Fault Tolerant Control based on Active Fault Diagnosis

Henrik Niemann

Abstract— An active fault diagnosis (AFD) method will be considered in this paper in connection with a Fault Tolerant Control (FTC) architecture based on the YJBK parameterization of all stabilizing controllers. The architecture consists of a fault diagnosis (FD) part and a controller reconfiguration (CR) part. The FTC architecture can be applied for additive faults, parametric faults, and for system structural changes. Only parametric faults will be considered in this paper.

The main focus in this paper is on the use of the new approach of active fault diagnosis in connection with FTC. The active fault diagnosis approach is based on including an auxiliary input in the system. A fault signature matrix is introduced in connection with AFD, given as the transfer function from the auxiliary input to the residual output. This can be considered as a generalization of the passive fault diagnosis case, where the diagnosis is only based on a residual vector. The fault diagnosis is then derived by on-line tests by using the residual vector.

I. INTRODUCTION

The area of fault tolerant control has received an increasing interest in recent years. The reason is the growing complexity of the control systems. This motivates the interest in the design of fault tolerant control systems, where the objective is to disallow one or several faults to develop into an overall system failure. This has resulted in an increasing research in the area of reliable and fault tolerant control of dynamic systems. A good introduction to the area can be found in [2], [18] and in the references herein. In the past years, a number of theoretic results has also been presented in this area, see e.g.[12], [20], [22], [23], [27].

One of the theoretic results that has been developed in this area is the FTC architecture based on the YJBK parameterization of all stabilizing controllers. A detailed description of the FTC architecture can be found in [12], [13], [14], [20]. The architecture consists of a fault diagnosis part and a controller reconfiguration part. Both the fault diagnosis part as well as for the controller reconfiguration part, standard methods can be applied. The main focus in [12], [13], [14], [20] has been on the CR part of the FTC architecture.

The architecture based on the YJBK parameterization results in a separation between the nominal (fault free) part of the closed loop system and the faulty part of the closed loop system. The equivalent separation between performance and robust stability has been shown in [21] when the YJBK controller parameterization is applied.

Minor attention has only attented until now the FD part of this FTC architecture. Just like the CR part, standard fault diagnosis methods can be applied directly. The FTC architecture directly gives a residual vector from where the possible faults in the system must be detected and/or isolated. Methods as e.g. CUSUM and GLR test, [1], can directly be applied for the fault diagnosis. These methods are known as passive fault diagnosis methods, i.e. the diagnosis is only based on available signals in the system. Instead, active fault diagnosis methods can be applied. Here, an auxiliary vector input is applied in connection with the fault diagnosis. Using a dedicated external input vector on the system will in general result in a much better and faster fault diagnosis. One active fault diagnosis method has been described in [3], [4], [16], [17]. The active fault diagnosis method described in [3], [4], [16], [17] is based on an off-line design of the auxiliary signal applied on the system followed by on-line tests.

The main focus in this paper will be a description of active fault diagnosis methods in closed-loop systems and the application of the method in the general FTC architecture. Here, it will be shown how the use of active fault diagnosis will increase the possibility for fault detection and isolation.

II. SYSTEM SETUP

Consider the following generalized nominal system:

$$\Sigma_P : \begin{cases} z = G_{zw}w + G_{zd}d + G_{zu}u \\ e = G_{ew}w + G_{ed}d + G_{eu}u \\ y = G_{yw}w + G_{yd}d + G_{yu}u \end{cases} \quad (1)$$

where $d \in \mathcal{R}^r$ is a disturbance signal vector, $u \in \mathcal{R}^m$ the control input signal vector, $e \in \mathcal{R}^q$ is the external output signal vector to be controlled, $y \in \mathcal{R}^p$ is the measurement vector, $w \in \mathcal{R}^k$ and $z \in \mathcal{R}^k$ are external input and output vectors. The connection between the external output and the external input is given by

$$w = \theta z$$

where θ is a diagonal matrix given by

$$\theta = diag(\theta_1, \cdots, \theta_i, \cdots, \theta_k)$$

represent the parametric faults in the system. We will use the notation $\theta_i \neq 0$ as a short form for

$$\theta = diag(0, \cdots, 0, \theta_i, 0, \cdots, 0)$$

i.e. $\theta_j = 0, \ j \neq i$.

Note that the above description is also applied in connection with description of systems including model uncertainties, see e.g. [26]. Closing the loop from w to z in Σ_P by using θ, we get

$$\Sigma_{P,\theta} = \mathcal{F}_u(\Sigma_P, \theta) \quad (2)$$

H. Niemann is with Ørsted•DTU, Automation, Technical University of Denmark, Building 326, DK-2800 Kgs. Lyngby, Denmark. E-mail: hhn@oersted.dtu.dk

Let the system be controlled by a stabilizing feedback controller given by:

$$\Sigma_K : \{ \ u = Ky \quad\quad\quad (3)$$

III. THE YJBK PARAMETERIZATION

Before describing a general FTC architecture for descriptor systems, the YJBK parameterization is shortly introduced. The YJBK parameterization has also been applied in connection with FTC in [12], [14], [20], [27].

