

Fault Isolability Conditions for Linear Systems with Additive Faults

Jakob Stoustrup and Henrik Niemann

Abstract—In this paper, we shall show that an *unlimited* number of additive single faults can be isolated under mild conditions if a general isolation scheme is applied. Multiple faults are also covered.

The approach is algebraic and is based on a set representation of faults, where all faults within a set can occur simultaneously, whereas faults belonging to different fault sets appear disjoint in time. The proposed fault detection and isolation (FDI) scheme consists of three steps. A fault detection (FD) step is followed by a fault set isolation (FSI) step. Here the fault set is isolated wherein the faults have occurred. The last step is a fault isolation (FI) of the faults occurring in a specific fault set, i.e. equivalent with the standard FI step.

I. INTRODUCTION

The ability to detect faults in safety critical systems by model based approaches have received strong and increasing attention recently. The number of sessions dedicated to this research area in the major control conferences have exploded during the past ten years and so has the research funding from public and industrial funds.

Merely detecting a fault, however, is not enough for systems which can not simply be shut down at the first suspicion of a fault. In order to obtain fault tolerance, it is required that the faults are also *isolated*, i.e. that their origin in the dynamical system is determined, such that the proper counter-measures can be taken.

To that end, it is interesting to observe that one of the most popular approaches to fault isolation has serious pitfalls. Indeed, the fault isolation problem has often been formulated as the task of generating signals which are non-zero in the presence of faults and zero otherwise. This is a handy and simple way to isolate faults. Necessary and sufficient conditions are known for the existence of filters for this purpose. However, these conditions are restrictive, e.g. in the sense that for this type of fault isolation, a bounded number of faults depending on the number of measurements can be isolated. In contrast, we shall show in the sequel that an *unlimited* number of additive single faults can be isolated under mild conditions if more general isolation filters are applied.

The detection and fault isolation problem has been considered in a large number of papers and books, see e.g. the books [1], [2], [3], [4], [6] and the references herein. The described methods include both stochastic based methods as

well as deterministic based methods. In the stochastic based methods, different test methods as e.g. a CUSUM or a GLR test are applied for detecting changes in the residual signals as an indication of faults in the system. The deterministic method are based on decoupling of disturbances in the residual signals by using different algebraic and geometric solutions. However, in practice, the two approaches are combined to give effective methods for fault detection and isolation.

The results presented in this paper are extensions of the FDI results given in [6], [7]. In [6], conditions are given for detection and isolation based on fault sets. The link to detect faults in a specific fault set was not considered in [6]. By doing this, it will be possible to isolate an unlimited number of faults, as long as the number of faults in the single fault sets satisfies some specified bounds.

II. SYSTEM SETUP

Consider the following state space description for a plant or a system given by

$$\Sigma : \begin{cases} \sigma x = Ax + \sum_{j=1}^m E_j d_j + \sum_{i=1}^k L_i f_i \\ = Ax + Ed + L_f f \\ y = Cx + \sum_{j=1}^m D_{d,j} d_j + \sum_{i=1}^k D_{f,i} f_i \\ = Cx + D_d d + D_f f, \end{cases} \quad (1)$$

where σ is an operator indicating the time derivation $\frac{d}{dt}$ for continuous-time systems and a forward unit time shift for discrete-time systems. Also, $x \in \mathcal{R}^n$ is the state vector, $d \in \mathcal{R}^m$ is a disturbance signal vector, and $y \in \mathcal{R}^p$ is the measurement vector. Furthermore, f_i signifies the i -th fault for each $i = 1, 2, \dots, k$. The coefficient matrices L_i and $D_{f,i}$ are referred to in the literature as failure signatures associated with the i -th fault, while f_i itself is called the i -th fault signal and $f \in \mathcal{R}^k$ the fault vector. Further, we will also use the short notation f_i for the fault vector with all elements equal to zero except for the i 'th position where it is equal to f_i . It is always clear from the context which interpretation we are using. The above system can be rewritten in a transfer function form as

$$\Sigma : \{ y = G_{yd}d + G_{yf}f \} \quad (2)$$

where, with some abuse of notation, we use the same symbols for the original signals and their Laplace transforms.

