FAULT TOLERANT FEEDBACK CONTROL USING THE YOULA PARAMETERIZATION

Jakob Stoustrup*, **Henrik Niemann**†

* Dept. of Control Engineering, Aalborg University
DK-9220 Aalborg, Denmark
e-mail: jakob@control.auc.dk
http://www.control.auc.dk/~jakob
† Ørsted●DTU, Automation, Technical University of Denmark
DK-2800 Lyngby, Denmark
e-mail: hhn@oersted.dtu.dk
http://www.oersted.dtu.dk/~hhn

Keywords: Fault diagnosis, fault estimation, state estimation, fault tolerant control, feedback control.

Abstract

An architecture for fault tolerant feedback controllers based on the Youla parameterization is suggested. It is shown that the Youla parameterization will give a residual vector directly in connection with the fault diagnosis part of the fault tolerant feedback controller. It turns out that there is a separation between the feedback controller and the fault tolerant part. The closed loop feedback properties are handled by the nominal feedback controller and the fault tolerant part is handled by the design of the Youla parameter. The design of the fault tolerant part will not affect the design of the nominal feedback controller.

1 Introduction

The area of fault tolerant control is a new area and not a very mature one. However, there is a number of survey papers that gives a good introduction to the area, see e.g. [1, 11, 12]. In spite of the area of fault tolerant control being a new area, there exists a number of different concepts/architectures for obtaining fault tolerant feedback control. Some of the applied methods/approaches are ad-hoc methods that work quite well in practice. Others are more theoretical based methods.

The concept of fault tolerant control (or reconfigurable control) is closely related to the area of robust control, fault diagnosis and supervision, see [12], where all the areas are shortly described together with a list of key results in every area the last years. The fault tolerant feedback control problem can be considered from an analytical point of view and uses standard design methods. A description of these analytical based methods can be found in see e.g. [6, 8, 9, 10, 14, 16]. As an alternative to the analytical methods, several algorithm based methods can be applied, see e.g. the suggested architecture for implementation of fault tolerant controllers given in [1]. The architecture consists of a number of levels, where some of the levels include analytical based algorithms, others logic based algorithms and others a combination. Most of the fault tolerant controller architectures include a combination of analytical and logic based algorithms, [1, 12]. Compared to standard robust feedback controllers, fault tolerant feedback controllers has a quite more complex structure, which make it more difficult to design optimal fault tolerant controllers than robust feedback controllers.

The concept/architecture for a fault tolerant controller that will be considered in this paper is based on the Youla parameterization of all stabilizing controllers for a dynamical system, [17]. The Youla controller architecture has a number of features that are very useful in connection with fault tolerant feedback controllers. This includes the simple way to describe all controllers that will stabilize a system, an easy way to change controllers on-line without affecting the stability. Another important aspect of the Youla architecture is the possibility to get a residual vector directly that can be applied for fault diagnosis. Using the reorganized implementation of the Youla parameterization described in [15], it turns out that the input vector to the Youla parameter is directly a residual vector, see the design of residual generators by using factorization in e.g. [3, 4]. All together, the Youla architecture includes the main parts of a fault tolerant feedback controller. It is therefore obvious to investigate the Youla architecture in connection with fault tolerant feedback control.

The main result in this paper is an architecture for fault tolerant feedback controllers based on the Youla architecture. It will be shown that by reorganizing the standard Youla controller as done in [15], it is possible to get a residual generator in the controller, and to get a separation between feedback control and fault tolerance with respect to additive faults. This separation gives a very simple design of the fault tolerant part of the controller. This design will not affect the closed loop performance obtained by the nominal controller.

The approach presented here is only assumed to handle a single fault at any time. It is quite easy to generalize the approach to handle more than a single fault at any time, but the controller structure can/will get more complicated in that case.

The rest of the paper is organized as follows. The system setup is given in Section 2 together with a short introduction to coprime factorization of dynamical systems and a formulation of a fault tolerant feedback control problem. Section 3 includes the main results of this paper, where the fault tolerant control problem is formulated as a number of $\mathcal{H}_\infty$ problems. The paper is closed by a conclusion in Section 4.

