FAULT DIAGNOSIS AND FAULT TOLERANT CONTROL: AN OPTIMIZATION BASED APPROACH

Jakob Stoustrup*

1. Introduction

There are many trends in the development of man-made systems, but one seems to be in common widely across industrial areas: the systems become ever increasingly more complex. Elementary reliability theory tells us at least one challenge in this connection, which is that as the complexity grows, so does the probability of critical faults occurring in the system.

This is the one of the motivations for the increasing interest in the design of fault tolerant control systems, where the objective is to disallowing one or several faults to develop into an overall system failure.

In the search for systematic design methods for fault tolerant control, the recent research efforts have been focused on deriving control laws based on a specific fault model. The best choice of fault model will depend on the purpose of the model. A number of faults can naturally be considered both as additive faults or as parametric faults (for a case study on parametric faults, please refer to [27]). However, a random choice might not be optimal. The fault model needs to be selected with respect to the design objectives, i.e. whether only fault diagnosis is required, the objective is to preserve stability in faulty situations, or even to recover performance during faults.

In the past, additive fault models have been the most popular, especially in connection with fault diagnosis. Modeling e.g. an actuator fault as an additive fault will in general be very useful in connection with fault detection and/or fault isolation (see e.g. [33]. In connection with closed-loop systems, an actuator fault might result in instability. Using an additive fault model description in this case, the fault will be considered as an external signal entering the system. The fault signal of the model will therefore not affect the stability of the system, at least not for bounded fault signals. This small example indicates clearly that the description of possible faults in a dynamic system needs to be selected in very close relation with the application of the fault description/fault model.

In this paper, three types of faults/fault models will be considered. The three types are as

* Automation & Control, Department of Electronic Systems, Aalborg University, Fredrik Bajers Vej 7C, Denmark. Email: jakob@es.aau.dk, URL: es.aau.dk/staff/jakob

follows:

- additive faults
- parametric faults
- system structural changes

The above fault models can be considered in connection with the following applications:

- fault detection, fault isolation and fault estimation.
- fault tolerant control with stability recovery, i.e. the control system can handle faults in the system without resulting in an unstable closed loop system. Note, that additive faults can not challenge the stability of a linear system.
- feedback control with performance recovery, i.e. the effect from the fault is minimized in the closed loop by a feedback controller.

In this paper only linear systems will be considered. However, a number of the presented results can be generalized to non-linear systems without further assumptions.

The results of this paper relates to the areas of fault tolerant control and of robust control and relies strongly on the results reported in [17]. For other recent results on robustness and fault diagnosis/fault tolerant control, please refer to [34]. These two areas are very well described in a large number of papers and books. Without going into details, let us mention the books by Basseville and Nikiforov [2], Gertler [13] and by Chen and Patton [9] for a good introduction to the area of fault diagnosis. In Blanke et al. [3, 4] and in Patton [23, 24] and in the references herein, good introductions to the area of fault tolerant control can be found. Most of these papers describe various concepts for FTC. However, in the past years, also a number of theoretical results has been presented in this area, see e.g. [31, 36, 37, 38, 39, 43, 28, 29]. The area of robust control has been investigated in a large number of books and papers. Let us only mention the books written by Skogestad and Postlethwaite [26] and by Zhou et al. [42].

A significant application area of fault tolerant control that deserves specific mention, is the area of reconfigurable flight systems, which has been a pioneering area for several of the methodologies. To mention a few references in this area, we point to [12, 6, 5], in which further references can be found.

Two main classes of approaches can be distinguished in the literature on fault tolerant control: active FTC and passive FTC. In active FTC, the controller is reconfigured whenever a fault is detected (for recent case studies, please refer to the papers [22, 20, 21]). In passive FTC, the controller is fixed; its fault tolerance is obtained by an a priori design based on the fault models, such that this fixed controller is able to handle all possible faults. Recently an existence result has been shown for the fault tolerant stabilization problem in the paper [30], where further references to passive FTC can be found. For a case study, please refer to [18]. Active FTC relies on fault detection, fault isolation, and fault estimation. An approach to fault estimation which can be integrated with the FTC approach presented in this paper, can be found in [32].

