INTEGRATING CONTROL AND FAULT DIAGNOSIS: A SEPARATION RESULT

Jakob Stoustrup * **Mike J. Grimble** **

* *Department of Control Engineering, Aalborg University, Fr. Bajersvej 7C, DK-9220 Aalborg, Denmark, Tlph: +45 9635 8749, Fax: +45 9815 1739, E-mail:* `jakob@control.auc.dk`, *WWW:* `www.control.auc.dk/~jakob`

** *Industrial Control Centre, University of Strathclyde, Graham Hills Building, 50 George Street, Glasgow G1 1QE, Scotland. E-mail:* `m.grimble@icu.strath.ac.uk`
Tlph: +44 141 548 2880 Fax: +44 141 548 4203

Abstract. A design method is presented which integrates control action and fault detection and isolation. Control systems operating under potentially faulty conditions are considered. The problem of designing a single unit which handles both the required control action, as well as identifying faults occuring in actuators and sensors is discussed. This unit is able to: (1) follow references and reject disturbances robustly, (2) control the system such that undetected failures do not have disastrous effects, (3) reduce the number of false alarms, and (4) identify which faults have occured. The method uses a type of separation principle which makes the design process very transparent, and a frequency domain $\mathcal{H}_\infty$ formulation which makes weight selection more straightforward. As a consequence of the separation between control and diagnosis, we shall prove that the controller needs not be detuned in order to improve the diagnosis capabilities, in contrast to common beliefs.

Keywords. Fault diagnosis; detection; isolation; model-based; $\mathcal{H}_\infty$ theory;

1. INTRODUCTION

In the control of industrial systems, it is rarely that a control system functions continuously throughout the scheduled life cycle of the plant and controller hardware. Due to wear of mechanical and/or electrical components both actuators and sensors can fail in more or less critical ways. For safety critical processes it is of paramount importance to detect when failures are likely to happen, and to identify as fast as possible which failures have taken place.

To meet such industrial needs, a number of schemes for Fault Detection and Isolation (FDI) have been put forward in the literature on automatic control. Most of the papers appearing in journals and in conference proceedings have dealt with the design of filters which monitor a process, and generate alarms when faults may have occured. In most cases, the filters are model based devices which act independently of the computer implemented digital controllers. In this paper, however, the advantages of combining the control algorithm and the FDI filter in a single module will be discussed, and a relatively simple methodology to design such combined modules will be described. It will be argued that a combined module will be beneficial in terms of implementation and reliability, but also that the quality of control and the quality of detection will not improve by the integrated design, compared to individual designs of the two components. We show this result in wide generality. A special case using an algebraic Riccati equation approach was presented in (Tyler and Morari, 1994).

A useful survey on early work on FDI can be found in (Frank, 1990) and in (Patton *et al.*, 1989). Many of these techniques are observer based, such as e.g. (Magni and Mouyon, 1991). These methods have since been refined and extended. A more recent reference in this line of research is (Frank and Ding, 1994). The original idea of utilizing the information already available in the 'observer' part of a controller for diagnostic purposes was given in (Nett *et al.*, 1988).

Early papers on FDI suffered from problems due to modeling uncertainties. In some cases false alarms were likely, due to imperfect modeling. This motivated incorporation of robustness issues into the FDI design algorithm. Specific robustness considerations to FDI problems were discussed in (Patton and Chen, 1991; Mangoubi *et al.*, 1995; Qiu and Gertler, 1993; Bokor and Keviczky, 1994; Wang and Wu, 1993). All these methods use frequency domain techniques in contrast to (Ajbar and Kantor, 1993) which uses ℓ_∞ techniques.

An interesting application of FDI techniques is presented in (Blanke *et al.*, 1995; Jørgensen *et al.*, 1995; Grainger *et al.*, 1995; Garcia *et al.*, 1995), suggesting a diesel engine actuator as an FDI benchmark.

2. PROBLEM FORMULATION

Figure 1 illustrates a control problem in the standard system configuration (see e.g. (Zhou *et al.*, 1996) for an introduction to the standard configuration paradigm). Here, w_d can be thought of as a collection of undesired signals (disturbances) entering the system $G(s)$ or as setpoints. The signals y_c are the measurements used by the controller $K(s)$ generating the control signals u_c in order to make the outputs to be controlled z_c sufficiently small.