2 System Setup and Problem Formulation

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

$$\Sigma : \left\{ \begin{array}{rclcccc} \dot{x} & = & Ax & + & B_f f & + & B_u u \\ z & = & C_z x & & & + & D_{zu} u \\ y & = & C_y x & + & D_{yf} f & + & D_{yu} u \end{array} \right. \tag{1}$$

where $x \in \mathcal{R}^n$ is the state vector, $u \in \mathcal{R}^m$ is the control input vector, $z \in \mathcal{R}^q$ is the output vector to be controlled, and $y \in \mathcal{R}^p$ is the measurement vector. The fault signal vector $f \in \mathcal{R}^k$ is a collection of fault signals f_i, $i = 1, 2, \ldots, k$, into a vector. Further, the coefficient matrices B_f and D_{yf} are referred to in the literature as failure signatures associated with the fault vector f. Furthermore, the coefficient matrices $B_{f,i}$ and $D_{yf,i}$ are referred to in the literature as failure signatures associated with the i-th fault, while f_i itself is called the i-th fault signal. Obviously, the failure signatures $B_{f,i}$ and $D_{yf,i}$ depend on the physics of the given system.

The system setup given in (1) can be rewritten in a transfer function form given by:

$$\begin{array}{rcl} z(s) & = & C_z(sI-A)^{-1}B_f f(s) \\ & & +(C_z(sI-A)^{-1}B + D_{zu})u(s) \\ & = & G_{zf}(s)f(s) + G_{zu}(s)u(s) \\ y(s) & = & (C_y(sI-A)^{-1}B_f + D_{yf})f(s) \\ & & +(C_y(sI-A)^{-1}B + D_{yu})u(s) \\ & = & G_{yf}(s)f(s) + G_{yu}(s)u(s) \end{array}$$

The above system description in (1) includes both actuator faults, sensor faults and plant faults by a proper selection of the failure signatures (B_f, D_{yf}), [14].

Now, let a coprime factorization of the system $G_{yu}(s) = C_y(sI-A)^{-1}B_u + D_{yu}$ from (1) and a stabilizing controller $K(s)$ be given by:

$$\begin{array}{lll} G_{yu} & = N_u M^{-1} = \tilde{M}^{-1}\tilde{N}_u, & N_u, M, \tilde{N}_u, \tilde{M} \in \mathcal{RH}_\infty \\ K & = UV^{-1} = \tilde{V}^{-1}\tilde{U}, & U, V, \tilde{U}, \tilde{V} \in \mathcal{RH}_\infty \end{array} \tag{2}$$

where the eight matrices in (2) must satisfy the double Bezout equation given by, see [17]:

$$\begin{array}{rcl} \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix} & = & \begin{pmatrix} \tilde{V} & -\tilde{U} \\ -\tilde{N}_u & \tilde{M} \end{pmatrix} \begin{pmatrix} M & U \\ N_u & V \end{pmatrix} \\ & = & \begin{pmatrix} M & U \\ N_u & V \end{pmatrix} \begin{pmatrix} \tilde{V} & -\tilde{U} \\ -\tilde{N}_u & \tilde{M} \end{pmatrix} \end{array} \tag{3}$$

Let the controller $K(s)$ be an observer based feedback controller given by:

$$K(s) = \left(\begin{array}{c|c} A + B_u F + HC_y + HD_{yu}F & -H \\ \hline F & 0 \end{array} \right) \tag{4}$$

where F is a stabilizing state feedback gain such that $A + B_u F$ is stable and H is a stabilizing observer gain such that $A + HC_y$ is stable. One possible way to construct the eight stable coprime matrices in (2) is then:

$$\begin{array}{rcl} \begin{pmatrix} M & U \\ N_u & V \end{pmatrix} & = & \left(\begin{array}{c|cc} A + B_u F & B_u & -H \\ \hline F & I & 0 \\ C_{yF} & D_{yu} & I \end{array} \right) \\ \begin{pmatrix} \tilde{V} & -\tilde{U} \\ -\tilde{N}_u & \tilde{M} \end{pmatrix} & = & \left(\begin{array}{c|cc} A + HC_y & -B_{yH} & H \\ \hline F & I & 0 \\ C_y & -D_{yu} & I \end{array} \right) \end{array} \tag{5}$$

with $C_{yF} = C_y + D_{yu}F$ and $B_{yH} = B_y + HD_{yu}$.