In modeling a given plant by the system (1), we assume that all the fault signals f_i , $i = 1, 2, \dots, k$, are quite arbitrary and that no information is known regarding their characteristics. That is, none of the signals $i = 1, 2, \dots, k$,

J. Stoustrup is with Dept. of Control Engineering, Aalborg University, Fr. Bajers Vej 7C, DK-9220 Aalborg, Denmark, jakob@control.aau.dk

H. Niemann is with Ørsted•DTU, Automation, Tech. Univ. of Denmark, Build. 326, DK-2800 Kgs. Lyngby, Denmark hnn@oersted.dtu.dk

are constrained to belong to any special class of functions. We now proceed to formulate certain fault detection and isolation problems.

Let the residual signal/vector r be given by

$$r = Fy = G_{rf}f + G_{rd}d = \Psi(d, f) \quad (3)$$

r is a time function that takes values in \mathcal{R}^q , F is linear stable residual generator.

Before we continue, some certain fault modeling aspects are considered. In a given situation, there exists always a number of possible faults. Some of these individual faults might occur simultaneously at any given time and others cannot. The tasks of fault detection and isolation depend on which faults can occur simultaneously and which cannot. Based on the information available as to what faults could occur simultaneously at any time and what cannot, one divides the set of all possible faults into mutually exclusive and exhaustive sets. To do so, let us introduce some notation. Let us denote the set of all possible faults by $\mathbf{k} = \{1, 2, \dots, k\}$. Based on the known information, let \mathbf{k} be partitioned into ℓ mutually exclusive and exhaustive sets, $\Omega_i, i = 1, 2, \dots, \ell$. That is, let $\Omega_i \cap \Omega_j = \emptyset$ for $i \neq j$, and $\Omega_1 \cup \Omega_2 \cup \dots \cup \Omega_\ell = \mathbf{k}$. Also, let k_i denote the number of elements in Ω_i . This leads us to define the following simultaneous occurrence property.

Simultaneous occurrence property: Only those faults that belong to any single set among the sets $\Omega_i, i = 1, 2, \dots, \ell$, can occur simultaneously at any given time. This implies that certain faults belonging to a set, say Ω_i , and others that belong to another set, say Ω_j with $i \neq j$, cannot occur simultaneously at any given time.

Two special and extreme cases of the general simultaneous occurrence property are interesting and important. The first extreme case where $\ell = 1$ is called **simultaneous occurrence property of type 1**. The other extreme case of simultaneous occurrence property corresponds to the case when $\ell = k$, and is called **simultaneous occurrence property of type 2**. In this case, each and every fault occurs by itself, i.e. it never occurs simultaneously with any other fault, and as such it is interesting and important. In the following, we will use f_{Ω_i} to describe the fault vector only including the faults in the fault set Ω_i . Further, $f_{\setminus \Omega_i}$ include all faults except the faults in the fault set Ω_i .

A. Problem Formulation

Only exact fault detection and isolation will be considered in this paper. It has been shown in [6], that if almost fault detection and isolation is possible, it is also possible to obtain exact fault detection and isolation. Thus, we do not consider the case, where exact FDI (and consequently almost FDI) is not possible, for which norm based approaches have been studied by several authors.

Problem 1: Consider the system Σ given by (2) under the simultaneous occurrence property. The problem of *exact fault detection* of a set of multiple faults f with signature

matrices L_f and D_f is defined as the problem of finding, if existent, a bounded-input-bounded-output stable residual generator F whose output is a scalar residual signal r such that

$$\Psi(d, 0) = 0 \text{ for all disturbances } d$$

$$\Psi(d, f) \neq 0 \text{ for all faults } f \neq 0$$

and for all disturbances d

The solvability condition for the above problem will in general be quite restrictive. The reason is that the effect from two or more faults on the residual signal r might just happen to cancel against each other. However, from a practical point of view, it will not be relevant to require such strong condition in connection with fault detection. Instead, generic fault detection, [6], can be considered. It is assumed that the faults are independent in the sense, that the fault signatures are independent. This means that

$$\begin{pmatrix} L_f \\ D_f \end{pmatrix}$$

is left-invertible. Based on this, we have the following problem for generic fault detection.