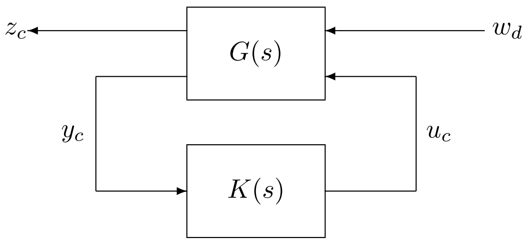

Fig. 1. Control system in standard $\mathcal{H}_\infty$ configuration

The system in Figure 1 can be described in either the state space formulation:

$$\begin{pmatrix} \dot{x} \\ z_c \\ y_c \end{pmatrix} = \begin{pmatrix} A & B_1 & B_2 \\ C_1 & D_{11} & D_{12} \\ C_2 & D_{21} & D_{22} \end{pmatrix} \begin{pmatrix} x \\ w_d \\ u_c \end{pmatrix}$$

or, alternatively, in transfer matrix function form:

$$\begin{pmatrix} z_c \\ y_c \end{pmatrix} = G(s) \begin{pmatrix} w_d \\ u_c \end{pmatrix}$$

$$= \begin{pmatrix} G_{11}(s) & G_{12}(s) \\ G_{21}(s) & G_{22}(s) \end{pmatrix} \begin{pmatrix} w_d \\ u_c \end{pmatrix} \qquad (1)$$

$$= \begin{pmatrix} C_1(sI-A)^{-1}B_1 + D_{11} & C_1(sI-A)^{-1}B_2 + D_{12} \\ C_2(sI-A)^{-1}B_1 + D_{21} & C_2(sI-A)^{-1}B_2 + D_{22} \end{pmatrix} \begin{pmatrix} w_d \\ u_c \end{pmatrix}$$

For the standard problem shown in Figure 1, a controller $K(s)$ making the $\mathcal{H}_\infty$ norm of the transfer function from w_d to z_c smaller than 1 can, if it exists, be found by standard $\mathcal{H}_\infty$ optimization tools.

Usually, the model $G(s)$ will contain the plant model itself, but it can also contain models of disturbances, measurement noises, time variations, nonlinearities, and unmodelled dynamics. Hence, making the $\mathcal{H}_\infty$ norm from w_d to z_c small ensures a number of performance and robustness properties.

The everyday operation of such a feedback system depends, needless to say, on reliable actuators and sensors. However, in most industrial environments both actuators and sensors can fail. One way to model this is depicted in Figure 2. Here, the measurements

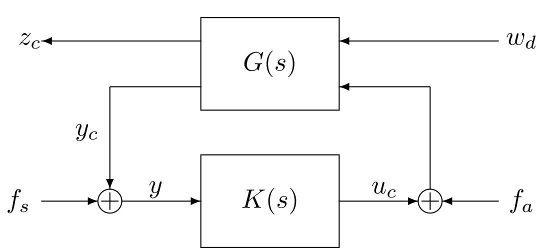

Fig. 2. Control system with actuator and sensor faults

used by the controller are $y = y_c + f_s$ rather than y_c and the controls acting on the plant are $u_c + f_a$ rather than u_c. For example $y_c + f_s \equiv 0$ or $u_c + f_a \equiv 0$ can represent completely defective sensors or actuators, respectively.

For safety critical processes in particular, faulty situations must be identified, and action taken. Two main paths of action can be taken: either the control design algorithm can be modified to tolerate minor errors, or using an estimator the faulty signal can be identified and action can be taken by the operator or by a supervisory system. In most applications the latter will be preferable.

A method will now be described, which allows for either or both approaches to be incorporated in a single design step which also comprises the controller design. This is achieved using a single module which generates both the control action and the fault estimates.

To succesfully identify individual faults, it is of paramount importance to have good fault models. One way to describe the fault models is to introduce frequency weightings on the fault signals:

$$f_a = W_a(s) w_a \qquad \text{and} \qquad f_s = W_s(s) w_s$$

where w_a and w_s are signals that are anticipated to have flat power spectra. These are fictitious signals with the sole purpose of generating the frequency coloured signals f_a and f_s.