The focus in this paper will be on using various fault models in connection with FTC. The paper will give an overview of the various design problems, depending on the type of faults.

A general architecture based on the Youla-Kucera parameterization will be proposed which allows to handle all fault model types, and to implement solutions for all the design problems described. The architecture is based on the results presented in [15, 16].

This paper is organized as follows. In Section 2, the system setup is given for three different fault types. The Youla-Kucera parameterization is first introduced in Section 3. A new controller architecture for FTC is introduced in Section 4 followed by a study of fault-tolerant control for the three types of fault models in Section 5. A passive FTC architecture is introduced in Section 6, where there is no switches included in the fault tolerant controller. Finally, we give a conclusion in Section 7.

1.1. Nomenclature

Capital letters will denote matrices or matrix valued functions. A^T is the transposed of A. A nominal system is described by Σ and a stabilizing feedback controller for Σ is given by Σ_C. Further, let an uncertain system or faulty system be given by Σ_Θ, where $\Theta \in \underline{\Theta}$ represents the model uncertainty, finite sets of the fault parameters or the input fault signals. A more detailed description of Σ_Θ is given below. The interconnection of the nominal system and the feedback controller is given by $\Sigma \times \Sigma_C$.

$\mathcal{F}_l(X,Y) = X_{11} + X_{12}Y(I - X_{22}Y)^{-1}X_{21}$ is the lower Linear Fractional Transformation (LFT) of (X,Y). The upper LFT of (X,Y) is given by $\mathcal{F}_u(X,Y) = X_{22} + X_{21}Y(I - X_{11}Y)^{-1}X_{12}$.

For simplicity, transfer functions are not equipped with an explicit dependency of a complex variable 's', as it should not be possible to confuse matrices and transfer functions when considering the context. In a few cases, the word 'dynamic' has been added to explicitly refer to a transfer function rather than a matrix.

2. System Setup

The general systems will now be described in details by using transfer functions. Consider the following generalized nominal $(r+m)\times(q+p)$ system,

$$\Sigma : \begin{cases} e = G_{ed}d + G_{eu}u \\ y = G_{yd}d + G_{yu}u \end{cases} \tag{1}$$

where $d \in \mathcal{R}^r$ is a disturbance signal vector, $u \in \mathcal{R}^m$ the control input signal vector, $e \in \mathcal{R}^q$ is the external output signal vector to be controlled, and $y \in \mathcal{R}^p$ is the measurement vector. $G_{\xi\zeta}$ is the transfer function between input ζ and output ξ.

Further, let the system be controlled by a stabilizing dynamic feedback controller given by:

$$u = Ky \tag{2}$$

Let Σ_Θ the generalized system in (1) including faults. Three different types of faults will now be introduced. First, let us consider systems with additive faults, Σ_Θ is then given by Σ_A

$$\Sigma_A : \begin{cases} e = G_{ed}d + \sum_{i=1}^{k} G_{ef,i}f_i + G_{eu}u \\ \quad = G_{ed}d + \quad G_{ef}f \quad + G_{eu}u \\ y = G_{yd}d + \sum_{i=1}^{k} G_{yf,i}f_i + G_{yu}u \\ \quad = G_{yd}d + \quad G_{yf}f \quad + G_{yu}u \end{cases} \tag{3}$$

where f_i signifies the i-th fault for each $i = 1,2,\ldots,k$. It is further assumed that the f_i is bounded and not correlated with the system state. 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. Also, it is common in the fault detection and isolation setting for model uncertainties to be described as external input signals in the same manner as disturbance signals w. In other words, w here can be thought of representing both external disturbance signals and signals that might arise due to model uncertainties, see e.g. [11].

