 1987.

On the Properties of Reduced-Order Kalman Filters

BERNARD FRIEDLAND

Abstract—**Several known results are unified by considering properties of reduced-order Kalman filters. For the case in which the number of noise sources equals the number of observations, it is shown that the reduced-order Kalman filter achieves zero steady-state variance of the estimation error if and only if the plant has no transmission zeros in the right-half plane, since these would be among the poles of the Kalman filter. The reduced-order Kalman filter cannot achieve zero variance of the estimation error if the number of independent noise sources exceeds the number of observations. It is also shown that the reduced-order Kalman filter achieves the generalized Doyle-Stein condition for robust-**

Manuscript received February 23, 1987; revised September 14, 1987. Paper recommended by Associate Editor, B. Sridhar.

The author is with the Kearfott Guidance and Navigation Corp., Little Falls, NJ 07424.

IEEE Log Number 8824286.

0018-9286/89/0300-0321$01.00 © 1989 IEEE