The module to be designed should, in addition to the control signal u_c, also generate a signal containing estimates of potential faults:

$$u_f = \begin{pmatrix} \hat{f}_a \\ \hat{f}_s \end{pmatrix}$$

This situation is depicted in Figure 3.

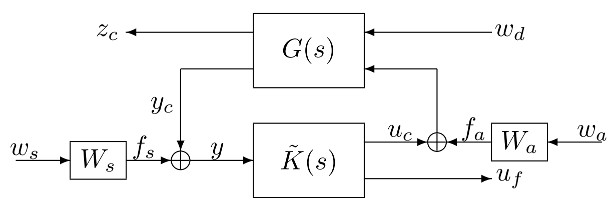

Fig. 3. Control system with faults and diagnostics

The final step is to define a fault estimation error z_f as:

$$z_f = \begin{pmatrix} f_a \\ f_s \end{pmatrix} - u_f$$

Using these signals a new augmented standard problem can be established as shown in Figure 4.

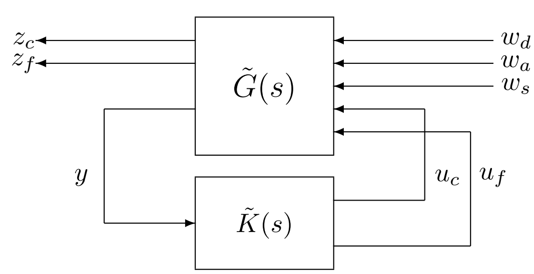

Fig. 4. Standard model for integrated control and FDI

Defining:

$$\xi = \begin{pmatrix} x \\ x_a \\ x_s \end{pmatrix},\ w = \begin{pmatrix} w_d \\ w_a \\ w_s \end{pmatrix},\ u = \begin{pmatrix} u_c \\ u_f \end{pmatrix}, \qquad (2)$$

$$z = \begin{pmatrix} z_c \\ z_f \end{pmatrix},\ y = y_c + f_s$$

the following standard problem is obtained in state space form:

$$\begin{aligned} \dot{\xi} &= \tilde{A}\xi + \tilde{B}_1 w + \tilde{B}_2 u \\ z &= \tilde{C}_1\xi + \tilde{D}_{11} w + \tilde{D}_{12} u \\ y &= \tilde{C}_2\xi + \tilde{D}_{21} w + \tilde{D}_{22} u \end{aligned} \qquad (3)$$

or in transfer matrix function form:

$$\begin{pmatrix} z \\ y \end{pmatrix} = \tilde{G}(s)\begin{pmatrix} w \\ u \end{pmatrix} = \begin{pmatrix} \tilde{G}_{11}(s) & \tilde{G}_{12}(s) \\ \tilde{G}_{21}(s) & \tilde{G}_{22}(s) \end{pmatrix}\begin{pmatrix} w \\ u \end{pmatrix}$$

(the explicit formulae are given below.)

Using $\mathcal{H}_\infty$ optimization, a generalized controller $u = \tilde{K}(s)y$ for the diagram shown in Figure 5 can now be computed, which will then be able to generate both control signals and failure estimates.

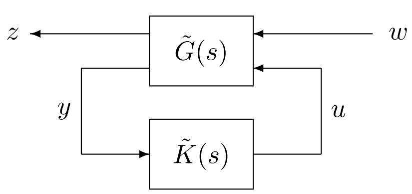

Fig. 5. $\mathcal{H}_\infty$ standard problem for optimization

In the next sections, the solution to the standard problem depicted in Figure 5 will be given, and the interpretation of that solution will be discussed.

We shall give explicit formulae for constraints given in the $\mathcal{H}_\infty$ norm. However, we would like to stress at this point, that the main observation which is a kind of separation principle, would hold for *any* criteria of the form:

$$\|z_c\| < 1\,, \qquad \|z_f\| < 1$$

subject to bounded sets of disturbances and fault signals.