Based on the above coprime factorization of the system $G_{yu}(s)$ and the controller $K(s)$, we can give a parameterization of all controllers that stabilize the system in terms of a stable parameter $Q_c(s)$, i.e. all stabilizing controllers are given by [15]:

$$K(Q_c) = U(Q_c)V(Q_c)^{-1} \tag{6}$$

where

$$U(Q_c) = U + MQ_c,\ V(Q_c) = V + N_u Q_c,\ Q_c \in \mathcal{RH}_\infty$$

or by using a left factored form:

$$K(Q_c) = \tilde{V}(Q_c)^{-1}\tilde{U}(Q_c) \tag{7}$$

where

$$\tilde{U}(Q_c) = \tilde{U} + Q_c\tilde{M},\ \tilde{V}(Q_c) = \tilde{V} + Q_c\tilde{N}_u,\ Q_c \in \mathcal{RH}_\infty$$

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

$$K(Q_c) = \mathcal{F}_l(J_K, Q_c) \tag{8}$$

where J_K is given by

$$J_K = \begin{pmatrix} UV^{-1} & \tilde{V}^{-1} \\ V^{-1} & -V^{-1}N_u \end{pmatrix} = \begin{pmatrix} \tilde{V}^{-1}\tilde{U} & \tilde{V}^{-1} \\ V^{-1} & -V^{-1}N_u \end{pmatrix} \tag{9}$$

Introducing the transfer function from fault f output y given by G_{yf} from (1) in connection with the coprime factorization of G_{yu} in (2), we obtain the following relationship:

$$y = \begin{pmatrix} G_{yf} & G_{yu} \end{pmatrix} \begin{pmatrix} f \\ u \end{pmatrix} = \tilde{M}^{-1} \begin{pmatrix} \tilde{N}_f & \tilde{N}_u \end{pmatrix} \begin{pmatrix} f \\ u \end{pmatrix}$$

Reorganizing the controller $K(Q_c)$ given by (8) results in the closed loop system depicted in Figure 1, [15].

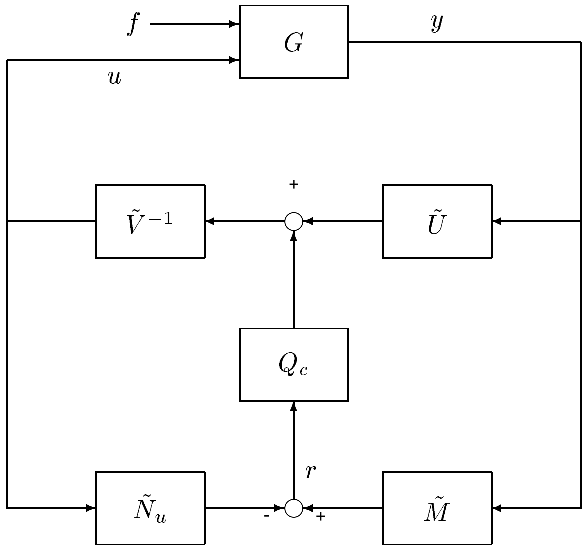

Figure 1: Controller structure with parameterization

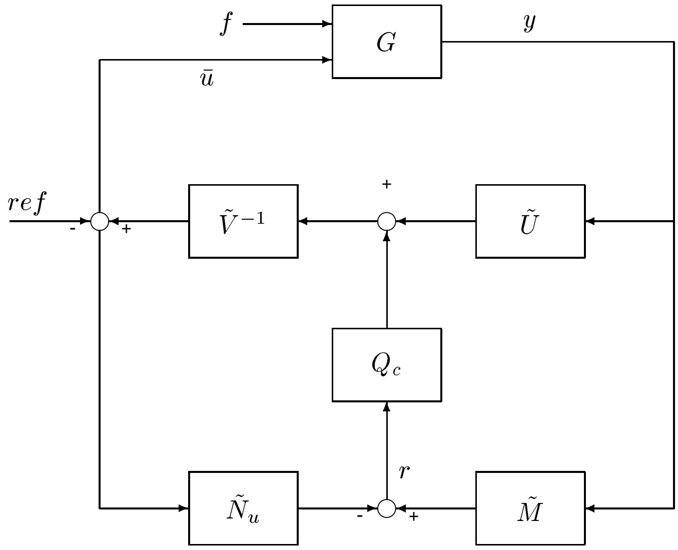

Figure 2: Controller structure with parameterization and reference input

The main observation which shall be exploited in the solution to the fault tolerant control problem, is the following very simple expression for the transfer function from faults to measurements in terms of the parameter Q_c:

$$\begin{aligned} y &= \tilde{M}^{-1}\left(\tilde{N}_f f + \tilde{N}_u u\right) \\ &= \tilde{M}^{-1}\left(\tilde{N}_f f + \tilde{N}_u \tilde{V}^{-1}\left(\tilde{U}y + Q_c \tilde{N}_f f\right)\right) \\ &= \left(\tilde{M} - \tilde{N}_u \tilde{V}^{-1}\tilde{U}\right)^{-1}\left(I + \tilde{N}_u \tilde{V}^{-1} Q_c\right)\tilde{N}_f f \\ &= V\left(\tilde{N}_u \tilde{V}^{-1} Q_c + I\right)\tilde{N}_f f \\ &= \left(V + N_u Q_c\right)\tilde{N}_f f \end{aligned}$$

where (3) has been exploited.

Another crucial observation is that the signal r in Figure 1 depends in a very simple way on the fault signals f:

$$r = \tilde{M}\left(\tilde{M}^{-1}\left(\tilde{N}_f f + \tilde{N}_u u\right)\right) - \tilde{N}_u u = \tilde{N}_f f$$

Hence, r is automatically a fault residual vector. This is equivalent with the calculation of the residual vector by using factorization as described in [3, 4].

In the setup given in Figure 1, the only input signal is the fault signal. Normally, a reference input vector will also be included. It is also possible to include a reference input vector in the setup given in Figure 1. However, the reference input vector cannot be placed arbitrarily in the setup. The input vector needs to be placed such that the fault residual vector r is independent of the input signal. The reference input vector needs to be placed inside the controller to obtain that the vector is not observable in r. In Figure 2, the reference input vector ref is included.

From Figure 2, we get directly that

$$\begin{aligned} r &= \tilde{M}y - \tilde{N}_u \bar{u} \\ &= \tilde{M}G(u - ref) - \tilde{N}_u(u - ref) \\ &= 0 \end{aligned}$$

for $f = 0$ and where $\bar{u} = u - ref$. This shows that it is possible to include a reference input vector in the setup without r depending on the vector. A reference input vector will not be included in the following, though.

3 Main Results

We propose a solution to the fault tolerant control problem which is depicted in Figure 3 for the case with three faults. The two controllers Q_c and Q_f are the controller for fault rejection and the “controller” for residual generation, respectively. Q_f is normally named as the residual generator, [2].

Each of the Q_{ci} in Figure 3 is a solution to an $\mathcal{H}_\infty$ model matching problem of the form:

$$\left\| W_{ci}\left(V + N_u Q_{ci}\right)\tilde{N}_{fi}\right\|_\infty < \gamma_{ci} \qquad (10)$$

where γ_{ci} is a real positive number, W_{ci} is some weighting matrix, and $\tilde{N}_{fi}$ denotes the ith column of $\tilde{N}_f$. This suboptimal formulation conforms with the commercial software packages, although (10) actually admits an optimal solution.

In connection with the optimization of the (10), it is important to note that V is a proper matrix. Therefore, if N_u is not a proper matrix, a lower bound on γ_{ci} is given by:

$$\left\| W_{ci}\tilde{N}_{fi}(\infty)\right\|_\infty < \gamma_{ci}$$

The weighting matrix W_{ci} that is included in (10) must be selected to take care of the $\mathcal{H}_\infty$ norm at high frequencies.

It needs to be pointed out that other design methods than $\mathcal{H}_\infty$ optimization of the transfer function from f to y can be applied.

Similarly, each of the Q_{fi} in Figure 3 is the ith row of Q_f which in turn is a solution to an $\mathcal{H}_\infty$ model matching problem

