July 1986 LIDS-P-1578

Failure Detection and Identification in Linear Time-Invariant Systems

MOHAMMAD-ALI MASSOUMNIA [1]

GEORGE C. VERGHESE [2]

ALAN S. WILLSKY [3]

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

June 23, 1986

Please send all correspondence to:
Professor Alan Willsky
MIT
Room 35-231
Cambridge, MA 02139

[1] The author was with Space Systems Laboratory. He is now at 18 Dabirestan Alborz Alley, Tehran, Iran, 15916

[2] Laboratory for Electromagnetic and Electronic Systems

[3] Laboratory for Information and Decision Systems

The work of (1) was supported by NASA Langley Research Center under Grant NAG1-126

The work of (2) and (3) was supported in part by the Air Force Office of Scientific Research under Grant AFOSR-82-0258

Failure Detection and Identification in Linear Time-Invariant Systems

MOHAMMAD-ALI MASSOUMNIA

GEORGE C. VERGHESE

ALAN S. WILLSKY

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Abstract

A solution to the problem of detecting and identifying control system component failures in linear time-invariant systems is given using the geometric concept of an unobservability subspace. Conditions are developed under which it is possible to design a causal linear processor that can be used to detect and uniquely identify a component failure in a linear time-invariant system, assuming either i) the components can fail simultaneously, or ii) the components can fail only one at a time. Explicit design algorithms are provided when those conditions are satisfied. In addition to the time domain solvability conditions, the frequency domain interpretation of the results are given, and connection is drawn with the results already available in the literature.

Table of Contents

List of Figures

1. Introduction

In many applications high reliability control systems are necessary. In some space missions, for example, a system with hundreds of components is required to operate for a period of several years. Such systems must naturally employ highly sophisticated fault tolerant control systems (FTCS) with redundant capacity to perform a given task. The need for very high reliability has led to extensive research into design of systems that can do their job using more than one configuration of their components.

Currently there are two different approaches to the design of reliable systems. In the first approach, the objective is to reduce the dependence of the system on the operation of individual components and develop systems that remain operational even in the presence of a failure without any corrective action being undertaken. A few examples of this *passive* approach to FTCS are quadriplexed fly-by-wire digital flight control systems and the mid-value select algorithm.

Instead of triplicating or quadriplicating the expensive hardware components or sacrificing the performance of the system under nominal operating conditions in order to gain fault tolerant capability, one can first *detect and identify* the failed component using additional information processing and then reconfigure the system to *accommodate* the failure. Clearly, this *active* approach requires more complex information processing capabilities, but with increasing availability of low cost digital computers this will be the preferred approach-- especially if it can result in superior performance.

The integral part of an FTCS is failure detection and identification (FDI). An FDI process essentially consists of two stages. The first stage is residual generation, and the second stage involves using the residuals to make the appropriate decisions. In this work we shall only concentrate on residual generation, and refer the reader to the extensive literature available for the decision making phase of FDI (see [23], [10], and [20] for comprehensive surveys).

The output of a residual generator is by definition a function of time that is nominally zero or close to zero when no failure is present, but is distinguishably different from zero when a component of the system fails. For example, a simple residual can be generated by differencing the outputs of two identical sensors that measure the same quantity. A failure of either sensor corrupts the residual and this can be used to detect a failure. The process of generating the residuals from relationships among instantaneous outputs of sensors is usually called *direct redundancy.* Two examples where direct redundancy was exploited are [7, 8].

It is also possible to generate the residuals using *temporal redundancy,* which is the process of exploiting the relationships among the histories of sensor outputs and actuator inputs. This is usually done by using a hypothesized model of the dynamics of the system to relate sensor outputs and actuator inputs at different instants of time. We refer the reader to [6] for an example of the use of temporal redundancy in residual generation.

Among all methods that employ temporal redundancy, two are distinguished as being applicable both to sensor and actuator FDI and, in addition, not requiring any assumption 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 [12, 13], and the *failure detection filter* introduced by Beard [2], which was later amplifed by Jones [11] and recently revisited by Massoumnia [14].

Each of these two methods involves the design of a linear processor of a particular type of structure. In failure detection and identification filters, 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 (hence greatly simplifying the subsequent decision-making process). The restriction to the class of full-state observer is, as we shall see, a rather severe constraint, as it not only restricts significantly the class of problems that have solutions (the set of possible failure modes must satisfy a strong *mutual detcetability* (cf. [14]) condition), but it also makes the design process and the nature of the FDI problem appear more complicated than they should.

In the case of generalized parity checks, the concept behind the design process is excedingly simple: we seek residuals generated by forming linear combinations of a finite window of sensor output and applied input values so that all of the residuals are zero when the components are functioning perfectly, but a particular subset of the residuals deviate from zero when a particular system component fails. Again the class of linear processors considered in this design procedure is severely restricted and does not, for example, allow one much freedom in adjusting any free parameters to optimize noise rejection.

In this paper we remove the constraints imposed in these previous studies. In particular, the only constraint we place on our residual generation mechanism are: (a) they produce residuals with the same desirable properties as in previous studies, namely that particular residuals are sensitive only to particular component failure modes; and (b) the mechanism must be a finite-dimensional, linear, time-invariant causal system--i.e., we *do not* restrict ourselves to the far smaller classes of processors considered in previous work. As we shall see, within this setting it is possible to construct such processors to uniquely identify failures under less restrictive conditions than those previously reported.

For solving the problem of residual generation, we shall rely heavily on a few geometric concepts. Most of these concepts are dual to the ones already developed in the control literature. In fact, by extending the results of [14], we more fully exploit the dual relationship and the subtle differences between the residual generation problem and the control decoupling problem [9, 24].

We begin in Section 2 by formulating the problem of residual generation, and show

how both sensor and actuator failures and also changes in the system parameters can be modeled in a unified manner as actuator failures. In Section 3, the fundamental problem of residual generation is defined. In this problem it is assumed that there are only two possible faulty components and it is desired to generate a residual that is affected by the failure of the first component but not by the failure of the second component. By comparing this residual with a threshold one can decide whether the first component is operating properly or not. In Section 4, the fundamental problem of residual generation is extended to the case of multiple simultaneous failures. The solvability condition of this problem leads to the introduction of the fundamental system theoretic concept of a strongly identifiable family of failure events. In Section 6, the most general form of the FDI problem (within the framework stated in Section 2) is solved. The solution of this problem leads to the introduction of the concept of an identifiable family of failure events.

Before proceeding with a complete formulation of the failure detection and identification problem, we review our notation. Throughout the paper real vector spaces are denoted by script letters $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$, and their typical elements by x, y, z. The symbol $d(\mathcal{X})$ denotes the dimension of $\mathcal{X}$. Matrices and linear maps are all represented by capital italic letters, e.g., A, B, C . For an arbitrary map L, the symbol Im L denotes the image of L; from time to time the subspace Im L is denoted by $\mathcal{L}$. Also Ker L denotes the null space of L. The maps $A : \mathcal{X} \rightarrow \mathcal{X}$, $B : \mathcal{U} \rightarrow \mathcal{X}$, and $C : \mathcal{X} \rightarrow \mathcal{Y}$ ($d(\mathcal{X}) = n$, $d(\mathcal{U}) = m$, $d(\mathcal{Y}) = l$) are fixed throughout and are associated with the "system (C,A,B)", namely

$$\overset{\circ}{x}(t) = A\,x(t) + B\,u(t), \quad y(t) = C\,x(t).$$

The spectrum of A is denoted by $\sigma(A)$ and $\uplus$ denotes union with any common elements repeated. We say a set Λ is symmetric if $\lambda \in \Lambda$ implies $\lambda^* \in \Lambda$ where * denotes the complex conjugate. With k a positive integer, $\mathbf{k}$ will denote the finite set $\{1,2, \ldots ,k\}$, and $\mathbf{k\text{-}1} = \{1, \ldots ,k{-}1\}$. Moreover, the Laplace transform of an arbitrary function $m(t)$ is denoted by $m(s)$.

2. Failure Representation and Problem Formulation

Assume our nominal linear time-invariant (LTI) system is described by the state-space model

$$\begin{aligned} \mathring{x}(t) &= A\,x(t) + B\,u(t), \\ y(t) &= C\,x(t). \end{aligned} \tag{1}$$

Here $x(t) \in \mathcal{X}$, $u(t) \in \mathcal{U}$, and $y(t) \in \mathcal{Y}$ with the dimensions of $\mathcal{X}$, $\mathcal{U}$, and $\mathcal{Y}$ being n, m, and l respectively. The nominal input $u(t)$ to the plant and the measurement $y(t)$ are assumed to be known and will be referred to as the observables of the system.

Now assume that some unknown disturbances affect the behavior of the plant. These disturbances can be sensor failures and disturbances at the output, which directly corrupt the measurement $y(t)$, or they can be actuator failures and external input disturbances, which will show up in $y(t)$ after their effects are integrated through the dynamics of the system. The most general form of disturbances that can affect the output of the system shown in (1) can be represented as follows:

$$\begin{aligned} \mathring{x}(t) &= A\,x(t) + B\,u(t) + \textstyle\sum_{i=1}^{k} L_i m_i(t), \\ y(t) &= C\,x(t) + \textstyle\sum_{i=1}^{q} J_i n_i(t). \end{aligned} \tag{2}$$

Here $m_i(t) \in \mathcal{M}_i$ ($d(\mathcal{M}_i) = k_i$) and $n_i(t) \in \mathcal{N}_i$ ($d(\mathcal{N}_i) = q_i$) are unknown functions of time and can be arbitrary. However, when no failure or disturbance is present, $m_i(t)$ and $n_i(t)$ are all, by definition, equal to zero. We refer to the functions $m_i(t)$ and $n_i(t)$ as *failure modes.*

In order to model the effect of failures in the j-th actuator, simply set $L_1 = B_j$ where B_j is the j-th column of the control effectiveness matrix B, for example, if the actuator does not respond to the applied input, then $m_1(t) = -u_j(t)$ where $u_j(t)$ is the j-th element of the input vector $u(t)$. If the actuator has a bias b, then $m_1(t) = b$. If the actuator becomes stuck at a value h, then $m_1(t) = h - u_j(t)$. Because we do not constrain $m_i(t)$ to any special function class, a wide variety of actuator failure modes fits this representation. From now on we shall refer to the maps $L_i : \mathcal{M}_i \rightarrow \mathcal{X}$ as *actuator failure signatures.* Note that the failure signatures L_i can be matrices, and are not constrained to just being vectors.

