Int. J. Appl. Math. Comput. Sci., 2012, Vol. 22, No. 1, 67–86
DOI: 10.2478/v10006-012-0005-x

A MODEL–BASED APPROACH TO FAULT–TOLERANT CONTROL

HANS HENRIK NIEMANN

Department of Electrical Engineering, Automation and Control
Technical University of Denmark, Building 326, DK-2800 Kgs. Lyngby, Denmark
e-mail: hhn@elektro.dtu.dk

A model-based controller architecture for Fault-Tolerant Control (FTC) is presented in this paper. The controller architecture is based on a general controller parameterization. The FTC architecture consists of two main parts, a Fault Detection and Isolation (FDI) part and a controller reconfiguration part. The theoretical basis for the architecture is given followed by an investigation of the single parts in the architecture. It is shown that the general controller parameterization is central in connection with both fault diagnosis as well as controller reconfiguration. Especially in relation to the controller reconfiguration part, the application of controller parameterization results in a systematic technique for switching between different controllers. This also allows controller switching using different sets of actuators and sensors.

Keywords: fault-tolerant control, controller architecture, fault diagnosis, active fault diagnosis, controller switching.

1. Introduction

Fault-Tolerant Control (FTC) (Blanke *et al.*, 2003) and high performance feedback control (Tay *et al.*, 1997), have been considered to be two distinct areas. In the high performance control area, the efficiency requirements are satisfied by the use of more advanced design methods. These include methods such as, e.g., $\mathcal{H}_2$, $\mathcal{H}_\infty$, LMI-design, μ-synthesis, etc. (Maciejowski, 1989; Skogestad and Postlethwaite, 2005; Zhou *et al.*, 1995). The price is complex controllers, where re-tuning of single parts is impossible. Using simpler controller architectures consisting of P, PI, PID controllers, etc., it is reasonably simple to re-tune single parameters in connection with implementation. The controller parameters are transparent to the operator, so redesign is possible. That is not the case for more advanced and complex controller architectures. This is one of the main reasons why advanced controllers are not always applied in real applications.

Fault-tolerant controllers deal with a concept for handling faulty situations by suitable reconfiguration of the feedback controller applied. If a fault is detected and isolated, we want to change from a high performance controller to a safe-mode controller. The change must be done in a reliable way, so that closed-loop stability can be guaranteed through the change. A number of different concepts have been described in books and papers (Blanke *et al.*, 1997; 2000; 2003; Niemann and Stoustrup, 2002; 2005; Stoustrup and Niemann, 2001).

The central issue in FTC is making the feedback controller tolerant with respect to faults or changes in the system and/or the instrumentation. This can be done on the basis of either a passive approach or an active approach. In the former, the nominal controller will be able to stabilize the system for possible faults. This is equivalent to robust feedback control. In the latter, the feedback controller is redesigned or reconfigured on the basis of the results from detection and isolation of faults. This concept is more complex than the passive approach, but in general it is also possible to handle a much larger number of faults. This architecture is shown in Fig. 1.

A number of different controller architectures for FTC have been suggested in the literature. One of the architectures is based on the Youla–Jabr–Bongiorno–Kucera (YJBK) parameterization described by Niemann and Stoustrup (2002; 2005), Stoustrop and Niemann (2001) as well as Zhou and Ren (2001). Here, the controller reconfiguration is obtained by design/redesign of the YJBK transfer matrix. The controller architecture is shown in Fig. 2.

The starting point for this paper is the mentioned FTC architecture shown in Fig. 2. Instead of using a standard nominal controller as the normal-mode controller, it has been selected as a safe-mode ONE. The reconfiguration controller is then designed to enhance performance in the system. This will allow a very fast switch from a

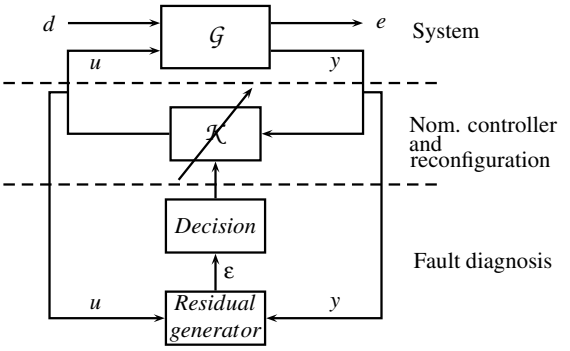

Fig. 1. Simple block diagram of fault-tolerant control including a residual generator, a decision block and a controller-change block.

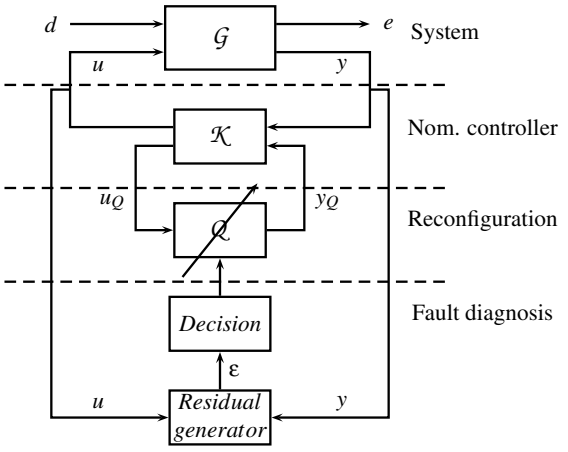

Fig. 2. Block diagram of fault-tolerant control including an FDI block and a controller-modification block.

normal-mode controller to a safe-mode one just by removing the reconfiguration loop in the controller architecture. The FTC set-up shown in Fig. 2 takes the form shown in Fig. 3.

The FTC block diagram shown in Fig. 3 can be considered from a more general point of view. The connection between the three different operation modes (that does not include the start-up mode and the close-down mode) is shown in Fig. 4.

The diagram shows that an FTC architecture should allow switching from one operation mode to one of the two other operation modes. It is required that a switch from the "Normal mode" operation to the "Safe mode" operation should be fast in the event of faults. This is very important in cases where faults result in unstable closed-loop feedback systems. The switching is done on-line, i.e., it is hot switching. This requires that the switching be done as a bump-less transfer between the different modes. This is to avoid introduction of large transients in the closed-loop system. As indicated in Fig. 4, only the switching from "Normal mode" to "Safe mode" is required to be fast in the event of faults in the system. In general, it will not be possible to guarantee that this switching is done as a bump-less transfer due to the requirement for fast switching.

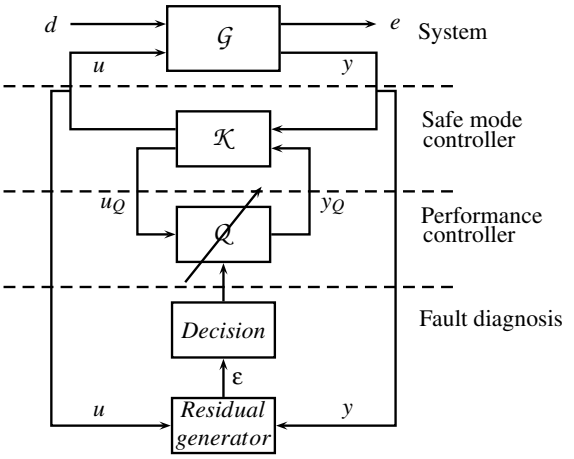

Fig. 3. Block diagram of a fault-tolerant controller with a safe-mode controller as the central controller.

Another issue is the sensors and actuators applied. In many cases, the feedback controller applied for the normal mode will in general be based on other sets of sensors and actuators than the safe-mode controller. The FTC architecture needs therefore to be able to handle changes in the sensors and actuators in connection with controller switching.

A similar concept can be used in relation to high performance controllers. Here, the nominal controller can be a robust one based on reliable sensors and actuators. As in the FTC case, the performance can be obtained by using a suitable transfer matrix for the free transfer matrix in

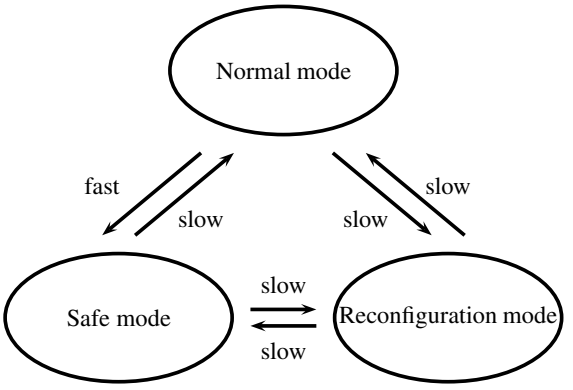

Fig. 4. FTC concept.

controller parameterization. The free transfer matrix can be included when the system is in the normal mode. The matrix can then either be decoupled or redesigned when the system is not in the nominal mode. This concept is in line with the ideas of Tay *et al*. (1997).

The main difference between the FTC concept and the high performance one described is how the free transfer matrix in controller parameterization is changed. In the FTC case, the change is a consequence of a fault diagnosis, whereas the change is typically handled by an operator in the high performance case.

An important aspect in connection with both FTC and high performance control is system uncertainties. In general, the systems are given by

$$\mathcal{G} = \mathcal{G}(\Delta),$$

where Δ describes the system uncertainties. Both fault diagnosis and controller design/redesign must be done with respect to the uncertainties in the system.

The main focus in this paper is to investigate the FTC controller architecture shown in Fig. 3 in greater detail. The concept described will be investigated with respect to fault diagnosis and controller reconfiguration. The change of sensors and actuators in connection with reconfiguration of the controller will also be investigated.

The rest of this paper is organized as follows. The system set-up is given in Section 2, followed by some preliminary results for controller parameterization in Section 3. The set-up for fault diagnosis is considered in Section 4. Active fault detection and active fault isolation are considered in Sections 5 and 6, respectively. The last part of the FTC architecture, controller reconfiguration, is considered in Section 7. Time aspects of the suggested FTC architecture are discussed in Section 8.

The paper ends with some closing remarks in Section 9.

2. System set-up

Let a general system be given by

$$\mathcal{G} : \left\{ \begin{pmatrix} z \\ e \\ y \end{pmatrix} = \begin{pmatrix} G_{zw} & G_{zd} & G_{zu} \\ G_{ew} & G_{ed} & G_{eu} \\ G_{yw} & G_{yd} & G_{yu} \end{pmatrix} \begin{pmatrix} w \\ d \\ u \end{pmatrix}, \right. \quad (1)$$

where $w \in \mathbb{R}^r$ is an external input vector, $d \in \mathbb{R}^s$ is a disturbance signal vector, $u \in \mathbb{R}^m$ is the saturated control input signal vector, $z \in \mathbb{R}^t$ is an external output vector, $e \in \mathbb{R}^q$ is the external output signal vector to be controlled, and $y \in \mathbb{R}^p$ is the measurement vector.

Let the external output z and the external input w be connected through the uncertain block Δ, i.e.,

$$w = \Delta z, \quad (2)$$

where Δ describes the uncertainty in the system. It can be a fully uncertain complex block or it can be structured, (see, e.g., Skogestad and Postlethwaite, 2005). It is further assumed that Δ is scaled such that

$$\|\Delta\| \leq 1, \quad \forall\omega.$$

The general uncertain system $\mathcal{G}(\Delta)$ is given by

$$\mathcal{G}((\Delta) = \mathcal{F}_u(\mathcal{G}, \Delta), \quad (3)$$

where $\mathcal{F}_u(\cdot,\cdot)$ is an upper Linear Fractional Transformation (LFT), (cf. Skogestad and Postlethwaite, 2005). Let the system be controlled by a stabilizing feedback controller given by

$$\mathcal{K} : \left\{ \; u = K_{uy} y. \right. \quad (4)$$

2.1. Parametric fault sets. Certain modeling aspects have to be considered in connection with FDI. The task of FDI depends on which parametric faults can occur simultaneously and which cannot. On the basis of the available information as to which parametric faults can occur simultaneously at any time and which cannot, one divides the set of all possible faults into a number of subsets. This aspect has been discussed by Saberi *et al*. (2000) in connection with additive faults. An equivalent definition of parametric fault sets is given in the following. The modeling of parametric faults can be described in the same way as modeling uncertainties. Let θ be a diagonal matrix given by $\theta = \mathrm{diag}(\theta_1, \ldots, \theta_i, \ldots, \theta_k)$, representing the parametric faults in the system. Let the connection between the external output and the external input be given by

$$w = \theta z,$$

i.e., $k = r = t$.

It is assumed that every single parametric fault θ_i is included in a parameter space, $\theta_i \in \Theta_i$, $i = 1, \cdots, k$, where Θ_i can be an interval $\Theta_i = [\theta_i^-, \theta_i^+]$. Note that the interval must include the nominal value for $\theta_i = 0$. The interval for Θ_i is a continuous one, where θ_i can take all values between θ_i^- and θ_i^+. This will not always be the case. In other cases, the parametric fault can only take a fixed number of values, i.e., $\Theta_i = \{0, \theta_{i,1}, \theta_{i,2}, \ldots\}$. Furthermore, let $\Theta_{i\backslash 0} = \Theta_i \backslash \{0\}$, i.e., the nominal value (the fault-free case) of θ_i is not included in $\Theta_{i\backslash 0}$. We will use the notation $\theta_i \neq 0$ as a short form for $\theta = \mathrm{diag}(0, \ldots, 0, \theta_i, 0, \ldots, 0)$, i.e., $\theta_i \neq 0$.

