# Active Fault Diagnosis by Controller Modification

Stoustrup, Jakob; Niemann, Henrik

*Published in:*
International Journal of Systems Science

*DOI (link to publication from Publisher):*
10.1080/00207720903470197

*Publication date:*
2010

*Document Version*
Early version, also known as pre-print

*International Journal of Systems Science*
2010, 1–12, iFirst

Taylor & Francis
Taylor & Francis Group

***Special Issue on Fault Diagnosis and Fault Tolerant Control***

# Active fault diagnosis by controller modification

Jakob Stoustrup[a]* and Henrik Niemann[b]

[a]*Department of Electronic Systems, Automation & Control, Aalborg University, Fr. Bajers Vej 7C, DK-9220, Aalborg, Denmark;* [b]*Department of Electrical Engineering, Automation and Control, Technical University of Denmark, Elektrovej, Building 326, 2800 Kgs. Lyngby, Denmark*

(*Received 4 December 2008; final version received 8 October 2009*)

Two active fault diagnosis methods for additive or parametric faults are proposed. Both methods are based on controller reconfiguration rather than on requiring an exogenous excitation signal, as it is otherwise common in active fault diagnosis. For the first method, it is assumed that the system considered is controlled by an observer-based controller. The method is then based on a number of alternate observers, each designed to be sensitive to one or more additive faults. Periodically, the observer part of the controller is changed into the sequence of fault sensitive observers. This is done in a way that guarantees the continuity of transition and global stability using a recent result on observer parameterization. An illustrative example inspired by a field study of a drag racing vehicle is given. For the second method, an active fault diagnosis method for parametric faults is proposed. The method periodically adds a term to the controller that for a short period of time renders the system unstable if a fault has occurred, which facilitates rapid fault detection. An illustrative example is given.

**Keywords:** active fault detection; parametric faults; observer parameterisation



## 1. Introduction

The task of designing a fault diagnosis system shares a number of challenges with that of performing a system identification, where the notion of persistent excitation is crucial to obtain a high quality model. Similarly, if a detection approach is based on a 'passive' approach, i.e. only by logging the unmodified inputs and outputs, faults can easily remain undetected, particularly if they are parametric and reside in a part of the system, which is never excited. Stoustrup and Niemann (1999) presents an approach to fault diagnosis for systems with parametric faults.

To that end, recently there has been significant attention to the so-called *active* fault diagnosis methods, (see e.g. Nikoukhah (1998); Nikoukhah, Campbell, and Delebecque (2000); Campbell, Nikoukhah, and Horton (2002); Campbell and Nikoukhah (2004); Niemann and Poulsen (2005); Niemann (2006) and references therein). In the active fault diagnosis methods, it is assumed to be admissible to superimpose the control input with a dedicated fault diagnosis signal, which is designed to excite the faults in such a way that they become better discernible at the output.

In this article, two other approaches are suggested to make indiscernible faults temporarily visible without having to add an external excitation signal.

The first approach proposed embarks from an observer-based controller. The main idea is then to temporarily change the observer into one, which has been tuned to be maximally sensitive to one or more specific faults. This procedure is then repeated cyclically for all faults that should be detected.

The assumption of an observer-based controller is without loss of generality, as any linear controller can be (re-) written as an observer-based controller, possibly extended by a Youla-Kucera parameter.

The proposed method can be used as an on-line algorithm, provided that emphasising the faults is acceptable. Otherwise, the method can be used off-line, meaning that the system is in a test mode (see below).

Along the same lines we will also propose a more radical approach in this article. Rather than just detuning the controller a bit to make it more sensitive to faults, in this more aggressive approach an additional term is added to the controller, intended to destabilise the system temporarily in the presence of a parametric fault. The rationale for this is that if the system becomes unstable, this will be apparent very quickly, no matter how much noise is present. Once the instability, and hence the fault has been detected, of course the destabilising controller part will be removed at once.

Destabilising the system is inadmissible for many systems. Examples of systems where the method could be applied is to discover short-circuits in electrical motors, where it might be admissible to let the magnetising currents increase shortly; a blocked air

*Corresponding author. Email: jakob@control.aau.dk

ISSN 0020–7721 print/ISSN 1464–5319 online

DOI: 10.1080/00207720903470197
http://www.informaworld.com

passage in a supermarket refrigeration system, where it could be admissible to let the air temperature drop or increase for a few minutes; or a clogging in a fermentation process, where a mass-flow can be allowed to change for some while.

Another approach for the latter method is to apply the method as an off-line fault diagnosis approach. It will be possible in many cases to do a fault diagnosis on the system when it is out of work. This example can be in connection with the service of the system. It will then be possible to do the fault diagnosis in a controlled environment. In some cases, it will be possible to place the system in a test bench. It is clear that this off-line approach can only be applied on systems with slowly varying parametric faults.

The rest of this article is organised as follows. A problem formulation is given in Section 2. Section 3 includes some preliminary results. The main results are given in Section 4 and two illustrative examples are given in Section 5. This article is closed with a conclusion in Section 6.



## 2. Problem formulation

As mentioned above, in this article we shall propose two methods for active fault diagnosis based on controller reconfiguration. In the first problem formulation, we shall seek to design the controller reconfiguration in order to sensitise the controller to a number of fault signals. In the second and more radical approach, we shall design the controller reconfiguration in order to destabilise the system temporarily in the presence of a fault.

In the sequel, we will consider a *fault* to be a phenomenon which causes a system to exhibit an abnormal and/or undesired behaviour. A *fault signal* is a signal that models the effect of a fault as a signal introduced in a differential equation or difference equation model of the nominal system. An *additive fault* is defined as a fault which can be modelled as introducing an additional additive term in the differential/difference equation model. In contrast, a *parametric fault* can be modelled better by changes to the parameters of the model. For example, for a linear system, a parametric fault could be modelled as changes to the matrices in a state space description of its model (see below).

Consider the following state space description of a given system:

$$\begin{aligned} \dot{x} &= Ax + Bu + B_d d + B_f f + B_w w, \\ z &= C_z x + D_{zu} u + D_{zd} d + D_{zf} f + D_{zw} w, \\ y &= Cx, \end{aligned} \tag{1}$$

where $u \in \mathcal{R}^{n_u}$ is the control input signal vector, $x \in \mathcal{R}^{n_x}$ is the state vector of the system, and $y \in \mathcal{R}^{n_y}$ is the measurement vector, $d \in \mathcal{R}^{n_d}$ is a vector of external disturbances and $f \in \mathcal{R}^{n_f}$ is the vector of potential additive fault signals. The auxiliary signal pair $w \in \mathcal{R}^{n_w}$ and $z \in \mathcal{R}^{n_z}$ is introduced in order to model parametric faults or faults of parasitic dynamics, which can in either case be done by closing a loop by an artificial feedback of the form

$$w = \Delta z, \tag{2}$$

where $\Delta$ represents the parametric faults in the system, or parasitic dynamics.