We can also model a change in the dynamics of the plant, i.e., a change in the A matrix, by choosing L_i appropriately; in this case $m_i(t)$ will be a linear combination of the states of the system $x(t)$. Thus, as far as failure modeling is concerned, a change in the dynamics of the system can be modeled in the same manner as an actuator failure. The term actuator failure will therefore be used to refer to any failure event that can be modeled by choosing L_i appropriately.

Similarly, to model the failure of the j-th sensor, simply set $J_1 = e_j$ where e_j is the j-th column of the $l \times l$ identity matrix. If for instance the sensor fails completely, i.e., gives a zero output, then $n_1(t) = -c_j^{\prime} x(t)$ where $c_j^{\prime}$ is the j-th row of the measurement matrix C. As should be clear by now, this representation can be used to model a wide variety of sensor failure modes. Moreover, as in the case of actuator failures, the J_i can be matrices, and are not constrained to be vectors. From now on we shall refer to the maps $J_i : \mathcal{N}_i \rightarrow \mathcal{Y}$ as *sensor failure signatures.*

One major distnction between our approach to failure modeling and the majority of approaches reported in the literature is that we do not assume any *a priori* mode of component failure, i.e., $m_i(t)$ and $n_i(t)$ in (2) can be arbitrary. However, here it is assumed that the failure can be represented by choosing an appropriate L_i or J_i. Note that the same assumption was the basis for the work of Beard and Jones [2, 11].

Since the $m_i(t)$ and $n_j(t)$ are arbitrary, there is no loss of generality in assuming (as we shall from now on) that the failure signatures are one-to-one. We shall at times make the assumption that the failure modes are generic in a sense that will be specified when the occasion arises.

We shall also find it more convenient to represent sensor failures by pseudo-actuator failures, as described next. In particluar, note that, without loss of generality, it can be assumed that the unknown function $n_i(t)$ is the output of some linear time-invariant system Σ_i with impulse response $h_i(t,\tau)$ and some arbitrary input $s_i(t)$. The only restriction on Σ_i is that it should be right invertible so that for any $n_i(t)$ there exists an $s_i(t)$ such that

$$n_i(t) = \int_0^t h(t,\tau)\, s_i(\tau)\, d\tau, \quad t \geq 0.$$

For the case where the $n_i(t)$ are simply scalars, we can assume without loss of generality that

$$\overset{\circ}{n}_i(t) = a_i\, n_i(t) + s_i(t)$$

for some scalars a_i and unknown functions $s_i(t)$. If the dynamics of the systems generating the sensor failure modes are added to the dynamics of the system, the sensor failures can be represented as actuator failures. In this augmented representation, $s_i(t)$ appears as a pseudo-actuator failure mode and consequently no sensor failure signature will be present. Hence, all the analysis that follows uses the model

$$\overset{\circ}{x}\,(t) = A\, x(t) + B\, u(t) + \textstyle\sum_{i=1}^{k} L_i m_i(t),$$
$$y(t) = C\, x(t). \tag{3}$$

It is assumed that the maps A, B, L_i, and C have already been appropriately modified so that the sensor failures are properly represented as pseudo-actuator failures. One caveat is that the augmented model (3) may not be observable even if the systems in (2) was observable. However, by properly choosing the augmented dynamics so that they do not coincide with the spectrum of A in (2), it is always possible to get an observable augmented model if the unagumented system was observable.

Considering now the system in (3), we define the failure detection and identification filter problem (FDIFP) as the problem of designing a dynamic residual generator, Σ_r, that takes the observables $u(t)$ and $y(t)$ as inputs and generates a set of residual vectors $r_i(t)$ ($i \in \mathbf{p}$) with the following properties:

1. When no failure is present, the residuals $r_i(t)$ ($i \in \mathbf{p}$) are identically equal to zero. Hence, the net transmission from the input of the system $u(t)$ to the residuals $r_i(t)$ ($i \in \mathbf{p}$) should be zero.

2. When the j-th component fails (i.e., $m_j(t) \neq 0$), the residuals $r_i(t)$ for $i \in \Omega_j$ should be nonzero, and the other residuals $r_s(t)$, $s \in \mathbf{p}-\Omega_j$, all should be identically equal to zero. Here the family of *coding sets* $\Omega_j \subseteq \mathbf{p}$ ($j \in \mathbf{k}$) are to be chosen such that we can uniquely identify the failed component or components by knowing which of the $r_i(t)$ are zero or not.

We say more about the coding sets Ω_j later in this section and also in Section 6. A block diagram of an FDIF is given in Figure 2-1.

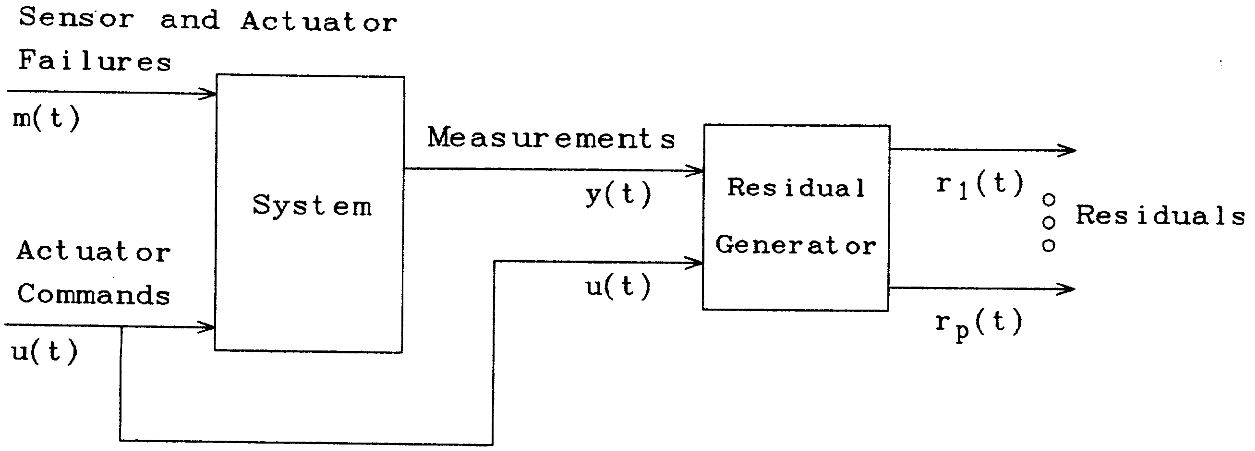

Figure 2-1: Block Diagram of an FDIF

Note that in the general problem there is no constraint on the number p of the residuals.

If we can generate a set of residuals with the above properties, then the identification task is trivial. One needs only to compare the magnitudes of the residuals against some appropriate thresholds to decide which ones correspond to responses to actual failures, and then by referring to the table of the coding sets one can identify the failure, if a failure is present.

One important design consideration is how to choose the coding sets Ω_i. The simplest choice is just to take $p=k$ and $\Omega_j = \{j\}$ ($j \in \mathbf{k}$), i.e., to let precisely one of the residuals be nonzero for any one failure. In addition, this coding scheme enables us to detect and correctly identify simultaneous failures. In Sections 5 and 6, we shall go over more complicated coding schemes. It should be noted that with some coding schemes it is not possible to detect and identify the presence of simultaneous failures. As a matter of fact, for some coding sets, simultaneous failures can lead to identification of the wrong component as failed. However, no matter what coding sets are used, there are families of components for which a failure of a component within the family cannot be uniquely identified. This fundamental limitation will be discussed in Section 6.

Now, consider the most general form of a realizable LTI processor that takes $y(t)$ and $u(t)$ as inputs and generates a set of residuals $r_i(t)$ ($i \in \mathbf{p}$) as outputs,

$$\begin{aligned} \overset{\circ}{w}(t) &= F\,w(t) - E\,y(t) + G\,u(t), \\ r_i(t) &= M_i\,w(t) - H_i\,y(t) + K_i\,u(t), \quad i \in \mathbf{p}, \\ r(t) &= [r_1'(t), \ \ldots, \ r_p'(t)]'. \end{aligned} \tag{4}$$

Here $r_i(t) \in \mathcal{R}_i$ and $r(t) \in \mathcal{R} := \mathcal{R}_1 \oplus \cdots \oplus \mathcal{R}_p$. Also the minus signs in E and H_i are just chosen for convenience in what follows.

We can now restate FDIFP as the problem of finding F, E, G, M_i, K_i, and H_i in (4) such that the transfer matrices relating the $m_i(t)$ and $r_i(t)$ have the properties mentioned previously that enable us to determiine from the residuals $r_i(t)$ which of the $m_j(t)$ are nonzero.

Before proceeding with the solution of FDIFP, we review a few geometric concepts that will be useful in solving the problem.

A subspace $\mathcal{S} \subseteq \mathcal{X}$ is termed A-invariant if $A\,\mathcal{S} \subseteq \mathcal{S}$. Let $\mathcal{S} \subseteq \mathcal{X}$ be A-invariant; we write $A: \mathcal{S}$ for the restriction of A to $\mathcal{S}$, and $A: \mathcal{X}/\mathcal{S}$ for the map induced by A on the factor space $\mathcal{X}/\mathcal{S}$. Moreover, if $\mathcal{S}$ and $\mathcal{T}$ are both A-invariant subspaces and $\mathcal{S} \subseteq \mathcal{T}$, we write $A: \mathcal{T}/\mathcal{S}$ for the operator induced by the restriction of A to $\mathcal{T}$ on the factor space $\mathcal{T}/\mathcal{S}$.

We write $\mathcal{B} = \operatorname{Im} B$ and $<A|\mathcal{B}> = \mathcal{B} + A\mathcal{B} + \cdots + A^{n-1}\mathcal{B}$ for the infimal A-invariant subspace containing $\mathcal{B}$, i.e., the reachable subspace of (A,B). We write $\mathcal{K} = \operatorname{Ker} C$ and $<\mathcal{K}|A> = \mathcal{K} \cap A^{-1}\mathcal{K} \cap \cdots \cap A^{-n+1}\mathcal{K}$ for the supremal A-invariant subspace contained in $\mathcal{K}$, i.e., the unobservable subspace of (C,A).

