Integrated Control and Fault Diagnosis Design: A Polynomial Approach

J. Stoustrup*   M.J. Grimble†

Abstract

A design method is presented which integrates control action and fault detection and isolation. Control systems operating under potentially faulty conditions are considered, and it is demonstrated how to design a single unit which handle both the required control action, as well as identifying faults occuring in actuators and sensors. 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 polynomial $\mathcal{H}_\infty$ formulation which makes weight selection straightforward. As a consequence of the separation between control and diagnosis, we shall prove that the controller needs not be detuned in order to get good diagnosis results, in contrast to common beliefs.

1 Introduction

In the control of industrial systems, it is rare 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. In this paper 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.

A useful survey on early work on FDI can be found in [Fra90] and in [PFC89]. Many of these techniques are observer based, such as e.g. [MM91]. These methods have since been refined and extended. A more recent reference in this line of research is [FD94]. The original idea of utilizing the information already available in the 'observer' part of a controller for diagnostic purposes was given in [NJM88].

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 [PC91, MAVV95, QG93, BK94, WW93]. All these methods use frequency domain techniques in contrast to [AK93] which uses ℓ_∞ techniques.

*Department of Mathematics, Technical University of Denmark, Building 303, DK-2800 Lyngby, Denmark. WWW: http://www.mat.dtu.dk/IEEE/js.html . E-mail: jakob@mat.dtu.dk .

†Industrial Control Centre, University of Strathclyde, Graham Hills Building, 50 George Street, Glasgow G1 1QE, Scotland. E-mail: m.grimble@eee.strath.ac.uk

2 Problem Formulation

We consider a control problem given in standard configuration (see e.g. [ZDG96] for an introduction to the standard configuration paradigm).

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

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 z_c sufficiently small.

For the standard problem (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 will 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 to introduce perturbed measurement and control signals, i.e., the measurements 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 $u_c + f_a \equiv 0$ could be the results of 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:

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

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 2. Defining:

$$\xi = \begin{pmatrix} x \\ x_a \\ x_s \end{pmatrix}, \; w = \begin{pmatrix} w_d \\ w_a \\ w_s \end{pmatrix}, \; u = \begin{pmatrix} u_c \\ u_f \end{pmatrix}, \; z = \begin{pmatrix} z_c \\ z_f \end{pmatrix}, \; y = y_c + f_s \tag{2}$$

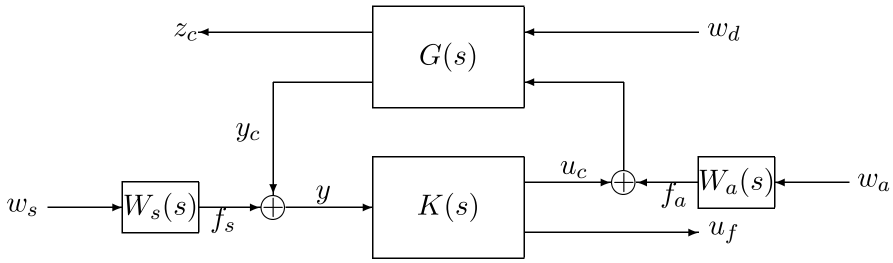

Figure 1: Control system with faults and diagnostics

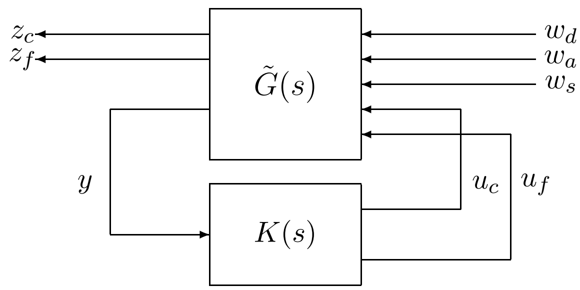

Figure 2: Standard model for integrated control and FDI

the standard problem depicted in Figure 2 takes the form (detailed formulae are given further below):

$$\begin{pmatrix} z \\ y \end{pmatrix} = \tilde{G}(s) \begin{pmatrix} w \\ u \end{pmatrix} = \begin{pmatrix} \tilde{G}_{11}(s) & \tilde{G}_{12}(s) \\ \tilde{G}_{21}(s) & \tilde{G}_{22}(s) \end{pmatrix} \begin{pmatrix} w \\ u \end{pmatrix} \tag{3}$$

Using $\mathcal{H}_\infty$ optimization, a generalized controller $u = K(s)y$ for Figure 2 can now be computed, which will then be able to generate both control signals and failure estimates.