Problem 2: Consider the system Σ given by (2) under the simultaneous occurrence property. The problem of *exact generic fault detection* of a set of multiple faults f with independent signature matrices L_f and D_f is defined as the problem of finding, if existent, a bounded-input-bounded-output stable residual generator F whose output is a scalar residual signal r such that there exist a genericity matrix V and such that

$$\Psi(d, 0) = 0 \text{ for all disturbances } d$$

$$\Psi(d, f) \neq 0 \text{ for all faults } f \text{ such that } Vf \neq 0$$

and for all disturbances d

where V is a square transfer matrix with k columns which are all unequal to zero.

Problem 3: Consider the system Σ given by (2) under the simultaneous occurrence property. The problem of *exact generic fault isolation* for a set of faults f with signature matrices L_f and D_f is defined as the problem of finding, if existent, a bounded-input-bounded-output stable residual generator F whose output is a residual vector r such that there exist a finite number of genericity matrices V_1, \dots, V_s such that for any fault $f_i, i = 1, \dots, k$, there exists a dedicated component r_i of r and that the transfer functions from d and f to r_i has the following properties:

$$\Psi(d, 0) = 0 \text{ for all disturbances } d$$

$$\Psi_i(d, f) = 0 \text{ for all disturbances } d \text{ and for any fault } f \text{ such that } V_j f \neq 0 \text{ for all } j = 1, \dots, s, \text{ and such that } f_i \text{ is identical to zero}$$

$$\Psi_i(d, f) \neq 0 \text{ for all disturbances } d \text{ and for any fault } f \text{ such that } V_j f \neq 0 \text{ for all } j = 1, \dots, s, \text{ and such that } f_i \text{ is not identical to zero}$$

Problem 4: Consider the system Σ given by (2) under

the simultaneous occurrence property. The problem of *exact generic fault set isolation* for a set of detectable faults f with signature matrices L_f and D_f is defined as the problem of finding, if existent, a bounded-input-bounded-output stable residual generator F whose output is a residual vector r such that there exist a finite number of genericity matrices V_1, \dots, V_s such that for any set of faults Ω_α , $\alpha = 1, \dots, \ell$, there exists a unique residual signature dedicated of r and that the transfer functions from d and the fault set Ω_α to r has the following properties:

$$\Psi(d, 0) = 0 \text{ for all disturbances } d$$

$$\Psi(d, f) \notin \mathcal{R}_{\Omega_\alpha} \text{ for all disturbances } d \text{ and any fault } f \text{ such that } V_j f \neq 0 \text{ for all } j = 1, \dots, s, \text{ and such that } f_i \text{ is identical to zero for all } i \in \Omega_\alpha$$

$$\Psi(d, f) \in \mathcal{R}_{\Omega_\alpha} \text{ for all disturbances } d \text{ and any fault } f \text{ such that } V_j f \neq 0 \text{ for all } j = 1, \dots, s, \text{ and such that } f_i \text{ is unequal to zero for at least one } i \in \Omega_\alpha \text{ where } \mathcal{R}_{\Omega_\alpha} \text{ is the residual vector signature with respect to the fault set } \Omega_\alpha.$$

In [6], generic classwise fault isolation has been introduced. Generic fault set isolation is a special case of generic classwise fault isolation.

Note that it is also possible to formulate Problem 3 more directly by using either direct residual signals, i.e. or a non-zero residual signal when faults in a specific fault set occur and zero when other faults occur or inverse residual signals, i.e. a zero residual signal when faults in a specific fault occur and non-zero when other faults occur.

Further, we have the following assumption:

Assumption 2.1: It is assumed that there is more than one measurement signal, i.e. $p > 1$.

If the system includes only a single measurement signal, it will not be possible to perform the isolation by separation in the residual vector. Then it will only be possible to obtain fault isolation by a dynamical investigation of the residual signal.

Assumption 2.2: It is assumed that the system Σ is stable.

This assumption causes without loss of generality provided that the pair (A, C) is detectable. If the system is not stable, it is possible to rewrite the system by using an observer into a stable system, see [6].

III. PRELIMINARY RESULTS

Some preliminary results based on the results given in [6] are now given.