We say a subspace $\mathcal{W} \subseteq \mathcal{X}$ is (C,A)-*invariant* if there exists a map $D: \mathcal{Y} \rightarrow \mathcal{X}$ such that $(A+DC)\,\mathcal{W} \subseteq \mathcal{W}$ [1, 22, 24]. Let $\mathcal{W}$ be (C,A)-invariant; we denote by $\underline{D}(\mathcal{W})$ the class of all maps D such that $(A+DC)\,\mathcal{W} \subseteq \mathcal{W}$. Let $\mathcal{L} \subseteq \mathcal{X}$; we denote the family of (C,A)-invariant subspaces containing $\mathcal{L}$ by $\underline{\mathcal{W}}(\mathcal{L})$. The family $\underline{\mathcal{W}}(\mathcal{L})$ is closed under intersection; hence, $\underline{\mathcal{W}}(\mathcal{L})$ contains an infimal element $\mathcal{W}^* := \inf \underline{\mathcal{W}}(\mathcal{L})$ [22]. Also $\mathcal{W}^* = \lim \mathcal{W}^k$ where $\mathcal{W}^k$ is given by the following recursive algorithm [24]

$$\mathcal{W}^{k+1} = \mathcal{L} + A\,(\mathcal{W}^k \cap \operatorname{Ker} C), \quad \mathcal{W}^0 = 0. \tag{5}$$

We say a subspace $\mathcal{S} \subseteq \mathcal{X}$ is a (C,A) ***unobservability subspace*** (u.o.s.) (complementary observability subspace according to [22]) if $\mathcal{S} = <\operatorname{Ker} HC|A+DC>$ for some output injection map $D: \mathcal{Y} \rightarrow \mathcal{X}$ and measurement mixing map $H: \mathcal{Y} \rightarrow \mathcal{Y}$ [15, 22]. Note that $\mathcal{S}$ is the unobservable subspace of the pair $(HC, A+DC)$, and the spectrum of $A+DC: \mathcal{X}/\mathcal{S}$ can be assigned to an arbitrary symmetric set by appropriate choice of D [15]. We use the notation $\underline{\mathcal{S}}(\mathcal{L})$ for the class of u.o.s.'s containing $\mathcal{L}$. The class $\underline{\mathcal{S}}(\mathcal{L})$ is closed under intersection; it therefore contains an infimal element $\mathcal{S}^* := \inf \underline{\mathcal{S}}(\mathcal{L})$ [22, 24]. Also $\mathcal{S}^* = \lim \mathcal{S}^k$ where $\mathcal{S}^k$ is given by the following recursive algorithm [24]

$$\mathcal{S}^{k+1} = \mathcal{W}^* + (A^{-1}\mathcal{S}^k) \cap \operatorname{Ker} C, \quad \mathcal{S}^0 = \mathcal{X}. \tag{6}$$

Moreover, for any $D \in \underline{D}(\mathcal{S}^*)$,

$$\mathcal{S}^* = <\mathrm{Ker}\, C + \mathcal{S}^*|A{+}DC>. \qquad (7)$$

Let $\{\mathcal{W}_i,\ i \in \mathbf{k}\}$ be a family of (C,A)-invariant subspaces of $\mathcal{X}$. We say $\{\mathcal{W}_i,\ i \in \mathbf{k}\}$ is *compatible* (cf. [14]) if

$$\cap_{i=1}^{k} \underline{D}(\mathcal{W}_i) \neq \emptyset\, ,$$

i.e., if there exists a D such that every $\mathcal{W}_i$ is $(A{+}DC)$-invariant.

Using the above geometric concepts, we first solve a restricted version of the FDIFP in Secton 3. The solution to this problem will then be used to tackle more general problems in the sections that follow.

3. The Fundamental Problem in Residual Generation

In this section, we assume that only two failure events are present, and examine when one can design a residual generator that is sensitive to the failure of the first actuator but is insensitive to the failure of the second actuator. This restricted version of FDIFP will be called the fundamental problem in residual generation (FPRG). Later on, FPRG will be extended to more general cases.

Consider the model given in (3) with $k = 2$,

$$\begin{aligned}\dot{x}(t) &= A\,x(t) + B\,u(t) + L_1\,m_1(t) + L_2\,m_2(t),\\ y(t) &= C\,x(t). \end{aligned} \qquad (8)$$

The dimensions of the maps shown in (8) are the same as the ones given in (1) and (2). 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 measurement $y(t) \in \mathcal{Y}$ and the known actuation signal $u(t) \in \mathcal{U}$.

Now consider a residual generator of the form

$$\begin{aligned} \mathring{w}(t) &= F\,w(t) - E\,y(t) + G\,u(t), \\ r(t) &= M\,w(t) - H\,y(t) + K\,u(t). \end{aligned} \tag{9}$$

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

First combine (8) and (9) as follows:

$$\begin{aligned} \begin{bmatrix} \mathring{x}(t) \\ \mathring{w}(t) \end{bmatrix} &= \begin{bmatrix} A & 0 \\ \text{-}EC & F \end{bmatrix} \begin{bmatrix} x(t) \\ w(t) \end{bmatrix} + \begin{bmatrix} B & L_2 \\ G & 0 \end{bmatrix} \begin{bmatrix} u(t) \\ m_2(t) \end{bmatrix} + \begin{bmatrix} L_1 \\ 0 \end{bmatrix} m_1(t), \\ r(t) &= [\ \text{-}HC \quad M\ ] \begin{bmatrix} x(t) \\ w(t) \end{bmatrix} + [\ K \quad 0\ ] \begin{bmatrix} u(t) \\ m_2(t) \end{bmatrix}. \end{aligned} \tag{10}$$

Define the extended spaces $\mathcal{X}^e := \mathcal{X} \oplus \mathcal{W}$ and $\mathcal{U}^e = \mathcal{U} \oplus \mathcal{M}_2$. Let $x^e := (x, w) \in \mathcal{X}^e$ and $u^e := (u, m_2) \in \mathcal{U}^e$. Equation (10) can then be rewritten as follows:

$$\begin{aligned} \mathring{x}^e(t) &= A^e x^e(t) + B^e\,u^e(t) + L^e m_1(t), \\ r(t) &= H^e x^e(t) + K^e u^e(t), \end{aligned} \tag{11}$$

where the definition of the matrices A^e, L^e, B^e, H^e, and K^e are evident from (10).

Now we formalize the statement that the failure of the first component should showup in the residual $r(t)$, i.e., that a nonzero $m_1(t)$ should showup in $r(t)$. There are several possible mathematically unequivalent formulation of the above statement. The most natural formulation is to require that the transfer matrix from $m_1(s)$ to $r(s)$ to be left invertible so that any nonzero $m_1(t)$ results in a nonzero $r(t)$.

However, another approach is to only require that the system relating $m_1(t)$ to $r(t)$ to 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,this is equivalent to the requirement that the columns of $C(sI-A)^{-1}B$ should be linearly independent over the field of real numbers. We note that even if the system relating $m_1(t)$ to $r(t)$ is not left invertible but is only input observable, it will be extremely unlikely that an arbitrary nonzero $m_1(t)$ will hide itself for all t in the null space of the mapping from $m_1(t)$ to $r(t)$ so that the failure can not be detected. Hence, if we only require input obvservability, then *almost any* nonzero $m_1(t)$ will produce a nonzero residual $r(t)$. Therefore, it may be argued that the ideal requirement of left invertibility is somewhat of an overkill for failure detection and identification purposes.

It may be further argued that we can even relax the condition of input observability and require only that the transfer matrix from $m_1(s)$ to $r(s)$ to be nonzero. However, it will then generally not be possible to reconstruct $m_1(t)$ from $r(t)$. By contrast, input observability implies that if the failure mode $m_1(t)$ has some rather mild properties, then it is possible to reconstruct $m_1(t)$ from $r(t)$. Note that during the failure accommodation, the one-to-one relation between $m_1(t)$ and $r(t)$ can be very valuable, since we can theoretically determine $m_1(t)$ from $r(t)$ and hence compensate for its adverse effects.

Finally, if we are dealing with a single-input multi-output system, i.e., if the transfer matrix is simply a column vector, then input observability automatically implies left invertibility. In the context of the FDI problem, the transfer matrix $T(s)$ relating $m_1(s)$ to $r(s)$ is usually a column vector (or a scalar), since the failure signature L_1 is usually a column vector. Therefore, in the FDI problem the input observability of $T(s)$ is typically equivalent to its left invertibility.

Based on these arguments, we state FPRG as follows. Consider the system given in (10) and (11). FPRG is the problem of finding F, E, G, M, H, and K such that:

$$u^e = (u,\, m_2) \mapsto r = 0, \qquad (12)$$

$$m_1 \mapsto r \text{ input observable.} \tag{13}$$

Furthermore, when the condition in (12) is satisfied and the first actuator is functioning properly, all signals $r(t)$ obtainable by varying the initial conditions $x(0)$ and $w(0)$ are exactly those outputs obtainable by varying the initial condition $e(0)$ of $\overset{\circ}{e} = F_0\, e$, $r = M_0\, e$, for some observable pair (M_0,F_0). The spectrum of F_0 determines the dynamics of the residual generator. In addition to the conditions in ((12) and (13) we shall require that, the dynamics of the residual generator be stable.

We need a few preliminary results for deriving the solvability condition for FPRG. First, let $\mathcal{X}^e$ be as defined previously in this section. With $x \in \mathcal{X}$, define the embedding map $Q : \mathcal{X} \rightarrow \mathcal{X}^e$ as follows:

$$Q\, x = \left| \begin{matrix} x \\ 0 \end{matrix} \right|. \tag{14}$$

Note that if $\mathcal{V} \subseteq \mathcal{X}^e$; then

$$Q^{-1}\mathcal{V} = \{x : x \in \mathcal{X} \;\&\; \left| \begin{matrix} x \\ 0 \end{matrix} \right| \in \mathcal{V}\}. \tag{15}$$

Less precisely, $Q^{-1}\mathcal{V}$ is the intersection of the subspaces $\mathcal{V}$ and $\mathcal{X}$.