3 Main Results

Using the partition (1), the following expressions for the standard problem (3), depicted in Figures 2, can be derived.

$$\begin{aligned} \left(\frac{z}{y}\right) &= \begin{pmatrix} z_c \\ z_f \\ \hline y \end{pmatrix} = \tilde{G}(s) \left(\frac{w}{u}\right) = \left(\begin{array}{c|c} \tilde{G}_{11}(s) & \tilde{G}_{12}(s) \\ \hline \tilde{G}_{21}(s) & \tilde{G}_{22}(s) \end{array}\right) \left(\frac{w}{u}\right) \\ &= \left(\begin{array}{ccc|cc} G_{11}(s) & G_{12}(s)W_a(s) & 0 & G_{12}(s) & 0 \\ 0 & W_a(s) & W_s(s) & 0 & -I \\ \hline G_{21}(s) & G_{22}(s)W_a(s) & W_s(s) & G_{22}(s) & 0 \end{array}\right) \begin{pmatrix} w_d \\ w_a \\ w_s \\ \hline u_c \\ u_f \end{pmatrix} \end{aligned}$$

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

$$\begin{pmatrix} z_c \\ z_f \end{pmatrix} = T_{zw}(s) \begin{pmatrix} w_d \\ w_a \\ w_s \end{pmatrix}, \quad \text{where} \quad T_{zw}(s) = \tilde{G}_{11}(s) + \tilde{G}_{12}(s)K(s)\left(I - \tilde{G}_{22}(s)K(s)\right)^{-1}\tilde{G}_{21}(s)$$

We shall now introduce a substitution, which for an open loop stable system would be simply the YJBK parameterization [YJB71] of all stabilizing controllers:

$$Q(s) = K(s)\left(I - \tilde{G}_{22}(s)K(s)\right)^{-1}, \qquad K(s) = Q(s)\left(I + \tilde{G}_{22}(s)Q(s)\right)^{-1}, \qquad Q(s) = \begin{pmatrix} Q_1(s) \\ Q_2(s) \end{pmatrix}$$

by which the following expression is obtained

$$T_{zw}(s) = \begin{pmatrix} G_{11}(s) + G_{12}(s)Q_1(s)G_{21}(s) & G_{12}(s)\left(I + Q_1(s)G_{22}(s)\right)W_a(s) & G_{12}(s)Q_1(s)W_s(s) \\ -Q_2(s)G_{21}(s) & \left(I - Q_2(s)G_{22}(s)\right)W_a(s) & -Q_2(s)W_s(s) \end{pmatrix}$$

Now, the crucial observation in this expression is that the each of the two rows of the block partitioned matrix 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. Doing the optimizations 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 [SN96].

Without loss of generality, it can be assume that all weightings have been chosen in order to normalize the $\mathcal{H}_\infty$ standard problem. This means that after separating the optimizations for z_c and z_f, we are faced with the following $\mathcal{H}_\infty$ optimization constraints:

$$\left\| \begin{pmatrix} G_{11}(s) + G_{12}(s)Q_1(s)G_{21}(s) & G_{12}(s)\left(I + Q_1(s)G_{22}(s)\right)W_a(s) & G_{12}(s)Q_1(s)W_s(s) \end{pmatrix} \right\|_\infty < 1 \tag{4}$$

and

$$\left\| \begin{pmatrix} -Q_2(s)G_{21}(s) & \left(I - Q_2(s)G_{22}(s)\right)W_a(s) & -Q_2(s)W_s(s) \end{pmatrix} \right\|_\infty < 1 \tag{5}$$

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:

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

For (5) the associated standard problem is:

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

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

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

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

$$K_1(s) = Q_1(s)\left(I + G_{22}(s)Q_1(s)\right)^{-1}, \qquad K_2(s) = Q_2(s)\left(I + G_{22}(s)Q_1(s)\right)^{-1} \tag{8}$$

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 the control action does not depend on the fault filtering dynamics.

The final step in devising the combined control and FDI device is to solve the two model matching problems (6) and (7). Using the separation idea above and polynomial $\mathcal{H}_\infty$ theory (see [Kwa93]) we can establish our main result.

Theorem 1 *Consider the setup depicted in Figure 1 where $K(s)$ is a combined controller and FDI module. Introduce the following two J-spectral factorizations:*

$$\Pi_1 = \begin{pmatrix} I & 0 \\ 0 & -G_{12}^{\sim} \end{pmatrix} \begin{pmatrix} -G_{21}G_{21}^{\sim} - G_{22}W_aW_a^{\sim}G_{22}^{\sim} - W_sW_s^{\sim} & -G_{21}G_{11}^{\sim} - G_{21}W_aW_a^{\sim}G_{12}^{\sim} \\ -G_{11}G_{21}^{\sim} - G_{12}W_aW_a^{\sim}G_{21}^{\sim} & I - G_{11}G_{11}^{\sim} - G_{12}W_aW_a^{\sim}G_{12}^{\sim} \end{pmatrix}^{-1} \times \begin{pmatrix} I & 0 \\ 0 & -G_{12} \end{pmatrix} = Z_1^{\sim}J_1Z_1$$

and

$$\Pi_2 = \begin{pmatrix} -G_{21}G_{21}^{\sim} - G_{22}W_aW_a^{\sim}G_{22}^{\sim} - W_sW_s^{\sim} & -G_{22}W_aW_a^{\sim} - W_sW_s^{\sim} \\ -W_aW_a^{\sim}G_{22}^{\sim} - W_sW_s^{\sim} & I - W_aW_a^{\sim} - W_sW_s^{\sim} \end{pmatrix}^{-1} = Z_2^{\sim}J_2Z_2$$

where $Z_i(s)$, $i \in \{1,2\}$, are square matrices which are invertible as elements of $\mathcal{RH}_\infty$, and J_i, $i \in \{1,2\}$, are constant matrices of the form