Let us denote the set of all possible parametric faults by $\mathbf{k} = \{1, \ldots, k\}$. Based on the known information, let $\mathbf{k}$ be partitioned into ℓ mutually exclusive and exhaustive sets, Ω_i, $i = 1, 2, \ldots, \ell$. That is, let $\Omega_i \cap \Omega_j = \emptyset$ for $i \neq j$, and $\Omega_1 \cup \Omega_2 \cup \cdots \Omega_\ell = \mathbf{k}$. Also, let k_i denote the number of elements in Ω_i. This leads us to defining the following simultaneous occurrence property.

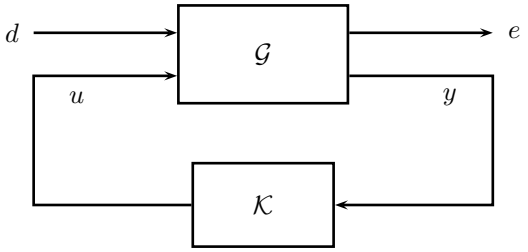

Fig. 5. Closed-loop system.

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

Two special and extreme cases of the general simultaneous occurrence property are interesting and important: the fault set of *simultaneous occurrence of property of Type* 1, where all possible faults can occur simultaneously at any time, and the fault set of *simultaneous occurrence of property of Type* 2, where every fault occurs by itself, i.e., it never occurs simultaneously with any other fault. The first case is the most general one. If it is possible to handle it, we do not need to consider other cases. The other case is the simplest one, but in general it will also be the most realistic one. Both fault sets of Type 1 and Type 2 will be considered in this paper. Other types of parametric faults sets can be derived based on the results given in this paper.

In the following, only system changes with respect to faults will be considered, i.e., $\Delta = \theta$.

3. Parameterization of controllers

Parameterization of feedback controllers is considered in the following. First, some simple calculations are derived, followed by a more detailed analysis.

Let us consider the feedback system shown in Fig. 5. The closed-loop transfer matrix T_{cl} is given by

$$T_{cl} = G_{ed} + G_{eu}K_{uy}(I - G_{yu}K_{uy})^{-1}G_{yd}. \quad (5)$$

Assume that $\mathcal{K}$ stabilizes $\mathcal{G}$, i.e., T_{cl} is stable. Let R be defined by

$$R = K_{uy}(I - G_{yu}K_{uy})^{-1}. \quad (6)$$

The relation between K_{uy} and R is given by

$$K_{uy} = (I + RG_{yu})^{-1}R.$$

Internal stability gives directly that R is stable (Boyd and Barratt, 1991). Using R in (5) gives directly

$$T_{cl} = G_{ed} + G_{eu}RG_{yd}. \quad (7)$$

Including a free stable transfer matrix Q gives the following closed-loop system:

$$T_{cl} = T_1 + T_2QT_3, \quad (8)$$

where T_1, T_2 and T_3 are specific, stable transfer matrices depending on $\mathcal{G}$ and $\mathcal{K}$.

Let us define D and $\tilde{D}$ of appropriate dimensions including the unstable poles from G_{yu} as zeros. D and $\tilde{D}$ are not unique. Any suitable choice of D and $\tilde{D}$ has the property that, if Q is stable, then each $DQ\tilde{D}$, $G_{eu}DQ\tilde{D}$, $DQ\tilde{D}G_{yd}$ and $G_{eu}DQ\tilde{D}G_{yd}$ is stable (Boyd and Barratt, 1991). Comparing with (7) gives

$$T_2 = G_{eu}D,$$
$$T_3 = \tilde{D}G_{yd}.$$

Now, T_1 can be selected as any closed-loop transfer matrix achieved by a stabilizing feedback controller. This results in the following closed-loop transfer matrix:

$$T_{cl}(Q) = G_{ed} + G_{eu}RG_{yd} + G_{eu}DQ\tilde{D}G_{yd}, \quad (9)$$

where Q is a free stable transfer matrix. It can be shown that this is a parameterization of all stabilizing feedback controllers for a given system in terms of the free stable transfer matrix Q (Boyd and Barratt, 1991).

Implementation of parameterization can be done as shown in Fig. 6. The complete feedback controller is given as an LFT of Q, i.e.,

$$K_{uy}(Q) = \mathcal{F}_l(\mathcal{K}, \mathcal{Q}).$$

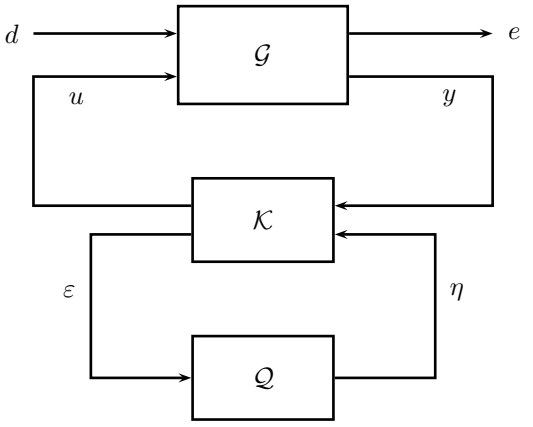

Fig. 6. Parameterization of all stabilizing controllers $K_{uy}(Q)$ for a given nominal system $\mathcal{G}$.

The construction of the architecture in Fig. 6 requires

that the transfer matrix from η to ε be zero in the nominal case. If this is not satisfied, the closed-loop transfer matrix will not be an affine matrix function of the free stable transfer matrix Q. Further, the transfer matrix from d to ε it is $\tilde{D}G_{yd}$ and from η to e is $G_{eu}D$. The $(1,1)$-element in $\mathcal{K}$ is the nominal feedback controller K_{uy}.

If $\mathcal{K}$ is selected such that the above conditions are satisfied, then the controller architecture in Fig. 6 gives a parameterization of all stabilizing linear controllers for the nominal plant $\mathcal{G}$ in terms of the free stable transfer matrix Q.

Let $\mathcal{K}$ be given by

$$\mathcal{K}: \left\{ \begin{pmatrix} u \\ \varepsilon \end{pmatrix} = \begin{pmatrix} K_{uy} & K_{u\eta} \\ \bar{K}_{\varepsilon y} & \bar{K}_{\varepsilon\eta} \end{pmatrix} \begin{pmatrix} y \\ \eta \end{pmatrix}, \right. \tag{10}$$

where K_{uy} is the nominal feedback controller.

Based on $\mathcal{K}$, the open-loop transfer matrices from d and η to ε are then given by

$$\begin{aligned} \varepsilon = {} & \bar{K}_{\varepsilon y}(I - G_{yu}(\theta)K_{uy})^{-1}G_{yd}(\theta)d \\ & + (\bar{K}_{\varepsilon\eta} + \bar{K}_{\varepsilon y}(I - G_{yu}(\theta)K_{uy})^{-1}G_{yu}(\theta)K_{u\eta})\eta, \end{aligned} \tag{11}$$

where $\mathcal{G}(\theta)$ has been applied. The condition that the transfer matrix from η to ε must be zero in the nominal case (fault free) gives the following condition for the selection of $K_{u\eta}$, $\bar{K}_{\varepsilon y}$ and $\bar{K}_{\varepsilon\eta}$:

$$0 = \bar{K}_{\varepsilon\eta} + \bar{K}_{\varepsilon y}(I - G_{yu}K_{uy})^{-1}G_{yu}K_{u\eta}. \tag{12}$$

Instead of using ε directly as given by (10), ε can be defined by

$$\varepsilon = K_{\varepsilon u}u + K_{\varepsilon y}y, \tag{13}$$

with u given by (10). This gives the following description of $\mathcal{K}$:

$$\mathcal{K}: \left\{ \begin{pmatrix} u \\ \varepsilon \end{pmatrix} = \begin{pmatrix} K_{uy} & K_{u\eta} \\ K_{\varepsilon u}K_{uy} + K_{\varepsilon y} & K_{\varepsilon u}K_{u\eta} \end{pmatrix} \begin{pmatrix} y \\ \eta \end{pmatrix}. \right. \tag{14}$$

The motivation for this small rewriting of ε is that we want to use the vector ε in connection with fault diagnosis. Introducing the measurement vector in (13) gives directly

$$\begin{aligned} \varepsilon &= K_{\varepsilon u}u + K_{\varepsilon y}G_{yd}d + K_{\varepsilon y}G_{yu}u \\ &= (K_{\varepsilon u} + K_{\varepsilon y}G_{yu})u + K_{\varepsilon y}G_{yd}d. \end{aligned}$$

A condition for using ε as a residual vector is that the input vector u is decoupled from ε (Blanke *et al.*, 2003), i.e.,

$$K_{\varepsilon u} + K_{\varepsilon y}G_{yu} = 0. \tag{15}$$

Applying the feedback controller $\mathcal{K}$ given by (14), ε takes the following form:

$$\begin{aligned} \varepsilon = {} & (K_{\varepsilon u}K_{uy} + K_{\varepsilon y})(I - G_{yu}(\theta)K_{uy})^{-1}G_{yd}(\theta)d \\ & + (K_{\varepsilon u}K_{u\eta} + (K_{\varepsilon u}K_{uy} + K_{\varepsilon y}) \\ & \times (I - G_{yu}(\theta)K_{uy})^{-1}G_{yu}(\theta)K_{u\eta})\eta. \end{aligned} \tag{16}$$

Using (15) in (16) gives

$$\begin{aligned} \varepsilon = {} & K_{\varepsilon y}(I - G_{yu}K_{uy})(I - G_{yu}(\theta)K_{uy})^{-1}G_{yd}(\theta)d \\ & + K_{\varepsilon y}((I - G_{yu}K_{uy})(I - G_{yu}(\theta)K_{uy})^{-1}G_{yu}(\theta) \\ & - G_{yu})K_{u\eta}\eta \\ = {} & P_{\varepsilon d}(\theta)d + S(\theta)\eta. \end{aligned} \tag{17}$$

S in the above equation is the dual transfer matrix of Q. Equivalent to Q, it gives a parameterization of all systems stabilized by given feedback controller. For more details, see the works of Niemann (2003) and Tay *et al.* (1997), where the dual parameterization has been considered in connection with the YJBK parameterization.

For the nominal case, (17) takes the following form:

$$\varepsilon = K_{\varepsilon y}G_{yd}d. \tag{18}$$

From the above equation, we can see that the decoupling condition in (15) also satisfies the condition in (15) in connection with controller parameterization. This means that the input vector ε to the free transfer matrix Q in controller parameterization can also be applied as a residual vector in connection with fault diagnosis. In the following, ε will be named the residual vector.

The residual vector given by (17) is applied in connection with both passive and fault diagnosis. In the passive case, the diagnosis is based on the transfer matrix from d to ε, $P_{\varepsilon d}(\theta)$, and in the active case on $S(\theta)$. This will be investigated further in the next section. Based on the above derivations, the block diagram shown in Fig. 6 now takes the form shown in Fig. 7.

The above parameterization cannot directly handle a change in the employed sets of sensors and actuators. As pointed out in Section 1, it is relevant to consider changes of the sensors and actuators applied in connection with controller reconfiguration. The controller architecture shown in Figs. 6 or 7 needs to be extended to handle the case where additional sensors and actuators can be applied. The change of the sets of sensors and actuators applied needs to be handled through the free transfer matrix Q in the controller. This is because we do not want to change the nominal (safe-mode) controller as it should always be possible to return to this controller.