3. MAIN RESULTS

Using the partition (1), the following expressions for the standard problem (3), depicted in Figures 4 and 5, can be derived.

$$\left(\frac{z}{y}\right) = \begin{pmatrix} z_c \\ z_f \\ \hline y \end{pmatrix} = \tilde{G}(s)\left(\frac{w}{u}\right)$$

$$= \left(\begin{array}{c|c} \tilde{G}_{11}(s) & \tilde{G}_{12}(s) \\ \hline \tilde{G}_{21}(s) & \tilde{G}_{22}(s) \end{array}\right)\left(\frac{w}{u}\right)$$

$$= \left(\begin{array}{ccc|cc} G_{11}(s) & G_{12}(s)W_a(s) & 0 & G_{12}(s) & 0 \\ 0 & \begin{pmatrix} W_a(s) \\ 0 \end{pmatrix} & \begin{pmatrix} 0 \\ W_s(s) \end{pmatrix} & 0 & -I \\ \hline G_{21}(s) & G_{22}(s)W_a(s) & W_s(s) & G_{22}(s) & 0 \end{array}\right)\begin{pmatrix} w_d \\ w_a \\ w_s \\ \hline u_c \\ u_f \end{pmatrix}$$

Introducing the control law $u = \tilde{K}(s)y$ the following closed loop formula can be obtained:

$$\begin{pmatrix} z_c \\ z_f \end{pmatrix} = T_{zw}(s)\begin{pmatrix} w_d \\ w_a \\ w_s \end{pmatrix}$$

where

$$T_{zw} = \tilde{G}_{11} + \tilde{G}_{12}\tilde{K}\left(I - \tilde{G}_{22}\tilde{K}\right)^{-1}\tilde{G}_{21}$$

$$= \begin{pmatrix} G_{11} & G_{12}W_a & 0 \\ 0 & \begin{pmatrix} W_a \\ 0 \end{pmatrix} & \begin{pmatrix} 0 \\ W_s \end{pmatrix} \end{pmatrix} +$$

$$\begin{pmatrix} G_{12} & 0 \\ 0 & -I \end{pmatrix}\tilde{K}\left(I - (G_{22}\ 0)\,\tilde{K}\right)^{-1}(G_{21}\ G_{22}W_a\ W_s)$$

Often $G(s)$ will be stable due to inner loops which are included in the $\mathcal{H}_\infty$ standard model. The following analysis can be carried out for unstable standard models as well, but for simplicity $G(s)$ will be assumed stable below. In that case, the YJBK parameterization (Youla *et al.*, 1971) of all stabilizing controllers can be obtained simply by making the substitution

$$Q = \tilde{K}\left(I - \tilde{G}_{22}\tilde{K}\right)^{-1}, \quad \tilde{K} = Q\left(I + \tilde{G}_{22}Q\right)^{-1}$$

Partitioning the control sensitivity function $Q(s)$ as

$$Q(s) = \begin{pmatrix} Q_1(s) \\ Q_2(s) \end{pmatrix}$$

the following expression is obtained

$$T_{zw}(s) = \begin{pmatrix} T^1_{zw}(s) \\ T^2_{zw}(s) \end{pmatrix}, \quad \text{where}$$

$$T^1_{zw}(s) =$$
$$(\,G_{11} + G_{12}Q_1G_{21}\ \ G_{12}\,(I + Q_1G_{22})\,W_a\ \ G_{12}Q_1W_s\,)$$

$$T^2_{zw}(s) =$$
$$\left(-Q_2G_{21}\ \begin{pmatrix} W_a \\ 0 \end{pmatrix} - Q_2G_{22}W_a\ \begin{pmatrix} 0 \\ W_s \end{pmatrix} - Q_2W_s\right)$$

Now, the crucial observation in this expression is that each of the $T^i_{zw}(s)$ depends on only one of the Q_i's, $i \in \{1, 2\}$. This has the following two consequences:

(1) Making the closed loop transfer function associated with the control objectives small and making the closed loop transfer function associated with the FDI objectives small can be achieved independently
(2) Optimizing independently eliminates some of the conservatism usually introduced in $\mathcal{H}_\infty$ optimization

This possibility for separation shall explicitly be exploited in the design procedure below. A separation principle similar in spirit to this is described in (**?**).