The feedback interconnection model of the system presented in (1) and (2) is based on the so-called standard model which is extensively used in robust control (see e.g. Zhou, Doyle, and Glover (1995)). It is well-known that a model structure of this type can be employed to represent parametric faults that can be modelled as parametric variations of the individual parameters in a state space model, where the parameters depend functionally on the faults as rational functions (of several variables). For non-rational functional dependency (e.g. $\log, \sin, \ldots,$), it can be exploited that all differentiable functions can be approximated arbitrarily well by rational functions.

Based on this general model, we shall address the following two design issues.

### 2.1. *Controller reconfiguration for fault sensitization*

We assume that the system (1) is controlled by a full-order observer-based controller given by

$$\begin{aligned} \dot{\hat{x}} &= A\hat{x} + Bu + L_0(y - C\hat{x}), \\ u &= F\hat{x}, \end{aligned}$$

where $\hat{x} \in \mathcal{R}^n$ is the estimate of the state vector, $L_0 \in \mathcal{R}^{p \times n}$ is an observer gain for which $A + L_0 C$ is Hurwitz and $F \in \mathcal{R}^{m \times n}$ is a feedback gain for which $A + BF$ is Hurwitz. Then, this controller is stabilising according to the separation theorem.

For this part, we shall consider only additive faults, i.e. we disregard the signals $w$ and $z$ in (1). Note that a diagnosis system that can detect an additive fault can also (under mild assumptions) detect a parametric fault. This holds even for closed-loop systems, provided that the control signal is known.

The challenge is now for each possible fault in the system to find alternate parameters for the observer gain $L_1, \ldots, L_q$, such that each of the corresponding observers becomes sensitive to one or more of the $q$ faults.

Furthermore, we wish to find a procedure which enables us to tune the observer gain from the nominal one-to-one of the faulty ones such that:

- the transition from the nominal observer with gain $L_0$ to any of the fault sensitised gains, $L_i$, should be performed such that no unacceptably large transients are created.
- the transition should be performed such that the stability is maintained throughout the transition.

In the subsequent sections, we shall describe a method, which embarks from such a preliminary design of a nominal and a number of fault sensitised observer gains, and constructs an observer-based feedback scheme which cycles through these observer gains in order to make sure that all faults are detected within a cycle, while at the same time preserving stability throughout the cycle.

### 2.2. *Controller reconfiguration for temporary destabilisation*

We assume that the system (1) is controlled by a stabilising feedback controller given by

$$u = K(s)\, y. \tag{3}$$

In this part, we focus on parametric faults, i.e. we disregard the signal $f$ in (1), and assume that the system is closed by an artificial feedback from $z$ to $w$, as described by (2).

The problem is now to devise a method which can discriminate a nonzero $\Delta$ as in (2) from the nominal situation, $\Delta \equiv 0$, possibly by modifying the controller $K(s)$.

In this case, the method will depend critically on the parametric nature of the fault, as an additive fault signal cannot destabilise a linear control system.

## 3. Preliminaries

In order to present the two methods proposed in this article, we shall introduce a number of preliminaries.

### 3.1. *Observer interpolation with guaranteed stability*

The first method proposed in this article relies on the following recent result from Stoustrup and Komareji (2008). The result establishes how one observer can be modified continuously into another one without transients. This idea will be exploited in the results section of this article to change a nominal observer into several other observers that have enhanced fault diagnosis properties.

**Lemma 3.1:** *Let $L_0$ and $L_1$ be two different Luenberger observer gains for the following system:*

$$\dot{x} = Ax + Bu, \quad y = Cx + du$$

*and suppose that*

$$V_0(x) = x^* Z_0 x \quad \text{and} \quad V_1(x) = x^* Z_1 x$$

*are the corresponding Lyapunov functions to $A + L_0 C$ and $A + L_1 C$, respectively, with $Z_i > 0$, $i = 0, 1$. Then a family of observer gains $L(\beta)$, $0 \le \beta \le 1$ is given by*

$$L(\beta) = \mathcal{F}_\ell\,(J_{L_0,L_1,Z}, \beta I), \tag{4}$$

*where*

$$J_{L_0,L_1,Z} = \begin{pmatrix} L_0 & I \\ Z(L_1 - L_0) & I - Z \end{pmatrix}, \quad Z = Z_0^{-1} Z_1$$

*and $\mathcal{F}_\ell(M, X)$ denotes a lower fractional transformation of $M$ by $X$ (see e.g. Stoustrup and Komareji (2008)).*

*Moreover, $L(\beta)$ satisfies $L(0) = L_0$ and $L(1) = L_1$.*

In Stoustrup and Komareji (2008) the dual result is proved. For completeness, we will give a direct proof of this (yet unpublished) result here.

**Proof:** The intermediate points admit the Lyapunov function given by

$$Z(\beta) = (1 - \beta) Z_0 + \beta Z_1.$$

To verify the above claim, we have to show that

$$Z(\beta)(A + L(\beta)C) + (A + L(\beta)C)^* Z(\beta) < 0.$$

The first term in the left-hand side of the Lyapunov inequality can be rewritten as

$$\begin{aligned}
&Z(\beta)(A + L(\beta)C) \\
&= ((1-\beta)Z_0 + \beta Z_1)(A + (L_0 + \beta(I - \beta(I - Z))^{-1} \\
&\quad \times Z(L_1 - L_0))C) \\
&= ((1-\beta)Z_0 + \beta Z_1)(A + L_0 C + \beta(I - \beta(I - Z_0^{-1} Z_1))^{-1} \\
&\quad \times Z_0^{-1} Z_1 (L_1 - L_0) C) \\
&= ((1-\beta)Z_0 + \beta Z_1)(A + L_0 C + \beta((1-\beta)Z_0 + \beta Z_1))^{-1} \\
&\quad \times Z_1 (L_1 - L_0) C) \\
&= (1-\beta) Z_0 (A + L_0 C) + \beta Z_1 (A + L_1 C).
\end{aligned}$$