Using the above definitions, it is relatively simple to relate the unobservability subspaces of the systems in (11) and (8). The following fundamental result, which exactly accomplishes this task, is crucial to the solvability condition of FPRG.

Proposition 1: Let $\mathcal{S}^e$ be the unobservable subspace of (H^e,A^e); then $Q^{-1}\mathcal{S}^e$ is a (C,A) unobservability subspace [21, 19, 18]. $\otimes$

With this result at our disposal, the solvability condition is immediate.

Theorem 2: FPRG has a solution if and only if

$$\mathcal{S}^* \cap \mathcal{L}_1 = 0, \tag{16}$$

where $\mathcal{S}^* = \inf \underline{\mathcal{S}}(\mathcal{L}_2)$. Also if (16) holds, then the dynamic of the residual generator can be assigned arbitrarily.

Proof: (only if) Consider the systems given in (11) and (10). For (12) to hold, we should have $K^e = 0$, and

$$<A^e|\mathcal{B}^e> \subseteq \mathcal{S}^e := <\mathrm{Ker}\, H^e|A^e>. \tag{17}$$

Equation (17) 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,

$$\mathcal{S} \in \underline{\mathcal{S}}(\mathcal{L}_2). \tag{18}$$

For (13) 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

$$\begin{aligned} Q^{-1}(\mathcal{L}^e \cap \mathcal{S}^e) &= Q^{-1}\mathcal{L}^e \cap Q^{-1}\mathcal{S}^e \\ &= \mathcal{L}_1 \cap \mathcal{S} = 0. \end{aligned} \tag{19}$$

Obviously (18) and (19) hold only if (16) is true.

(if) Let $D_0 \in \underline{D}(\mathcal{S}^*)$, $P: \mathcal{X} \rightarrow \mathcal{X}/\mathcal{S}^*$ be the canonical projection, and $A_0 := (A+D_0C : \mathcal{X}/\mathcal{S}^*)$. Let H be a solution of $\mathrm{Ker}\, HC = \mathcal{S}^* + \mathrm{Ker}\, C$ and M be the unique solution of $MP = HC$. By construction, the pair (M,A_0) is observable, hence there exists a D_1 such that $\sigma(F) = \Lambda$ where $F := A_0+D_1M$ and Λ is an arbitrary symmetric set. Let $D = D_0+P^{-r}D_1H$, $E = PD$, $G = PB$, and $K = 0$. Define $e(t) := w(t) - Px(t)$. Then it simply follows that

$$\mathring{e} = Fe - PL_1m_1,$$

$$r = Mw - Hy = Me.$$

Thus $r_1(s) = -T(s)\,m(s)$ with $T(s) = M(sI-F)^{-1}PL_1$. Obviously, the requirement in (12) is satisfied. Furthermore, $\mathcal{S}^* \cap \mathcal{L}_1 = 0$ and L_1 monic imply 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 (13) is satisfied. $\otimes$

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 unobservable subspace so that the order of the filter is reduced. Also, the condition (16) simply states that the image of the first failure signature should not intersect the unobservable subspace of the residual generator, so that a failure of the first actuator shows up in the residual $r(t)$.

It is clear that the order of the residual generator given in Theorem 2 is $n-d(S^*)$, and this order is in general conservative. This is because there may be a u.o.s., S, that satisfies (16) and contains S^*. Clearly, using this S the order of the residual generator can be further reduced. Unfortunately, there is no systematic way of constructing such non-infimal unobservability subspaces. However, for the case of monic C, the minimal solution is easy (see [15]).

The reader who is familiar with the disturbance decoupled estimation problem (DDEP) [21, 3] will readily recognize the relationship between DDEP and FPRG. However, these two problems have subtle differences 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* the part of the state space that can be estimated even in the presence of unknown input $m_2(t)$.

An interesting interpretation of the solution to FPRG can be given. Referring to Theorem 2, the residual generator can be rewritten as follows:

$$\begin{aligned} \mathring{w}(t) &= A_0\, w(t) - PD_0 y(t) + G\, u(t) + D_1 r(t), \\ r(t) &= M\, w(t) - H\, y(t). \end{aligned} \tag{20}$$

Note that by choosing D_0 and H appropriately, we change the observability properties of $(HC,A+D_0C)$ in such a way that the second actuator failure becomes unobservable from the residual. Next, by injecting the residual $r(t)$ back in the filter, the spectrum of the residual generator can be modified as desired. Clearly, the residual generator given in (20), can be thought of as an observer for the hypothetical system

$$\begin{aligned}\dot{z}(t) &= A_0\, z(t) + u_h(t),\\ y_h(t) &= M\, z(t),\end{aligned} \tag{21}$$

where $u_h(t) := P(Bu(t) - D_0 y(t))$ is the hypothetical input, and $y_h(t) := H\, y(t)$ is the hypothetical measurement. This interpretation of the residual generator can be used effectively in computing a gain D_1 that shapes the dynamics of the residual $r(t)$ in some desired fashion.

To illustrate this point, consider the original system model given in (8) and assume that an additive zero-mean white noise $v_1(t)$ with covariance $E[v_1(t)v_1'(\tau)] = R_1\, \delta(t-\tau)$ enters the system as an input. Also assume that the measurement $y(t)$ is corrupted by an additive zero-mean white noise $v_2(t)$ with covariance $E[v_2(t)v_2'(\tau)] = R_2\, \delta(t-\tau)$ and uncorrelated with the input noise $v_1(t)$. Incorporating the effect of v_1 and v_2 on the hypothetical system of (21), we get

$$\begin{aligned}\dot{z}(t) &= A_0\, z(t) + u_h(t) + v_3(t),\\ y_h(t) &= M\, z(t) + v_4(t),\end{aligned} \tag{22}$$

where $v_3(t) := P(v_1(t) - D_0 v_2(t))$ and $v_4(t) := Hv_2(t)$. Note that v_3 and v_4 are now correlated. A simple computation shows that the intensity R_{34} of the noise driving the system in (22) is

$$R_{34} = \begin{bmatrix} PR_1P' + PD_0R_2D_0'P' & -PD_0R_2H' \\ -HR_2'D_0'P' & HR_2H' \end{bmatrix}. \tag{23}$$

If the objective now is to whiten the residual $r(t)$ (note that white residuals are desirable in the decision making phase of FDI), simply design a steady state Kalman filter for the system given in (22) with the noise statistics in (23). Then use this steady state Kalman gain for the matrix D_1 of (20).

An alternate non stochastic approach is to choose D_1 so that the transfer matrix $T(s) = M(sI - A_0 - D_1 M)^{-1} P L_1$ has certain nice properties. For example, it is not difficult to see that increasing the bandwidth of $T(s)$, which is desirable for fast response, can translate into low steady state gain which can lead to difficulty in distinguishing the response due to a failure from that due to background noise. Therefore, the gain matrix D_1 can be used to find a compromise between conflicting objectives.

Next the generic solvability of FPRG is discussed.

Proposition 3: Let us assume that A, C, L_1, and L_2 are arbitrary matrices with the 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

$$k_1 + k_2 \leq n, \tag{24}$$

$$k_2 < l. \tag{25}$$

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

Note that if the S^* defined in Theorem 2 is used to design a residual generator, then the generic order of the processor is $n - k_2$. Also, the condition given in (24) is quite intuitive, since if $k_1 + k_2 > n$ then the image of L_1 and L_2 intersect, and hence there exists failure modes such that $L_1 m_1(t) = L_2 m_2(t)$. Therefore both failures affect the output exactly the same way, and thus they can not be distinguished from each other.

Now we solve a simple example to illustrate the design procedure.

Example 1: Consider the system given in (8) with

$$A = \begin{bmatrix} 0 & 3 & 4 \\ 1 & 2 & 3 \\ 0 & 2 & 5 \end{bmatrix}, L_1 = \begin{bmatrix} 1 \\ -.5 \\ .5 \end{bmatrix}, \ L_2 = \begin{bmatrix} -3 \\ 1 \\ 0 \end{bmatrix}, \ C = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

and $B = [L_1, L_2]$. Now assume we want to design a residual that is sensitive to the failure of the first actuator, and is insensitive to the failure of the second actuator. First, let us compute $\mathcal{S}^*$ defined in Theorem 2. Using 6,

$$\mathcal{S}^* := \mathrm{Im} \begin{bmatrix} -3 & 1 \\ 1 & 0 \\ 0 & 0 \end{bmatrix}.$$

Clearly $\mathcal{L}_1 \cap \mathcal{S}^* = 0$; therefore, FPRG is solvable. Now we follow the procedure outlined in Theorem 2 to design a residual generator. One possible choice for $D_0 \in \underline{D}(\mathcal{S}^*)$ is

$$D_0 := \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ -2 & 0 \end{bmatrix}.$$

This results in $A_0 = A + D_0 C : \mathcal{X}/\mathcal{S}^* = 5$. Also $H = [0, 1]$ is an appropriate solution of $\mathrm{Ker}\, HC = \mathcal{S}^* + \mathrm{Ker}\, C$. With this H, we have $M = 1$. Now if we choose $\Lambda = \{-5\}$ and continue the design procedure, we find

$$\mathring{w}(t) = -5\; w(t) - [-2, -10]\; y(t) + [.5, 0]\; u(t),$$

$$r(t) = w(t) - [0, 1]\; y(t). \tag{26}$$

Note that if the first failure signature had been

$$L_1 = [1, 0, 0]\,',$$

then clearly $\mathcal{L}_1 \subseteq \mathcal{S}^*$ and FPRG would not have had a solution. We shall continue this example in the next subsection after some additional theoretical developments.

4. Extension of FPRG to Multiple Failure Events

In this section we extend FPRG to the case of multiple failures. Let us assume that k failure events are present, and we want to design a processor that generates k residuals, $r_i(t)$ $(i \in \mathbf{k})$, such that a failure of the i-th component, i.e., a nonzero $m_i(t)$, can only affect the i-th residual $r_i(t)$ and no other residuals $r_j(t)$ $(j \neq i)$. More precisely, what we require is that the transfer matrix relating $m_i(s)$ to $r_i(s)$ should be input observable, and the transfer matrix from $m_i(s)$ to all other $r_j(s)$ should be zero.