Without loss of generality, it can be assumed that all weightings have been chosen in order to normalize the $\mathcal{H}_\infty$ standard problem (3). Then since the upper row partition of $T_{zw}(s)$ depends only upon $Q_1(s)$ and the lower row partition depends upon $Q_2(s)$, the $\|T_{zw}\|_\infty$ can be optimized by individually optimizing the different block terms. Hence, after separating the optimizations for z_c and z_f, we are faced with the following $\mathcal{H}_\infty$ optimization constraints:

$$\left\| T^1_{zw}(s) \right\|_\infty < 1 \tag{4}$$

and

$$\left\| T^2_{zw}(s) \right\|_\infty < 1 \tag{5}$$

The $\mathcal{H}_\infty$ problems corresponding to (4) and (5) are both model matching problems, which are simpler special cases of the general 4-block $\mathcal{H}_\infty$ problem, and can be solved as Nehari problems.

The standard problem formulation corresponding to (4) is:

$$\begin{pmatrix} z_c \\ \hline y_{Q_1} \end{pmatrix} \left(\begin{array}{ccc|c} G_{11} & G_{12}W_a & 0 & G_{12} \\ \hline G_{21} & G_{22}W_a & W_s & 0 \end{array} \right) \begin{pmatrix} w_d \\ w_a \\ w_s \\ \hline u_{Q_1} \end{pmatrix} \tag{6}$$

where u_{Q_1} is the output of the $Q_1(s)$ partition and y_{Q_1} is the input to the $Q_1(s)$ subsystem.

For (5) the associated standard problem is:

$$\begin{pmatrix} z_f \\ \hline y_{Q_2} \end{pmatrix} = \left(\begin{array}{ccc|c} 0 & \begin{pmatrix} W_a \\ 0 \end{pmatrix} & \begin{pmatrix} 0 \\ W_s \end{pmatrix} & -I \\ \hline G_{21} & G_{22}W_a & W_s & 0 \end{array} \right) \begin{pmatrix} w_d \\ w_a \\ w_s \\ \hline u_{Q_2} \end{pmatrix} \tag{7}$$

where u_{Q_2} is the output of the $Q_2(s)$ partition and y_{Q_2} is the input to the $Q_2(s)$ subsystem.

Given Q_1 and Q_2, the solution to the standard problem (3):

$$\tilde{K}(s) = \begin{pmatrix} K_1(s) \\ K_2(s) \end{pmatrix}$$

where $K_1(s)$ and $K_2(s)$ are the feedback control part and the FDI part, respectively, can be computed as:

$$K_1 = Q_1 \left(I + G_{22}Q_1 \right)^{-1} \tag{8}$$

and

$$\begin{aligned} K_2 &= Q_2 \left(I + G_{22}Q_1 \right)^{-1} \\ &= Q_2 \left(I - G_{22}Q_1 \left(I + G_{22}Q_1 \right)^{-1} \right) \\ &= Q_2 \left(I - G_{22}K_1 \right) \end{aligned} \tag{9}$$

Remark 1. It is important to note that the expression (8) for K_1 does not depend on Q_2 but only on Q_1 which is found by an optimization which does also not depend on Q_2. This means that in this formulation of the problem, the control action does not directly depend on the fault filtering dynamics. Still, the regulating controller can be detuned compared to a non-faulty setup, since the control design algorithm regards the faults as disturbances and noise as can be seen from (6). In cases, where this is not desirable, some attention must be paid to the weighting selection scheme to avoid detuning. Alternatively, the optimization problem (4) can be completely reformulated by virtue of the separation principle described above. The expression (9) for K_2 depends on Q_1. This is obvious, since the fault detection and isolation filter has to use the 'observer' part of the controller to identify the faults.

The final step in devising the combined control and FDI device is to solve the two model matching problems (6) and (7). Using polynomial $\mathcal{H}_\infty$ theory (see (Kwakernaak, 1993)) the following results are obtained.