From this we can conclude that

$$\begin{aligned}
&Z(\beta)(A + L(\beta)C) + (A + L(\beta)C)^* Z(\beta) \\
&\quad = (1 - \beta)(Z_0(A + L_0 C) + (A + L_0 C)^* Z_0) \\
&\qquad + \beta(Z_1(A + L_1 C) + (A + L_1 C)^* Z_1) \\
&\quad = (1 - \beta)\Psi_0 + \beta \Psi_1,
\end{aligned}$$

where

$$\Psi_0 = Z_0(A + L_0C) + (A + L_0C)^* Z_0$$

and

$$\Psi_1 = Z_1(A + L_1C) + (A + L_1C)^* Z_1.$$

According to the assumptions, $Z_0$ and $Z_1$ are Lyapunov functions for $A + L_0C$ and $A + L_1C$, respectively, i.e.

$$\Psi_0 < 0 \quad \text{and} \quad \Psi_1 < 0$$

from which we infer that

$$(1 - \beta)\Psi_0 + \beta\Psi_1 < 0,$$

which completes the proof. □

### 3.2. *The Youla-Kucera parameterisation*

The second method proposed in this article is based on the primary and dual Youla-Kucera parameterisations (see e.g. Zhou et al. 1995; Tay, Mareels, and Moore 1997), which will be introduced shortly in this section. In particular, the second method in this article proceeds by modifying the controller in terms of designing explicitly a Youla-Kucera parameter.

Let a coprime factorisation of the system $G_{yu}(s) = C(sI - A)^{-1}B$ from (1) and a stabilising controller $K(s)$ from (3) be given by:

$$\begin{aligned} G_{yu} &= NM^{-1} = \tilde{M}^{-1}\tilde{N}, \\ K &= UV^{-1} = \tilde{V}^{-1}\tilde{U}, \\ N, M, \tilde{N}, \tilde{M}, U, V, \tilde{U}, \tilde{V} &\in \mathcal{RH}_\infty, \end{aligned} \tag{5}$$

where the eight matrices in (5) must satisfy the double Bezout equation given by

$$\begin{aligned} \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix} &= \begin{pmatrix} \tilde{V} & -\tilde{U} \\ -\tilde{N} & \tilde{M} \end{pmatrix} \begin{pmatrix} M & U \\ N & V \end{pmatrix} \\ &= \begin{pmatrix} M & U \\ N & V \end{pmatrix} \begin{pmatrix} \tilde{V} & -\tilde{U} \\ -\tilde{N} & \tilde{M} \end{pmatrix}. \end{aligned} \tag{6}$$

Explicit formulae for these eight transfer matrices can be found, e.g. in Zhou et al. (1995).

Based on the above coprime factorisation of the system $G_{yu}(s)$ and the controller $K(s)$, we can give a parameterisation of all controllers that stabilise the system in terms of a stable parameter $Q(s)$, i.e. all stabilising controllers are given by Tay et al. (1997):

$$K_Q = U(Q)V(Q)^{-1}, \tag{7}$$

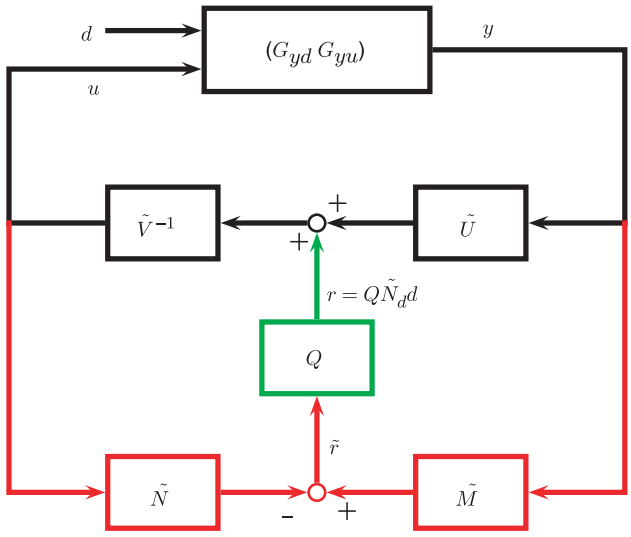


Figure 1. Controller structure with parameterisation.

where

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

or by using a left-factored form

$$K_Q = \tilde{V}(Q)^{-1}\tilde{U}(Q), \tag{8}$$

where

$$\tilde{U}(Q) = \tilde{U} + Q\tilde{M}, \quad \tilde{V}(Q) = \tilde{V} + Q\tilde{N}, \quad Q \in \mathcal{RH}_\infty.$$

Using the Bezout equation, the controller given either by (7) or by (8) can be realised as a linear fractional transformation (LFT) in the parameter $Q$,

$$K_Q = \mathcal{F}_l(J_K, Q), \tag{9}$$

where $J_K$ is given by

$$J_K = \begin{pmatrix} UV^{-1} & \tilde{V}^{-1} \\ V^{-1} & -V^{-1}N \end{pmatrix}. \tag{10}$$

Reorganising the controller $K_Q$ given by (9) results in the closed-loop system depicted in Figure 1.

Similarly, all plants stabilised by a given controller can be described by the so-called *dual* Youla-Kucera parameterisation. Indeed, all plants stabilised by a controller $K(s)$ can be described by:

$$G_f(s) = \big(N(s) + V(s)S_f(s)\big)\big(M(s) + U(s)S_f(s)\big)^{-1} \tag{11}$$

$$= \big(\tilde{M}(s) + S_f(s)\tilde{U}(s)\big)^{-1}\big(\tilde{N}(s) + S_f(s)\tilde{V}(s)\big), \tag{12}$$

where $N$, $M$, $U$, $V$ and $\tilde{N}$, $\tilde{M}$, $\tilde{U}$, $\tilde{V}$ are as described in (5) and (6), and $S_f(s) \in \mathcal{RH}_\infty$. This structure is depicted in Figure 2.

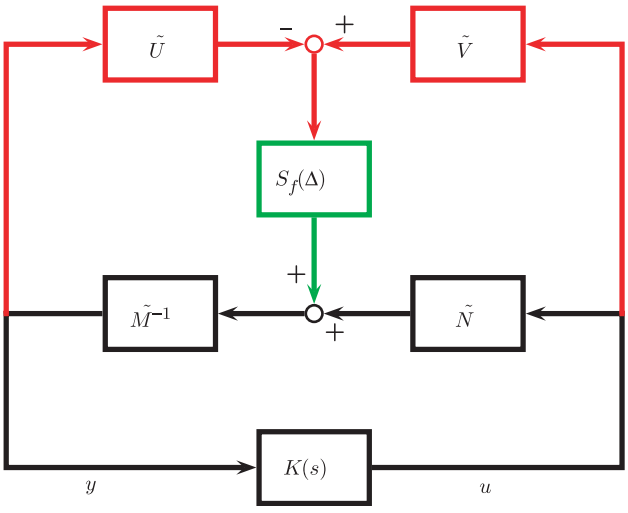


Figure 2. Plant structure with parameterisation.