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

with a suitable number of 1's and -1's. J_i, $i \in \{1,2\}$, are called the signature matrices of Π_i, $i \in \{1,2\}$. Moreover, define the following two transfer functions

$$Q_i(s) = \begin{pmatrix} 0 & I \end{pmatrix} Z_i^{-1}(s) \begin{pmatrix} I \\ 0 \end{pmatrix} \left(\begin{pmatrix} I & 0 \end{pmatrix} Z_i^{-1}(s) \begin{pmatrix} I \\ 0 \end{pmatrix} \right)^{-1} \tag{9}$$

Then, the following two statements are equivalent:

1. *There exists a transfer matrix $K(s)$ 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 controllers $Q_1(s)$ and $Q_2(s)$ given by (9) stabilize the standard problems given by (6) and (7), respectively.*

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

Using Theorem 1 for solving the $\mathcal{H}_\infty$ problem depicted in Figure 2 actually implies making six transfer functions small due to the definitions (2) of w and z. In fact, the essential instrument for creating a well functioning module for control action and fault detection and isolation is to apply an optimization 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:

- making $\|T_{z_cw_d}\|_\infty$ small implies good disturbance rejection and robustness, i.e. the original control objectives are achieved

- making $\|T_{z_c w_a}\|_\infty$ and $\|T_{z_c w_s}\|_\infty$ small implies that undetected failures do not cause disastrous effects
- 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
- 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

In order not to complicate the exhibition 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 (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 1 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 and reducing the number of false alarms. 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, and also making the control design tolerant to minor undiscovered errors.

4 Conclusions

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

The design method is very flexible. Manipulating weights, the following four objectives can be traded off 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 proces 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 have been separated, but also the design *criteria*. 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 any choice of norm based design criteria formulated as one condition for the controller and another for the filter.

References

[AK93] H. Ajbar and J.C. Kantor. An ℓ_∞ approach to robust control and fault detection. In *Proceedings of the American Control Conference*, pages 3197–3201, San Francisco, CA, USA, 1993.

[BK94] E.A.J. Bokor and L. Keviczky. An $\mathcal{H}_\infty$ filtering approach to robust detection of failures in dynamical systems. In *Proceedings of the 33rd Conference on Decision and Control*, pages 3037–3039, Lake Buena Vista, FL, USA, 1994.

[FD94] P.M. Frank and X. Ding. Frequency domain approach to optimally robust residual generation and evaluation for model-based fault diagnosis. *Automatica*, 30:789–804, 1994.

[Fra90] P.M. Frank. Fault diagnosis in dynamic systems using analytic and knowledge-based redundancy - A survey and some new results. *Automatica*, 26:459–474, 1990.

[Kwa93] H. Kwakernaak. Robust control and $\mathcal{H}_\infty$-optimization. *Automatica*, 29(2):255–273, March 1993.

[MAVV95] R.S. Mangoubi, B.D. Appleby, G.C. Verghese, and W.E. VanderVelde. A robust failure detection and isolation algorithm. In *Proceedings of the 34th Conference on Decision and Control*, pages 2377–2382, New Orleans, LA, USA, 1995.

[MM91] J.F. Magni and P. Mouyon. A generalized approach to observers for fault diagnosis. In *Proceedings of the 30th Conference on Decision and Control*, pages 2236–2241, Brighton, England, 1991.

[NJM88] C.N. Nett, C.A. Jacobson, and A.T. Miller. An integrated approach to controls and diagnostics: The 4-parameter controller. In *Proceedings of the American Control Conference*, pages 824–835, 1988.

[PC91] R.J. Patton and J. Chen. Robust fault detection using eigenstructure assignment: A tutorial consideration and some new results. In *Proceedings of the 30th Conference on Decision and Control*, pages 2242–2247, Brighton, England, 1991.

[PFC89] R. Patton, P. Frank, and R. Clark. *Fault diagnosis in dynamic systems - Theory and application*. Prentice Hall, 1989.

[QG93] Z. Qiu and J. Gertler. Robust FDI systems and $\mathcal{H}_\infty$ optimization. In *Proceedings of the 32nd Conference on Decision and Control*, pages 1710–1715, San Antonio, Texas, USA, 1993.

[SN96] J. Stoustrup and H.H. Niemann. Multi objective control for multivariable systems with mixed sensitivity specifications. *International Journal of Control*, 1996. To appear.

[WW93] Y.Y. Wang and N.E. Wu. An approach to configuration of robust control systems for robust failure detection. In *Proceedings of the 32nd Conference on Decision and Control*, pages 1704–1709, San Antonio, Texas, USA, 1993.

[YJB71] D.C. Youla, H.A. Jabr, and J.J. Bongiorno. Modern Wiener-Hopf design of optimal controllers, part II. *IEEE Transactions on Automatic Control*, 21:319–338, 1971.

[ZDG96] Kemin Zhou, John C. Doyle, and Keith Glover. *Robust and Optimal Control*. Prentice Hall, 1996.