Lemma 1. Consider the following J-spectral factorization:

$$\begin{aligned} \Pi_1 &= \begin{pmatrix} I & 0 \\ 0 & -G_{12}^\sim \end{pmatrix} \begin{pmatrix} \Psi^1_{11} & \Psi^1_{12} \\ \Psi^1_{21} & \Psi^1_{22} \end{pmatrix}^{-1} \begin{pmatrix} I & 0 \\ 0 & -G_{12} \end{pmatrix} \\ &= Z_1 J_1 Z_1 \end{aligned}$$

where

$$\begin{aligned} \Psi^1_{11} &= -G_{21}G_{21}^\sim - G_{22}W_aW_a^\sim G_{22}^\sim - W_sW_s^\sim \\ \Psi^1_{12} &= -G_{21}G_{11}^\sim - G_{21}W_aW_a^\sim G_{12}^\sim \\ \Psi^1_{21} &= -G_{11}G_{21}^\sim - G_{12}W_aW_a^\sim G_{21}^\sim \\ \Psi^1_{22} &= I - G_{11}G_{11}^\sim - G_{12}W_aW_a^\sim G_{12}^\sim \end{aligned}$$

$Z_1(s)$ is a square matrix which is invertible as an element of $\mathcal{R}H_\infty$, and J_1 is a constant matrix of the form

$$J_1 = \begin{pmatrix} I & 0 \\ 0 & -I \end{pmatrix}$$

with a suitable number of 1's and -1's. J_1 is called the signature matrix of Π_1.

The model matching problem (6) has a solution if and only if the following the following controller is stabilizing:

$$Q_1^c = \left(0 \;\; I \right) Z_1^{-1} \begin{pmatrix} I \\ 0 \end{pmatrix} \left(\left(I \;\; 0 \right) Z_1^{-1} \begin{pmatrix} I \\ 0 \end{pmatrix} \right)^{-1} \tag{10}$$

Moreover, in that case, all solutions are given by:

$$Q_1 = Y_1 X_1^{-1} \tag{11}$$

where

$$\begin{pmatrix} X_1 \\ Y_1 \end{pmatrix} = Z_1^{-1} \begin{pmatrix} A_1 \\ B_1 \end{pmatrix}$$

and A_1 and B_1 are (free) stable rational matrices, $\det A_1$ having all its roots in the open left half complex plane, satifying:

$$A_1^\sim A_1 \geq B_1^\sim B_1$$

Similarly, for (7):

Lemma 2. Consider the following J-spectral factorization:

$$\Pi_2 = \begin{pmatrix} \Psi^2_{11} & \Psi^2_{12} \\ \Psi^2_{21} & \Psi^2_{22} \end{pmatrix}^{-1} = Z_2 J_2 Z_2$$

where

$$\begin{aligned} \Psi^2_{11} &= -G_{21}G_{21}^\sim - G_{22}W_aW_a^\sim G_{22}^\sim - W_sW_s^\sim \\ \Psi^2_{11} &= \left(-G_{22}W_aW_a^\sim \;\; -W_sW_s^\sim \right) \\ \Psi^2_{11} &= \begin{pmatrix} -W_aW_a^\sim G_{22}^\sim \\ -W_sW_s^\sim \end{pmatrix} \\ \Psi^2_{11} &= \begin{pmatrix} I - W_aW_a^\sim & 0 \\ 0 & I - W_sW_s^\sim \end{pmatrix} \end{aligned}$$

$Z_2(s)$ is a square matrix which is invertible as an element of $\mathcal{R}H_\infty$, and J_2 is the signature matrix of Π_2.

The model matching problem (7) has a solution if and only if the following controller is stabilizing:

$$Q_2^c = \begin{pmatrix} 0 & I \end{pmatrix} Z_2^{-1} \begin{pmatrix} I \\ 0 \end{pmatrix} \left(\begin{pmatrix} I & 0 \end{pmatrix} Z_2^{-1} \begin{pmatrix} I \\ 0 \end{pmatrix} \right)^{-1} \quad (12)$$

Moreover, in that case, all solutions are given by:

$$Q_2 = Y_2 X_2^{-1} \quad (13)$$

where

$$\begin{pmatrix} X_2 \\ Y_2 \end{pmatrix} = Z_2^{-1} \begin{pmatrix} A_2 \\ B_2 \end{pmatrix}$$

and A_2 and B_2 are (free) stable rational matrices, $\det A_2$ having all its roots in the open left half complex plane, satifying:

$$A_2^{\sim} A_2 \geq B_2^{\sim} B_2$$

Employing the separation principle described above, and combining Lemmas 1 and 2, the main result can be stated.