In the notation of Section 2, the problem we have just formulated is the same as the FDIFP with the the coding sets $\Omega_i = \{i\}$ $(i \in \mathbf{k})$. This particular version of the FDIFP will be called the extension of the fundamental problem in residual generation (EFPRG).

Obviously, if EFPRG has a solution, then it is possible to detect and identify even *simultaneous* failures with almost arbitrary modes for each component failure. Note that for identifying simultaneous failures, we need at least as many residuals as there are failure events. In this sense, the coding set $\Omega_i = \{i\}$ $(i \in \mathbf{k})$ (or any permutation of it) is minimal.

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

$$\overset{\circ}{w}(t) = (A+DC)\, w(t) - D\, y(t) + B\, u(t),$$

$$r_i(t) = H_i(w(t) - y(t)), \tag{27}$$

such that a nonzero $m_i(t)$ only shows up in the residual $r_i(t)$. This problem is a slight generalization of the 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 FPRG that we have formulated here since in FPRG 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 now follows immediately from that of the FPRG.

Theorem 4: EFPRG has a solution if and only if

$$\mathcal{S}_i^* \cap \mathcal{L}_i = 0, \quad i \in \mathbf{k}, \tag{28}$$

where $\mathcal{S}_i^* := \inf \underline{\mathcal{S}}(\sum_{j \neq i} \mathcal{L}_j)$, $i \in \mathbf{k}$.

Proof: (only if) The necessity follows immediately from the proof of Theorem 2. Just replace the $\mathcal{L}_1$ and $\mathcal{L}_2$ in Theorem 2 with $\mathcal{L}_i$ and $\sum_{j \neq i} \mathcal{L}_j$ respectively.

(if) For sufficiency, the procedure given in Theorem 2 can be used to design k different residual generators, Σ_{ri}, each generating the residual $r_i(t)$. Let $D_i \in \underline{D}(\mathcal{S}_i^*)$ and $F_i = (A+D_iC : \mathcal{X}/\mathcal{S}_i^*)$. Obviously, D_i can be chosen such that $\sigma(F_i) = \Lambda_i$ for arbitrarily given symmetric sets Λ_i (see Theorem 2). Let $E_i = P_iD_i$, $G_i = P_iB$, H_i be any solution of $\operatorname{Ker} H_iC = \mathcal{S}_i^* + \operatorname{Ker} C$, M_i the unique solution of $M_iP_i = H_iC$, and $K_i = 0$. A simple computation shows that $r_i(s) = -T_i(s)\, m_i(s)$ with $T_i(s) = M_i(sI-F_i)^{-1}P_iL_i$. Using the same argument as in Theorem 2, the system relating $m_i(t)$ and $r_i(t)$ is input observable; thus the collection of the residual generators Σ_{ri} $(i \in \mathbf{k})$, viewed as one large system, is a solution to EFPRG. $\otimes$

A family of failure signatures satisfying the conditions in (28) will be called a *strongly identifiable family.* Theorem 4 shows the system theoretic consequences of this concept; it is posiible to design an LTI residual generator that identifies simultaneous failures within a familly 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 k different residual generators, can be quite large. Nevertheless, in this filter, the residuals are generated by k completely decoupled filters, and there is a great deal of freedom in choosing the F_i matrices 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 supressing the effect of noise on the residual through the procedure that was outlined in Section 3. Now we proceed with stating the generic solvability conditions for EFPRG.

Proposition 5: Let us assume that (A,C,L_i) are arbitrary matrices with dimensions $n \times n$, $l \times n$, and $n \times k_i$ respectively. Let $\nu := \sum_{i=1}^{k} k_i$. Then EFPRG generically has a solution if and only if

$$\nu \leq n. \tag{29}$$

$$\nu - \min \{k_i, i \in \mathbf{k}\} < l. \tag{30}$$

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

Note that if the family $\{S_i^*, i \in \mathbf{k}\}$ defined in Theorem 4 is used to design a residual generator, then the generic order of the processor is

$$\sum_{i=1}^{k} (n - \sum_{j \neq i} k_j) = k(n-\nu)+\nu. \tag{31}$$

To illustrate the design procedure given in Theorem 4, we now continue Example 1 of Section 3.

Example 2: The residual generator we designed previously is the same as Σ_{r1} of Theorem 4. Therefore, rename the $r(t)$ given in (26) as $r_1(t)$, and we only need to design the residual generator, Σ_{r2}, which is sensitive to the failure of the second actuator but is not affected by the failure of the first actuator. Using (6), we have

$$S_2^* := \mathrm{Im} \begin{bmatrix} 1 \\ -.5 \\ .5 \end{bmatrix},$$

and hence EFPRG is solvable. Choosing $\Lambda_2 = \{-2, -3\}$, the residual generator Σ_{r2} is simply

$$\overset{\circ}{w}_2(t) = \begin{bmatrix} 2 & -20 \\ 1 & -7 \end{bmatrix} w_2(t) - \begin{bmatrix} -23 & -30 \\ -9 & -15 \end{bmatrix} y(t) + \begin{bmatrix} 0 & -1 \\ 0 & 1 \end{bmatrix} u(t), \qquad (32)$$

$$r_2(t) = [\ 0 \quad 1\ ]\, w_2(t) - [\ 1 \quad 1\ ]\, y(t).$$

With the residual $r(t)$ given in (26) renamed as $r_1(t)$, (26) and (32) can be combined in a single equation as follows:

$$\overset{\circ}{w}(t) = \begin{bmatrix} -5 & 0 & 0 \\ 0 & 2 & -20 \\ 0 & 1 & -7 \end{bmatrix} w(t) - \begin{bmatrix} -2 & -10 \\ -23 & -30 \\ -9 & -15 \end{bmatrix} y(t) + \begin{bmatrix} .5 & 0 \\ 0 & -1 \\ 0 & 1 \end{bmatrix} u(t), \qquad (33)$$

$$r(t) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} w(t) - \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} y(t),$$

where $r(t) := [r_1(t),\, r_2(t)]'$.

To gain some insight into the problem, let us compute several different transfer matrices associated with this example. First denote the transfer matrix relating $m(s) = [m_1(s),\, m_2(s)]'$ to $y(s)$ by $G_m(s)$. A simple computation shows

$$G_m(s) = \frac{1}{s^3-7s^2+s+7} \begin{bmatrix} -.5(s^2-10s+6) & (s-3)(s-5) \\ .5(s^2-4s+1) & 2(s-3) \end{bmatrix}.$$

Now consider the residual generator given in (33) and let us compute the transfer matrix, $H_y(s)$, relating $y(s)$ to $r(s)$. It is easily determined that

$$H_y(s) = \begin{bmatrix} \frac{2}{(s+5)} & \frac{-(s-5)}{(s+5)} \\ \frac{-(s^2-4s+1)}{(s+2)(s+3)} & \frac{-(s^2-10s+6)}{(s+2)(s+3)} \end{bmatrix}.$$

The transfer matrix relating $m(s)$ to $r(s)$ is then simply

$$H_y(s)\, G_m(s) = \begin{bmatrix} \frac{-.5}{(s+5)} & 0 \\ 0 & \frac{-(s-3)}{(s+2)(s+3)} \end{bmatrix}.$$

As was required, m_1 affects r_1 and only r_1, while m_2 affects r_2 and only r_2. It can also be shown that the transfer function from $u(s)$ to $r(s)$ is zero; hence, the nominal input $u(t)$ does not affect the residual $r(t)$. Therefore, EFPRG is really the problem of designing a stable, diagonalizing post-compensator. $\otimes$

Motivated by the last example, the solvability condition of the EFPRG in the frequency domain is now developed. For the remainder of this section, it is assumed that the failure signatures are simply column vectors.

We can rewrite (3) as follows:

$$y(s) = G_u(s)\, u(s) + G_m(s)\, m(s), \tag{34}$$

by taking the Laplace transform of both sides. In (34), $G_u(s) := C(sI{-}A)^{-1}B$, $G_m(s) := C(sI{-}A)^{-1}[L_1, \ldots ,L_k]$, and $m(s) = [m_1(s), \ldots ,m_k(s)]\,'$. The objective of EFPRG can now be restated as generating a k dimensional vector $r(t)$ by passing the observation vector $z(t) = [y'(t),\ u'(t)]\,'$ through a causal LTI system characterized by the transfer matrix $H(s)$, i.e,

$$r(s) = H(s)\, z(s) = [H_y(s),\, H_u(s)] \begin{bmatrix} y(s) \\ u(s) \end{bmatrix}, \tag{35}$$

such that the net transmission from the input $u(t)$ to the residual vector $r(t)$ is zero, and the failure mode $m_i(t)$ only affects the i-th component of the residual vector $r(t)$. In other words, the objective is to find a proper post compensator $H(s)$ such that

$$H(s)G(s) = [\, \text{-}T(s),\, 0\,], \tag{36}$$

where

$$G(s) = \begin{bmatrix} G_m(s) & G_u(s) \\ 0 & I \end{bmatrix}, \tag{37}$$

the 0 in (36) is a $k \times m$ matrix, and $T(s)$ is a $k \times k$ diagonal matrix with nonzero diagonal elements $T_i(s)$.

In addition, when no failure is present, the residuals due to initial conditions in the system and in the post-compensator should die away so. ,The residual due to a nonzero initial condition $x(0)$ is simply $H_y(s)G_s(s)x(0)$ where

$$G_s(s) := C(sI-A)^{-1}. \tag{38}$$

Hence the transfer matrix $H_y(s)G_s(s)$ should be stable. Also the residual due to nonzero initial conditions of the post compensator should die away, so we require that $H(s)$ be stable.

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 (28) is equivalent to the left invertibility of

$$C(sI-A)^{-1}[L_1, \ldots, L_k]. \tag{39}$$

The reader who is familar with the control decoupling problem [9, 24] should readily recognize the dual relationship between the EFPRG and that problem. Despite of this duality, the structure of the residual generator proposed in Theorem 4 is quite different from that of the extended decoupling controllers given in the fundamental reference [24]. This is because of the fact that here we are concerned with designing observers and there is more flexibility, but in the decoupling problem the objective is to design control systems and the problem is more restrictive. However, it is interesting to note that the generic order of the residual generator given in (31) is exactly equal to the generic order of the extended decoupling controller given in Theorem ? of [24] if the matrices involved are properly transposed.