A. The Primary YJBK Parameterization

The (primary) YJBK parameterization was first derived by Youla et al. and independently by Kucera. It has been described in [24], [25] and later used in many cases in connection with feedback control.

Let a coprime factorization of the system $G_{yu}(s)$ from (1) and a stabilizing controller $K(s)$ from (3) be given by:

$$
\begin{aligned}
G_{yu} &= NM^{-1} = \tilde{M}^{-1}\tilde{N}, \quad N,M,\tilde{N},\tilde{M} \in \mathcal{RH}_\infty \\
K &= UV^{-1} = \tilde{V}^{-1}\tilde{U}, \quad\ \ U,V,\tilde{U},\tilde{V} \in \mathcal{RH}_\infty
\end{aligned}
\quad (4)
$$

where the eight matrices in (4) must satisfy the double Bezout equation given by, see [21]:

$$
\begin{aligned}
\begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix} &= \begin{pmatrix} \tilde{V} & -\tilde{U} \\ -\tilde{N} & \tilde{M} \end{pmatrix} \begin{pmatrix} M & U \\ N & V \end{pmatrix} \\
&= \begin{pmatrix} M & U \\ N & V \end{pmatrix} \begin{pmatrix} \tilde{V} & -\tilde{U} \\ -\tilde{N} & \tilde{M} \end{pmatrix}
\end{aligned}
\quad (5)
$$

Based on the above coprime factorization of the system $G_{yu}(s)$ and the controller $K(s)$, we can give a parameterization of all controllers that stabilize the system in terms of a stable parameter $Q(s)$, i.e. all stabilizing controllers are given by [21], [26]:

$$K(Q) = (U+MQ)(V+NQ)^{-1}, \ Q \in \mathcal{RH}_\infty \quad (6)$$

or by using a left factored form:

$$K(Q) = (\tilde{V}+Q\tilde{N})^{-1}(\tilde{U}+Q\tilde{M}), \ Q \in \mathcal{RH}_\infty \quad (7)$$

Using the Bezout equation, the controller given either by (6) or by (7) can be realized as an LFT in the parameter Q,

$$K(Q) = \mathcal{F}_l\left(\begin{pmatrix} UV^{-1} & \tilde{V}^{-1} \\ V^{-1} & -V^{-1}N \end{pmatrix}, Q\right) = \mathcal{F}_l(J_K, Q) \quad (8)$$

B. The Dual YJBK Parameterization

In the same way, it is possible to derive a parameterization in terms of a stable parameter S of all systems that are stabilized by one controller, i.e. the dual YJBK parameterization. The parameterization is given by [21]:

$$G_{yu}(S) = (N+VS)(M+US)^{-1}, \ S \in \mathcal{RH}_\infty \quad (9)$$

or by using a left factored form:

$$G_{yu}(S) = (\tilde{M}+S\tilde{U})^{-1}(\tilde{N}+S\tilde{V}), \ S \in \mathcal{RH}_\infty \quad (10)$$

An LFT representation of (9) or (10) is given by:

$$G_{yu}(S) = \mathcal{F}_l\left(\begin{pmatrix} NM^{-1} & \tilde{M}^{-1} \\ M^{-1} & -M^{-1}U \end{pmatrix}, S\right) = \mathcal{F}_l(J_G, S) \quad (11)$$

It has been shown in e.g. [21], that the dual YJBK parameter S transfer function can be calculated by using the primary YJBK parameterization. It turns out that S is given by:

$$S = \mathcal{F}_u(J_K, G_{yu}(S)) \quad (12)$$

IV. PASSIVE FAULT DIAGNOSIS

It has been shown in [5] that it is possible to parameterize all residual generators by using the YJBK parameterization. All residual signals r_q for the $\Sigma_{P,\theta}$ given by (2) can be described by

$$r_q = Q_{\text{FDI},O}(\tilde{M}y - \tilde{N}u) = Q_{\text{FDI}}r \quad (13)$$

where $Q_{\text{FDI},O}$ is a stable and proper filter of suitable order. $Q_{\text{FDI},O}$ needs to be designed such that the residual signal/vector r_q satisfies the following conditions, [19]:

- Fault detection

$$
\begin{aligned}
r_q(t) &= 0 \quad \text{for} \quad \theta = 0, \ \forall (d(t), u(t)) \\
r_q(t) &\neq 0 \quad \text{for} \quad \theta \neq 0, \ \forall (d(t), u(t)) \neq (0,0)
\end{aligned}
$$