For any parametric fault, there exists a unique dual Youla-Kucera parameter, Niemann (2003). In Table 1, $S_f$ has been calculated for a number of different types of parametric faults. An explicit formula for $S_f$ is

$$S_f(s) = \big(G_f(s)M(s) - N(s)\big)\big(V(s) - G_f(s)U(s)\big)^{-1} \quad (13)$$

$$= \big(\tilde{V}(s) - \tilde{U}(s)G_f(s)\big)^{-1}\big(\tilde{M}(s)G_f(s) - \tilde{N}(s)\big). \quad (14)$$

We shall use the following result in the sequel (see e.g. Tay et al. (1997)).

**Lemma 3.2:** *Let a nominal system $G_{yu}(s)$ and a nominal controller $K(s)$ with factorisations as in (5) be given. Assume that $G_f$ is given by the parameter $S_f$ as (11), and $K_Q$ is given by the parameter $Q$ as (7) or (8). The closed-loop system formed by $G_f$ and $K_Q$ is stable if and only if:*

(1) *$K$ internally stabilises $G$ and*
(2) *$Q$ internally stabilises $S_f$.*

## 4. Main results

In the sequel, we shall state two results, which will be used as a background for two corresponding algorithms.

### 4.1. *Observer tuning for fault sensitivity*

The method proposed below is based on the following theorem.

**Theorem 4.1:** *Consider a system given by a model of the form*

$$\dot{x} = Ax + B_u u,$$
$$y = Cx.$$

*Assume that a number of stabilising observer gains $L_0, L_1, \ldots, L_q$ have been designed for this system, i.e. such that $A + L_iC$, $i = 0, 1, \ldots, q$ are all Hurwitz. Further, assume that $Z_i$, $i = 0, 1, \ldots, q$ are Lyapunov matrices for the matrices $A + L_iC$, $i = 0, 1, \ldots, q$.*

*Consider an observer-based controller of the form*

$$\Sigma_C: \begin{cases} \dot{\hat{x}} = A\hat{x} + Bu + L(\beta(t))(y - C\hat{x}) \\ u = F\hat{x} \end{cases}, \quad (15)$$

*where*

$$L(\beta(t)) = \begin{cases} \mathcal{F}_\ell(J_{L_{i_0}, L_{i_1}, Z_{i_0,i_1}}, \beta(t)I) & \text{for } t_0 \le t < t_1 \\ \vdots & \\ \mathcal{F}_\ell(J_{L_{i_{q-1}}, L_{i_q}, Z_{i_{q-1},i_q}}, \beta(t)I) & \text{for } t_{N-1} \le t < t_N, \end{cases}$$

*where $Z_{i_k,i_{k+1}} = Z_k^{-1}Z_{k+1}$, and $\beta(t)$ is a slowly varying continuous function, chosen such that $L(\beta(t))$ is continuous. This latter condition is equivalent to requiring that $\beta(t_i) = 0$ or $\beta(t_i) = 1$ for all $i = 0, \ldots, N$.*

*Then, $\Sigma_C$ is a stabilising controller.*

**Proof:** Theorem 4.1 follows from Lemma 3.1. It should be noted that as the controller in Theorem 4.1 is time-varying, the Lyapunov inequalities will have an additional term. This term, however, will tend to zero as the rate of the time variation tends to zero. Note that it is straightforward to evaluate whether a given solution is actually stable by evaluating the Lyapunov function. This is only a sufficient condition, so in principle the system could be stable even if this test fails. In practice, however, this test is very useful. □

Based on this result, the fault diagnosis algorithm can now be formulated.

**Algorithm 1:** Let a system with a nominal model of the form (1) be given.

**Step 1:** Design (any) nominal observer-based controller with observer gain $L_0$ and feedback gain $F$

**Step 2:** For each fault, design a new observer gain $L_i$, $i = 1, \ldots, q$, that makes the corresponding observer sensitive to that fault.

**Step 3:** Choose a sequence of these observer gains, such that every gain appears at least once in the sequence.

**Step 4:** Design $\beta(t)$ as a continuous function that varies between 0 and 1, where constant intervals with value 0 or 1 are intervals where a certain observer is fully active.

**Step 5:** Design $\Sigma_C$ as given by (15).

Table 1. The connection between different system parametric faults in terms of $\Delta$ and the dual Youla-Kucera parameter $S_f$.

| Fault description, $G_{yu}(\Delta)$ | The dual Youla-Kucera parameter, $S_f(\Delta)$ |
|---|---|
| $G_{yu}(\Delta) = (I+\Delta)G_{yu}$ | $S_f(\Delta) = \tilde{M}\Delta(I - N\tilde{U}\Delta)^{-1}N$ |
| $G_{yu}(\Delta) = G_{yu}(I+\Delta)$ | $S_f(\Delta) = \tilde{N}\Delta(I - U\tilde{N}\Delta)^{-1}M$ |
| $G_{yu}(\Delta) = G_{yu} + \Delta$ | $S_f(\Delta) = \tilde{M}\Delta(I - U\tilde{M}\Delta)^{-1}M$ |
| $G_{yu}(\Delta) = G_{yu}(I+\Delta)^{-1}$ | $S_f(\Delta) = -\tilde{N}\Delta(I + M\tilde{V}\Delta)^{-1}M$ |
| $G_{yu}(\Delta) = (I+\Delta)^{-1}G_{yu}$ | $S_f(\Delta) = -\tilde{M}\Delta(I + V\tilde{M}\Delta)^{-1}N$ |
| $G_{yu}(\Delta) = G_{yu}(I+\Delta G_{yu})^{-1}$ | $S_f(\Delta) = -\tilde{N}\Delta(I + N\tilde{V}\Delta)^{-1}N$ |
| $G_{yu}(\Delta) = (N+\Delta_N)(M+\Delta_M)^{-1}$ | $S_f(\Delta) = \begin{pmatrix} -\tilde{N} & \tilde{M} \end{pmatrix}\begin{pmatrix} \Delta_M \\ \Delta_N \end{pmatrix}\left(I + \begin{pmatrix} V & -U \end{pmatrix}\begin{pmatrix} \Delta_M \\ \Delta_N \end{pmatrix}\right)^{-1}$ |
| $G_{yu}(\Delta) = (\tilde{M}+\Delta_{\tilde{M}})^{-1}(\tilde{N}+\Delta_{\tilde{N}})$ | $S_f(\Delta) = \left(I + \begin{pmatrix} \Delta_{\tilde{M}} & \Delta_{\tilde{N}} \end{pmatrix}\begin{pmatrix} U \\ V \end{pmatrix}\right)^{-1}\begin{pmatrix} \Delta_{\tilde{M}} & \Delta_{\tilde{N}} \end{pmatrix}\begin{pmatrix} M \\ -N \end{pmatrix}$ |



The outputs of the observer needs subsequent signal processing in the standard fashion.