Now, an interesting question is how to reduce the order of the processor given 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 deleting 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 paper, by considering more complicated coding schemes than the one dealt with in this section.

5. Triangular Detection Filter Problem

The first problem in the above category that we formulate and solve is the triangular detection filter problem (TDFP). Consider the system in (3) and the residual generator (27). In TDFP the objective is to design k residuals $r_i(t)$ ($i \in \mathbf{k}$) such that a nonzero m_1 affects r_1 and possibly affects $r_2, \ldots, r_k$; a nonzero m_2 affects r_2 without affecting r_1 but possibly affecting $r_3, \ldots, r_k$; ... finally, a nonzero m_k affects r_k without affecting $r_1, \ldots, r_{k-1}$. In the notation of Section 2, this process of relating the failure events to the residuals corresponds to the coding sets $\Omega_i = \{i\} \cup \Lambda_i$ where Λ_i is some subset of $\{i+1, \ldots, k\}$. The input-output relation of TDFP is shown in Figure 5-1, which shows the origin of its name.

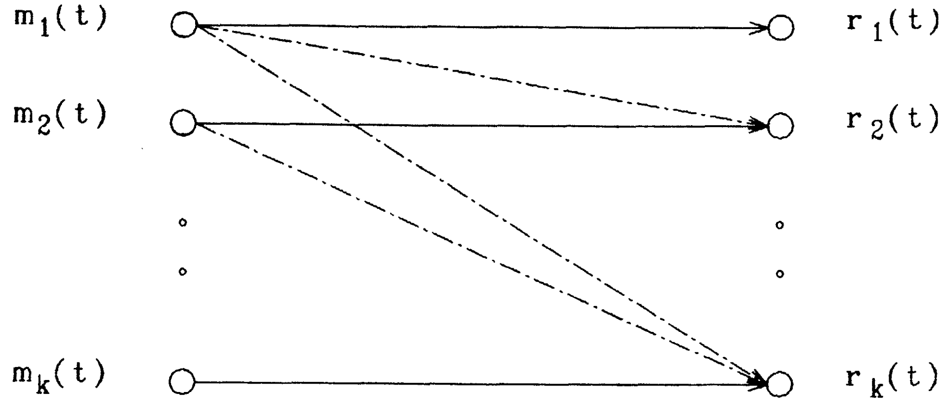

Figure 5-1: Input Output Relationship of TDFP

The concept of TDFP is an exact dual of the triangular decoupling control problem introduced and solved in [17]. Interestingly enough, this formulation is quite appropriate for failure detection and identification problem if it is assumed that simultaneous failures are not possible. Even if simultaneous failures do occur, their presence in the TDFP will not lead to incorrect identification as it may in other coding schemes. In such cases, at least the failure of the component with ***highest priority*** (i.e., the $m_i(t)$ with the smallest value of i) can be correctly identified.

Using the statement of the problem, TDFP can be stated in geometric language as follows: Given A, C, and $\mathcal{L}_i$ ($i \in \mathbf{k}$), find an output injection map $D : \mathcal{Y} \rightarrow \mathcal{X}$ and a family of compatible u.o.s.'s $\{\mathcal{S}_i,\ i \in \mathbf{k}\}$ such that

$$\mathcal{S}_i := <\text{Ker}\, H_iC|A{+}DC> = <\text{Ker}\, C + \mathcal{S}_i|A{+}DC>, \quad i \in \mathbf{k},$$

$$\textstyle\sum_{j=i+1}^{k} \mathcal{L}_j \subseteq \mathcal{S}_i \quad i \in \mathbf{k\text{-}1}, \text{ and } \quad 0 \subseteq \mathcal{S}_k, \tag{40}$$

$$\mathcal{S}_i \cap \mathcal{L}_i = 0 \quad i \in \mathbf{k}. \tag{41}$$

The requirement given in (40) implies that the failures of (i+1)-th up to k-th component should not affect the i-th residual, and (41) implies that the failure of the i-th component should at least show up in the i-th residual. Now the solvability conditions of TDFP are stated.

Theorem 6: Let (C,A) be observable. TDFP has a solution if and only if

$$\mathcal{S}_i^* \cap \mathcal{L}_i = 0, \quad i \in \mathbf{k},$$

where $\mathcal{S}_i^* := \inf \underline{\mathcal{S}}(\sum_{j=i+1}^{k} \mathcal{L}_j)$ $(i \in \mathbf{k\text{-}1})$, and $\mathcal{S}_k^* = 0$. Moreover,

$$\sigma(A{+}DC : \mathcal{S}_{i-1}^*/\mathcal{S}_i^*) = \Lambda_i, \quad i \in \mathbf{k},$$

$$\sigma(A{+}DC) = \uplus_{i=1}^{k} \Lambda_i,$$

where $\mathcal{S}_0^* = \mathcal{X}$, and Λ_i $(i \in \mathbf{k})$ are arbitrary symmetric sets.

Proof: The proof is the dual of the one given in [17], and hence is omitted.

A family of failure signatures satisfying the solvability conditions of TDFP is not necessarily a strongly identifiable family. However, it is clear from Theorem 6 that any strongly identifiable family of failure signatures satisfies the solvability conditions of TDFP. For such families, the order of the filter that solves TDFP is only n (same as the order of the system model). On the other hand, RDDFP may not have a solution for this family of failure signatures; since Massoumnia showed in [14] that strong identifiability is a necessary but not sufficient condition for the solvability of RDDFP.

Our last remark concerns the case of simple sensor failures that can be modeled by taking J_i in (2) as columns of the identity matrix. Using some of the results of [14], we know that a family of failure signatures with output separable detection spaces (cf. [14]) is strongly identifiable. Recall that the *detection space* $\mathcal{T}_i^*$ of the failure signature L_i was defined in [14] as follows (also see [2]:

$$\mathcal{T}_i^* := \inf \underline{\mathcal{S}}(\mathcal{L}_i), \tag{42}$$

and that a family of detection spaces $\{\mathcal{T}_i^*, i \in \mathbf{k}\}$ was termed output separable if the output images of the detection spaces were independent, i.e., if

$$C\mathcal{T}_i^* \cap (\textstyle\sum_{j \neq i} C\mathcal{T}_j^*) = 0, \quad i \in \mathbf{k}.$$

Using the state space augmentation procedure given in Section 2, it is always possible to model l simple sensor failures as a family of l pseudo-actuator failures with output separable detection spaces. Now using the preceding remarks, it follows immediately that *there always exists an $n+l$ dimensional filter with arbitrarily assignable spectrum that triangularly detects and identifies any family of l sensor failures, assuming that the actuators are fully reliable.* This fact is one of the most useful applications of TDFP. For more details we refer the reader to [15].

6. Failure Detection and Identification Filter Problem

Our objective in this section is to state necessary and sufficient conditions for it to be possible to design a residual generator that can be used to 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 problem will lead to the introduction of the fundamental concept of an identifiable family of failure signatures.

In order to treat the above problem, it is necessary to more concretely define the coding sets Ω_i $(i \in \mathbf{k})$ introduced in Section 2. Define an auxiliary *coding matrix* $\Delta = [\delta_{ij}]$ with $\delta_{ij} = 1$ if $i \in \Omega_j$ for $i \in \mathbf{p}$, and $\delta_{ij} = 0$ otherwise. An element $\delta_{ij} = 0$ implies that the j-th component failure should not affect the i-th residual, while, $\delta_{ij} = 1$ implies that the j-th component failure should affect the i-th residual, in the sense that the transfer matrix relating the j-th component failure to the i-th residual should be input observable. Hence, our goal is to design a residual generator such that the transfer matrix relating the failure events to the residual vectors is structurally the same as the coding matrix Δ defined.

Example 3: Assume that six failure events are present, and three residuals are defined such that $\Omega_1=\{1\}$, $\Omega_2=\{2\}$, $\Omega_3=\{1,2\}$, $\Omega_4=\{3\}$, $\Omega_5=\{1,3\}$, and $\Omega_6=\{2,3\}$. Using the definition of a coding matrix, we construct Δ:

$$\Delta = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix} \qquad (43)$$

The coding scheme used in this example is called a *binary coding.* This is because the columns of Δ (e.g., $[0, 1, 1]'$) are just the binary representations of the corresponding column indices of Δ (e.g., 6). When binary coding is used, the minimum number, p, of residuals is simply

$$p = [\log_2 (k+1)], \qquad (44)$$

where $[x]$ is the smallest integer such that $[x] \geq x$. It is simple to show that the number given in (44) is the minimum number of residuals required, no matter what coding scheme is used. This is the major desirable attribute of binary coding. However, intuitively speaking, the probability of false identification associated with this coding scheme can be large. In the event of a failure, some of the residuals may not cross the threshold, and therefore a totally incorrect component may be identified as having failed. $\otimes$

Now some of the fundamental properties of the coding matrix Δ are pointed out. First of all, no row of Δ should be identically zero, since a zero row implies that none of the failure events affect the residual corresponding to this row, hence this residual is superfluous. Also, no column of Δ should be identically zero since the failure event corresponding to this column would not affect any of the residuals and therefore could not be detected. Most importantly, *no two columns of Δ should be the same*, since otherwise the failures of the components corresponding to these columns could not be distinguished from each other. Finally, note that permutation of the rows and columns of Δ corresponds to a renumbering of the residuals and the failure events respectively.

We also define the sum (+) of any two rows of Δ as the Boolean OR of the elements of one row with the corresponding elements of the other row. Using this definition, one has for example

$$[1, 0, 0] + [1, 1, 0] = [1, 1, 0].$$

Clearly, any row of Δ that is the sum of other rows of Δ is redundant. For example, assume that for some coding matrix the first row is the same as the sum of the second and third rows. Then the second and third residuals are sufficient for FDI purposes, and the first residual is not necessary; however, this redundant residual may be useful in the decision making process, given the presence of noise and uncertainties.