- Fault isolation

$$
\begin{aligned}
r_q(t) &= 0 \quad \text{for} \quad \theta = 0, \ \forall (d(t), u(t)) \\
r_{q,i}(t) &\neq 0 \quad \text{for} \quad \theta_i \neq 0, \ \forall (d(t), u(t)) \neq (0,0) \\
r_{q,j}(t) &= 0 \quad \text{for} \quad \theta_j = 0, \ j \neq i, \ \forall (d(t), u(t))
\end{aligned}
$$

Note that the definitions of fault detection and fault isolation given above are not unique. Depending on how many faults that can appear simultaneously, different definitions can be given, [19]. It is also important to point out that it is not always possible to design $Q_{\text{FDI},O}$ so that it is possible to obtain exact fault detection or exact fault isolation. Instead, different forms of approximative fault detection and/or fault isolation need to be considered, [5].

V. FAULT TOLERANT CONTROLLER ARCHITECTURE

In the sequel, the architecture for fault tolerant controllers for systems with parametric faults will shortly be described.

A fault tolerant controller mainly consists of two parts, a fault diagnosis (FDI) part and a controller reconfiguration (CR) part. The fault diagnosis part consist of a residual generator and a decision/evaluation block. Based on the output from the decision block, the controller is reconfigured by using the YJBK parameter. This means that the CR part of the feedback controller is a modification of the existing controller. Thus, a controller change when a fault appears in the system is not a complete shift to another controller, but only a modification of the existing controller by adding a correction signal in the nominal controller. However, it should be pointed out that it is possible to modify the controller arbitrarily by designing the YJBK parameter Q, see e.g. [15]. The reconfiguration can be derived in different

way. It could be a direct redesign, a selection between a number of pre-designed controllers etc.

All together, the complete architecture is shown in Fig. 1. Here $Q_{\text{FDI},O}$ is the YJBK parameter used in connection with fault diagnosis and Q_{RC} is the YJBK parameter used in connection with controller reconfiguration. This architecture shows that it is possible to combine both fault diagnosis and controller reconfiguration in the same architecture and use the same input and output vectors for both the FDI part and the CR part.
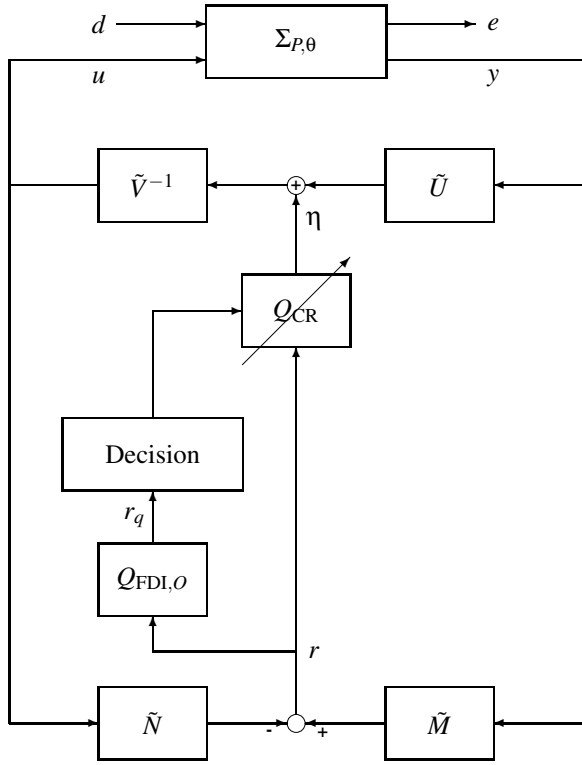

Fig. 1. A fault tolerant controller architecture.

The above controller architecture applied for FTC shown in Fig. 1 has a fixed structure with respect to the number of measurement signals and control signals. This will not in general be the case in real applications. This type of system change has not directly been included in the system description given by (1). However, it is possible to include change of sensors and/or actuators in the FTC architecture given above. This has been considered in connection with a regular system in [14].