Let the system $\mathcal{G}$ be extended with additional inputs

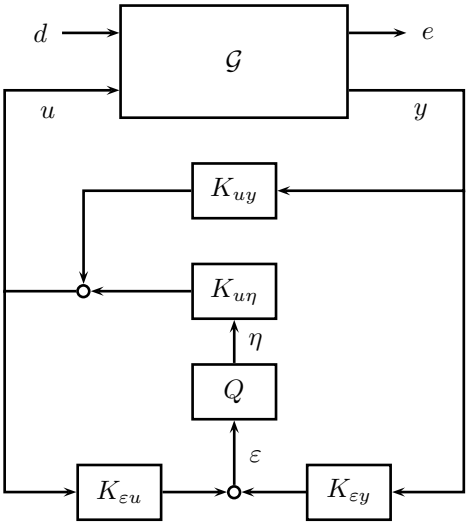

Fig. 7. Parameterization of all stabilizing controllers based on the controller $\mathcal{K}$ given by (14).

u_a and outputs y_a. The general system in (1) is given by

$$\mathcal{G}\ :\ \left\{ \begin{pmatrix} z \\ e \\ y \\ y_a \end{pmatrix} = \begin{pmatrix} G_{zw} & G_{zd} & G_{zu} & G_{zu_a} \\ G_{ew} & G_{ed} & G_{eu} & G_{eu_a} \\ G_{yw} & G_{yd} & G_{yu} & G_{yu_a} \\ G_{y_aw} & G_{y_ad} & G_{y_au} & G_{y_au_a} \end{pmatrix} \begin{pmatrix} w \\ d \\ u \\ u_a \end{pmatrix} \right. . \tag{19}$$

The nominal controller for the extended system in (19) is given by

$$\mathcal{K}\ :\ \left\{ \bar{u} = \begin{pmatrix} K_{uy} & 0 \\ 0 & 0 \end{pmatrix} \bar{y}, \right. \tag{20}$$

where

$$\bar{u} = \begin{pmatrix} u \\ u_a \end{pmatrix}, \quad \bar{y} = \begin{pmatrix} y \\ y_a \end{pmatrix}.$$

The free transfer matrix $\mathcal{Q}$ in controller parameterization needs to be extended with additional inputs and outputs for handling the extended system. $\mathcal{Q}$ is then given by

$$\mathcal{Q}\ :\ \left\{ \begin{pmatrix} \eta \\ u_a \end{pmatrix} = \begin{pmatrix} Q_{\eta\varepsilon} & Q_{\eta y_a} \\ Q_{u_a\varepsilon} & Q_{u_a y_a} \end{pmatrix} \begin{pmatrix} \varepsilon \\ y_a \end{pmatrix}, \right. \tag{21}$$

where $Q_{\eta\varepsilon}$ is the free transfer matrix in the standard controller architecture in Figs. 6 or 7.

The architecture for controller parameterization in the extended case is shown in Fig. 8. A more detailed analysis of controller parameterization for this case is given in connection with controller reconfiguration in Section 7.

3.1. Closed-loop stability. The stability of the closed-loop system is discussed briefly here. First, let us consider

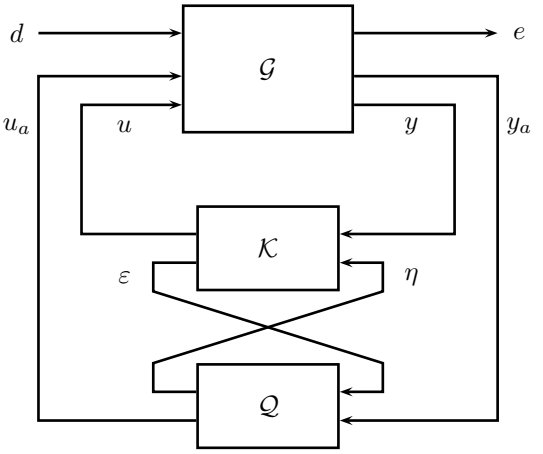

Fig. 8. Parameterization of all stabilizing controllers for a nominal system $\mathcal{G}$ with additional inputs u_a and outputs y_a.

the connection between the two transfer matrices Q and S. The interpretation of S can be investigated on the basis of a general controller parameterization. It turns out that S is the open-loop transfer matrix from η to ε, i.e., closing the loop around Q,

$$S = \mathcal{F}_u(J_K, G_{yu}(S)), \tag{22}$$

where J_K is given by

$$J_K = \begin{pmatrix} K_{uy} & K_{u\eta} \\ K_{\varepsilon u}K_{uy} + K_{\varepsilon y} & K_{\varepsilon u}K_{u\eta} \end{pmatrix},$$

see (14). As a direct consequence of (22), the stability of the closed-loop system can be analyzed using Q and S.

The closed-loop system shown in Fig. 9 is not guaranteed to be stable by requiring that Q and S be stable transfer matrices. Using the relation in (22), it can be shown that the closed-loop system shown in Fig. 9 is stable if, and only if, the nominal feedback loop given by (G_{yu}, K_{uy}) and the feedback loop given by (Q, S) are both stable. This is shown in Fig. 10. This result was also shown by Tay *et al.* (1997), who applied the YJBK parameterization.

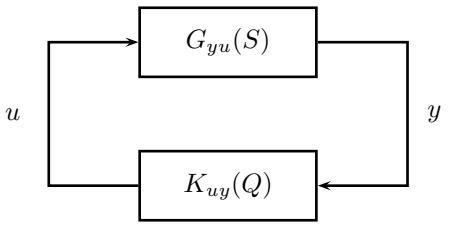

Fig. 9. Closed-loop feedback system including a parameterization of all stabilizing controllers $K_{uy}(Q)$ and S that describe a parameterization of all systems $G_{yu}(S)$.

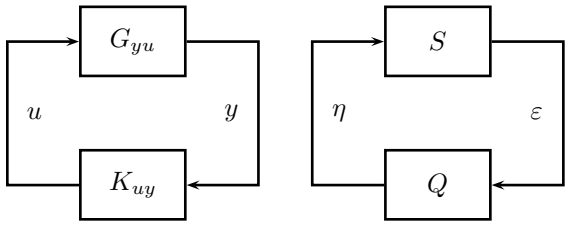

Fig. 10. Two closed-loop feedback systems occur from controller parameterization and a system change.

4. Fault diagnosis

The fault diagnosis part of the FTC architecture is considered in this section. The reliability of the final FTC controller depends strongly on that of the diagnosis part. The controller reconfiguration depends on the information from the diagnosis.

The main focus in this section is on Active Fault Diagnosis (AFD). This area has been considered in a number of papers (Campbell *et al.*, 2000; 2002; Campbell and Nikoukhah, 2004b; Keresteciogluand Zarrop, 1994; Niemann, 2006b; Nikoukhah, 1994; 1998; Nikoukhah *et al.*, 2000; Poulsen and Niemann, 2008) and books (Campbell and Nikoukhah, 2004a; Keresteciogluu, 1993; Zhang, 1989).

AFD is based on inclusion of an auxiliary (test) input signal into the system. The auxiliary input can be injected into either the open-loop system or in the closed-loop system. As output from the diagnosis system, a standard residual signal known from the passive FDI approach is applied (Frank and Ding, 1994). Using the AFD approach of Niemann (2005; 2006b), as well as Poulsen and Niemann (2008), the auxiliary input is injected into the closed-loop system in such a way that the residual is decoupled from the auxiliary input in the nominal case. In the event of parametric faults (system changes), the residual will contain a component related to the auxiliary input.

4.1. Active fault diagnosis set-up. An AFD set-up based on controller parameterization in Section 3 is shown in Fig. 11, where η is an excitation/auxiliary input vector and ε is the error/residual vector.

By suitable selection of $K_{u\eta}$, it is possible to change the placement of the auxiliary input vector η in the AFD set-up shown in Fig. 11. By selecting $K_{u\eta} = I$, the auxiliary input is injected at the output point of the controller, i.e.,

$$u = K_{uy}y + \eta.$$

Using $K_{u\eta} = K_{uy}$ gives an injection at the input point of the controller, i.e.,

$$u = K_{uy}(y + \eta).$$

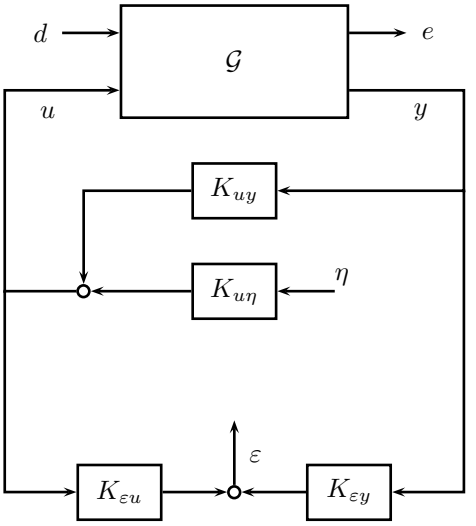

Fig. 11. Controller structure including the residual vector ε and the auxiliary input vector η.

From (17), we have directly that the connection between d, η, and ε is given by

$$\varepsilon = P_{\varepsilon d}(\theta)d + S(\theta)\eta. \tag{23}$$

This means that not only do we have a relation between η and ε as a function of the parametric faults (system variations), but we also have a relation with the closed-loop stability in the event of parametric faults. A consequence of this is that the faulty system is closed-loop stable if $S(\theta)$ is stable, as discussed in Section 3.

Consider the closed-loop system shown in Fig. 11 with the two inputs d, η and the two outputs e, ε. Let the relation between the inputs and outputs be given by

$$\mathcal{P} : \left\{ \begin{pmatrix} e \\ \varepsilon \end{pmatrix} = \begin{pmatrix} P_{ed}(\theta) & P_{e\eta}(\theta) \\ P_{\varepsilon d}(\theta) & S(\theta) \end{pmatrix} \begin{pmatrix} d \\ \eta \end{pmatrix}, \right. \tag{24}$$

where

$$\begin{aligned} P_{ed}(\theta) &= G_{ed}(\theta) \\ &\quad + G_{eu}(\theta)K_{uy}(I - G_{yu}(\theta)K_{uy})^{-1}G_{yd}(\theta), \\ P_{e\eta}(\theta) &= G_{eu}(\theta)(I - K_{uy}G_{yu}(\theta))^{-1}K_{u\eta} \end{aligned}$$

and $P_{\varepsilon d}(\theta), S(\theta)$ are given by (17).

Only the residual vector ε is important in connection with AFD. As can be seen from (23) and (24), $S(\theta)$ is very important in connection with the residual vector ε. Equivalent to the definition of *fault signature* for additive faults (Massoumnia, 1986), $S(\theta)$ will be called the *fault signature matrix* for parametric faults (Niemann, 2005; 2006b). The reason behind it 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 on $S(\theta)$ in connection with FDI is investigated in detail in the following. Furthermore, the transfer matrix from disturbance d to the residual vector ε is called the disturbance signature matrix.

Inspired by the passive FDI approach, a parameterization of the residual generators for AFD can be determined. Parameterization in the AFD case is obtained by including a stable filter W_I at the input vector η and a stable filter W_O at the output vector ε. This approach can be considered a generalization of the parameterization of all residual generators in the passive FDI case. The parameterization of all residual generators in the AFD case reflects the additional freedom obtained by using an auxiliary input vector in the set-up.

Including the pre- and the post-filter in the system set-up, the closed-loop system given by (24) takes the following form:

$$\mathcal{P}_W \; : \; \left\{ \begin{pmatrix} e \\ \varepsilon_w \end{pmatrix} = \begin{pmatrix} P_{ed}(\theta) & P_{e\eta}(\theta)W_I \\ W_O P_{\varepsilon d}(\theta) & S_W(\theta) \end{pmatrix} \begin{pmatrix} d \\ \eta_w \end{pmatrix}, \right. \tag{25}$$

where $S_W(\theta) = W_O S(\theta) W_I$.

The design of the pre- and post-filter strongly depends on the number of parametric faults, inputs and outputs and the disturbance in the system. This will be considered in more detail in the following.

Finally, let us consider the connection with the passive FDI approach considered by, e.g., Frank and Ding (1994). By moving the auxiliary input vector η from the system shown in Fig. 11, the passive FDI set-up is obtained. It was shown by Frank and Ding (1994) that all residual vectors ε_w can be described by

$$\varepsilon_w = W_O(K_{\varepsilon y} y + K_{\varepsilon u} u) = W_O \varepsilon, \tag{26}$$

where W_O is a stable and proper filter of suitable order. Rewriting (26) by including the controller in the loop gives (Niemann, 2003)

$$\varepsilon_w = W_O P_{\varepsilon d} d. \tag{27}$$

Here it is important to point out that fault detection and fault isolation are based on the external disturbance d. This can be seen from (27). A consequence of this is that parametric faults will not necessarily be detected immediately after the faults have occurred in the system. The faults need to be observable from ε, which requires that it be excited by the disturbance input d. If this is not the case, it will not be possible to detect the faults using a passive approach.

4.2. Active fault diagnosis. On the basis of the set-up for active fault diagnosis in the closed-loop system given in Section 4.1, general conditions for active fault diagnosis are considered in this section.

We want to set up conditions for both fault detection and fault isolation based on the fault signature matrix. However, it is not possible to measure the fault signature matrix directly, as we only have the input/output vectors (η, ε) available for the diagnosis. The diagnosis must be carried out by considering the signature from the auxiliary input in the residual vector. Isolation between different fault situations can then only be obtained if it is possible to separate the associated fault signatures in the residual vector. This results in requirements for the auxiliary input vector; it needs to excite the fault signature matrix enough to separate different fault situations. This is equivalent to excitation inputs in connection with system identification.

To be more specific, let $\mathcal{S}(\theta, \eta)$ be the fault signature space for a specific input η, i.e.,

$$\varepsilon_\eta = S(\theta)\eta \in \mathcal{S}(\theta, \eta),$$

where the residual vector ε is separated into a part from the auxiliary input η and a part from the disturbance d, i.e.,

$$\varepsilon = \varepsilon_\eta + \varepsilon_d,$$

Based on the fault signature space, it is possible to set up a definition for fault isolation. For a given input η, the two faults θ_i and θ_j are isolable if

$$\begin{aligned} &\mathcal{S}(\theta_i, \eta) \cap \mathcal{S}(\theta_j, \eta) = \emptyset, \\ &\forall \theta_i \in \Theta_{i\backslash 0}, \; \forall \theta_j \in \Theta_{j\backslash 0}, \; i \neq j. \end{aligned} \tag{28}$$

(28) gives a separation in the fault signature output space. An equivalent definition for fault isolation was also given by Campbell and Nikoukhah (2004a). Fault detection is also included in the above general definition as a special case.