Theorem 3.1: Consider the system Σ in (1) under the simultaneous occurrence property. The problem of exact fault detection with signature matrices L_f and D_f is solvable if and only if

$$\text{norm rank} \begin{pmatrix} G_{yd} & G_{yf\Omega_\alpha} \end{pmatrix} \geq \text{norm rank}(G_{yd}) + k_i \text{ for } i = 1, \dots, \ell$$

Theorem 3.2: Consider the system Σ in (1) under the simultaneous occurrence property. The problem of exact

generic fault detection with signature matrices L_f and D_f is solvable if and only if

$$\text{norm rank} \begin{pmatrix} G_{yd} & G_{yf_i} \end{pmatrix} > \text{norm rank}(G_{yd}) \text{ for } i = 1, \dots, k$$

Based on this result, we get directly the following result:

Corollary 3.3: Consider the system Σ in (1) under the simultaneous occurrence property of type 1. The total number of faults that can be isolated while solving exact isolation is equal to

$$\text{norm rank} \begin{pmatrix} G_{yd} & G_{yf} \end{pmatrix} - \text{norm rank}(G_{yd})$$

From this corollary, we have that the maximal number of faults that can be isolated exactly is equal to the number of measurement signals in the disturbance free case.

Theorem 3.4: Consider the system Σ in (1) under the simultaneous occurrence property. The problem of exact generic fault isolation for a set of faults f with signature matrices L_f and D_f is solvable if and only if the following condition is true: For any $i = 1, \dots, k$ with α such that $i \in \Omega_\alpha$, we have

$$\text{norm rank} \begin{pmatrix} G_{yd} & G_{yf_i} & G_{yf_{\text{rest}}} \end{pmatrix} > \text{norm rank} \begin{pmatrix} G_{yd} & G_{yf_{\text{rest}}} \end{pmatrix}$$

where f_{rest} is the subset of faults in Ω_α excluding f_i .

Theorem 3.5: Consider the system Σ in (1) under the simultaneous occurrence property. The problem of exact fault set isolation for a set of faults f with signature matrices L_f and D_f is solvable if and only if the following condition is true: For any $i, j = 1, \dots, \ell$, $i \neq j$, we have

$$\text{norm rank} \begin{pmatrix} G_{yd} & G_{yf\Omega_{ij}} \end{pmatrix} > \text{norm rank} \begin{pmatrix} G_{yd} & G_{yf\Omega_j} \end{pmatrix}$$

where $G_{yf\Omega_{ij}}$ is the subsystem with inputs f_{Ω_i} and f_{Ω_j} and output y of system (2)

IV. MAIN RESULTS

The introduction of faults sets in Section II is the basis for the following fault isolation approach. It will result in a three step FDI approach given by:

- Fault detection.
- Fault isolation of the fault set Ω_i , $i = 1, \dots, \ell$.
- Fault isolation in the fault set Ω_i , $i = 1, \dots, \ell$.

The first step is the standard fault detection step, where faults are detected when they occur in the system. In the second step, the fault set wherein the faults occurring in the system belong to is identified. In the last step, the faults in the specified fault set Ω_i are isolated.

A. The Disturbance Free Case

In the disturbance free case, the general system in (1) or (2) take the following form:

$$\Sigma : \{ y = G_{yf} f \} \quad (4)$$

First, let us consider the case of fault detection. The design of a filter/residual generator with a transfer function F_{FD} must be done such that a detection of the additive faults can be done directly by considering the residual vector r_{FD} , when it is possible. From Theorem 3.2, we have that it will always be possible to obtain generic fault detection in the disturbance free case. The residual signal r_{FD} is given by

$$r_{FD} = F_{FD}G_{yf}f \quad (5)$$

The conditions for fault detection take then the following well-known form:

- Fault detection

$$\begin{aligned} r_{FD} &= 0 & \text{for } f &= 0 \\ r_{FD} &\neq 0 & \text{for } f_i &\neq 0 \end{aligned}$$

The next step is to isolate faults in the system. Now the design of a filter/residual generator with a transfer function F_{FI} must be done such that an isolation (separation) of the additive faults can be done directly by considering the residual vector r_{FI} , when it is possible.