However, in the cases where we want to detect, isolate and/or estimate parameter changes or uncertainty variations in the system, the fault model described by (3) can not in general be applied. In the case where the system includes parametric faults, Σ_Θ can be described by Σ_P:

$$\Sigma_P \; : \; \begin{cases} z = G_{zw}w + G_{zd}d + G_{zu}u \\ e = G_{ew}w + G_{ed}d + G_{eu}u \\ y = G_{yw}w + G_{yd}d + G_{yu}u \end{cases} \tag{4}$$

where $w \in \mathcal{R}^{k_w}$ and $z \in \mathcal{R}^{k_z}$ are the external input and output vectors. The connection between the external output and the external input is given by

$$w = \theta z$$

where θ represent the parametric faults in the system. Note that the above description is also applied in connection with description of systems including model uncertainties, see e.g. [42]. In this case, the connection between the external output and the external input is given by

$$w = \Delta z$$

where $\Delta \in \underline{\Delta}$ represent the model uncertainties. The system is the described by Σ_Δ. Closing the loop from w to z in Σ_P by using θ, we get

$$\Sigma_{P,\theta} = \mathcal{F}_u(\Sigma_P, \theta)$$

Faults might change the structure of the system. Based on a structural change of the nominal system in (1) due to faults, the general system Σ_Θ then takes the following form:

$$\Sigma_{S_i} \; : \; \begin{cases} e = \tilde{G}_{ed,i}d + \tilde{G}_{eu,i}u \\ y = \tilde{G}_{yd,i}d + \tilde{G}_{yu,i}u \end{cases}, \; i = 0, \cdots, k \tag{5}$$

where $\tilde{\cdot}$ indicates a change in transfer matrix, a change in the number of system states and number of inputs and outputs. Note that $i = 0$ is defined as the nominal model, $\Sigma_{S_0} = \Sigma$. Below, it will be argued in more detail, that it is unnecessary to define new input, output, or disturbance signals, as 'missing' signals can be modeled by transfer matrices with appropriate zero entries.

It should be pointed out in connection with the fault model given by (5) is the most direct way to describe a change in the system as a consequence of faults in the system. However, in many cases a much detailed model description can be obtained by using a parametric fault model.

Throughout the paper, it will be assumed that faults only occur one at the time.

In some of the stability results of this paper, it is an implicit assumption, that the system remains detectable and stabilizable after a fault has occurred, such that set of stabilizing controllers remains non-empty.

Finally, the methods proposed, assume that knowledge of post-fault scenarios are available a priori. As an alternative, they can be identified. Such an approach, however, lies outside the scope of this paper.

3. The Youla-Kucera Parameterization

Before considering the three different FTC design cases, the (primary) Youla-Kucera parameterization and the dual Youla-Kucera parameterization is shortly introduced. The controller architecture applied for the FTC in the following will be based on the Youla-Kucera parameterization. The Youla-Kucera parameterization has also been applied in connection with FTC in [31, 43].

The Youla-Kucera parameterization was first derived by Youla et al. and independently by Kucera. It has been described in [40, 41] and later used in many cases in connection with feedback control, see e.g. [1, 8, 7, 10, 14, 35, 42].

3.1. The Primary Youla-Kucera Parameterization

Let a coprime factorization of the system $G_{yu}(s)$ from (1) and a stabilizing controller $K(s)$ from (2) be given by:

$$\begin{aligned} G_{yu} &= NM^{-1} = \tilde{M}^{-1}\tilde{N}, \quad N, M, \tilde{N}, \tilde{M} \in \mathcal{RH}_\infty \\ K &= UV^{-1} = \tilde{V}^{-1}\tilde{U}, \qquad U, V, \tilde{U}, \tilde{V} \in \mathcal{RH}_\infty \end{aligned} \tag{6}$$

where the eight matrices in (6) must satisfy the double Bezout equation given by, see [42]:

$$\begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix} = \begin{pmatrix} \tilde{V} & -\tilde{U} \\ -\tilde{N} & \tilde{M} \end{pmatrix} \begin{pmatrix} M & U \\ N & V \end{pmatrix} = \begin{pmatrix} M & U \\ N & V \end{pmatrix} \begin{pmatrix} \tilde{V} & -\tilde{U} \\ -\tilde{N} & \tilde{M} \end{pmatrix} \tag{7}$$