In many cases, it will not be possible to make a direct separation on the basis of the residual output space. Therefore, let the definition of the fault signature space be generalized to

$$f(\varepsilon_\eta, \eta) = f(S(\theta)\eta, \eta) \in \mathcal{S}_f(\theta, \eta), \tag{29}$$

where $f(\varepsilon_\eta, \eta)$ is a linear or a non-linear function of the auxiliary input η and the signature from the input in the residual output ε_η. The function can be, e.g., an evaluation function of the residual vector in a specific frequency range, in a specific direction, a statistical test, etc. Some of these functions are applied in the following.

Based on the general definition of by fault signature space given by (29), the definition of fault detection and fault isolation given above is still valid.

It is important to point out that the auxiliary input η must be selected/designed with respect to obtaining a fault detection and/or a fault isolation. The design of the auxiliary input vector is a trade-off between maximizing the

effect in the residual vector ε for fast detection and minimizing the effect on the external output e. Another important aspect in this connection is the design of the two input and output filters W_I and W_O. By suitable design of these two filters, it is possible to simplify both the detection as well as the isolation problem. This is investigated in the following.

4.3. Time to detect. The time between a fault occurring in the system to when it is detected and a controller switches to the safe-mode controller is very critical. The FTC architecture suggested in Section 1 will allow a fast switch from the nominal feedback controller to a safe-mode controller. This leaves the diagnosis part of the architecture as the most critical part with respect to time delays. The aspect of time delay in connection with fault diagnosis and isolation will not be discussed in further detail here. A more detailed analysis of the time delay problem can be found in the work of Stoorvogel *et al*. (2001).

5. Active fault detection

First, let us consider the fault-detection problem in the disturbance-free case. Detection is based on the equation for the residual vector in (23) or (24) with $d = 0$. From (23) we have directly that the fault signature matrix is equal to zero in the fault-free case and non-zero in the faulty case, i.e.,

$$\begin{aligned} S(\theta) &= 0 \quad \text{for} \quad \theta = 0 \\ S(\theta) &\neq 0 \quad \text{for} \quad \theta \neq 0. \end{aligned} \tag{30}$$

Using $f(\cdot)$ as the identity function, we get directly that the fault signature space in the fault-free case is empty for all non-zero auxiliary inputs by using the simple observation from (30). This gives the following condition for fault detection:

$$\text{Fault detection:} \quad \begin{aligned} &\mathcal{S}(0,\eta) = 0, \quad \forall \eta \neq 0 \\ &\mathcal{S}(\theta,\eta) \neq 0, \quad \forall \eta \neq 0, \quad \text{for } \theta \neq 0. \end{aligned} \tag{31}$$

It is clear that using (31) gives a direct fault detection based on the fault signature space result in a direct fault detection, i.e., detection based on an empty or a non-empty fault signature space. The above condition in (31) is independent of both the auxiliary input and the design of the two filters W_I, W_O, assuming that the two filters are non-zero and stable. Detection based on (31) gives a complete decoupling of the signature from η in the residual vector.

In the case where disturbance is included, the simple conditions cannot be applied directly. The fault signature space will not be an empty space in the fault-free case due to the disturbance. It will therefore be necessary to use a statistical test on the residual vector. This is considered below.

In the special case, where the number of residual signals is larger than the number of disturbance signals, i.e., $p > s$, it is possible to design W_O such that we get $p - s$ disturbance-free residual signals in the nominal case. This means that we can get exact disturbance decoupling in the residual signals for $\theta = 0$. Following (Saberi *et al*., 2000), we have that it is possible to design W_O such that

$$\begin{pmatrix} \varepsilon_{w,1} \\ \varepsilon_{w,2} \end{pmatrix} = W_O P_{\varepsilon d}(0) d = \begin{pmatrix} P_{\varepsilon_w d} \\ 0 \end{pmatrix} d. \tag{32}$$

With this design of W_O, we can use the last $p - s$ residual signals $\varepsilon_{w,2}$ for active fault detection. Note that the parametric faults will change the system and there will be no guarantee for disturbance decoupling in the faulty case. However, this will not change the detectability of the faults. A non-zero $\varepsilon_{q,2}$ will always indicate parametric faults. Generically, it will be possible to detect all parametric faults from $\varepsilon_{w,2}$, but there is no guarantee. To see this, consider the residual vector in the faulty case given by

$$\begin{aligned} \begin{pmatrix} \varepsilon_{w,1} \\ \varepsilon_{w,2} \end{pmatrix} &= W_O S(\theta)\eta + W_O P_{\varepsilon d}(\theta) d \\ &= \begin{pmatrix} S_{W,1}(\theta) \\ S_{W,2}(\theta) \end{pmatrix} \eta + \begin{pmatrix} P_{W,\varepsilon d,1}(\theta) \\ P_{W,\varepsilon d,2}(\theta) \end{pmatrix} d, \end{aligned} \tag{33}$$

where $P_{W,\varepsilon d,2}(0) = 0$. If $S_{W,2}(\theta)$ depends on all parametric faults, it will be possible to detect all parametric faults by using $\varepsilon_{w,2}$. The auxiliary input vector η just needs to be selected such that it is possible to see a signature of η in the residual vector $\varepsilon_{w,2}$ in the faulty case, i.e., the fault signature space needs to be non-empty for all faults.

5.1. Stochastic active fault detection. In the case where disturbance is included, the simple conditions cannot be applied directly. The fault signature space will not be an empty space in the fault-free case due to the disturbance. It will therefore be necessary to use a statistical test on the residual vector. The detection (isolation) of faults can then be based on the following hypothesis:

$$\begin{aligned} H_0 &: \quad S(\theta) = 0, \\ H_1 &: \quad S(\theta) \neq 0. \end{aligned} \tag{34}$$

Standard statistical test methods such as CUSUM or GLR tests can be applied directly, but they will not be optimal. That would be equivalent to using the passive fault detection approach.

The statistical test methods must be dedicated to detect if ε includes a signature from a specific, employed auxiliary input or not. For simplifying this task, it is rele-

vant to use simple auxiliary inputs. A periodic input will in general be useful. The output in the residual vector will also be periodic in the case of parametric faults in the system. For optimizing the detection of a periodic signature in the residual vector, let us only consider the residual vector at the specific frequency given by

$$\eta = \begin{pmatrix} a_{1,\omega} \\ \vdots \\ a_{i,\omega} \\ \vdots \\ a_{m,\omega} \end{pmatrix} \sin(\omega_0 t) = A_\omega \sin(\omega_0 t), \qquad (35)$$

where A_ω is the input vector with the input amplitudes and the frequency ω_0 represents the tuning parameters in the auxiliary input. The choice of tuning parameters should also be related to the frequency distribution of noise such that the signature of the residual is not covered by noise. However, it is also possible to use other types of auxiliary inputs than periodic signals. For example, this was done in the approach used by Campbell and Nikoukhah (2004a) as well as Zhang (1989).

Using the auxiliary input given by (35), the i-th residual signal is given by

$$\varepsilon_i = \xi_i, \qquad \xi_i \in N(0, \sigma_i^2) \qquad (36)$$

in the nominal case. If the parameter is changed (from nominal values),

$$\varepsilon_i = |g_i(S(\theta), A_\omega)| \sin(\omega_0 t + \phi_i) + \xi_i, \qquad \xi_i \in N(m_i, \bar{\sigma}_i^2), \qquad (37)$$

where $g_i(S(\theta), A_\omega) = \sum_{j=1}^{p} S_{ij}(\theta) a_{j,\omega}$ and ϕ_i are respectively the (non-zero) gain and phase shift through the fault signature matrix S at the chosen frequency ω_0 from η to the ε_i. For brevity, we have omitted the dependence on θ and ω_0 in $S = S(\theta, \omega_0)$, $\phi_i = \phi_i(\theta, \omega_0)$, $m_i = m_i(\theta)$ and $\bar{\sigma}_i = \bar{\sigma}_i(\theta)$. In general, m_i will be zero. Both the amplitude and the phase of the periodic signal in ε_i depend on θ and on the chosen frequency, ω_0. The periodic signal in ε_i is the signature of the periodic auxiliary input η.

Detection of parameter changes is then based on detection of the signature from η in ε. Furthermore, isolation of parameter changes may be possible from an investigation of the amplitude and phase of the signature in ε_i. In some cases it may be necessary to include more than one single periodic signal in η in order to isolate different parameter changes. Here we will only consider a single periodic auxiliary input vector.

Assume that the auxiliary input vector has been selected, i.e., the amplitude vector A_ω and the frequency ω_0 in (35) have been specified. The focus here will be on how the hypothesis and the alternative in (34) can be implemented. As mentioned in the previous section, the approach taken here is to test whether the signature of the auxiliary input is present in the residual. In order to do so, the following two signals are formed:

$$s_i = \varepsilon_i \ \sin(\omega_0 t), \qquad c_i = \varepsilon_i \ \cos(\omega_0 t), \qquad (38)$$

where, according to (37) and some trigonometric relations,

$$\begin{aligned} s_i &= |g_i(S(\theta), A_\omega)| \frac{1}{2} \Big(\cos(\phi_i) - \cos(2\omega_0 t + \phi_i) \Big) \\ &\quad + \xi_i \ \sin(\omega_0 t), \\ c_i &= |g_i(S(\theta), A_\omega)| \frac{1}{2} \Big(\sin(\phi_i) + \sin(2\omega_0 t + \phi_i) \Big) \\ &\quad + \xi_i \ \cos(\omega_0 t). \end{aligned} \qquad (39)$$

From this it is clear that in the normal (or the fault-free) situation

$$\begin{aligned} s_i &= \xi_i \ \sin(\omega_0 t) \in N(0, \sigma_i^2 \sin^2(\omega_0 t)), \\ c_i &= \xi_i \ \cos(\omega_0 t) \in N(0, \sigma_i^2 \cos^2(\omega_0 t)). \end{aligned}$$

Additionally, the two signals are white when a filter parameterization is applied. The time average variance is equal to $\frac{1}{2}\sigma_i^2$.

If a change has occurred, then the fault signature matrix, S, will be different from zero and the two detection signals, s_i, c_i, will have a constant, deterministic component

$$|g_i(S(\theta), A_\omega)| \frac{1}{2} \begin{pmatrix} \cos(\phi_i) \\ \sin(\phi_i) \end{pmatrix}. \qquad (40)$$

This component can be used for detection and isolation.

Besides the mentioned component, the detector signals will also have a time varying deterministic component

$$|g_i(S(\theta), A_\omega)| \frac{1}{2} \begin{pmatrix} -\cos(2\omega_0 t + \phi_i) \\ \sin(2\omega_0 t + \phi_i) \end{pmatrix}, \qquad (41)$$

which on the (time) average is zero. The effect of this component can be eliminated by means of an averaging or integration technique such as in the CUSUM methodology.

In the literature, the CUSUM technique is normally connected with detection of changes in the mean and/or variance in a signal. In the normal situation it is assumed that the signal is white and has a specific mean or variance (see Basseville and Nikiforov, 1993; Gustafsson, 2000). Detection is implementation of a sequential test in which the inspection data are increased successively. CUSUM methods are normally based on simple (specified) hypotheses and simple (specified) alternatives which have to be given as tuning parameters. The simple

alternative then forms a situation that should be detected. In a heuristic setting, CUSUM methods can be regarded as being a test of whether the slope of the integral of the signal in question is larger than a certain critical value. In this work we have transformed the problem and we test whether the mean of the vector $(s_i \quad c_i)^T$ has a zero mean (vector) or has the component given in (40). Introduce the tuning parameters B and γ. The detection can be implemented as a CUSUM detection given by

$$\frac{\mathrm{d}}{\mathrm{d}t}z = \begin{cases} 0 & \text{for } z = 0 \text{ and } \dfrac{\delta_i}{\bar{\sigma}} - \dfrac{\gamma}{2} < 0, \\ \dfrac{\delta_i}{\bar{\sigma}} - \dfrac{\gamma}{2} & \text{otherwise,} \end{cases} \tag{42}$$

where

$$\delta_i = \begin{pmatrix} s_i \\ c_i \\ -s_i \\ -c_i \end{pmatrix}, \quad \bar{\sigma}_i^2 = \frac{1}{2}\sigma_i^2.$$

The hypothesis H_0 is accepted if z is smaller than the threshold h, i.e.,

$$z \;\leq\; \frac{\log(B)}{\gamma} \;=\; h,$$

where the inequality is to be understood component-wise. The parameter B in this CUSUM detector is related to the average length between false detections. The other parameter, γ, is chosen as a typical lower limit for changes to be detected. Furthermore note that the time average variance of c_i and s_i has been used in (42).