Let F_{FI} be designed such that

$$F_{FI}G_{yf} = G_{rf} = (\Xi \quad \bar{G}_{rf}) \quad (6)$$

where Ξ is stable diagonal matrix of dimension $p \times p$, and \bar{G}_{rf} is a stable transfer matrix of suitable dimension. Note that if G_{yf} is left invertible, we can obtain diagonalization of G_{yf} by the design of F_{FI} . G_{yf} is left invertible when $k \leq p$, i.e. the number of additive faults is smaller than or equal to the number of measurement signals.

In the case where complete fault isolation is possible, we have the following well-known conditions for fault isolation, see e.g. [1], [3], [4], [6]:

- Complete fault isolation for $k \leq p$

$$\begin{aligned} r_{FI} &= 0 & \text{for } f &= 0 \\ r_{FI,i} &\neq 0 & \text{for } f_i &\neq 0 \\ r_{FI,j} &= 0 & \text{for } f_i &\neq 0, j \neq i \end{aligned}$$

As it can be seen from (6), it will not in the general case be possible to obtain a complete diagonalization of the transfer function G_{rf} from fault f to the residual vector r_{FI} . If it is impossible to diagonalize G_{rf} , it will not be possible to obtain a complete fault separation in G_{rf} for fault sets of simultaneous occurrence of property of type 1.

When complete fault isolation is not possible, fault isolation in a fault set might be possible. This will depend on the simultaneous occurrence property of the k faults. Let the k faults be arranged into $\ell > 1$ fault sets. Fault isolation in a fault set Ω_i can then be derived in the same way as shown above for complete fault isolation, if it is possible.

Before it is possible to isolate the faults in a specific fault set Ω_i , the fault set needs to be isolated. This problem can be solved by using the result from the generic fault detection problem considered in Theorem 3.2. The design of a residual signal (or vector) for fault set isolation can be done in the following way. Consider e.g. the fault set Ω_i . Let the residual signal $r_{FSI,i}$ for FSI be constructed such

that it is independent of the k_i faults in the fault set Ω_i and depends on all other faults in f . FSI can then be done in the following way (assuming that faults has been detected in the system):

- Fault set isolation for Ω_i

$$\begin{aligned} r_{FSI,\Omega_i} &= 0 & \text{for } f_{\Omega_i} &\neq 0, f_{\setminus\Omega_i} = 0 \\ r_{FSI,\Omega_i} &\neq 0 & \text{for } f_{\Omega_i} &= 0, f_{\setminus\Omega_i} \neq 0 \end{aligned}$$

Based on Theorem 3.2, it is possible to design a residual generator F_{FSI} that satisfy the above condition if, in general, the number of measurement signals p is larger than the number of fault signals k_i in the fault set Ω_i . As a result of this, k_i must satisfy $k_i \leq p - 1$, $i = 1, \dots, \ell$.

For simplicity, let the fault vector f be arranged such that the first k_1 faults in f belong to the first fault set Ω_1 , the next k_2 faults belong to Ω_2 etc. By doing this, the system Σ given by (4) can now be written as:

$$\Sigma : \begin{cases} y = (G_{yf,1} \cdots G_{yf,\ell}) \begin{pmatrix} f_{\Omega_1} \\ \vdots \\ f_{\Omega_\ell} \end{pmatrix} \end{cases} \quad (7)$$

Based on this partition of the system given in (7), the system related with the Ω_i is given by:

$$\Sigma_{\Omega_i} : \{ y = G_{yf,i}f_{\Omega_i} \} \quad (8)$$

This system include k_i additive faults and has $p > k_i$ measurement signals. It is therefore possible to design a residual generator for Σ_{Ω_i} given by (8) that result in complete fault isolation. This mean that we can design a residual generator $F_{FI,i}$ such that

$$r_{FI,\Omega_i} = F_{FI,i}G_{yf,i}f_{\Omega_i} = \Xi_{\Omega_i}f_{\Omega_i} \quad (9)$$

where Ξ_{Ω_i} is stable diagonal matrix of dimension $k_i \times k_i$.