Now define the finite set Γ_i as the collection of all those $j \in \mathbf{k}$ for which $\delta_{ij} = 0$. For example, the family Γ_i $(i \in \mathbf{p})$ associated with the binary coding sets we used in Example 3 is simply:

$$\Gamma_1 = \{2,4,6\}, \quad \Gamma_2 = \{1,4,5\}, \quad \Gamma_3 = \{1,2,3\}.$$

Note that the sets Γ_i $(i \in \mathbf{p})$ contain all the information required for specifying the structure of the transfer matrix relating the failure events to the residuals.

Using the above preliminary concepts, we now derive the solvability condition for FDIFP.

Theorem 7: FDIFP with a given family of coding sets and the assumption that there is only one failure present at a time has a solution if and only if

$$S_{\Gamma_i} \cap \mathcal{L}_j = 0, \quad j \in \mathbf{k} - \Gamma_i, \quad i \in \mathbf{p}, \tag{45}$$

where

$$S_{\Gamma_i} := \inf \underline{S}(\textstyle\sum_{j \in \Gamma_i} \mathcal{L}_j), \quad i \in \mathbf{p}. \tag{46}$$

Proof: (only if) Recall that the objective of FDIFP is to generate p residuals, $r_l(t)$ $(l \in \mathbf{p})$, such that when the j-th component fails, the residuals $r_i(t)$ for $i \in \Omega_j$ should be nonzero, and the other residuals all should be identically zero. We can think of FDIFP as p separate FPRG (see Section 3)- one for each row of Δ- which should be solvable simultaneously. Using the necessary condition for solvability of FPRG (see Theorem 2) and the assumption that there is only one failure present at a time, the condition given in (45) follows immediately.

(if) Simply use the unobservability subspaces S_{Γ_i} $(i \in \mathbf{p})$ to design p separate residual generators each being the solution to an FPRG corresponding to different rows of the coding matrix (see Theorem 2 for construction of the residual generator). $\otimes$

Note that all of our remarks in Section 3 about accommodating the effect of sensor and process noise hold equally well for the residual generators of Theorem 7.

The following example illustrates the design procedure.

Example 4: Consider the system in (3), with

$$A = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & 0 & -2 \end{bmatrix}, B = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix},$$

$$C = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix},$$

and the failure signature L_i being the i-th column of B. The problem is to design a residual generator using the binary coding scheme of Example 3. The coding matrix Δ for this example is given in (43). First, the infimal subspaces S_{Γ_i} defined in (46) are computed. One can show that

$$S_{\Gamma_1} = \mathcal{L}_2 \oplus \mathcal{L}_4$$

$$S_{\Gamma_2} = \mathcal{L}_1 \oplus \mathcal{L}_4 \oplus \mathcal{L}_5$$

$$S_{\Gamma_3} = \mathcal{L}_1 \oplus \mathcal{L}_2 \oplus \mathcal{L}_3$$

A simple check shows that the necessary condition in (45) is satisfied. Hence S_{Γ_i} can be used to design a residual generator Σ_i according to the procedure in Theorem 2. It is clear that Σ_1 will be a third order filter, and the other two residual generators Σ_2 and Σ_3 will each be second order filters. Therefore, the over all residual generator is 7-th order.

We also point out that if the columns of L are permuted (this permutation corresponds to a renumbering of the failure signatures), then the problem may not have a solution. First note that the failure signature L_6 is a linear combination of the failure signatures L_2 and L_4, and now consider interchanging the fifth and the sixth columns of L but still using the coding matrix in (43). It is immediate that the new problem does not have a solution, since the new L_5 is a linear combination of L_2 and L_4, and the solvability conditions of FDIFP are not satisfied. Thus, in practice, care should be taken to specify the coding sets in a way that avoids such easily resolved difficulties.

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

The following result will be crucial to our derivation.

Lemma 8: Let (C,A) be observable, $d(\mathcal{L}_1) = d(\mathcal{L}_2) = 1$, and $\mathcal{L}_1 \subseteq \mathcal{T}_2{}^*$ where $\mathcal{T}_2{}^* := \inf \underline{S}(\mathcal{L}_2)$. Then $\mathcal{T}_1{}^* = \mathcal{T}_2{}^*$ where $\mathcal{T}_1{}^* := \inf \underline{S}(\mathcal{L}_1)$.

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

$$\mathcal{T}_1{}^* + \text{Ker}\, C = \mathcal{T}_2{}^* + \text{Ker}\, C := \mathcal{V}. \tag{47}$$

Also $\mathcal{T}_2{}^*$ and $\mathcal{T}_1{}^*$ are compatible since $\mathcal{T}_1{}^* + \mathcal{T}_2{}^* = \mathcal{T}_2{}^*$ is (C,A)-invariant (see [15]). Let $D \in \cap \underline{D}(\mathcal{T}_i{}^*)$. Using (47) and (7), we have

$$\mathcal{T}_2{}^* = <\mathcal{V}|A+DC> = \mathcal{T}_1{}^*.$$

$\otimes$

Theorem 9: Given an LTI system (C,A,B) with a family of failure signatures $\{L_i,\ i \in \mathbf{k}\}$ with arbitrary modes of failures, 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

$$\mathcal{L}_l \cap \mathcal{T}_j^* = 0, \quad l,j \in \mathbf{k},\, l \neq j, \tag{48}$$

where $\mathcal{T}_i^* := \inf \underline{\mathcal{S}}(\mathcal{L}_i)$.

Proof: (only if) Suppose that we have designed a residual generator with an appropriate family of coding sets. Recall that no two columns of the coding matrix associated with these coding sets should be the same. Using this property, it follows that for any two distinct integers $l,j \in \mathbf{k}$, there should exist an i such that either

$$j \in \Gamma_i \text{ but } l \notin \Gamma_i, \tag{49}$$

or

$$l \in \Gamma_i \text{ but } j \notin \Gamma_i. \tag{50}$$

Now let the family of detection spaces $\{\mathcal{T}_i^*, i \in \mathbf{k}\}$ be as defined in (42). If (50) holds, then obviously $\mathcal{T}_l^* \subseteq \mathcal{S}_{\Gamma_i}$. Similarly, if (49) holds, then $\mathcal{T}_j^* \subseteq \mathcal{S}_{\Gamma_i}$. Now using the necessary condition given in (45) and the argument in (49) and (50), it follows that for any $l,j \in \mathbf{k}$

$$\text{either } \mathcal{L}_l \cap \mathcal{T}_j^* = 0 \text{ or } \mathcal{L}_j \cap \mathcal{T}_l^* = 0. \tag{51}$$

Using (51) and Lemma 8, we then conclude that (48) necessarily should hold. Because of Lemma 8, the condition given in (48) is also equivalent to

$$\mathcal{L}_l \cap \mathcal{T}_j^* = 0, \quad l \in \mathbf{k}, \quad j \in \{l+1, \ldots, k\}. \tag{52}$$

(if) We need to show that if a family of failure signatures satisfies the condition given in (52), then there exists a family of coding sets for which the FDIFP, with the assumption that only one failure is present at a time, has a solution. For this, just use the coding sets

$$\Omega_i = \{1, \ldots, i-1, i+1, \ldots, k\}, \quad i \in \mathbf{k}, \tag{53}$$

to design k different residual generators such that the unobservable subspace of the i-th residual is simply $\mathcal{T}_i^*$, so that the failure of the i-th component will not show up in this residual. $\otimes$

Note that if we are using the coding sets (53) to design the residual generator, then the unobservable subspace of the i-th residual is exactly the detection space we defined earlier. Hence, a more appropriate name for such a subspace seems to be the undetectable subspace of a failure signature, but in order to conform with the notions introduced in the work of Beard [2], we chose to continue to use the name detection spaces.

A family of scalar failure signatures $\{L_i, i \in \mathbf{k}\}$ satisfying the condition given in (52) 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 with which it is possible to detect and identify the failures in the sense of Section 2.

It is also possible to state the frequency domain counterpart of the failure identifiability condition given in (52). From (39), we know that the condition

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

is equivalent to the statement that the transfer matrix $C(sI-A)^{-1}[L_i, L_j]$ is left invertible. Hence, the condition in (52) is equivalent to the statement that the rational vector subspaces spanned by $C(sI-A)^{-1}L_i$ are nonintersecting. Note that 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 there exist failure modes for the i-th and the j-th components that result in the same output; hence, it will be impossible to distinguish between the failure of these two components with these failure modes by observing the output of the system.

7. Conclusion

In this paper we have solved the problem of generating residuals for the purpose of detecting and identifying control system component failures by processing the commanded inputs and measured outputs of a linear time-invariant system. We have also developed simple design procedures for generating the residuals when the solvability conditions are satisfied.

We should mention that all of our results hold equally well for discrete-time systems, since our approach has been entirely geometric. Therefore, the left hand side of (3) can be replaced with $x(t+1)$ and the solvability condition for all of the problems that we have formulated here will remain unchanged. An interesting characteristic of residual generators for discrete-time systems is that we can assign the spectrum of the filter to the origin of the complex plane, and hence obtain dead-beat behavior. It can be shown that the residuals thus obtained are the generalized parity relations introduced by Chow [5]. 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 article.

A challenging problem that we did not address in this paper is the task of generating residuals that are robust to the modeling errors. Lou [12, 13] and Chow [4, 5] have done some preliminary work on the problem of robust parity relations. Using our results, it is clear that the residual generator is a finely tuned processor that relies on the given dynamics of the plant. Speciffically, for actuator failures, the design of the processor relies on inverting the transfer matrix of the system, which can be quite sensitive to changes in the system parameters. We also point out that the issue in robust residual generation is not simply the stability of the perturbed system as in many robust control system problems, but the preservation as nearly as possible of the diagonal structure of the transfer matrices in the presence of plant uncertainties. This is a much more complicated problem and deserves the attention of researchers in linear system theory and robust control.

References

[1] BASILE, G. and MARRO, G.
Controlled and Conditioned Invariant Subspaces in Linear System Theory.
J. Optim. Theory Appl. 3:306-315, 1969.

[2] BEARD, R.V.
Failure Accommodation in Linear Systems Through Self-Reorganization.
PhD thesis, Department of Aeronautics and Astronautics, MIT, February, 1971.