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 $Q(s)$, i.e. all stabilizing controllers are given by [35]:

$$K(Q) = U(Q)V(Q)^{-1} \tag{8}$$

where

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

or by using a left factored form:

$$K(Q) = \tilde{V}(Q)^{-1}\tilde{U}(Q) \tag{9}$$

where

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

Using the Bezout equation, the controller given either by (8) or by (9) can be realized as an LFT in the parameter Q,

$$K(Q) = \mathcal{F}_l(J_K, Q) \tag{10}$$

where J_K is given by

$$J_K = \begin{pmatrix} UV^{-1} & \tilde{V}^{-1} \\ V^{-1} & -V^{-1}N \end{pmatrix} = \begin{pmatrix} \tilde{V}^{-1}\tilde{U} & \tilde{V}^{-1} \\ V^{-1} & -V^{-1}N \end{pmatrix} \tag{11}$$

Reorganizing the controller $K(Q)$ given by (10) results in the closed loop system depicted in Figure 1, see also [35].

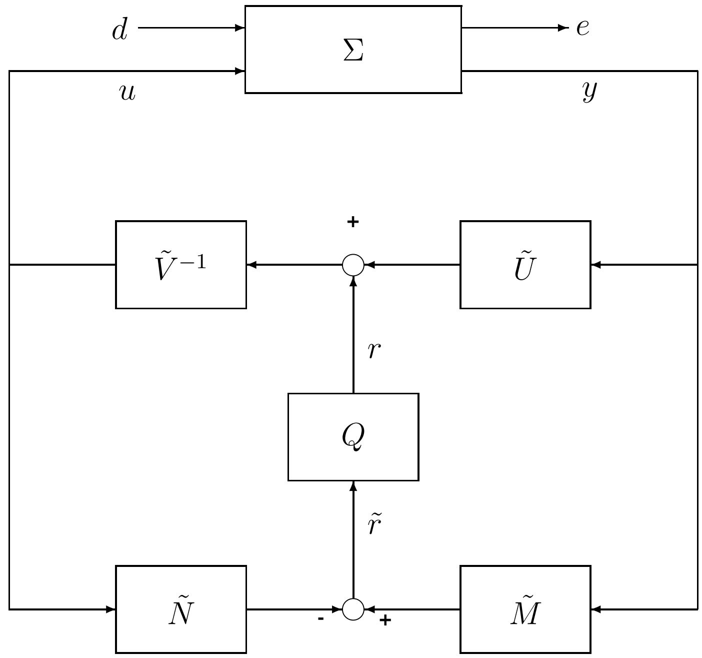

Fig. 1. Controller structure with parameterization

The main observation which shall be exploited in the solution to the fault tolerant control problem, is the following relatively simple expression for the transfer function from the external input d to the external output e terms of the parameter Q:

$$\begin{aligned} e &= (G_{ed} + G_{eu}K(Q)(I - G_{yu}K(Q))^{-1}G_{yd})d \\ &= (G_{ed} + G_{eu}U\tilde{M}G_{yd} + G_{eu}MQ\tilde{M}G_{yd})d \end{aligned}$$

where (7) has been exploited. Note, that the transfer function relating d and e is affine in Q.