All together, fault isolation in fault sets will require three different sets of residual generators. A single residual generator F_{FD} for fault detection, ℓ residual generators F_{FSI,Ω_i} for fault set isolation and also ℓ residual generators F_{FI,Ω_i} for fault isolation in the ℓ fault sets. All together, the detection and isolation scheme take then the following form:

- Fault detection

$$\begin{aligned} r_{FD} &= 0 & \text{for } f &= 0 \\ r_{FD} &\neq 0 & \text{for } f &\neq 0 \end{aligned}$$

- Fault set isolation for Ω_i

$$\begin{aligned} r_{FSI,\Omega_i} &= 0 & \text{for } f_{\Omega_i} &\neq 0, f_{\setminus\Omega_i} = 0 \\ r_{FSI,\Omega_i} &\neq 0 & \text{for } f_{\Omega_i} &= 0, f_{\setminus\Omega_i} \neq 0 \end{aligned}$$

- Fault isolation in the fault set Ω_i

$$\begin{aligned} r_{FI,\Omega_i,\xi} &= 0 & \text{for } f_{\Omega_i,\xi} &= 0 \\ r_{FI,\Omega_i,\xi} &\neq 0 & \text{for } f_{\Omega_i,\xi} &\neq 0 \\ r_{FI,\Omega_i,\zeta} &= 0 & \text{for } f_{\Omega_i,\xi} &\neq 0, \zeta \neq \xi \end{aligned}$$

for $\xi, \zeta = 1, \dots, k_i$.

Based on the above discussion and the described FDI

scheme, we have the following result.

Theorem 4.1: Consider the disturbance free system Σ given by (4) under the simultaneous occurrence property. Then the problem of exact generic fault isolation with signature matrices L_f and D_f is solvable if and only if the following conditions are satisfied:

1) Fault set isolation

$$\text{norm rank}(G_{yf_{\Omega_{ij}}}) > \text{norm rank}(G_{yf_{\Omega_j}})$$

for $i, j = 1, \dots, \ell, \ell > 1, i \neq j$

$$\text{norm rank}(G_{yf_{\Omega_1}}) = k \leq p, \text{ for } \ell = 1$$

where $G_{yf_{\Omega_{ij}}}$ is the subsystem with inputs f_{Ω_i} and f_{Ω_j} and output y of system (4).

2) Fault isolation in a fault set

$$\text{norm rank} \left(\begin{array}{cc} G_{yf_{\xi}} & G_{y\Omega_{i,\text{rest}}} \end{array} \right) >$$

$$\text{norm rank}(G_{yf_{\Omega_{i,\text{rest}}}}) \text{ for } \xi = 1, \dots, k_i$$

where $f_{\Omega_{i,\text{rest}}}$ is the subset of faults in Ω_i excluding f_{ξ} .

Proof: The proof of Theorem 4.1 follows immediately from the proof of the next theorem which deals with the general case. ■

This result show that it will in general be possible to isolate an unlimited number of faults in the system as long as the conditions in Theorem 4.1 are satisfied.

The fault isolation based on fault sets given above depend strongly on the fault modeling of the fault sets. In the case where the simultaneous occurrence property is not satisfied for the fault modeling, the above FDI scheme will not give a correct fault isolation. It is here important to point out that it is possible to validate the fault set modeling. If faults from different fault sets occur simultaneously, the fault set isolation step in the above FDI scheme will not be able to isolate a fault set. All residual signals r_{FSI,Ω_i} will be non-zero indicating that the faults has not occurred in the fault set $\Omega_i, i = 1, \dots, \ell$.

B. The General Case

Based on the result given by Theorem 4.1 for the disturbance free case, it is simple to extend the result to the general case. The general result then takes the following form.