The design of the reconfiguration part of the fault tolerant controller can be derived by considering the closed loop transfer function from external input d to external output e. The closed loop transfer function is given by:

$$e = T_{ed}d \tag{14}$$

where

$$
\begin{aligned}
T_{ed} = & G_{ed}(\theta) + G_{eu}(\theta)(U + MQ_{\text{CR}})((V - G_{yu}(\theta)U) \\
& + (N - G_{yu}(\theta)M)Q_{\text{CR}})^{-1}G_{yd}(\theta)
\end{aligned}
$$

The closed loop transfer function $T_{ed}(s)$ can then be rewritten as an LFT of the open loop transfer function with Q_{CR} in the feedback loop given by:

$$T_{ed} = \mathcal{F}_l(P, Q_{\text{CR}}) \tag{15}$$

and P is given by

$$
\begin{aligned}
P_{ed} &= G_{ed}(\theta) + G_{eu}(\theta)U(V - G_{yu}(\theta)U)^{-1}G_{yd}(\theta) \\
P_{e\eta} &= G_{eu}(M - U(V - G_{yu}(\theta)U)^{-1}(N - G_{yu}(\theta)M)) \\
P_{rd} &= (V - G_{yu}(\theta)U)^{-1}G_{yd}(\theta) \\
P_{r\eta} &= -(V - G_{yu}(\theta)U)^{-1}(N - G_{yu}(\theta)M)
\end{aligned}
$$

The design of the Q_{CR} can be considered either as a stabilization problem or as a performance design problem.

The above FTC design problems has been investigated in details in connection with the proposed controller architecture for standard continuous-time systems in [12] and for sampled-data systems in [14].

VI. ACTIVE FAULT DIAGNOSIS

The general FTC architecture shown in Fig. 1 is based on passive fault diagnosis as griefly described in Section IV. However, without any modifications, it is possible to apply an active fault diagnosis method in the FTC architecture.

The idea of active fault diagnosis is to disturb the system by auxiliary input signals. Based on the signal and the measurement signal, faults are detected/isolated by using on-line tests. The method is related with system identification.

First, let's consider the general FTC architecture in Fig. 1. Consider the residual vector r as a function of the external input d and the controller correction vector η, see Fig. 2.

From Fig. 2 and (15) we have that the residual vector r_q is given by

$$
\begin{aligned}
r_q &= Q_{\text{FDI},O}S(\theta)Q_{\text{FDI},I}\eta_q + Q_{\text{FDI},O}P_{rd}d \\
&= S_Q(\theta)\eta_q + Q_{\text{FDI},O}P_{rd}d
\end{aligned} \tag{16}
$$

by using that $P_{r\eta} = S$ from (12). Further, $Q_{\text{FDI},I}$ and $Q_{\text{FDI},O}$ are a pre- and a post filter equivalent with the filter used in the passive case. Both S and P_{rd} are functions of the parametric fault vector θ. Using (12) together with the system setup Σ_P in (1), $S(\theta)$ is given by, [7]:

$$S(\theta) = \tilde{M}G_{yw}\theta(I - (G_{zw} + G_{zu}U\tilde{M}G_{yw})\theta)^{-1}G_{zu}M \tag{17}$$

and P_{rd} is given by

$$
\begin{aligned}
P_{rd}(\theta) &= (V - G_{yu}(\theta)U)^{-1}G_{yd}(\theta) \\
&= \tilde{M}(I - G_{yw}\theta(I - G_{zw}\theta)^{-1}G_{zu}U\tilde{M})^{-1} \\
&\quad (G_{yd} + G_{yw}\theta(I - G_{zw}\theta)^{-1}G_{zd})
\end{aligned} \tag{18}
$$

In the fault free case, i.e. $\theta = 0$, we have that (16) is given by
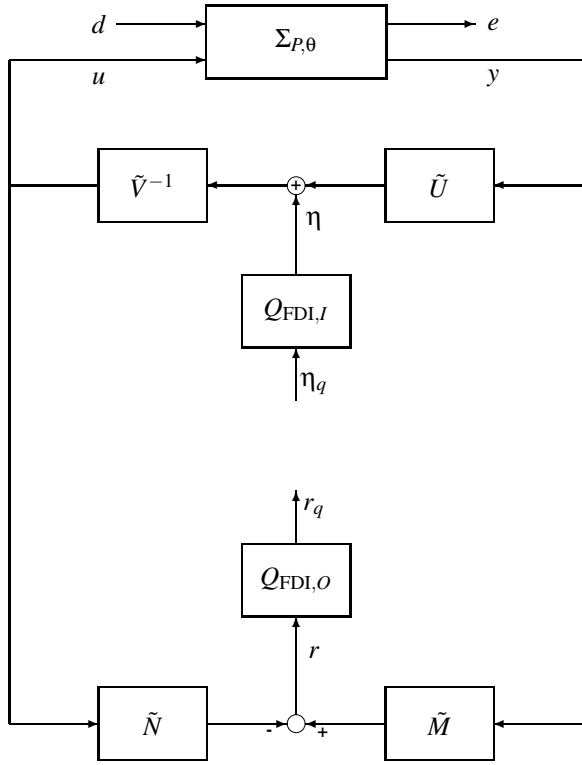
$$r_q = Q_{\text{FDI},O}\tilde{M}G_{yd}d \tag{19}$$