Normally, the CUSUM detector will not be implemented in the continuous-time version given by (42). Instead, a discrete-time version will be applied. The discrete-time version of the CUSUM detector is given by

$$z_{t+1} = \max\left(0, z_t + \left(\frac{\delta_t}{\sigma_1} - \frac{1}{2}\,\gamma\right)\right). \tag{43}$$

For more details, see the work of Poulsen and Niemann (2008).

6. Active fault isolation

The fault isolation case is more complicated than the detection case. The main reason for this is that the elements in $S(\theta)$ in general depend on more than a single parametric fault. This was an advantage in the fault detection case which makes it easy to detect faults. A consequence of this is that it is generally impossible to isolate single parametric faults directly by evaluating single elements in $S(\theta)$. Isolation also depends on which parametric faults 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 matrices $S(\theta)$ or $S_W(\theta)$ with respect to the associated fault set type, so that it is possible to give simple fault signature output spaces that can be separated.

In contrast to the detection case, where the detection condition can be derived on the basis of the general set-up in Fig. 11, this is not possible for fault isolation. Here, a more detailed set-up is needed to be able to come up with conditions for fault isolation. This can be obtained by using an FTC architecture based on the YJBK parameterization described in Appendix. Using the YJBK parameterization, the transfer matrices given in (14) for the general parameterization are given by

$$\begin{aligned} K_{uy} &= \tilde{V}^{-1}\tilde{U}, \\ K_{u\eta} &= \tilde{V}^{-1}, \\ K_{\varepsilon u} &= -\tilde{N}, \\ K_{\varepsilon y} &= \tilde{M}, \end{aligned} \tag{44}$$

which gives the YJBK parameterization in (77).

Further, let the system $\mathcal{G}(\theta)$ be described by (1) with $w = \theta z$. The transfer matrices from d and η to ε are given by (Niemann, 2003; 2006b)

$$\begin{aligned} P_{\varepsilon d}(\theta) &= \tilde{M}(I - G_{yw}\theta(I - G_{zw}\theta)^{-1}G_{zu}U\tilde{M})^{-1} \\ &\quad \times (G_{yd} + G_{yw}\theta(I - G_{zw}\theta)^{-1}G_{zd}), \\ S(\theta) &= \tilde{M}G_{yw}\theta(I - (G_{zw} + G_{zu}U\tilde{M}G_{yw})\theta)^{-1} \\ &\quad \times G_{zu}M \\ &= \tilde{M}G_{yw}\theta(I - T_{zw,cl}\theta)^{-1}G_{zu}M, \end{aligned} \tag{45}$$

where $T_{zw,cl}$ is the closed-loop transfer matrix from w to z. The dimension of $S(\theta)$ is $p \times m$, i.e., the same dimension as G_{yu}.

Based on these two transfer matrices, conditions for fault isolation using the active approach are derived in the following.

6.1. Direct fault isolation. Let us start with direct fault isolation in the disturbance-free case. Including disturbance can be handled in the same way as in the fault detection case considered in the previous section. By direct fault isolation, we mean that a fault can be isolated directly by a validation of a certain transfer function in $S(\theta)$, if it is zero or not, equivalent to the detection case considered above.

First, let the set of all possible faults be divided into a number of fault sets as described in Section 2, depending on which faults can occur simultaneously and which cannot.

Let us consider $S_W(\theta)$. Using the fact that both $\tilde{M}G_{yw}$ and $G_{zu}M$ are two stable transfer matrices, it is

possible to design W_I and W_O such that

$$G_{zu}MW_I = \begin{pmatrix}\Lambda_I \\ \Xi_I\end{pmatrix}, \quad W_O\tilde{M}G_{yw} = \begin{pmatrix}\Lambda_O & \Xi_O\end{pmatrix}, \tag{46}$$

where Λ_I and Λ_O are two stable diagonal matrices of dimension $m \times m$ and $p \times p$, respectively, and Ξ_I, Ξ_O are two stable transfer matrices of suitable dimensions. Using W_I and W_O satisfying (46) in $S_W(\theta)$ gives directly

$$S_W(\theta) = \begin{pmatrix}\Lambda_O & \Xi_O\end{pmatrix}\theta(I - T_{zw,cl}\theta)^{-1}\begin{pmatrix}\Lambda_I \\ \Xi_I\end{pmatrix}. \tag{47}$$

Note that, if $G_{zu}M$ is right invertible, we can obtain a complete diagonalization of $G_{zu}M$ by the design of W_I. Similarly, if $\tilde{M}G_{yw}$ is left invertible, a complete diagonalization of $\tilde{M}G_{yw}$ can be obtained by the design of W_O.

Let us assume that the dimension of the residual vector is greater than or equal to the dimension of the auxiliary input vector, i.e., $p \geq m$. Furthermore, assume that $k_i \leq p-1$, $i = 1, \ldots, l$, i.e., the number of faults in the l-th fault sets Ω_i is less than the number of residual signals. Let θ, $T_{zw,cl}$ and $G_{zu}M$ be rearranged and partitioned into

$$\theta = \operatorname{diag}(\theta_{\Omega_i}, \theta_{\Omega_{\setminus i}}),$$
$$T_{zw,cl} = \begin{pmatrix} T_{zw,cl,11} & T_{zw,cl,12} \\ T_{zw,cl,21} & T_{zw,cl,22}\end{pmatrix},$$
$$G_{zu}M = \begin{pmatrix}G_{M,1} \\ G_{M,2}\end{pmatrix},$$

where θ_{Ω_i} includes the k_i faults in fault set Ω_i and $\theta_{\Omega_{\setminus i}}$ includes the other $k - k_i$ parametric faults. Now, let $\begin{pmatrix}\Lambda_O & \Xi_O\end{pmatrix}$ be partitioned into

$$\begin{pmatrix}\Lambda_O & \Xi_O\end{pmatrix} = \begin{pmatrix}\tilde{\Lambda}_O & \tilde{\Xi}_O\end{pmatrix},$$

where $\dim(\tilde{\Lambda}_O) = p \times k_i$. Using the fact that Λ_O is a diagonal matrix, $\begin{pmatrix}\Lambda_O & \Xi_O\end{pmatrix}$ can then be partitioned into

$$\begin{pmatrix}\Lambda_O & \Xi_O\end{pmatrix} = \begin{pmatrix} \tilde{\Lambda}_{O,1} & \tilde{\Xi}_{O,1} \\ 0 & \tilde{\Xi}_{O,2}\end{pmatrix}, \tag{48}$$

where $\dim(\tilde{\Lambda}_{O,1}) = k_i \times k_i$. Using W_O given by (46), the fault signature matrix with respect to θ_{Ω_i} is given by

$$\begin{aligned} S_{W,i}(\theta) = {} & \begin{pmatrix}\Lambda_O & \Xi_O\end{pmatrix}\begin{pmatrix}\theta_{\Omega_i} & 0 \\ 0 & \theta_{\Omega_{\setminus i}}\end{pmatrix} \\ & \times \left(I - \begin{pmatrix} T_{zw,cl,11} & T_{zw,cl,12} \\ T_{zw,cl,21} & T_{zw,cl,22}\end{pmatrix}\right. \\ & \left. \times \begin{pmatrix}\theta_{\Omega_i} & 0 \\ 0 & \theta_{\Omega_{\setminus i}}\end{pmatrix}\right)^{-1}\begin{pmatrix}G_{M,1} \\ G_{M,2}\end{pmatrix}W_I, \end{aligned} \tag{49}$$

where the index i in $S_{W,i}(\theta)$ is related to the separation of Ω into Ω_i and $\Omega_{\setminus i}$. In the event of faults, either $\theta_{\Omega_i} \neq 0$ or $\theta_{\Omega_{\setminus i}} \neq 0$, but not at the same time. $S_{W,i}(\theta)$ in (49) will be given by

$$\begin{aligned} S_{W,i}(\theta) &= \begin{pmatrix}S_{W,i,1}(\theta) \\ S_{W,i,2}(\theta)\end{pmatrix} \\ &= \begin{pmatrix}\tilde{\Lambda}_{O,1} \\ 0\end{pmatrix}\theta_{\Omega_i}(I - T_{zw,cl,11}\theta_{\Omega_i})^{-1}G_{M,1}W_I \end{aligned} \tag{50}$$

for $\theta_{\Omega_i} \neq 0$, or

$$\begin{aligned} S_{W,i}(\theta) &= \begin{pmatrix}S_{W,i,1}(\theta) \\ S_{W,i,2}(\theta)\end{pmatrix} \\ &= \begin{pmatrix}\tilde{\Xi}_{O,1} \\ \tilde{\Xi}_{O,2}\end{pmatrix}\theta_{\Omega_{\setminus i}}(I - T_{zw,cl,22}\theta_{\Omega_{\setminus i}})^{-1}G_{M,2}W_I \end{aligned} \tag{51}$$

for $\theta_{\Omega_{\setminus i}} \neq 0$. Equivalently, $l-1$ other output filters are designed with respect to the other $l-1$ fault sets. The l fault signature matrices $S_{W,i}(\theta)$ given by (50) and (51) can now be used for both fault-set isolation as well as fault isolation in a specific fault set. The fault-set isolation can be derived directly by using $S_{W,i,2}(\theta)$. From (50), it is clear that

$$S_{W,i,2}(\theta) = 0 \quad \text{for } \theta \in \Omega_i,\ i = 1, \ldots, l$$

If the fault is not included in the given fault set, $S_{W,i,2}(\theta)$ will be non-zero, i.e.,

$$S_{W,i,2}(\theta) \neq 0 \quad \text{for } \theta \notin \Omega_i,\ i = 1, \ldots, l.$$

The above condition on $S_{W,i,2}(\theta)$ will in general be satisfied, because all elements in $\tilde{\Xi}_{O,2}$ will in general be non-zero. However, if $\tilde{\Xi}_{O,2}$ includes a single column with only zeros, it is still possible to get an isolation of the single fault sets. It will only require that the fault set isolation be combined with the isolation of the single faults in the specific fault set. This aspect is considered later in this section. Let $h(\cdot)$ be the identity function in the following, the associated fault signature space for $S_{W,i,2}(\theta)$ is given by $\mathcal{S}_{W,i,2}(\theta, \eta)$. Therefore, the condition for fault-set isolation is

$$\text{Fault-set isolation:} \quad \begin{aligned} \mathcal{S}_{W,i,2}(\theta,\eta) &= 0, \quad \forall \eta \neq 0 \\ &\text{for} \quad \theta \in \Omega_i \\ \mathcal{S}_{W,i,2}(\theta,\eta) &\neq 0, \quad \forall \eta \neq 0 \\ &\text{for} \quad \theta \notin \Omega_i. \end{aligned} \tag{52}$$

The last step is isolation of the single faults in the isolated fault set Ω_i. For simplicity, consider the case where faults occur in Ω_1. Assume that θ_i in Ω_1 is non-zero. This will give a non-zero element in $\Lambda_{O,1}\theta_{\Omega_1}$ at the diagonal

element (i,i), i.e.,

$$\Lambda_{O,1}\theta_{\Omega_1} = \text{diag}(0,\ \ldots, \xi_i\theta_i, 0,\ \ldots, 0).$$

Further, the columns of $T_{zw,cl,11}\theta_{\Omega_1}$ are given by

$$T_{zw,cl,11}\theta_{\Omega_i} = (0,\ \ldots, t_i\theta_i,\ 0, \ldots, 0),$$

where t_i is the i-th column of $T_{zw,cl,11}$. This gives

$$(I - T_{zw,cl,11}\theta_{\Omega_1})^{-1}_{(:,i)} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1_i \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad \text{for } \theta_i = 0,$$

$$(I - T_{zw,cl,11}\theta_{\Omega_1})^{-1}_{(:,i)} = \begin{pmatrix} x_{1,i} \\ \vdots \\ x_{i-1,i} \\ x_{i,i} \\ x_{i+1,i} \\ \vdots \\ x_{k,i} \end{pmatrix} \quad \text{for } \theta_i \neq 0,$$

where $x_{\varsigma,i}$ are non-zero transfer functions. Combine this with the diagonal structure in $\Lambda_{O,1}\theta_{\Omega_1}$; the i-th row in $S_{W,1,1}(\theta)$ is only non-zero if θ_i is non-zero. When two faults θ_i and θ_j have occurred in the system, the i-th and the j-th row in $S_{W,1,1}(\theta)$ will be non-zero, etc. This gives a complete fault isolation in the fault set based on the fault signature matrix given by (50).