Theorem 4.2: Consider the general system Σ given by (2) under the simultaneous occurrence property. Then the problem of exact generic fault isolation with signature matrices L_f and D_f is solvable if and only if the following conditions are satisfied:

1) Fault set isolation

$$\text{norm rank} \left(\begin{array}{cc} G_{yd} & G_{yf_{\Omega_{ij}}} \end{array} \right) >$$

$$\text{norm rank} \left(\begin{array}{cc} G_{yd} & G_{yf_{\Omega_j}} \end{array} \right), \text{ for } i, j = 1, \dots, \ell$$

$\ell > 1, i \neq j$

$$\text{norm rank} \left(\begin{array}{cc} G_{yd} & G_{yf_{\Omega_1}} \end{array} \right)$$

– norm rank(G_{yd}) $\geq k$ for $\ell = 1$

where $G_{yf_{\Omega_{ij}}}$ is the subsystem with inputs f_{Ω_i} and f_{Ω_j} and output y of system (2).

2) Fault isolation in a fault set

$$\text{norm rank} \left(\begin{array}{ccc} G_{yd} & G_{yf_{\xi}} & G_{y\Omega_{i,\text{rest}}} \end{array} \right) >$$

$$\text{norm rank} \left(\begin{array}{cc} G_{yd} & G_{yf_{\Omega_{i,\text{rest}}}} \end{array} \right) \text{ for } \xi = 1, \dots, k_i$$

where $f_{\Omega_{i,\text{rest}}}$ is the subset of faults in Ω_i excluding f_{ξ} .

Proof: Theorem 4.2 consist of two parts, conditions for isolating a fault set and condition for isolating faults in a specific fault set. The first part is a special case of the classwise fault isolation problem considered in [6]. Let the fault classes be identical with the fault sets defined in Section II. The condition for classwise fault isolation take then the conditions given in part 1. Part 2 is equivalent with generic fault isolation, now only with respect to a single fault set. ■

In the case when it is not possible to obtain both disturbance decoupling simultaneously with fault detection and/or fault isolation, it is still possible to use the above results. Assume that the conditions for generic fault set detection and fault isolation are satisfied in the disturbance free case, i.e. conditions in Theorem 4.1. It is then possible to design a number of residual generators that will give residual signals for fault detection, fault set isolation and fault isolation in a fault set. Due to the fact that the system does not satisfy the general conditions in Theorem 4.2, it is not possible to get a decoupling of all disturbance signals in the residual signals. This problem needs to be handled by using statistical tests of the residual signals to detect changes with respect to faults. Here, methods as CUSUM or GLR tests, [1], [2], [5] can be applied with advantages.

C. A Special Case: Single Fault Occurrences

Based on the results given in Theorem 4.2, we have then the following result.

Theorem 4.3: Consider the general system Σ given by (2) under the simultaneous occurrence property of type 2. Then the problem of exact generic fault isolation with signature matrices L_f and D_f is solvable if and only if

$$\text{norm rank} \left(\begin{array}{cc} G_{yd} & G_{yf_{ij}} \end{array} \right) = 2 + \text{norm rank}(G_{yd})$$

for $i, j = 1, \dots, k, i \neq j$

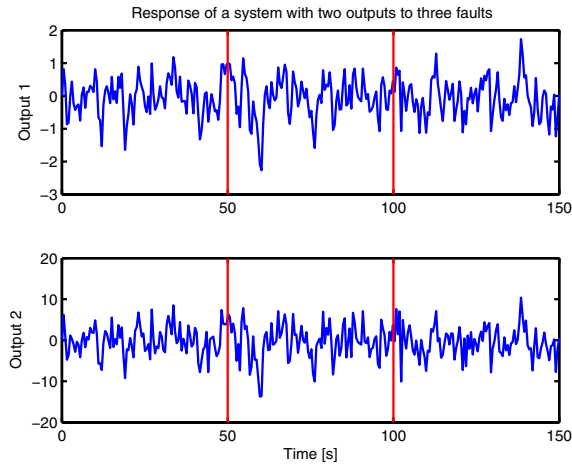


Fig. 1. The two outputs in response to three single faults

where $G_{yf_{ij}}$ is the subsystem with inputs f_i and f_j and output y of system (2).

This result in Theorem 4.3 has been applied in connection with fault signal estimation in [7].

V. EXAMPLE

In the following example we show that in the absence of disturbances, three faults can be isolated using only two measurements, following the filter bank idea below. In the example, the filters will be designed, such that the output of the i th residual generator is zero, if the i th fault occurs, and the two other residual generators have non-zero outputs.