Fig. 2. The controller structure including pre- and post-filtering matrices at the external input η and at the residual vector r, respectively.

i.e. the dual YJBK parameter S is identical zero. This shows the separation between the nominal closed loop system and the faulty part of the closed loop feedback system. Using the dual YJBK parameterization, a faulty closed loop system is closed loop stable if and only if the nominal closed loop system is stable and the dual YJBK parameter is stable, [12], [14], [21]. Consequently, if the faulty closed loop system is unstable, the closed loop system can be stabilized only by closing a loop around the dual YJBK parameter $S(\theta)$. This can be done by designing a YJBK controller Q_{CR} that stabilizes the closed loop given by

$$(I - Q_{CR}S(\theta))^{-1} \qquad (20)$$

For further details, see e.g. [12], [14].

The dimension of $S(\theta)$ is $p \times m$, i.e. the same dimension as G_{yu}.

As it can be seen from (16), (17), $S(\theta)$ is very important in connection with residual signal r_q. Equivalent with the definition of *fault signature* for additive faults, [6], $S(\theta)$ will be called the *fault signature matrix* for parametric faults, [9]. The reason is that both fault detection and fault isolation using an active method will be based directly on the fault signature matrix $S(\theta)$. This strong dependency of $S(\theta)$ in connection with FDI will be investigated in details in the following.

A. Active Fault Detection

Let's consider fault detection based on the equation for the residual vector in (16). Based on the definitions of fault detection given in Section IV, the definition of fault detection based on the fault signature matrix can then be given by:

- Fault detection

$$\begin{aligned} S_Q(\theta) &= 0 \quad \text{for} \quad \theta = 0 \\ S_Q(\theta) &\neq 0 \quad \text{for} \quad \theta \neq 0 \end{aligned}$$

It is clear from this definition that the fault detection based on the fault signature matrix results in a direct fault detection, i.e. the detection based on a zero or a non-zero fault signature matrix. Note that this direct fault detection is independent of the design of filters, assuming that the two filters are non-zero and stable. This means that the two filters must be designed with respect to minimizing the effect from the d on the residual vector r_q and maximize the effect from η_q on r_q with bounded performance degradation .

B. Active Fault Isolation

The fault isolation case is more complicated than fault detection. The main reason is that all elements in $S(\theta)$ will in general depend on all parametric faults. This means that it will be impossible to isolate the single parametric faults be evaluating the single elements in $S(\theta)$, i.e. direct fault isolation. Further, it will also depend on which parametric faults that can occur simultaneously and which cannot.

As in the fault detection case, we want to come up with conditions for fault isolation based directly on the fault signature matrix $S(\theta)$ or $S_Q(\theta)$.

First, let's consider the fault signature matrix without any pre- and post-filters for a preliminary analysis. As pointed out above, all elements in $S(\theta)$ will in general depend on all parametric faults in θ. For simplifying the analysis, assume that only a single parametric fault can occur at the time. The general case can be derived in the same way. For each parametric fault θ_i, define an associated fault signature matrix set $\mathcal{S}_i$ for a specified frequency interval $\bar{\omega}$, such that the fault signature matrix $S(\theta_i)$ is included in the $\mathcal{S}_i$ for all possible values of the $i'th$ fault, i.e.

$$S(\theta_i) \in \mathcal{S}_i, \text{ for } \forall \theta_i \in \Theta_i, \ \omega \in \bar{\omega} \qquad (21)$$

The frequency interval $\bar{\omega}$ can be a single frequency ω_0, a number of frequencies $\omega_1, \omega_1, \ldots$, an interval $[\omega_1, \omega_2]$ or the hole frequency range $[0, \infty[$. Further, the frequency intervals $\bar{\omega}$ might be different for the different fault signature matrix sets. It is further assumed that the fault signature matrix sets satisfy:

$$\mathcal{S}_i \cap \mathcal{S}_j = \emptyset, \ \forall \theta_i \in \Theta_i, \ \forall \theta_j \in \Theta_j, \ i \neq j, \ \omega \in \bar{\omega}$$

Based on this, we get directly

• Complete fault isolation of θ_i

$$
\begin{array}{rcll}
S(\theta) & = & 0 & \text{for} \quad \theta = 0 \\
S(\theta) & \in & \mathcal{S}_i & \text{for} \quad \theta_i \neq 0, \ \omega \in \bar{\omega} \\
S(\theta) & \notin & \mathcal{S}_j & \text{for} \quad \theta_i \neq 0, \ \theta_j = 0, \ \forall j \neq i, \ \omega \in \bar{\omega}
\end{array}
$$

The FDI approach just described is directly based on the use of the fault signature matrix. This will not in general give elements in $S(\theta)$ that only depend on a reduced number of parametric faults. If the single elements in $S(\theta)$ only depend on a reduced number of parametric faults, the fault isolation can be derived by checking the single elements in $S(\theta)$ if they are zero or not, i.e. equivalent with the fault detection based on $S(\theta)$. This will be much more easy compared with isolation based on dynamic separation.