Let the i-th row of $S_{W,1,1}(\theta)$ be given by $S^i_{W,1,1}(\theta)$. The fault isolation conditions are as follows:

$$\begin{aligned} S^i_{W,1,1}(\theta) &\neq 0 \quad \text{for} \quad \theta_i \neq 0, \\ S^j_{W,1,1}(\theta) &= 0 \quad \text{for} \quad \theta_i \neq 0,\ \theta_j = 0,\ i \neq j \end{aligned}$$

Following the line from fault-set isolation, let $\mathcal{S}^i_{W,1,1}(\theta,\eta)$ be the associated fault signature space for $S^i_{W,1,1}(\theta,\eta)$. Based on this, the condition for fault isolation in the fault set Ω_1 is

$$\text{Fault isolation in } \Omega_1\text{:} \quad \begin{aligned} &\mathcal{S}^i_{W,1,1}(\theta,\eta) \neq 0,\ \forall \eta \neq 0 \\ &\qquad \text{for } \theta_i \neq 0, \\ &\mathcal{S}^j_{W,1,1}(\theta,\eta) = 0,\ \forall \eta \neq 0 \\ &\text{for } \theta_i \neq 0,\ \theta_j = 0,\ i \neq j. \end{aligned} \tag{53}$$

The complete fault isolation consists of three steps: a fault detection given by (31), a fault-set isolation given by (52) and, finally, a fault isolation in a specific fault set given by (53). This is shown in Fig. 12.

The only problem remaining is when $H_{O,2}$ includes

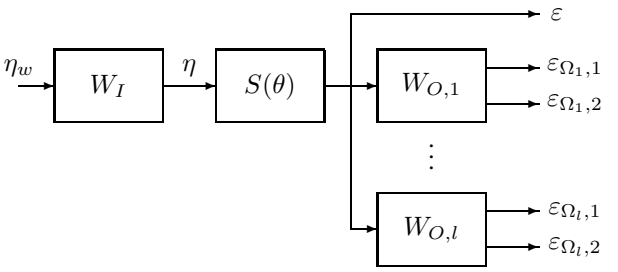

Fig. 12. Fault detection and isolation on the basis of fault occurrence in fault sets. Here ε is the residual vector for fault detection, $\varepsilon_{\Omega_1,1}$ is the residual vector for fault isolation in the fault set Ω_1, $\varepsilon_{\Omega_1,2}$ is the residual signal applied for isolation of the fault sets, $\varepsilon_{\Omega_l,1}$ is the residual vector for fault isolation in the fault set Ω_l, and $\varepsilon_{\Omega_l,2}$ is the residual signal applied for isolation of the fault sets.

a column with only zero elements. A consequence is that there is a single fault that will not affect the residual output from $S_{W,\Omega_i,2}\eta$. Assume that this fault belongs to Ω_j. If the fault occurs by itself, there will be no signature from η in both $r_{\Omega_i,2}$ and $\varepsilon_{\Omega_j,2}$, i.e., the two fault sets Ω_i and Ω_j have been isolated. It might be possible to reject one of the fault sets directly by using the knowledge about the residual generators. If this is not possible, the isolation can then be derived by using the two sets of residual signals $\varepsilon_{\Omega_i,1}$ and $\varepsilon_{\Omega_j,1}$, if $k_i > 1$. The single fault will result in a number of residual signals in $\varepsilon_{\Omega_i,1}$ with a signature from η, whereas only a single residual signal from $\varepsilon_{\Omega_j,1}$ will include a signature from η. Furthermore, the specific signal will be known in advance.

Consider the special case where the faults only occur by themselves, i.e., fault sets of simultaneous occurrence of property of Type 2. In this case, an isolation of a fault set is also an isolation of the fault, because the single fault sets will only include a single fault. The complete fault isolation consists then only of two steps: a fault detection given by (31) and a fault isolation given by

$$\text{Fault isolation:} \quad \begin{aligned} &\mathcal{S}_{W,\Omega_i,2}(\theta,\eta) = 0,\ \forall \eta \neq 0, \\ &\qquad \text{for } \theta_i \neq 0, \\ &\mathcal{S}_{W,\Omega_j,2}(\theta,\eta) \neq 0,\ \forall \eta \neq 0 \\ &\text{for } \theta_i \neq 0,\ i \neq j. \end{aligned} \tag{54}$$

Consider again the fault signature matrix given in (45); it might be concluded that making the fault isolation by using input filters W_I instead of the output filters W_O is dual. This is correct if we only consider $S_W(\theta)$ in isolation. If the isolation problem instead is considered from an input/output point of view, the two cases will not be dual. The reason is very simple. When the fault isolation is derived by using W_I, the isolation is derived by an investigation of the transfer matrix from the single aux-

iliary inputs to the residual output. This means that an auxiliary signal must be applied sequentially on the single inputs. Alternatively, different auxiliary inputs can be applied on the different inputs. The disadvantage with the first method is that the isolation time will increase. In the other approach, a number of different detection tests need to be applied to detect the different signatures from the inputs.

Let η_i, $i = 1, \ldots, m$ be the m auxiliary inputs. They can be identical or different. Using the same notation as above, the fault signature matrices in (50) and (51) are given by

$$\begin{aligned} S_{W,\Omega_1}(\theta) &= \begin{pmatrix} S_{W,\Omega_1,1}(\theta) & S_{W,\Omega_1,2}(\theta) \end{pmatrix} \\ &= W_O G_{\tilde{M},1}(I - \theta_{\Omega_1} T_{zw,cl,11})^{-1} \theta_{\Omega_1} \\ &\quad \times \begin{pmatrix} \Xi_{I,1} & 0 \end{pmatrix} \end{aligned} \tag{55}$$

for $\theta_{\Omega_1} \neq 0$, or

$$\begin{aligned} S_{W,\Omega_1}(\theta) &= \begin{pmatrix} S_{W,\Omega_1,1}(\theta) & S_{W,\Omega_1,2}(\theta) \end{pmatrix} \\ &= W_O G_{\tilde{M},2}(I - \theta_{\Omega_{2-l}} T_{zw,cl,22})^{-1} \\ &\quad \times \theta_{\Omega_{2-l}} \begin{pmatrix} H_{I,1} & H_{I,2} \end{pmatrix} \end{aligned} \tag{56}$$

for $\theta_{\Omega_{2-l}} \neq 0$. Furthermore, let the fault signature output space for $S_{W,\Omega_i}(\theta)\eta_j$, $j = 1, \ldots, m$ be given by $\mathcal{S}_{W,\Omega_i}(\theta, \eta_j)$. Based on this, the condition for fault-set isolation is

$$\text{Fault-set isolation:} \quad \begin{aligned} &\mathcal{S}_{W,\Omega_i}(\theta, \eta_j) = 0, \ \forall \eta_j \neq 0 \\ &j \in [k_i + 1, \ m], \ \text{for } \theta \in \Omega_i, \\ &\mathcal{S}_{W,\Omega_i}(\theta, \eta_j) \neq 0, \ \forall \eta_j \neq 0 \\ &j \in [k_i + 1, \ m], \ \text{for } \theta \notin \Omega_i. \end{aligned} \tag{57}$$

The fault isolation is a fault set given by

$$\text{Fault isolation in } \Omega_1: \quad \begin{aligned} &\mathcal{S}_{W,\Omega_1,i}(\theta, \eta_i) \neq 0, \ \forall \eta_i \neq 0 \\ &\qquad \text{for } \theta_i \neq 0, \\ &\mathcal{S}_{W,\Omega_1,j}(\theta, \eta_j) = 0, \ \forall \eta_j \neq 0 \\ &\quad \text{for } \theta_i \neq 0, \ \theta_j = 0, \ i \neq j, \end{aligned} \tag{58}$$

where $\mathcal{S}_{W,\Omega_1,i}(\theta, \eta_i)$ is the fault signature space for the auxiliary input η_i.

6.2. Indirect fault isolation. It is important to point out that the above fault-isolation approach, based on fault sets, does not give an upper bound on the number of faults that can be isolated. The limitation is on the number of faults in the fault sets. It is required that the maximal number of faults k_i in the fault sets satisfies

$$k_i \leq \max\{p, m\} - 1, \quad i = 1, \ldots, l. \tag{59}$$

If (59) is not satisfied, it is not possible to base the isolation on a decoupling of the signature from the auxiliary input in specific residual signals. Instead, the fault isolation must be derived indirectly. This can be done by an investigation of the signature from η in the residual output space. This is not a possibility in the passive fault isolation case, where the input to the system is not well-defined and therefore there is not a well-defined signature in the residual output.

To get fast fault isolation, it is possible to use optimally designed auxiliary inputs, as considered by Campbell and Nikoukhah (2004a). However, a good alternative to this is again to use simple periodic inputs which give simple signatures in ε that are easy to detect (Niemann and Poulsen, 2006). Let us only consider fault sets of simultaneous occurrence of property of Type 2 in the following.

Assume that a simple periodic auxiliary input vector $\eta(\omega_0)$ is applied. The residual vector $\varepsilon(\omega_0)$ will also be periodic with the same frequency. The amplitude and the phase of single signals in $\varepsilon(\omega_0)$ will depend on θ through $S(\theta)$. The single residual signals can then be investigated in the complex plane.

Let the residual vector $\varepsilon(\omega_0)$ be given by

$$\varepsilon_{sc}(\omega_0) = \begin{pmatrix} s_1 \\ c_1 \\ \vdots \\ s_i \\ c_i \\ \vdots \\ s_p \\ c_p \end{pmatrix},$$

where s_i and c_i are given by (38). The single signals in ε_{sc} will both include a constant part and a time-varying part. The constant part is given by (40). The directions given by (40) can now be applied for fault isolation. The nominal directions for the single faults given by $\varepsilon_{sc,\mathrm{nom}}(\theta_i, \omega_0)$ can be calculated. Based on this, the following condition for isolation is given:

$$\begin{aligned} &\varepsilon_{\mathrm{nom},sc}(\theta_i, \omega_0) \times \bar{\varepsilon}_{sc}(\omega_0) = 0 \quad \text{for} \quad \theta_i \neq 0, \\ &\varepsilon_{\mathrm{nom},sc}(\theta_i, \omega_0) \times \bar{\varepsilon}_{sc}(\omega_0) \neq 0 \quad \text{for} \quad \theta \neq 0, \ \theta_i = 0, \end{aligned} \tag{60}$$

where $\bar{\varepsilon}_{sc}(\omega_0)$ is the mean value of $\varepsilon_{sc}(\omega_0)$. In theory, an unlimited number of faults can be isolated. In practice, it will not be possible to isolate an unlimited number of faults. The reason is that $\varepsilon_{sc}(\omega_0)$ is a non-linear function of θ. The direction of $\varepsilon_{sc}(\omega_0)$ is not constant for different values of θ_i. Instead, the isolation needs to be based on sectors in the complex plane. Then (60) cannot be used directly. Instead, isolation can be done by

$$\hat{i} = \arg\min_i \ \varepsilon_{nom,sc}(\theta_i, \omega_0) \times \bar{\varepsilon}_{sc}(\omega_0).$$

In the general case, where there are p residual signals, this means that $\varepsilon_{sc}(\omega_0)$ is in a $2p$ dimension space. In theory, it should be possible to isolate $2p-1$ simultaneous faults, but in practice it will be less. To increase the signature space further, the auxiliary input can be extended with other periodic input signals. Using, e.g., an auxiliary input η with two periodic signals will give two residual outputs $\varepsilon(\omega_0)$ and $\varepsilon(\omega_1)$ that can be applied for isolation, i.e., the dimension of the signature space is increased by a factor of 2.

7. Controller reconfiguration

The controller reconfiguration part of the FTC architecture is considered in this section. The reconfiguration is based on the diagnosis part, the controller is modified when faults have been detected or isolated in the system. The reconfiguration is derived by using the YJBK transfer matrix Q.

Following the discussion in Section 1, the nominal feedback controller K_{uy} is assumed to be a safe-mode one. The nominal feedback is then obtained by a controller switching using the YJBK parameterization. This is described in the following.

7.1. Controller switching. One application of the YJBK parameterization is controller switching, in which the YJBK transfer matrix Q is used. It is possible to change the nominal controller K_{uy} to another stabilizing controller $K_{uy,i}$ by suitable selection of Q. Assume the existence of a co-prime factorization of the system and the new controller

$$G_{yu} = N_i M_i^{-1} = \tilde{M}_i^{-1}\tilde{N}_i, \quad K_{uy,i} = U_i V_i^{-1} = \tilde{V}_i^{-1}\tilde{U}_i$$

which satisfy the double Bezout equation given in (74). Then a switching from K_{uy} to $K_{uy,i}$ can be obtained by using Q_i given by (Niemann and Poulsen, 2009a; Niemann *et al.*, 2004)

$$Q_i = M^{-1}M_i(\tilde{U}_i V - \tilde{V}_i U) = Z_i(\tilde{U}_i V - \tilde{V}_i U) \quad (61)$$

or

$$Q_i = Z_i \begin{pmatrix} \tilde{U}_i & -\tilde{V}_i \end{pmatrix} \begin{pmatrix} V \\ U \end{pmatrix}$$

in (75). The transfer matrix $Z_i = M^{-1}M_i$ is stable, (Niemann and Poulsen, 2009a; Niemann *et al.*, 2004). In some special cases, we will have that $M = M_i$ and $N = N_i$ and therefore with the result $Z_i = I$.