### 4.2. *Controller retuning for destabilisation of faulty system*

The method proposed in this section proceeds by detecting unstable trajectories for very short periods of time that are provoked by controller modifications that are designed to generate such behaviours in faulty situations. Needless to say, this method should not be used uncritically. The authors believe, however, that there are cases, especially for systems with significant noise/disturbances where parametric faults might remain undetected by any other method. In such cases, perhaps it can be acceptable to perform a test of the proposed nature in an off-line situation, e.g. in a test bench. For some less safety-critical systems it might even be feasible to allow unstable behaviours in on-line situations for ultra-short periods of time. It should be noted that the unstable mode is exited as soon as the fault is detected.

The method proposed below relies on the following theorem.

**Theorem 4.2:** *Let $K(s)$ be a controller for a given plant, which internally stabilises both the nominal model $G(s)$ and also the model $G_f(s) \neq G(s)$ for a faulty situation. Then there exists a modification $K_Q$ of the controller such that*

(1) *$K_Q$ internally stabilises $G$ and*
(2) *$K_Q$ does* not *internally stabilise $G_f$*

**Proof:** Since $K$ stabilises $G_f$, $G_f$ can be written in the form (11) with a dual Youla-Kucera parameter $S_f$. Introducing also a primary Youla-Kucera parameter $Q$ in the controller $K_Q$ as in (7) or (8), stability of the closed-loop between $G_f$ and $K_Q$ is equivalent to the stability of a closed loop interconnection between $S_f$ and $Q$.

By a standard root locus argument, it is always possible to choose a stable value of $Q$ such that $Q$ itself is stable, and such that $Q$ renders $S_f$ unstable. This can be done by introducing a number of right half-plane zeros in $Q$ and increasing the gain of $Q$ until the poles of the closed-loop cross the imaginary axis on their way to the RHP zeros.

With this construction, $K_Q$ renders $G$ stable since $Q$ is stable, and it renders $G_f$ unstable, since the feedback interconnection of $Q$ and $S_f$ is unstable. □

Based on this result, the fault diagnosis algorithm can now be formulated.

**Algorithm 2:** Let a system with nominal model $G(s)$ and faulty model $G_f(s)$ be given, and let a controller $K(s)$ that stabilises both be given.

**Step 1:** Compute $S_f$, e.g. by using (13).

**Step 2:** Find $Q$ as any stable transfer function that destabilises $S_f$ (see, e.g. the constructive proof of Theorem 4.2).
**Step 3:** Compute $K_Q$ by (7) or (8).
**Step 4:** Switch periodically between $K$ and $K_Q$ as frequently as required (see below).
**Step 5:** Detect if unstable trajectories are found during the duty cycle of $K_Q$.

Note that it is assumed that $K$ also stabilises the faulty system. The reason for this is that otherwise there would be no reason to destabilise the system by another controller. The phrase 'as often as required' in Step 2 should be taken to mean the following:

(1) the switching *period* should be determined as a trade-off between the cost of postponing the detection of the fault and the cost of running the non-nominal controller $K_Q$,
(2) the *duty cycle* of the switch to $K_Q$ should be determined by the noise level, i.e. how long an unstable transient is needed to detect the fault with sufficient certainty.

The switching controller approach has been applied in Stoustrup and Niemann (2004) in connection with fault tolerant control. Here, it has been shown that it is possible to stabilise a faulty system by switching between a number of controllers. Allowing that some of the single controllers will destabilise the closed-loop system, it is possible to get a stable closed-loop system by switching between the controllers.

As an alternative $K_Q$ can be run all the time, replacing $K$ (see the example of Section 5). This is only admissible, if some detuning of the controller can be allowed permanently. Fault isolation is also possible by using a number of $Q$'s, where every single is designed with respect to a single fault. Since this method is based on the Youla-Kucera parameterisation, it is well suited as a basis for the fault tolerant control scheme proposed in Niemann and Stoustrup (2005).

## 5. Examples

Above, two methods for active fault diagnosis based on controller reconfiguration have been proposed. In this section, we shall give a numerical example illustrating the use of either method.

### 5.1. *A drag race car with faulty oscillations*

The example below is inspired by a drag race car project (Sørensen 2003). In this reference, a field study of a real drag race vehicle is presented, where a fault model of the type suggested below is described and verified against real data. In this section, however, this model is used only for inspiring and for motivating a fault model with two oscillations, as was verified for the real vehicle.

In a much simplified version of this system, the basic dynamics of the drive line is a second order system

$$G(s) = \frac{1}{s^2 + as + b},$$

with two real poles having negative eigenvalues. In the numerical example, the two poles were assumed to be $-10$ and $-20\,\mathrm{rad\,s^{-1}}$, so the nominal transfer function becomes

$$G(s) = \frac{200}{s^2 + 30s + 200}.$$

The car can be subjected to two distinct faults both of which manifest as oscillations caused by two different physical phenomena. One type of oscillation is caused by micro-slip friction phenomena in the clutch of the vehicle, the other is caused by oscillations in the rubber of the tyres.

It is of ultimate importance to discover the possible presence of these two faults during test drives, as the added acceleration of these oscillations to the huge acceleration of the drag race drive itself might exceed that admissible to the human body, such that the inner organs of the driver might be damaged during the actual race.

In this example we shall describe these two phenomena as additive faults, i.e. the overall model becomes

$$G_f(s) = G(s)\begin{pmatrix} 1 & G_{f_1} & G_{f_2} \end{pmatrix},$$

where $G_{f_1}$ and $G_{f_2}$ are second other resonant system

$$G_{f_1} = \frac{1}{s^2 + 2\zeta_1\omega_1 s + \omega_1^2}$$

and

$$G_{f_2} = \frac{1}{s^2 + 2\zeta_2\omega_2 s + \omega_2^2},$$

chosen with resonance frequencies of 5 and 20 Hz, and damping coefficients of 5% and 1%, respectively. For this system, a nominal observer-based controller is designed based on an LQG design, i.e. a second-order controller.

In addition to the nominal observer, two observers are designed to be sensitive to the two faults that are anticipated to occur. In this case, this is particularly simple, as the obvious choice is to assign poles for each of the two observers to coincide with the resonance frequencies.