Instead of using the fault signature matrix directly in connection with fault isolation, let's consider the fault signature matrix given by (17), where the pre- and post-filters $Q_{\text{FDI},I}$ and $Q_{\text{FDI},O}$, have been included. The design of $Q_{\text{FDI},I}$ and $Q_{\text{FDI},O}$ must be done such that an isolation (separation) of the parametric faults can be done directly by considering $S_Q(\theta)$, when it is possible. Using the fact that both $\tilde{M}G_{yw}$ and $G_{zu}M$ are two stable transfer functions, it is possible to design $Q_{\text{FDI},I}$ and $Q_{\text{FDI},O}$ such that

$$
\begin{array}{rcl}
G_{zu}MQ_{\text{FDI},I} & = & \begin{pmatrix} \Xi_I \\ H_I \end{pmatrix} \\
Q_{\text{FDI},O}\tilde{M}G_{yw} & = & \begin{pmatrix} \Xi_O & H_O \end{pmatrix}
\end{array} \tag{22}
$$

where Ξ_I and Ξ_O are two stable diagonal matrices of dimension $m \times m$ and $p \times p$, respectively, and H_I, H_O are two stable transfer matrices of suitable dimensions. Note that if $G_{zu}M$ is right invertible, we can obtain diagonalization of $G_{zu}M$ by the design of $Q_{\text{FDI},I}$. Equivalent, if $\tilde{M}G_{yw}$ is left invertible, a diagonalization of $\tilde{M}G_{yw}$ can be obtained by the design of $Q_{\text{FDI},O}$.

Using the $Q_{\text{FDI},I}$ and $Q_{\text{FDI},O}$ satisfying (22), gives directly

$$
S_Q(\theta) = \begin{pmatrix} \Xi_O & H_O \end{pmatrix} \theta (I - T_{zw,cl}\theta)^{-1} \begin{pmatrix} \Xi_I \\ H_I \end{pmatrix} \tag{23}
$$

As it can be seen from (23), it will not in the general case be possible to obtain a complete diagonalization of the input and output transfer functions. If it is not possible to diagonalize either the input or the output transfer functions by the design of $Q_{\text{FDI},I}$ or $Q_{\text{FDI},O}$, it will not be possible to obtain a complete fault separation in $S_Q(\theta)$.

Assume that $p \geq 2$ or $m \geq 2$. Further, it is assumed in this paper that $p \geq m$. The parametric fault matrix θ is then arranged such that the first $p-1$ (or less) faults belong to the first fault set Ω_1. The next faults belong to the second fault set Ω_2 etc. Only faults belonging to a specific fault set can occur simultaneously. Using a $Q_{\text{FDI},O,1}$ satisfying (22) with respect to the first fault set Ω_1 gives the following fault signature matrix:

$$
S_{Q,\Omega_1}(\theta) = \begin{pmatrix} \Xi_O & H_O \end{pmatrix} \theta (I - T_{zw,cl}\theta)^{-1} G_{zu}MQ_{\text{FDI},I} \tag{24}
$$

Assume that the first fault set Ω_1 includes $p-1$ parametric faults. Then, let $S_{Q,\Omega_1}(\theta)$ be partitioned into

$$
S_{Q,\Omega_1}(\theta) = \begin{pmatrix} S_{Q,\Omega_1,1}(\theta) \\ S_{Q,\Omega_1,2}(\theta) \end{pmatrix}
$$

where $S_{Q,\Omega_1,1}(\theta)$ is the first $p-1$ rows in $S_{Q,\Omega_1}(\theta)$ with respect to the faults in fault set Ω_1 and $S_{Q,\Omega_1,2}(\theta)$ is the last row in $S_{Q,\Omega_1}(\theta)$.

Based on (24), the faults in Ω_1 can now be isolated. This will require a three step procedure: first a fault detection, secondly a fault set isolation and finally a fault isolation in the specific fault set. The three steps are as follows:

• Fault detection

$$
\begin{array}{rcll}
S_Q(\theta) & = & 0 & \text{for} \quad \theta = 0 \\
S_Q(\theta) & \neq & 0 & \text{for} \quad \theta \neq 0
\end{array}
$$

• Fault isolation of the fault set Ω_1

$$
\begin{array}{rcll}
S_{Q,\Omega_1,2}(\theta) & = & 0 & \theta \neq 0, \ \theta \in \Omega_1 \\
S_{Q,\Omega_1,2}(\theta) & \neq & 0 & \theta \neq 0, \ \theta \notin \Omega_1
\end{array}
$$