An alternative to (61) is given by

$$Q_i = (\tilde{V}U_i - \tilde{U}V_i)\tilde{Z}_i, \quad (62)$$

where $\tilde{Z}_i = \tilde{M}_i\tilde{M}^{-1}$.

It should be pointed out that the stability properties depend on the FTC concept applied. Using the FTC concept described in Section 1, it will be more reasonable to guarantee closed-loop stability both in the nominal case as well as in the faulty case. In the latter, only the central controller K_{uy} is applied. The closed-loop system is stable if the faulty system is stabilized by K_{uy}. In the former, where the system is controlled by $K_{uy}(Q)$, the closed-loop system is stable if the nominal closed-loop system given by (G_{yu}, K_{uy}) is stable and Q is stable. If the nominal controller has been applied as the central controller, the closed-loop stability of the faulty case will require that the nominal closed-loop system given by (G_{yu}, K_{uy}) and Q be stable together, and that closed-loop system $(Q, S(\theta))$ be stable. This is a direct consequence of the stability result given in Section 3.1.

7.2. Sensor and actuator extension. The controller architecture considered in Section 1 is based on a general controller parameterization. This architecture does not directly allow a change in the sensor and/or actuator configuration. A change from a safe-mode or a reliable robust controller to a controller with high performance will in many cases also require a change of sensors and/or actuators. To handle this problem, let us consider the extended system $\mathcal{G}$ given by (19), where additional inputs u_a and outputs y_a have been included.

On the basis of the partitioned system in (19) and the feedback controller in (20), the following representation of the eight co-prime matrices for the partitioned system and controller can be derived (Niemann, 2006a):

$$M_{\text{ext}} = \begin{pmatrix} M & M_{12} \\ 0 & I \end{pmatrix}, \qquad U_{\text{ext}} = \begin{pmatrix} U & 0 \\ 0 & 0 \end{pmatrix},$$

$$N_{\text{ext}} = \begin{pmatrix} N & N_{12} \\ N_{12} & N_{22} \end{pmatrix}, \qquad V_{\text{ext}} = \begin{pmatrix} V & 0 \\ V_{21} & I \end{pmatrix},$$

$$\tilde{V}_{\text{ext}} = \begin{pmatrix} \tilde{V} & \tilde{V}_{12} \\ 0 & I \end{pmatrix}, \qquad \tilde{U}_{\text{ext}} = \begin{pmatrix} \tilde{U} & 0 \\ 0 & 0 \end{pmatrix},$$

$$\tilde{N}_{\text{ext}} = \begin{pmatrix} \tilde{N} & \tilde{N}_{12} \\ \tilde{N}_{21} & \tilde{N}_{22} \end{pmatrix}, \qquad \tilde{M}_{\text{ext}} = \begin{pmatrix} \tilde{M} & 0 \\ \tilde{M}_{21} & I \end{pmatrix}, \quad (63)$$

where the eight co-prime matrices will satisfy the double Bezout equation.

This structure can be obtained directly by using an observer-based feedback controller or by using the state space description for general controllers given by Niemann (2006a) and Tay *et al.* (1997). It is important to point out that a general co-prime factorization of the partitioned system and controller will not have this structure. However, using the equations given above for the observer-based feedback controller case or the equations

for a general feedback controller of Tay *et al.* (1997), it will always possible to obtain the structure given in (63).

The Bezout equation in (74) for the extended system described by the co-prime matrices in (63) can be found in the work of Niemann (2006a). The YJBK parameterized controller given by (75) can now be developed for the extended system. The controller takes the following form:

$$\begin{aligned} K_{uy}(Q_{\text{ext}}) &= U_{\text{ext}}(Q_{\text{ext}})V_{\text{ext}}(Q_{\text{ext}})^{-1} \\ &= \begin{pmatrix} K_1(0) & 0 \\ 0 & 0 \end{pmatrix} \\ &\quad + \tilde{V}_{\text{ext}}^{-1}Q_{\text{ext}}\left(V_{\text{ext}} + N_{\text{ext}}Q_{\text{ext}}\right)^{-1}, \end{aligned} \tag{64}$$

where the YJBK transfer matrix Q_{ext} is given by

$$Q_{\text{ext}} = \begin{pmatrix} Q_{\varepsilon\eta} & Q_{\varepsilon y_a} \\ Q_{u_a\eta} & Q_{u_a y_a} \end{pmatrix}, \tag{65}$$

where $Q_{\varepsilon\eta} = Q$ is the YJBK transfer matrix for the original controller given by (75), $Q_{\varepsilon y_a}$ is the YJBK transfer matrix related with the additional sensors, $Q_{u_a\eta}$ is the YJBK transfer matrix related with the additional actuators, and $Q_{u_a y_a}$ is the YJBK transfer matrix related with the additional actuators and sensors.

The transfer matrix from η to ε is zero in the nominal case, (Niemann and Poulsen, 2009b). As a consequence, the closed-loop transfer matrix will be an affine function of the Q transfer matrix. Using the feedback controller given by (64) on the partitioned nominal system $\mathcal{G}$ gives the following closed loop:

$$\begin{aligned} e &= G_{ed}d + G_{eu}K_{uy}(Q_{\text{ext}})(I - G_{yu}K_{uy}(Q_{\text{ext}}))^{-1}G_{yd}d \\ &= T_{ed}(Q_{\text{ext}})d. \end{aligned} \tag{66}$$

Furthermore, rewriting (66) gives the following equation for the closed-loop transfer matrix

$$T_{ed}(Q) = (T_1 + T_2Q_{\varepsilon\eta}T_3) + G_{eu}M(Q_{\text{ext}})G_{yd}, \tag{67}$$

where

$$T_1 = G_{ed} + G_{eu}U\tilde{M}G_{yd}, \quad T_2 = G_{eu}M, \quad T_3 = \tilde{M}G_{yd}$$

and

$$\begin{aligned} &M(Q_{\text{ext}}) \\ &= \begin{pmatrix} \bar{M}_{11}(Q_{\text{ext}}) & MQ_{\varepsilon y_a} + M_{12}Q_{u_a y_a} \\ Q_{u_a\eta}\tilde{M} + Q_{u_a y_a}\tilde{M}_{12} & Q_{u_a y_a} \end{pmatrix}, \\ &\bar{M}_{11}(Q_{\text{ext}}) \\ &= M_{12}Q_{u_a\eta}\tilde{M} + MQ_{\varepsilon y_a}\tilde{M}_{12} + M_{12}Q_{u_a y_a}\tilde{M}_{12} \end{aligned}$$

Here we have used the fact that the transfer matrix from η to ε is zero. This shows that the above closed-loop transfer matrix is an affine function in the YJBK transfer matrix Q_{ext} when additional sensors and actuators are included.

Note that $T_1 + T_2Q_{\varepsilon\eta}T_3$ represents the closed-loop system when only the original measurement y and control input u are applied.

It is clear from (64) that the controller architecture will allow the use of other sensors and/or actuators than the sensors and/or actuators used in connection with the nominal controller K_{uy}.

7.3. Controller switching for extended systems. It is possible to extend (61) or (62) to handle the case where the two controllers do not apply the same set of sensors and actuators. This is relevant in connection with optimizing the closed-loop performance.

Consider the general case where the feedback controller $K_{uy,i}$ is based on a subset of measurements $\bar{y}$ as well as inputs $\bar{u}$ given by y_i and u_i. For simplicity, let y_i and u_i be assumed as the last signals in $\bar{y}$ and $\bar{u}$, respectively, i.e., the feedback controller $K_{uy,i}$ is given by

$$\bar{u} = \begin{pmatrix} 0 & 0 \\ 0 & K_{uy,i} \end{pmatrix}\bar{y}. \tag{68}$$

Let the associated co-prime factorization of $G_{yu,i}$ (the transfer matrix from input u_i to output y_i) and $K_{uy,i}$ be given by

$$\begin{aligned} &G_{yu,i} = N_iM_i^{-1} = \tilde{M}_i^{-1}\tilde{N}_i, \quad N_i, M_i, \tilde{N}_i, \tilde{M}_i \in \mathcal{RH}_\infty, \\ &K_{uy,i} = U_iV_i^{-1} = \tilde{V}_i^{-1}\tilde{U}_i, \quad U_i, V_i, \tilde{U}_i, \tilde{V}_i \in \mathcal{RH}_\infty. \end{aligned} \tag{69}$$

Based on this feedback controller, the associated coprime matrices in (69) are given by

$$\begin{aligned} &M_{\text{ext},i} = \begin{pmatrix} I & 0 \\ M_{i,21} & M_i \end{pmatrix}, \qquad U_{\text{ext},i} = \begin{pmatrix} 0 & 0 \\ 0 & U_i \end{pmatrix}, \\ &N_{\text{ext},i} = \begin{pmatrix} N_i & N_{i,12} \\ N_{i,12} & N_{i,22} \end{pmatrix}, \qquad V_{\text{ext},i} = \begin{pmatrix} I & V_{i,12} \\ 0 & V_i \end{pmatrix}, \\ &\tilde{V}_{\text{ext},i} = \begin{pmatrix} I & 0 \\ \tilde{V}_{i,21} & \tilde{V}_i \end{pmatrix}, \qquad \tilde{U}_{\text{ext},i} = \begin{pmatrix} 0 & 0 \\ 0 & \tilde{U}_i \end{pmatrix}, \\ &\tilde{N}_{\text{ext},i} = \begin{pmatrix} \tilde{N}_i & \tilde{N}_{i,12} \\ \tilde{N}_{i,21} & \tilde{N}_{i,22} \end{pmatrix}, \qquad \tilde{M}_{\text{ext},i} = \begin{pmatrix} I & \tilde{M}_{i,12} \\ 0 & \tilde{M}_i \end{pmatrix}. \end{aligned} \tag{70}$$

Using these matrices in $Q_{\text{ext},i}$ given by (61) results in

the following:

$$\begin{aligned} Q_{\text{ext},i} &= Z_{\text{ext},i}(\tilde{U}_{\text{ext},i}V_{\text{ext}} - \tilde{V}_{\text{ext},i}U_{\text{ext}}) \\ &= Z_{\text{ext},i}\left(\begin{pmatrix} 0 & 0 \\ 0 & \tilde{U}_i \end{pmatrix}\begin{pmatrix} V & 0 \\ V_{21} & I \end{pmatrix} \right. \\ &\quad \left. - \begin{pmatrix} I & 0 \\ \tilde{V}_{i,21} & \tilde{V}_i \end{pmatrix}\begin{pmatrix} U & 0 \\ 0 & 0 \end{pmatrix}\right), \\ Z_{\text{ext},i} &= \begin{pmatrix} M & M_{12} \\ 0 & I \end{pmatrix}^{-1}\begin{pmatrix} I & 0 \\ M_{i,21} & M_i \end{pmatrix} \in \mathcal{RH}_\infty. \end{aligned} \tag{71}$$

Note that the structure in U_{ext}, V_{ext} and in $\tilde{U}_{\text{ext},i}$, $\tilde{V}_{\text{ext},i}$ is not the same. Therefore, it is not possible to multiply the matrices by using the structure.

A special case is when the feedback controller $K_{uy,i}$ is only based on y_a and u_a. Using the co-prime matrices in (70) and $Q_{\text{ext},i}$ given by (61) results in the following:

$$\begin{aligned} Q_{\text{ext},i} &= Z_{\text{ext},i}(\tilde{U}_{\text{ext},i}V_{\text{ext}} - \tilde{V}_{\text{ext},i}U_{\text{ext}}) \\ &= Z_{\text{ext},i}\left(\begin{pmatrix} 0 & 0 \\ \tilde{U}_iV_{21} & \tilde{U}_i \end{pmatrix} - \begin{pmatrix} U & 0 \\ \tilde{V}_{i,12}U & 0 \end{pmatrix}\right) \\ &= Z_{\text{ext},i}\begin{pmatrix} -U & 0 \\ \tilde{U}_iV_{21} - \tilde{V}_{i,12}U & \tilde{U}_i \end{pmatrix}, \\ Z_{\text{ext},i} &= \begin{pmatrix} M & M_{12} \\ 0 & I \end{pmatrix}^{-1}\begin{pmatrix} I & 0 \\ M_{i,21} & M_i \end{pmatrix} \\ &= \begin{pmatrix} M^{-1}(I - M_{12}M_{i,21}) & -M^{-1}M_{12}M_i \\ M_{i,21} & M_i \end{pmatrix} \\ &\quad \in \mathcal{RH}_\infty. \end{aligned} \tag{72}$$

Using the above equation for $Q_{\text{ext},i}$, it is possible to switch from a nominal feedback controller based on y, u to a controller based on other sensors and actuators, without decoupling the first controller K_{uy}. K_{uy} will still be included as part of the new feedback controller.