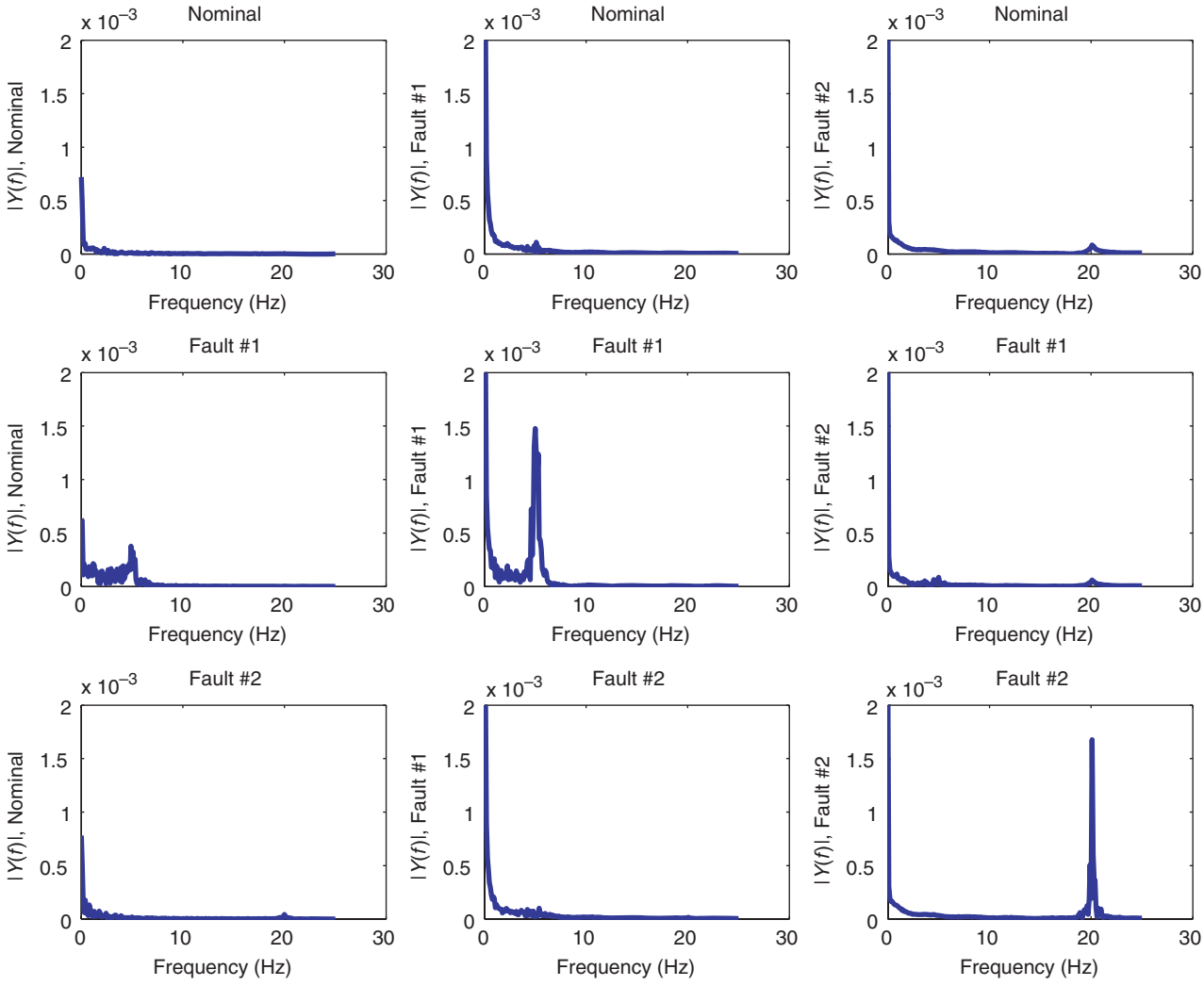


Figure 3. Single-sided spectra of output from observers. The title of each subplot indicates the state of the system, either nominal or in one of the faulty states. The vertical label indicates which observer has been applied, either the nominal or one designed to be sensitive to one of the faults. Spikes are clearly discernible in the diagonal where either of the two faults have occurred.



Figure 3 shows single-sided spectra of output from these three observers in three different cases. The title of each subplot indicates the state of the system, either in nominal or in one of the faulty states. The vertical label indicates for which observer has been applied, either the nominal or one designed to be sensitive to one of the faults. In all cases, the controlled system is driven by a low-frequency random reference with some measurement noise. In the plots shown in the first row, no faults have occurred. This is reflected in the FFTs, all of which have LF components exclusively with exception from two almost undiscernible spikes at the resonance frequencies for the two sensitised observers. In the second and the third row of plots, either of the two faults are introduced (as random signals driving the two oscillators). In these cases, the observer sensitised at 5 Hz has a clear spike at that frequency for the first fault, and likewise with the other observer. The two fault sensitised observers, however, have no significant spikes at the frequency of the non-occurrent fault. The nominal observer has only insignificant frequency contributions at the two fault frequencies.

Next, we proceed with Step 3 of Algorithm 1, where the following sequence of observer gains are chosen for each cycle:

$$L_0,\ L_1,\ L_0,\ L_2,\ L_0$$

and the corresponding $\beta(t)$ is shown in Figure 4.

Based on these choices of observer gain sequence and selection parameter $\beta(t)$, we can now calculate $\Sigma_C$ by (15). This has been done, and Figure 5 shows three simulations based on the same reference signal.

Figure 5 shows a simulation of the system with an observer cycling controller. As indicated by the labels, the controller has transitions back and forth between the nominal observer and the two fault

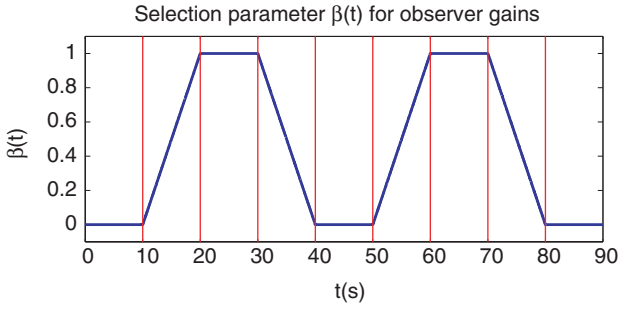


Figure 4. Observer selection parameter $\beta(t)$. In this case, the transitional periods have been chosen to be of the same length as the stationary periods for each observer.

sensitive observers. In Figure 5(a), the nominal situation is shown. No oscillations are seen in any period. In Figure 5(b), the first fault has been introduced. An oscillation is clearly visible in the third period, where the corresponding fault sensitive filter is fully active. No oscillations are seen elsewhere. In Figure 5(c), the second fault has been introduced. In this case, an oscillation is seen in the seventh period, which corresponds exactly to the period, where the observer that has been sensitised to the second fault is fully active.