Theorem 3. Consider the setup depicted in Figure 3 where $\tilde{K}(s)$ is a combined controller and FDI module.

The following two statements are equivalent:

(1) There exists a transfer matrix $\tilde{K}(s)$ making the transfer function from disturbances to controlled outputs smaller than 1, and making the transfer function from actuator and sensor faults to the fault estimation error smaller than 1
(2) The controller Q_1^c given by (10) stabilizes the standard problem given by (6) and, likewise, the controller Q_2^c given by (12) stabilizes the standard problem given by (7)

Moreover, when these conditions are satisfied, a possible choice of $\tilde{K}(s) = \begin{pmatrix} K_1 \\ K_2 \end{pmatrix}$ is given by (8) and (9) where $Q_1(s)$ and $Q_2(s)$ are given by (11) and (13), respectively.

4. DISCUSSION

Solving the $\mathcal{H}_\infty$ problem depicted in Figure 5 implies making six transfer functions small due to the definitions (2) of w and z. These six transfer functions are:

$T_{z_c w_d}$: Transfer function from external disturbances to inferred outputs
$T_{z_c w_a}$: Transfer function from actuator faults to inferred outputs
$T_{z_c w_s}$: Transfer function from sensor faults to inferred outputs
$T_{z_f w_d}$: Transfer function from external disturbances to fault estimation error
$T_{z_f w_a}$: Transfer function from actuator faults to fault estimation error
$T_{z_f w_s}$: Transfer function from sensor faults to fault estimation error

The essential instrument for creating a well functioning module for control action and fault detection and isolation is to apply an optimization algorithm which makes these transfer functions small, and trades off the individual functions by careful weight selection.

Making each of the six transfer functions small has its own (important) interpretation.

(1) making $\|T_{z_c w_d}\|_\infty$ small implies good disturbance rejection and robustness, i.e. the original control objectives are achieved
(2) making $\|T_{z_c w_a}\|_\infty$ and $\|T_{z_c w_s}\|_\infty$ small implies that undetected failures do not cause disastrous effects
(3) making $\left\|T_{z_f w_d}\right\|_\infty$ small implies that disturbances are not readily interpreted as faults, i.e. the risk of false alarms is reduced
(4) making $\left\|T_{z_f w_a}\right\|_\infty$ and $\left\|T_{z_f w_s}\right\|_\infty$ small implies that u_f becomes a good estimate of potential actuator and sensor faults

From the results in this paper, it is clear that objective 1 has to be traded off against objective 2, and that objective 3 has to be traded off against objective 4, but also that the design process does not involve a trade-off between the two pairs of objectives, once the standard model (1) has been specified.

In order not to complicate the explanation in this paper the control weights related to control performance and control robustness have not been explicitly included, but they are of course present in terms of the original standard problem formulation depicted in Figure 1. Needless to say, the choice of the internal weightings of the original system, are very significant to the overall performance of the combined control and FDI module.

First of all, in order for the optimization in Theorem 3 to give a useful result, it is of great importance to choose the weightings associated with the original standard problem, the weightings associated with actuator failures and the weightings associated with sensor failures, such that all these weightings are separated in frequency.

Choosing large weights for the disturbance models means that the design algorithm is encouraging disturbance rejection, control robustness.

Choosing large weights for the actuator and sensor failure models means that the design algorithm is putting emphasis on the quality of the failure estimates, making sure that very few faults are undetected.

As mentioned in Remark 1, the faults are considered to be disturbances in the control subproblem (6) and, dually, the disturbances are implicitly represented in the detection subproblem (7) in terms of the standard problem parameters. There is no principal limitation in the design method suggested in this paper which forbid two different standard problems with different internal weightings to be applied in the control design subproblem (6) and the FDI design subproblem (7). However, it will complicate the design process and must be motivated well by the specific application.

5. CONCLUSIONS

In this paper an algorithm has been provided for designing a single module which comprises both feedback control action and fault diagnosis and isolation.