8. Time aspects of the FTC architecture

Some time aspects of the suggested FTC architecture are discussed in the following. The described FTC architecture includes the following time steps:

1. $t \in [0, t_0[$, start-up mode or safe mode. The safe-mode controller K_{uy} is applied.
2. $t \in [t_0, t_{\text{fault}}[$, normal mode. The nominal controller $K_{uy}(Q)$ is applied, where Q is the performance part of the controller shown in Fig. 3. The controller is running in this mode until faults occur in the system.
3. $t \in [t_{\text{fault}}, t_{\text{detection}}[$, the controller $K_{uy}(Q)$ continues to run in the normal mode until faults have been detected in the system.
4. $t \in [t_{\text{detection}}, t_{\text{isolation}}[$, the controller is running in the safe mode until the faults have been isolated.
5. $t \in [t_{\text{isolation}}, \ldots[$, depending on the faults in the system, the system will either be closed down or continue to operate with full or reduced performance. This is obtained by re-including the performance controller Q in the feedback controller. A reduced performance requires a redesign of Q.

The third step is the most critical one in the FTC architecture. Here the normal-mode controller is applied on a faulty system. The time period from the faults first occurring to when the faults are detected, $\Delta_t = t_{\text{detection}} - t_{\text{fault}}$, is critical. This time period Δ_t will depend on both the faults, the systems, and the residual generator and detector applied. An analysis of the transient system response in the case of faults when the nominal feedback controller is applied gives an upper bound on how large Δ_t can be accepted. It is not directly a matter of the closed-loop system being unstable or not, but it is more a matter of how much the system has moved away from the nominal operation point. If the faulty system is closed-loop stable, the system might run into different limitations that will make it difficult to get the system back to the normal operation point. Using AFD, it will in some cases be possible to detect faults before they have affected the closed-loop system. This could be faults that are slowly increasing. Here quite a large Δ_t can be accepted.

The residual generator and change detector need to be designed with respect to the upper bound on Δ_t. When exact fault detection is possible (Saberi *et al.*, 2000), an upper bound on the time to detection can be derived. This was done by Stoorvogel *et al.* (2001), who considered both the continuous-time as well as the discrete-time case. In the former, the time to detection can be arbitrarily small. In the latter, the maximal number of samples required for detection depends on the order of the infinite zeros in the system.

Normally, a statistical test needs to be applied on top of a residual generator. Applying the CUSUM method (Basseville and Nikiforov, 1993), the mean time to detect can be calculated based on the ARL function. The latter can be applied in connection with both the passive as well as the active FD approach (Basseville and Nikiforov, 1993; Poulsen and Niemann, 2008). As a consequence, the mean time between false alarms cannot be optimized; it will be a result of the selected mean time to detection.

When faults have been detected, the performance part of the controller is decoupled by removing Q from the controller (in Step 4). The faults need to be isolated before

it is possible to decide whether the system should continue in operation with reduced performance or whether it should be closed down. In general, there will not be strong limitations on the time used for isolation.

9. Closing remarks

A concept for FTC has been suggested in this paper. The implementation of the FTC architecture has been based on the YJBK parameterization. Both fault diagnosis as well as controller reconfiguration can be based on the same set of signal vectors in the architecture. The architecture allows application of both passive and active fault diagnosis methods. In connection with the controller reconfiguration, it is shown how it is possible to switch to feedback controllers using another set of sensors and actuators.

References

Basseville, M. and Nikiforov, I. (1993). *Detection of Abrupt Changes—Theory and Application*, Prentice Hall, Upper Saddle River, NJ.

Blanke, M., Frei, C., Kraus, F., Patton, R. and Staroswiecki, M. (2000). What is fault-tolerant control?, *Preprints of the 4th IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes, SAFEPROCESS'2000, Budapest, Hungary*, pp. 40–51.

Blanke, M., Izadi-Zamanabadi, R., Bøgh, S. and Lunau, C. (1997). Fault tolerant control systems—A holistic view, *Control Engineering Practice* **5**(5): 693–702.

Blanke, M., Kinnart, M., Lunze, J. and Staroswiecki, M. (2003). *Diagnosis and Fault-Tolerant Control*, Springer, Berlin/Heidelberg.

Boyd, S. and Barratt, C. (1991). *Linear Controller Design—Limits of Performance*, Prentice Hall, Upper Saddle River, NJ.

Campbell, S., Horton, K. and Nikoukhah, R. (2002). Auxiliary signal design for rapid multi-model identification using optimization, *Automatica* **38**(8): 1313–1325.

Campbell, S., Horton, K., Nikoukhah, R. and Delebecque, F. (2000). Rapid model selection and the separability index, *Proceedings of Safeprocess 2000, Budapest, Hungary*, pp. 1187–1192.

Campbell, S. and Nikoukhah, R. (2004a). *Auxiliary Signal Design for Failure Detection*, Princeton University Press, Princeton, NJ.

Campbell, S. and Nikoukhah, R. (2004b). Software for auxiliary signal design, *Proceedings of the American Control Conference, Boston, MA, USA*, pp. 4414–4419.

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

Gustafsson, F. (2000). *Adaptive Filtering and Change Detection*, Wiley & Sons, Chichester.

Keresteciogl u, F. (1993). *Change Detection and Input Design in Dynamic Systems*, Research Studies Press, Baldock, Hertfordshire.

Kerestecioglu, F. and Zarrop, M. (1994). Input design for detection of abrupt changes in dynamical systems, *International Journal of Control* **59**(4): 1063–1084.

Maciejowski, J. (1989). *Multivariable Feedback Control*, Addison Wesley, Boston, MA.

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

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

Niemann, H. (2005). Fault tolerant control based on active fault diagnosis, *Proceedings of the American Control Conference, Portland, OR, USA*, pp. 2224–2229.

Niemann, H. (2006a). Parameterization of extended systems, *IEE Proceedings—Control Theory and Applications* **153**(2): 221–227.

Niemann, H. (2006b). A setup for active fault diagnosis, *IEEE Transactions on Automatic Control* **51**(9): 1572–1578.

Niemann, H. and Poulsen, N. (2006). Fault tolerant control for uncertain systems with parametric faults, *Preprints of the 6th IFAC Symposium on Fault Detection, Supervision ans Safety for Technical Processes, SAFEPROCESS'2006, Beijing, China*, pp. 517–522.

Niemann, H. and Poulsen, N. (2009a). Controller architectures for switching, *Proceedings of the American Control Conference, St. Louis, MO, USA*, pp. 1098–1103.

Niemann, H. and Poulsen, N. (2009b). A concept for fault tolerant controllers, *in* Z. Kowalczuk (Ed.) *Diagnosis of Processes and Systems*, Pomeranian Science and Technology Publishers PWNT, Gdańsk, pp. 107–114.

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

Niemann, H. and Stoustrup, J. (2005). An architecture for fault tolerant controllers, *International Journal of Control* **78**(14): 1091–1110.

Niemann, H., Stoustrup, J. and Abrahamsen, R. (2004). Switching between multivariable controllers, *Optimal Control—Application and Methods* **25**(2): 51–66.

Nikoukhah, R. (1994). Innovations generation in the presence of unknown inputs: Application to robust failure detection, *Automatica* **30**(12): 1851–1867.

Nikoukhah, R. (1998). Guaranteed active failure detection and isolation for linear dynamical systems, *Automatica* **34**(11): 1345–1358.

Nikoukhah, R., Campbell, S. and Delebecque, F. (2000). Detection signal design for failure detection: A robust approach, *International Journal of Adaptive Control and Signal Processing* **14**(7): 701–724.

Poulsen, N. and Niemann, H. (2008). Active fault diagnosis based on stochastic tests, *International Journal of Applied Mathematics and Computer Science* **18**(4): 487–496, DOI: 10.2478/v10006-008-0043-6.

Saberi, A., Stoorvogel, A., Sannuti, P. and Niemann, H. (2000). Fundamental problems in fault detection and identification, *International Journal of Robust and Nonlinear Control* **10**(14): 1209–1236.

Skogestad, S. and Postlethwaite, I. (2005). *Multivariable Feedback Control: Analysis and Design*, Wiley, Hoboken, NJ.

Stoorvogel, A., Niemann, H. and Saberi, A. (2001). Delays in fault detection and isolation, *Proceedings of the American Control Conference, Washington, DC, USA*, pp. 459–463.

Stoustrup, J. and Niemann, H. (2001). Fault tolerant feedback control using the Youla parameterization, *Proceedings of the 6th European Control Conference, Porto, Portugal*, pp. 1970–1974.

Tay, T., Mareels, I. and Moore, J. (1997). *High Performance Control*, Birkhäuser, Boston, MA.

Zhang, X. (1989). *Auxiliary Signal Design in Fault Detection and Diagnosis*, Springer-Verlag, Heidelberg.

Zhou, K., Doyle, J. and Glover, K. (1995). *Robust and optimal control*, Prentice Hall, Upper Saddle Rider, NJ.

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

Hans Henrik Niemann was born in Denmark in 1961. He received the M.Sc. degree in mechanical engineering in 1986 and the Ph.D. degree in 1988 from the Technical University of Denmark. From 1988 to 1994 he held a research position and since 1994 he has been an assistant professor of control engineering at the Technical University of Denmark. His research interests include optimal and robust control, fault detection and isolation, active fault diagnosis, fault tolerant control, controller architecture for controller switching and fault tolerant control, system and performance monitoring, controller anti-windup.

Appendix

Co-prime factorization

A number of preliminary results for co-prime factorization and parameterization are given in this appendix.

Co-prime factorization. Let a co-prime factorization of the system G_{yu} from (1) and the stabilizing controller K_{uy} from (4) be given by

$$\begin{aligned} G_{yu} &= NM^{-1} = \tilde{M}^{-1}\tilde{N}, \quad N, M, \tilde{N}, \tilde{M} \in \mathcal{RH}_\infty, \\ K_{uy} &= UV^{-1} = \tilde{V}^{-1}\tilde{U}, \quad U, V, \tilde{U}, \tilde{V} \in \mathcal{RH}_\infty, \end{aligned} \tag{73}$$

where the eight matrices in (73) must satisfy the double Bezout equation given by (see Tay *et al.*, 1997):

$$\begin{aligned} \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix} &= \begin{pmatrix} \tilde{V} & -\tilde{U} \\ -\tilde{N} & \tilde{M} \end{pmatrix} \begin{pmatrix} M & U \\ N & V \end{pmatrix} \\ &= \begin{pmatrix} M & U \\ N & V \end{pmatrix} \begin{pmatrix} \tilde{V} & -\tilde{U} \\ -\tilde{N} & \tilde{M} \end{pmatrix}. \end{aligned} \tag{74}$$

State space descriptions of the above eight co-prime matrices can be derived. The standard description is based on using an observer-based feedback controller (Tay *et al.*, 1997), but state space descriptions can also be derived for other types of feedback controllers.

YJBK parameterization. Based on the above co-prime factorization of the system G_{yu} and the controller K_{uy}, we can give a parameterization of all controllers that stabilizes the system in terms of a stable transfer matrix Q, i.e., all stabilizing controllers are given by using a right-factored form (Tay *et al.*, 1997):

$$K_{uy}(Q) = (U+MQ)(V+NQ)^{-1}, \quad Q \in \mathcal{RH}_\infty, \tag{75}$$

or by using a left-factored form:

$$K_{uy}(Q) = (\tilde{V}+Q\tilde{N})^{-1}(\tilde{U}+Q\tilde{M}), \quad Q \in \mathcal{RH}_\infty. \tag{76}$$

Using the Bezout equation, the controller given either by (75) or by (76) can be realized as an LFT in the parameter Q:

$$\begin{aligned} K_{uy}(Q) &= \mathcal{F}_l\left(\begin{pmatrix} UV^{-1} & \tilde{V}^{-1} \\ V^{-1} & -V^{-1}N \end{pmatrix}, Q\right) \\ &= \mathcal{F}_l(J_K, Q). \end{aligned} \tag{77}$$

Dual YJBK parameterization. The dual YJBK parameterization gives a parameterization in terms of a stable transfer matrix S of all systems stabilized by a given controller. The dual YJBK parameterization was considered in detail by Niemann (2003), who also described the connection between the dual YJBK transfer matrix and changes in the system. The parameterization is given by Niemann (2003) and Tay *et al.* (1997):

$$G_{yu}(S) = (N+VS)(M+US)^{-1}, \quad S \in \mathcal{RH}_\infty, \tag{78}$$

or by using a left-factored form:

$$G_{yu}(S) = (\tilde{M}+S\tilde{U})^{-1}(\tilde{N}+S\tilde{V}), \quad S \in \mathcal{RH}_\infty. \tag{79}$$

An LFT representation of (78) or (79) is given by

$$\begin{aligned} G_{yu}(S) &= \mathcal{F}_l\left(\begin{pmatrix} NM^{-1} & \tilde{M}^{-1} \\ M^{-1} & -M^{-1}U \end{pmatrix}, S\right) \\ &= \mathcal{F}_l(J_G, S). \end{aligned} \tag{80}$$

The interpretation of the dual YJBK transfer matrix S can be investigated from the primal YJBK parameterization. It turns out that the dual YJBK transfer matrix S is the open-loop transfer matrix from η to ε, i.e., closing the loop around Q

$$S = \mathcal{F}_u(J_K, G_{yu}(S)) \tag{81}$$

equivalent to (22).

Received: 12 January 2011
Revised: 16 July 2011