3.2. The Dual Youla-Kucera Parameterization

The dual Youla-Kucera parameterization, gives a parameterization in term of a stable parameter S of all systems stabilized by a given controller. The parameterization is given by [35]:

$$G(S) = N(S)M(S)^{-1} \tag{12}$$

where

$$N(S) = N + VS,\ M(S) = M + US,\ S \in \mathcal{RH}_\infty$$

or by using a left factored form:

$$G(S) = \tilde{M}(S)^{-1}\tilde{N}(S) \tag{13}$$

where

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

An LFT representation of (12) or (13) is given by:

$$G(S) = \mathcal{F}_l(J_G, S) \tag{14}$$

where J_G is given by

$$J_G = \begin{pmatrix} NM^{-1} & \tilde{M}^{-1} \\ M^{-1} & -M^{-1}U \end{pmatrix} \tag{15}$$

The interpretation of the dual Youla-Kucera parameter S can be investigated from the primal Youla-Kucera parameterization shown in Figure 1. It turns out that the dual Youla-Kucera parameter S is the open loop transfer function from r to $\tilde{r}$ in Figure 1, [35], i.e.

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

This fact can be used in connection with estimation of the system parameters.

In Table 1, S has been calculated for a number of different types of model uncertainties, These equations for S will be applied in the following in connection with parametric faults.

Tab. 1. The connection between different system uncertainty descriptions in terms of Δ and the dual Youla-Kucera parameter S.

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

4. Fault Tolerant Controller Architecture

In the sequel, an architecture for fault tolerant controllers will be proposed, based on the Youla-Kucera parameterization shown in the block diagram in Figure 1. There is a number of reasons for using the architecture from the Youla-Kucera parameterization in connection with FTC. Using this architecture, the Q parameter will be the FTC part of the controller. This means that the FTC part of the feedback controller is a modification of the existing controller. Thus, a controller change when a fault appears in the system is not a complete shift to another controller, but only a modification of the existing controller by adding a correction signal in the nominal controller, the r signal in Figure 1. However, it should be pointed out that it is possible to modify the controller arbitrarily by designing the Youla-Kucera parameter Q, see e.g. [19, 35].

Another important thing is that the architecture includes also a parameterization of all residual generators. All residual signals can be described by, [11, 13]

$$r = Q_{FDI}\tilde{r} = Q_{FDI}(\tilde{M}y - \tilde{N}_u u) \tag{16}$$

This means that it is possible to combine both fault diagnosis and fault tolerant control in the same architecture without any problems. A block diagram for this combined FDI and FTC architecture based on the Youla-Kucera parameterization is shown in Figure 2 for three potential parametric faults - the generalization to any number of faults should be obvious.