In conclusion, the control scheme shown would clearly stimulate oscillations in the vehicle caused by the two faults in a test drive, even if they are present to an extent, where the driver would not notice them with the nominal controller. This gives a valuable dimension to the test drive, where the drive can be discontinued immediately, if one of the dangerous oscillations is discovered.

It should be noted that the above example does in fact not disclose the full power of the method. Indeed, in the model approach taken, the faulty states are not controllable by the control signal. That means that the results displayed above are in a way obtained just by using the closed-loop system as a 'signal processor' for an oscillation of a fixed amplitude. In general, however, it could be anticipated that fault states would often be controllable, which means that they would be stimulated by the proposed controller, not just emphasised in the observer.

### 5.2. *Destabilising a system with a parametric fault*

We consider a system with the transfer function

$$G(s) = \frac{1}{s+p} = \frac{1}{s+1},$$

where the parameter $p$ has the nominal value $p=1$. A parametric fault is considered, which increases the parameter by 10% when it occurs, i.e.

$$G_f(s) = \frac{1}{s+p_f} = \frac{1}{s+1.1}.$$

For this system, a nominal controller is considered, which assigns poles in $\{-2,-3\}$. With a positive feedback convention, such a controller has a transfer function given by

$$K(s) = -\frac{2}{s+4}.$$

Figure 6 shows a simulation with this controller, where the above mentioned fault occurs at $t=27$ s. The system is driven by a reference of 1 and Gaussian noise with $\sigma=0.1$. The occurrence of the fault is hardly discernible.

A doubly coprime factorisation of the plant and the given controller is

$$G(s) = N(s)M^{-1}(s), \quad K(s) = U(s)V^{-1}(s),$$

where

$$N(s) = \frac{1}{s+2}, \quad M(s) = \frac{s+1}{s+2},$$
$$U(s) = -\frac{2}{s+2}, \quad V(s) = \frac{s+4}{s+2}.$$

The $S_f(s)$ parameter of the dual Youla-Kucera parameterisation for the faulty model can now be found as

$$S_f(s) = \big(G_f(s)M(s) - N(s)\big)\big(V(s) - G_f(s)U(s)\big)^{-1} = -\frac{0.1}{s^2+5.1s+6.4}.$$

A primary Youla-Kucera parameter $Q(s)$ which assigns poles of the closed loop between $S_f(s)$ and $Q(s)$ in

$$\{0.1, -6, -5, -3\}$$

is given by

$$Q(s) = -\frac{252.5s+750.5}{s^2+8.8s+10.32}.$$

Thus, this $Q(s)$ is indeed a stable transfer function that destabilises the $Q-S_f$ loop.

The fault can now be diagnosed by switching in this $Q(s)$ in the structure shown in Figure 1. During the diagnosis period, the resulting controller becomes

$$K_Q(s) = (U(s)+M(s)Q(s))(V(s)+N(s)Q(s))^{-1} = -\frac{254.5s+257}{s^2+9.8s-236.4}.$$

A simulation with the $Q$ parameter switched in permanently, i.e. both through the nominal and the

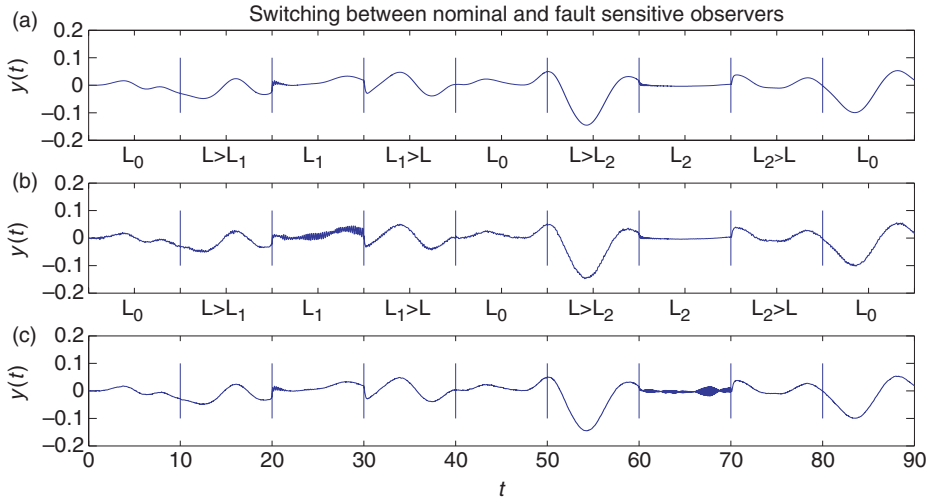


Figure 5. Simulation of system with observer cycling controller. As indicated by the labels, the controller has transitions back and forth between the nominal observer and the two fault sensitive observers. In (a) no fault occurs. In the second plot (b), Fault #1 has occurred and in (c), Fault #2 has occurred. Oscillations are clearly discernible in the windows where the two sensitive observers are active and nowhere else.



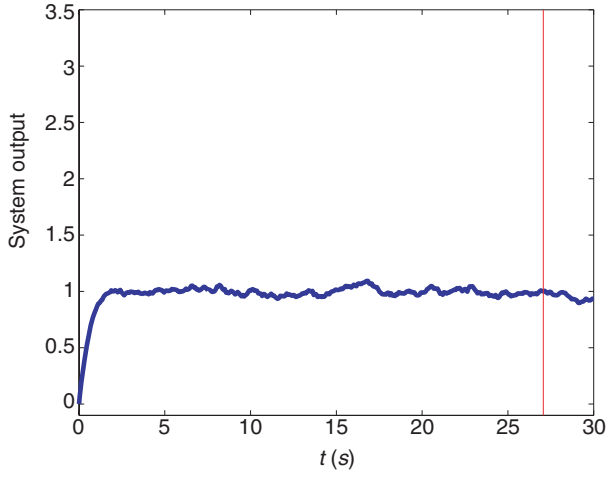


Figure 6. Simulation of system with nominal controller. The fault occurrence is indicated with the vertical line.