• Fault isolation of the faults in the fault set Ω_1.
  The i'th fault in the fault set Ω_1 occurs in the system if and only if:

$$
S_{Q,\Omega_1,1,i,j}(\theta) \quad \neq \quad 0 \quad \theta_i \neq 0, \ i = 1, \cdots, p-1, \ \forall j
$$

The i'th fault in the fault set Ω_1 does not occur in the system if and only if:

$$
S_{Q,\Omega_1,1,i,j}(\theta) \quad = \quad 0 \quad \theta_i = 0, \ i = 1, \cdots, p-1, \ \forall j
$$

where $S_{Q,\Omega_1,1,i,j}(\theta)$ is the (i,j) element in $S_{Q,\Omega_1,1}(\theta)$.

Note that the last row in $S_{Q,\Omega_1}(\theta)$ given by $S_{Q,\Omega_1,2}(\theta)$ is used for detection of faults in other fault sets than Ω_1. From the definition of the fault sets, the faults related to the last row in $S_{Q,\Omega_1}(\theta)$ will not belong to the specific fault set. Further note that faults that do not belong to the specified fault set will either result in a non-zero last row of $S_{Q,\Omega_1}(\theta)$ or result in all rows in $S_{Q,\Omega_1}(\theta)$ will be non-zero. The reason is that if the faults in θ are isolable, then the faults not belonging to the specific fault set will affect the non-diagonal matrix H_0. As a result of this, a single fault that does not belong to the specific fault set might therefore affect all rows in $S_{Q,\Omega_1}(\theta)$.

A block diagram of the complete fault isolation setup based on fault sets is shown in Fig. 3.

VII. CONCLUSION

Fault tolerant control based on using active fault diagnosis has been considered in this paper. The FTC architecture is based on the YJBK parameterization. It is shown that the setup gives a direct separation in terms of the fault signature matrix. The fault signature matrix can be applied directly for fault detection, by using the fact that the fault signature matrix is non-zero in the faulty case. Fault isolation is a little more complicated, but including pre- and post filters around the fault signature matrix, it is possible to obtain
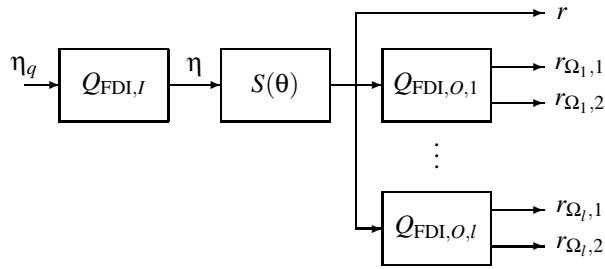
Fig. 3. Fault detection and isolation based on fault occurrence in fault sets. r is the residual vector for fault detection, $r_{\Omega_1,1}$ is the residual vector for fault isolation in fault set Ω_1, $r_{\Omega_1,2}$ is the residual signal applied for isolation of the fault sets, $r_{\Omega_l,1}$ is the residual vector for fault isolation in fault set Ω_l and $r_{\Omega_l,2}$ is the residual signal applied for isolation of the fault sets.

direct fault isolation. If direct fault isolation is not possible, a dynamic fault isolation needs to be used instead.

Using both input and output signals in the active fault diagnosis approach, the active fault diagnosis approach can be considered as a generalization of the passive fault diagnosis approach. The passive approach is based on a residual vector, whereas the active approach is based on a matrix. The possibility for fault detection and isolation will increase compared with the passive approach. Further, in the active approach, the system is disturbed by auxiliary input vector to make an early fault detection/isolation. In the passive approach, we must wait until we get a non-zero residual vector. The system must be activated by external disturbance.

One of the consequences of the active approach is that additive faults cannot be detected or isolated by this approach. The reason is that the faults must affect the fault signature matrix to be detected or isolated. This is equivalent with the requirement that the faults must affect the closed-loop stability via the dual YJBK matrix, i.e. the fault signature matrix. In a pure linear system, additive faults will not affect the closed-loop stability.

A more detailed analysis of the AFD in closed-loop systems is given in [9] for the nominal case and in [8]. The focus in this paper and in [9] has been based on a closed-loop setup. However, it has been shown in [10], that the setup can also be applied directly on both open-loop systems as well as on reconfigurated closed-loop systems. As a direct result of this, AFD based on a nominal feedback controller might not be affected by a later controller reconfiguration. This is important in connection with FTC.

Some application of AFD using a closed-loop setup can be found in [11].

REFERENCES

[1] M. Basseville and I.V. Nikiforov. *Detection of abrupt changes - theory and application*. Prentice Hall, 1993.