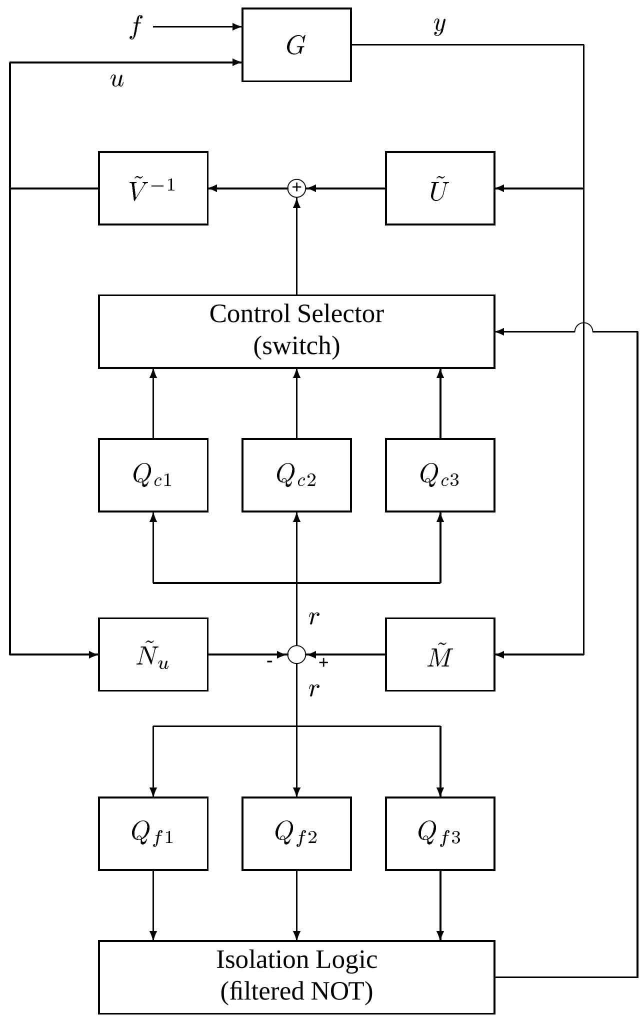

Figure 3: Fault tolerant scheme with three potential faults, $f = (f_1\ f_2\ f_3)^T$

of the form:

$$\left\| W_f \left(I - Q_f \tilde{N}_f \right) \right\|_\infty < \gamma_f \qquad (11)$$

where γ_f is a real positive number and W_f is some weighting matrix. The design of Q_f in (11) can also be separated into single designs of each Q_{fi} as in (10). The disadvantage in both cases to apply 3 single designs for Q_c and Q_f is the order of the controller dynamic will be 3 times larger compared with two combined designs.

A possible suboptimal solution can be found in just one design step from the following $\mathcal{H}_\infty$ (model matching) standard model:

$$\tilde{G} = \begin{pmatrix} \tilde{G}_{\tilde{z}\tilde{w}} & \tilde{G}_{\tilde{z}\tilde{u}} \\ \tilde{G}_{\tilde{y}\tilde{w}} & \tilde{G}_{\tilde{y}\tilde{u}} \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} W_c V \tilde{N}_f \\ W_f \end{pmatrix} & \begin{pmatrix} W_c N_u \\ W_f \end{pmatrix} \\ \tilde{N}_f & 0 \end{pmatrix}$$

A solution Q that makes

$$\left\| \mathcal{LFT} \left(\tilde{G}, Q \right) \right\|_\infty < \gamma$$

can be partitioned as

$$Q = \begin{pmatrix} Q_c \\ Q_f \end{pmatrix}$$

where the rows of Q_c constitutes the Q_{ci}'s and the rows of Q_f constitutes the Q_{fi}'s.

In fact, a rational suboptimal implementation uses only *one multivariable* Q which provides all Q_{ci} and Q_{fi} outputs.

However, the design of the residual generator Q_f does not necessarily have to be done by using an $\mathcal{H}_\infty$ optimization method. Instead of using an $\mathcal{H}_\infty$ optimization of the residual generator, methods as e.g. eigenstructure assignment, parity equations, to mention a few methods. An introduction to these design methods together with other design methods can be found in e.g. [2, 5]. In the case when it is possible to obtain exact fault isolation, [7, 13], the design methods from [13] can be applied.

Until now, only the disturbance free nominal fault tolerant feedback control problem has been considered. In real applications, the system will include both disturbances and model uncertainties. Both disturbances and model uncertainties will affect the design of the fault tolerant feedback controller. Let us consider a system including disturbances described by:

$$\Sigma : \left\{ \begin{array}{ccccccccc} \dot{x} & = & Ax & + & B_d d & + & B_f f & + & B_u u \\ z & = & C_z x & + & D_{zd} d & & & + & D_{zu} u \\ y & = & C_y x & + & D_{yd} d & + & D_{yf} f & + & D_{yu} u \end{array} \right. \qquad (12)$$

where $d \in \mathcal{R}^t$ is the disturbance vector. The system can also be described by using coprime factorizations. It is then given by:

$$\begin{aligned} y &= \begin{pmatrix} G_{yf} & G_{yd} & G_{yu} \end{pmatrix} \begin{pmatrix} f \\ d \\ u \end{pmatrix} \\ &= \tilde{M}^{-1} \begin{pmatrix} \tilde{N}_f & \tilde{N}_d & \tilde{N}_u \end{pmatrix} \begin{pmatrix} f \\ d \\ u \end{pmatrix} \end{aligned}$$