We consider a random system of the form (1) with:

$$A = \begin{pmatrix} -3 & 1 \\ 1 & -4 \end{pmatrix}, \quad E = 0, \quad L_f = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 2 \end{pmatrix},$$

$$C = \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix}, \quad D_d = 0, \quad D_f = 0$$

We assume that f_1 occurs in the time interval $[0 - 50]s$, f_2 occurs in the time interval $[50 - 100]s$, f_3 occurs in the time interval $[100 - 150]s$. Figure 1 shows a simulation of such a fault scenario, where each fault signal is taken as a white noise sequence. Also the control signal is chosen as a white noise sequence. The latter choice might appear rather bizarre, but is just made to show that also the effect of the control signal can be decoupled from the residuals. Note, that it is virtually impossible to distinguish the three faults by visual inspection.

Define

$$G_{yf} = (G_{yf_1} \quad G_{yf_2} \quad G_{yf_3}) = C(sI - A)^{-1}L_f + D_f$$

A bank of three fault filters F_i , $i = 1, 2, 3$, is designed, such that F_i is an annihilator to G_{yf_i} , $F_i G_{yf_i} = 0$. For two outputs this gives the result:

$$F_i = (-G_{yf_i,2} \quad G_{yf_i,1})$$

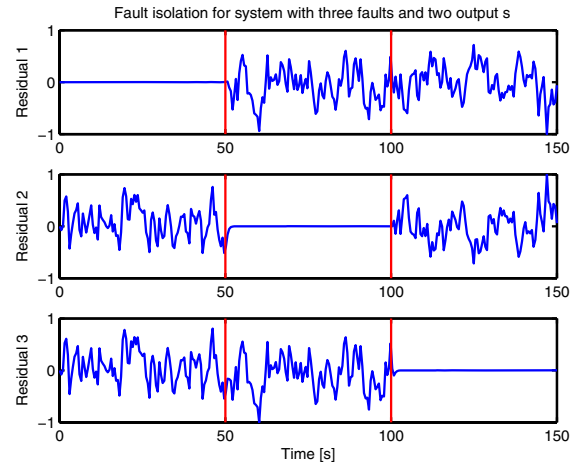


Fig. 2. Fault residuals for three single faults. The i th residual is seen to be zero in the time window where the i th fault occurs

(which is actually unique up to scaling with a rational function). The result of these three filters applied to the simulation in Figure 1, is shown in Figure 2. It is clearly seen, that the i th residual is zero in the time window where the i th fault occurs, whereas the other two residuals remain non-zero.

VI. CONCLUSION

In this paper, necessary and sufficient conditions for fault isolability have been given for systems with single or multiple additive faults.

The conditions show that isolation is possible if and only if some simple rank conditions are satisfied.

It is interesting to note, however, that the *generic* conditions are even simpler. Generically, an unlimited number of single additive faults can be isolated in the disturbance free case for any system having more than one output.

For systems with significant disturbances, the same result holds generically, required that the number of outputs exceeds the number of disturbances with more than one. In that case, an unlimited number of single faults can, generically, be isolated.

REFERENCES

- [1] M. Basseville and I.V. Nikiforov. *Detection of abrupt changes - theory and application*. Prentice Hall, 1993.
- [2] M. Blanke, M. Kinnart, J. Lunze, and M. Staroswiecki. *Diagnosis and Fault-Tolerant Control*. Springer, 2003.
- [3] J. Chen and R. Patton. *Robust model-based fault diagnosis for dynamic systems*. Kluwer Academic Publishers, 1998.
- [4] J. Gertler. *Fault detection and diagnosis in engineering systems*. Marcel Dekker, 1998.
- [5] F. Gustafsson. *Adaptive filtering and change detection*. Wiley & Sons, Chichester, England, 2000.
- [6] A. Saberi, A.A. Stoorvogel, P. Sannuti, and H.H. Niemann. Fundamental problems in fault detection and identification. *International Journal of Robust and Nonlinear Control*, 10(14):1209–1236, 2000.
- [7] A.A. Stoorvogel, H.H. Niemann, A. Saberi, and P. Sannuti. Optimal fault signal estimation. *International Journal of Robust and Nonlinear Control*, 12:697–727, 2002.