[2] M. Blanke, C.W. Frei, F. Kraus, R.J. Patton, and M. Staroswiecki. What is fault-tolerant control? In *Preprints of 4th IFAC Symposium on Fault Detection Supervision ans Safety for Technical Processes, SAFEPROCESS'2000*, pages 40–51, Budapest, Hungary, 2000.

[3] S.L. Campbell and R. Nikoukhah. *Auxiliary signal design for failure detection*. Princeton University Press, Princeton, NJ, USA, 2004.

[4] S.L. Campbell and R. Nikoukhah. Software for auxiliary signal design. In *Proceedings of the American Control Conference*, pages 4414–4419, Boston, MA, USA, 2004.

[5] P.M. Frank and X. Ding. Frequency domain approach to optimally robust residual generation and evaluation for model-based fault diagnosis. *Automatica*, 30:789–804, 1994.

[6] M. Massoumnia. A geometric approach to the synthesis of failure detection filters. *IEEE Transactions on Automatic Control*, 31(9):839–846, 1986.

[7] H.H. Niemann. Dual Youla parameterization. *IEE Proceedings - Control Theory and Applications*, 150(5):493–497, 2003.

[8] H.H. Niemann. Active fault diagnosis in closed-loop uncertain systems. Submitted to CDC-ECC'05, also avaible at www.oersted.dtu.dk under "Publications", 2005.

[9] H.H. Niemann. Algebraic aspect of active fault diagnosis in closed-loop systems. Submitted for publication, avaible at www.oersted.dtu.dk under "Publications", January 2005.

[10] H.H. Niemann. A unified setup for active fault diagnosis. Submitted to CDC-ECC'05, also avaible at www.oersted.dtu.dk under "Publications", January 2005.

[11] H.H. Niemann and N.K. Poulsen. Active fault diagnosis in closed-loop systems. In *Proceedings of the 16th IFAC World Congress*, page 6p, Prague, Czech Republic, 2005.

[12] H.H. Niemann and J. Stoustrup. Reliable control using the primary and dual Youla parameterization. In *Proceedings of the 41st IEEE Conference on Decision and Control*, pages 4353–4358, Las Vegas, NV, USA, 2002.

[13] H.H. Niemann and J. Stoustrup. Passitive fault tolerant control of a double inverted pendulum - A case study example. In *Proceedings of IFAC SAFEPROCESS 2003*, pages 1029–1034, Washington, DC, USA, 2003.

[14] H.H. Niemann and J. Stoustrup. Fault tolerant controllers for sampled-data systems. In *Proceedings of the American Control Conference*, pages 3490–3495, Boston, MA, USA, 2004.

[15] H.H. Niemann, J. Stoustrup, and R.B. Abrahamsen. Switching between multivariable controllers. *Optimal Control - Application and Methods*, pages 51–66, 2004.

[16] R. Nikoukhah. Innovations generation in the presence of unknown inputs: Application to robust failure detection. *Automatica*, 30:1851–1867, 1994.

[17] R. Nikoukhah, S.L. Campbell, and F. Delebecque. Detection signal design for failure detection: a robust approach. *International Journal of Adaptive Control and Signal Processing*, 14:701–724, 2000.

[18] R. Patton. Fault tolerant control: The 1997 situation. In *Proceedings of the IFAC Symposium SAFEPROCESS'97*, pages 1033–1055, Hull, England, 1997.

[19] 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.

[20] J. Stoustrup and H.H. Niemann. Fault tolerant feedback control using the youla parameterization. In *Proceedings of the 6th European Control Conference*, pages 1970–1974, Porto, Portugal, September 2001.

[21] T.T. Tay, I.M.Y. Mareels, and J.B. Moore. *High performance control*. Birkhäuser, 1997.

[22] N.E. Wu and T.J. Chen. Feedback design in control reconfigurable systems. *International Journal of Robust and Nonlinear Control*, 6(6):561–570, 1996.

[23] N.E. Wu, K. Zhou, and G. Salomon. Control reconfigurability of linear time-invariant systems. *Automatica*, 36:1767–1771, 2000.

[24] D.C. Youla, J.J. Bongiorno, and H.A. Jabr. Modern Wiener-Hopf design of optimal controllers - Part I: The single-input-output case. *IEEE Transactions on Automatic Control*, 21(1):3–13, 1976.

[25] D.C. Youla, H.A. Jabr, and J.J. Bongiorno. Modern Wiener-Hopf design of optimal controllers - Part II: The multivariable case. *IEEE Transactions on Automatic Control*, 21(3):319–338, 1976.

[26] K. Zhou, J.C. Doyle, and K. Glover. *Robust and optimal control*. Prentice Hall, 1995.

[27] K. Zhou and Z. Ren. A new controller architecture for high performance robust, and fault-tolerant control. *IEEE Transactions on Automatic Control*, 46(10):1613–1618, 2001.