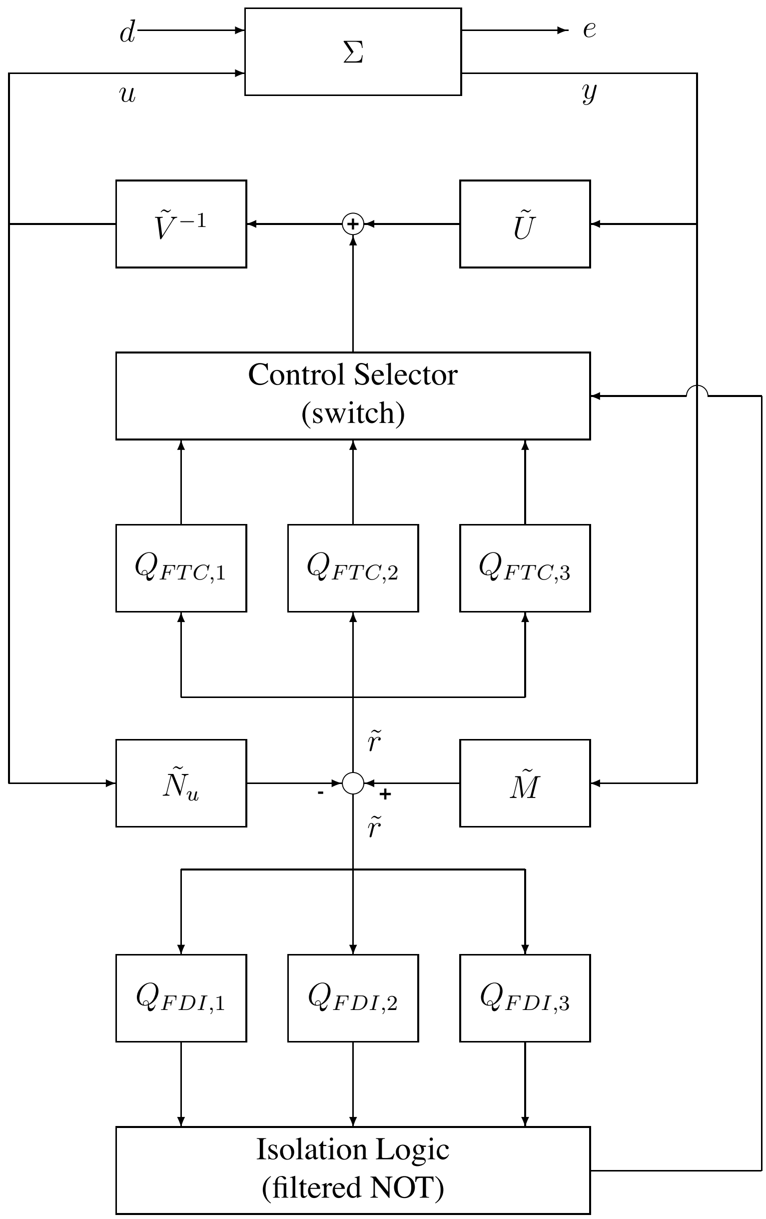

Fig. 2. Fault tolerant scheme with three potential parametric faults. The residual signal is used both for isolation and for feedforward in the fault handling.

The above controller architecture applied for FTC shown in Figures 1 and 2 has a fixed structure with respect to the number of measurement signals and control signals. This will not in general be the case in real applications. Here, faults in e.g. sensors can be handled by applying other sensors in the system, i.e. the measurement output from the system is changed. Equivalent with faults in connection with the actuators in the system. This type of system change has not directly been included in the system description given by (4) or (5). However, it is possible to include change of sensors and/or actuators in the FTC architecture given above.

Let us consider the system G_{yu} given by (1). Assume that only a subset of the sensors and the actuators has been applied for the nominal feedback controller $K(s)$ given by (2). Let the system G_{yu} be partitioned as follows

$$G_{yu} = \begin{pmatrix} G_{yu,00} & G_{yu,01} \\ G_{yu,10} & G_{yu,11} \end{pmatrix} \tag{17}$$

Further, let us use controller given by

$$K(s) = \begin{pmatrix} K_0 & 0 \\ 0 & 0 \end{pmatrix} \tag{18}$$

Based on this controller, the Youla-Kucera matrices then take the following form:

$$\begin{aligned} \begin{pmatrix} M & U \\ N_u & V \end{pmatrix} &= \begin{pmatrix} \begin{pmatrix} M_0 & M_1 \\ 0 & I \end{pmatrix} & \begin{pmatrix} U_0 & 0 \\ 0 & 0 \end{pmatrix} \\ N_u & \begin{pmatrix} V_0 & 0 \\ V_1 & I \end{pmatrix} \end{pmatrix} \\ \begin{pmatrix} \tilde{V} & -\tilde{U} \\ -\tilde{N}_u & \tilde{M} \end{pmatrix} &= \begin{pmatrix} \begin{pmatrix} \tilde{V}_0 & \tilde{V}_1 \\ 0 & I \end{pmatrix} & \begin{pmatrix} -\tilde{U}_0 & 0 \\ 0 & 0 \end{pmatrix} \\ -\tilde{N}_u & \begin{pmatrix} \tilde{M}_0 & 0 \\ \tilde{M}_1 & I \end{pmatrix} \end{pmatrix} \end{aligned}$$