The design method is very flexible. Manipulating weights, the following four objectives can be designed for explicitly:

- following references and rejecting disturbances robustly
- controlling the system such that undetected failures do not have disastrous effects
- reducing the number of false alarms
- identifying which faults have occured

The algorithm was based on a type of separation principle which facilitates transparency in the design process with respect to the fundamental trade-offs related to diagnosing and controlling a system.

Not only the *processes* of designing a filter and a controller, but also the design *criteria* have been separated. This shows that the controller does not need to be detuned in order to implement a good fault detection mechanism. Moreover, this statement holds for optimization with respect to any choice of (norm based) design criteria, formulated as one criterion for the controller and another for the filter.

6. REFERENCES

Ajbar, H. and J.C. Kantor (1993). An ℓ_∞ approach to robust control and fault detection. In: *Proceedings of the American Control Conference*. San Francisco, CA, USA. pp. 3197–3201.

Blanke, M., S.A. Bøgh, R.B. Jørgensen and R.J. Patton (1995). Fault detection for a diesel engine actuator - A benchmark for FDI. *Control Eng. Practice* **3**, 1731–1740.

Bokor, E.A.J. and L. Keviczky (1994). An $\mathcal{H}_\infty$ filtering approach to robust detection of failures in dynamical systems. In: *Proceedings of the 33rd Conference on Decision and Control*. Lake Buena Vista, FL, USA. pp. 3037–3039.

Frank, P.M. (1990). Fault diagnosis in dynamic systems using analytic and knowledge-based redundancy - A survey and some new results. *Automatica* **26**, 459–474.

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

Garcia, E.A., B. Köppen-Seliger and P.M. Frank (1995). A frequency domain approach to residual generation for the industrial actuator benchmark. *Control Eng. Practice* **3**, 1747–1750.

Grainger, R.W., J. Holst, A.J. Isaksson and B.M. Ninness (1995). A parameteric statistical approach to FDI for the industrial actuator benchmark. *Control Eng. Practice* **3**, 1757–1762.

Jørgensen, R.B., R.J. Patton and J. Chen (1995). An eigenstructure assignment approach to FDI for the industrial actuator benchmark test. *Control Eng. Practice* **3**, 1751–1756.

Kwakernaak, H. (1993). Robust control and $\mathcal{H}_\infty$-optimization. *Automatica* **29(2)**, 255–273.

Magni, J.F. and P. Mouyon (1991). A generalized approach to observers for fault diagnosis. In: *Proceedings of the 30th Conference on Decision and Control*. Brighton, England. pp. 2236–2241.

Mangoubi, R.S., B.D. Appleby, G.C. Verghese and W.E. VanderVelde (1995). A robust failure detection and isolation algorithm. In: *Proceedings of the 34th Conference on Decision and Control*. New Orleans, LA, USA. pp. 2377–2382.

Nett, C.N., C.A. Jacobson and A.T. Miller (1988). An integrated approach to controls and diagnostics: The 4-parameter controller. In: *Proceedings of the American Control Conference*. pp. 824–835.

Patton, R., P. Frank and R. Clark (1989). *Fault diagnosis in dynamic systems - Theory and application*. Prentice Hall.

Patton, R.J. and J. Chen (1991). Robust fault detection using eigenstructure assignment: A tutorial consideration and some new results. In: *Proceedings of the 30th Conference on Decision and Control*. Brighton, England. pp. 2242–2247.

Qiu, Z. and J. Gertler (1993). Robust FDI systems and $\mathcal{H}_\infty$ optimization. In: *Proceedings of the 32nd Conference on Decision and Control*. San Antonio, Texas, USA. pp. 1710–1715.

Tyler, M.L. and M. Morari (1994). Optimal and robust design of integrated control and diagnostic modules. Baltimore, MD. pp. 2060–2064.

Wang, Y.Y. and N.E. Wu (1993). An approach to configuration of robust control systems for robust failure detection. In: *Proceedings of the 32nd Conference on Decision and Control*. San Antonio, Texas, USA. pp. 1704–1709.

Youla, D.C., H.A. Jabr and J.J. Bongiorno (1971). Modern Wiener-Hopf design of optimal controllers, part II. *IEEE Transactions on Automatic Control* **21**, 319–338.

Zhou, Kemin, John C. Doyle and Keith Glover (1996). *Robust and Optimal Control*. Prentice Hall.