[3] BHATTACHARYYA, S.P.
Observer Design for Linear Systems with Unknown Inputs.
IEEE Trans. Automat. Contr. AC-23:483-484, June, 1978.

[4] CHOW, E.Y.
A Failure Detection System Design Methodology.
PhD thesis, Department of Electrical Engineering and Computer Science, MIT, October, 1980.

[5] CHOW, E.Y. and WILLSKY, A.S.
Analytical Redundancy and the Design of Robust Failure Detection Systems.
IEEE Trans. Automat. Contr. AC-29:689-691, July, 1984.

[6] DECKERT, J.C.; DESAI, M.N.; DEYST, J.J.; and WILLSKY, A.S.
F-8 DFBW Sensor Failure Identification Using Analytic Redundancy.
IEEE Trans. Automat. Contr. AC-22:795-803, October, 1977.

[7] EVANS, F.A. and WILCOX, J.C.
Experimental Strapdown Redundant Sensor Inertial Navigation Systems.
J. Spacecraft Rockets 7:1070-1074, September, 1970.

[8] GILMORE, J.P. and McKERN, R.A.
A Redundant Strapdown Inertial Reference Unit (SIRU).
J. Spacecraft Rockets 9:39-47, January, 1972.

[9] HAUTUS, M.L.J. and HEYMANN, M.
Linear Feedback Decoupling - Transfer Function Analysis.
IEEE Trans. Automat. Contr. AC-28:823-832, August, 1983.

[10] ISERMANN, R.
Process Fault Detection Based on Modeling and Estimation Methods- A Survey.
Automatica 20:387-404, Jully, 1984.

[11] JONES, H.L.
Failure Detection in Linear Systems.
PhD thesis, Department of Aeronautics and Astronautics, MIT, August, 1973.

[12] LOU, X.C.
A System Failure Detection Method -- Failure Projection.
Master's thesis, Department of Electrical Engineering and Computer Science, MIT, June, 1982.

[13] LOU, X.C.; WILLSKY, A.S.; and Verghese, G.C.
Optimally Robust Redundancy Relations.
Automatica 22:333-344, ?, 1986.

[14] MASSOUMNIA, M.A.
A Geometric Approach to the Synthesis of Failure Detection Filters.
IEEE Trans. Automat. Contr. 31:?, September, 1986.

[15] MASSOUMNIA, M.A.
A Geometric Approach to Failure Detection and Identification in Linear Systems.
PhD thesis, Department of Aeronautics and Astronautics, MIT, February, 1986.

[16] MASSOUMNIA, M.A. and VANDER VELDE, W.E.
Generating Prity Relations for Detecting and Identifying Control System Component Failure.
AIAA Journal of Guidance and Control ?:?, ?, 1986.

[17] MORSE, A.S. and WONHAM, W.M.
Triangular Decoupling of Linear Multivariable Systems.
IEEE Trans. Automat. Contr. AC-15:447-447, August, 1970.

[18] SCHUMACHER, J.M.
Compensator Synthesis Using (C,A,B)-pairs.
IEEE Trans. Automat. Contr. AC-25:1133-1138, December, 1980.

[19] SCHUMACHER, J.M.
Regulator Synthesis Using (C,A,B)-pairs.
IEEE Trans. Automat. Contr. AC-27:1211-1221, December, 1982.

[20] WALKER, B.K.
Recent Developments in Fault Diagnosis and Accommodation.
AIAA Guidance and Control Conference , August, 1983.

[21] WILLEMS, J.C. and COMMAULT, J.
Disturbance Decoupling by Measurement Feedback with Stability or Pole Placement.
SIAM J. Contr. Optimiz. 19:490-504, July, 1981.

[22] WILLEMS, J.C.
Almost Invariant Subspaces: An Approach to High Gain Feedback Design-Part II: Almost Conditionally Invariant Subspaces.
IEEE Trans. Automat. Contr. AC-27:1071-1084, October, 1982.

[23] WILLSKY, A.S.
A Survey of Design Methods for Failure Detection in Dynamic Systems.
Automatica 12:601-611, November, 1976.

[24] WONHAM, W.M.
Linear Multivariable Control: A Geometric Approach.
Springer-Verlag, 1985.

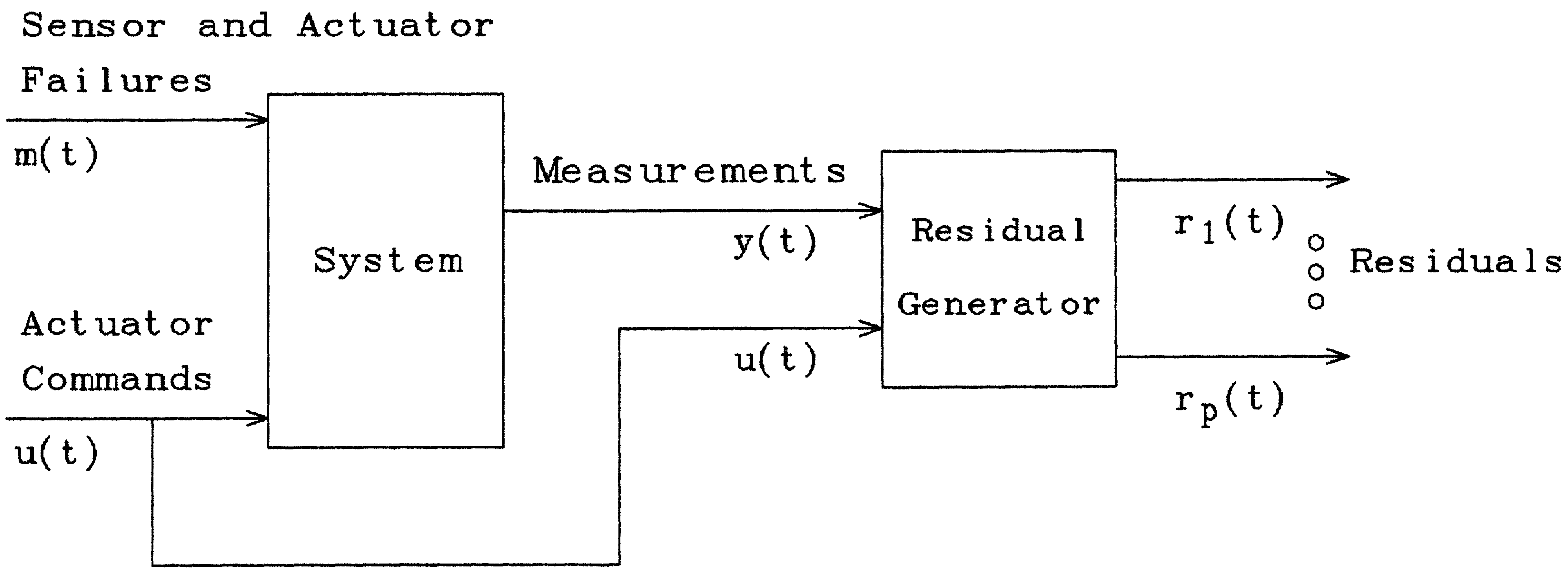

Figure 2-1
Block Diagram of an FDIF

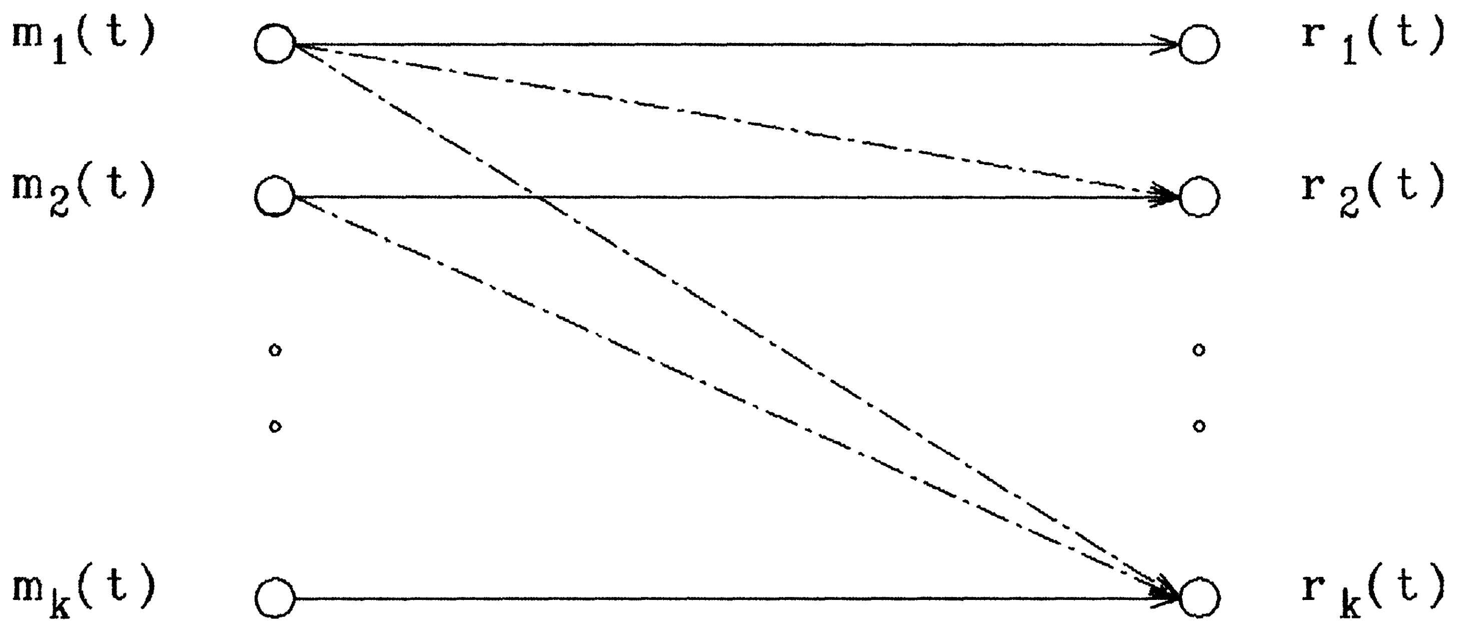

Figure 5-1
Input Output Relationship of TDFP