The residual signal now takes the following form:

$$r = \begin{pmatrix} \tilde{N}_f & \tilde{N}_d \end{pmatrix} \begin{pmatrix} f \\ d \end{pmatrix} \tag{13}$$

It can be seen from (13) that r will depend on the disturbance. The closed loop transfer function from f and d to z is now given by

$$z = (V - N_u Q) \begin{pmatrix} \tilde{N}_f & \tilde{N}_d \end{pmatrix} \begin{pmatrix} f \\ d \end{pmatrix}$$

In the design of the Q_{ci}, the effect from the disturbance needs to be taken into account to get an optimal fault tolerant feedback controller. If the effect from the disturbance is neglected in the design of the Q_{ci}, the effect from disturbances could be increased instead of reduced in z when a fault appear in the system.

Including disturbance in the system, the design problem for Q_{ci} from (10) is then given by:

$$\left\| W_{ci} \left(V + N_u Q_{ci} \right) \begin{pmatrix} \tilde{N}_{fi} & \tilde{N}_d \end{pmatrix} \right\|_\infty < \gamma_{ci} \tag{14}$$

Only single faults appearing at the time has been considered in this paper. However, there is no restriction that limits the number of faults that appear at any time. It needs to be pointed out that conservatism might be introduced in an $\mathcal{H}_\infty$ design of the Youla parameter Q_c, if the number of faults that can appear simultaneously are higher than it will be in the actual case.

4 Conclusion

A fault tolerant feedback control problem has been considered in this paper. The connection between using the Youla parameterization to describe all stabilizing closed-loop controllers and residual generators has been considered. Using a special implementation of the Youla parameterization, the input vector to the Youla parameter is a residual vector. Based on this connection, an architecture for fault tolerant feedback controllers has been formulated. Using this fault tolerant controller architecture, there is a separation between the feedback controller part and the fault tolerant part. The design of the Youla parameter/controller turns out to be a model matching problem, that takes care of the effect from faults in the external output.

References

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

[2] J. Chen and R.J. Patton. *Robust model-based fault diagnosis for dynamic systems*. Kluwer Academic Publishers, 1999.

[3] P.M. Frank. Analytical and qualitative model-based fault diagnosis - A survey and some new results. *European Journal of Control*, 2:6–28, 1996.

[4] P.M. Frank and X. Ding. Survey of robust residual generation and evaluation methods in observer-based fault detection systems. *Journal of Process Control*, 7(6):403–424, 1997.

[5] J. Gertler. *Fault detectionand diagnosis in engineering systems*. Marcel Dekker, 1998.

[6] C.A. Jacobson and C.N. Nett. An integrated approach to controls and diagnostics using the four parameter controller. *IEEE Control Systems*, 11(6):22–29, 1991.

[7] M. Massoumnia, G.C. Verghese, and A.S. Willsky. Failure detection and identification. *IEEE Transactions on Automatic Control*, 34:316–321, 1989.

[8] G.A. Murad, I. Postlethwaite, and D.W. Gu. A robust design approach to integrated controls and diagnostics. In *Proceedings of the 13th IFAC World Congress*, volume N, pages 199–204, San Francisco, CA, USA, 1996.

[9] L.H. Mutuel and J.L. Speyer. Fault-tolerant estimation. In *Proceedings of the American Control Conference, ACC'00*, pages 3718–3722, Chicago, IL, USA, 2000.

[10] C.N. Nett, C.A. Jacobson, and A.T. Miller. A robust failure detection and isolation algorithm. In *Proceedings of American Control Conference*, pages 824–835, Atlanta, GA, USA, 1988.

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

[12] R. Patton. Where are we in fault tolerant control. Seminar notes, June 1997. Centre for Systems and Control, Faculty of Engineering, Glasgow University, Glasgow, G12 8QQ, UK.

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

[14] J. Stoustrup, M.J. Grimble, and H.H. Niemann. Design of integrated systems for control and detection of actuator/sensor faults. *Sensor Review*, 17:157–168, 1997.

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

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

[17] K. Zhou, J.C. Doyle, and K. Glover. *Robust and optimal control*. Prentice Hall, 1996.