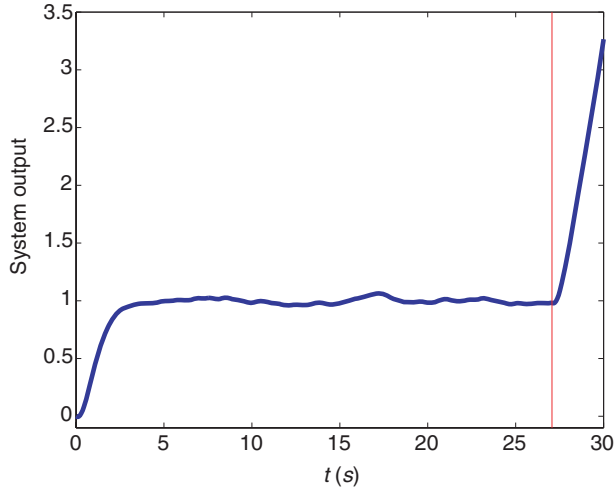


Figure 7. Simulation of system with fault destabilising controller. The fault occurrence is indicated with the vertical line.

faulty situation, is shown in Figure 7. The system remains stable, whenever the system has its nominal value, but turns unstable immediately when the fault occurs, which can be detected very rapidly. The inputs for the simulation in Figure 7 were the same as in the simulation shown in Figure 6.

## 6. Conclusions

A method has been proposed for active detection of faults without an exogenous excitation signal. The method relies on a result on parameterisation of observers that interpolate two given observers in such a way that all intermediate observers are guaranteed to be stable. The approach proceeds by an initial design of a number of observers that are each sensitive to one or more faults and which together span all faults that should be detected. The fault detection is then established through a transition cycle that encompasses all the observers in turn and thereby enables detection by emphasising an occurred fault, that might otherwise have been indiscernible.

An important tuning parameter of the proposed method is the ratio of duration between the sensitised observers and the nominal observer. Clearly, it will

have a performance degrading effect to have long durations of the sensitised observers, whereas it will give a greater risk of undetected false if they are made too short.

Also, a method has been proposed for active detection of parametric faults, which requires that it is admissible to render the system unstable for a short period of time. It should be noted that many fault diagnosis methods can be reformulated to detect other types of fault, whereas this specific method is exclusively applicable to internal faults, as a bounded, additive signal can never destabilise a stable, linear closed-loop system.

The method can be implemented both as a periodic switching between a nominal and an active fault diagnosing controller. Alternatively, the method can be implemented as a permanent modification of the controller. The advantage of the former method is that the detuning of the controller only takes place in short time intervals. The advantage of the latter method is that it facilitates very rapid fault detection.

For both methods, there are several systematic design methods that can be applied to obtain the filters for the former method and the controllers for the latter method, some of which are mentioned above. Most candidate methods, however, are frequency domain methods. This leaves a significant challenge for practical fault diagnosis methods, however, where time-to-detect is an important parameter. Since time-to-detect is primarily based on transient properties, it is difficult to handle this by frequency domain-based methods. Incorporating a time-to-detect specification to the design is therefore a topic of further research.



## Notes on contributors

***Jakob Stoustrup*** received his MSc degree in EE in 1987, and the PhD degree in Applied Mathematics in 1991, both from the Technical University of Denmark. In the period 1991–1996, Jakob Stoustrup held several positions at the Department of Mathematics, Technical University of Denmark. He has been a Visiting Professor at the University of Strathclyde, Glasgow, UK, and at the Mittag-Leffler Institute, Stockholm, Sweden. Since 1997 he was a Professor at Automation & Control, Aalborg University, Denmark, and since 2006 was Head of Research for the Department of Electronic Systems. He has acted as Associate Editor, Guest Editor and Editorial Board Member of several international journals. He is an IEEE SM, and has been Chairman of an IEEE CSS/RAS Joint Chapter. Since 2008, he has been Chairman for the IFAC Technical Committee SAFEPROCESS. He has received the Statoil Prize, the Dannin Award for Scientific Research, and is a member of The Danish Academy of Technical Sciences. The main contributions of Stoustrup have been to robust control theory and to the theory of fault tolerant control systems, with more than 200 peer-reviewed scientific papers. Apart from the theoretical work, he has carried out industrial applications in cooperation with more than 50 industrial companies.

***Hans Henrik Niemann*** was born in Denmark in 1961. He received his MSc degree in mechanical engineering in 1986 and PhD degree in 1988 from Technical University of Denmark. From 1988 to 1994 he had a research position and from 1994 he has been an Associate Professor in control engineering at Technical University of Denmark. His research interests are: 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.

## References


Campbell, S., Horton, K., and Nikoukhah, R. (2002), 'Auxiliary Signal Design for Rapid Multimodel Identification using Optimization', *Automatica*, 38, 1313–1325.

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

Niemann, H., and Stoustrup, J. (2005), 'An Architecture for Fault Tolerant Controllers', *International Journal of Control*, 78, 1091–1110.

Niemann, H. (2003), 'Dual Youla Parameterisation', *IEE Proceedings – Control Theory and Applications*, 150, 493–497.

Niemann, H. (2006), 'A Setup for Active Fault Diagnosis', *IEEE Transactions on Automatic Control*, 51, 1572–1578.

Niemann, H., and Poulsen, N. (2005), 'Active Fault Diagnosis in Closed-loop Systems', in *Proceedings of the IFAC World Congress*, Prague, Czech Republic, July, Prague, Czech Republic, 448–453.

Nikoukhah, R. (1998), 'Guaranteed Active Failure Detection and Isolation for Linear Dynamical Systems', *Automatica*, 34, 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, 701–724.

Sørensen, M. (2003), 'Top Fuel Drag Race Drive Line Modeling and Control', MSc thesis, Department of Electronic Systems, Aalborg University, Automation & Control, Aalborg, Denmark.

Stoustrup, J., and Komareji, M. (2008), 'A Parameterisation of Observer-Based Controllers: Bumpless Transfer by Covariance Interpolation'. In *Proceedings of the 2009*

*American Control Conference*, St. Louis, Missouri, USA, June 2009, 1871–1875.

Stoustrup, J., and Niemann, H. (1999), 'Fault Detection and Isolation in Systems with Parametric Faults', in *Proceedings of the 14th IFAC World Congress*, Beijing, China, July, Beijing, China, Invited paper, pp. 139–144.

Stoustrup, J., and Niemann, H. (2004), 'Fault Tolerant Control for Unstable Systems: A Linear Time Varying Approach', in *Proceedings of the American Control Conference*, Boston, MA, USA, Jun, Boston, MA, USA, pp. 1794–1799.

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

Zhou, K., Doyle, J., and Glover, K. (1995), *Robust and Optimal Control*, Upper Saddle River, NJ: Prentice Hall.