This in turn implies that the Youla-Kucera parameterized controller $K(Q)$ given by (8) takes the following form:

$$\begin{aligned} K(Q) &= U(Q)V(Q)^{-1} \\ &= \begin{pmatrix} K_0 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} \tilde{V}_0^{-1} & -\tilde{V}_0^{-1}\tilde{V}_1 \\ 0 & I \end{pmatrix} Q \left(I + \begin{pmatrix} V_0^{-1} & 0 \\ -V_1 V_0^{-1} & I \end{pmatrix} N_u Q \right)^{-1} \begin{pmatrix} V_0^{-1} & 0 \\ -V_1 V_0^{-1} & I \end{pmatrix} \end{aligned} \tag{19}$$

A block diagram of the $K(Q)$ given by (19) is shown in Figure 3.

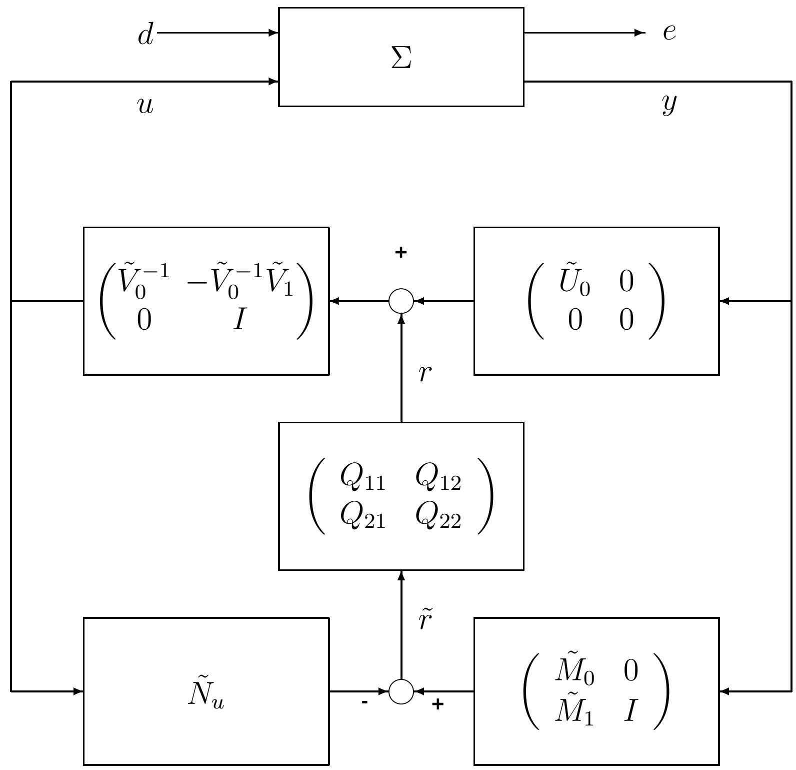

Fig. 3. Block diagram for controller with a Q parameterization. Note that the nominal controller does not use the measurements employed after reconfiguration.

From Figure 3, it is possible to calculate the transfer function from r to $\tilde{r}$. The open loop transfer function is the zero transfer function in the fault free case. As a direct consequence of this, the closed loop transfer function will be an affine function of the Q parameter. Note that the $\tilde{r}$ (or r) vector still can be applied in connection with fault diagnosis and/or fault isolation.

It is clear from both Figure 3 and (19) that the controller architecture will allow to use other sensors and/or actuators that is used in connection with the nominal controller K_0.

The result of this generalization of applying the Youla-Kucera parameterization in connection with fault tolerant control is that it is not a limitation of the controller structure. The structure can without any problems handle the problem of changing sensors and/or actuators, which is normal in connection with fault tolerant control. The above general controller architecture can directly be applied in connection with the results given in Section 5.

A simplified FTC architecture is applied in Section 6 in connection with passive fault tolerant control. The idea in the passive FTC is to remove the FDI part in the architecture. The single FTC controller Q is designed to handle all faults in the system. Further, the FTC controller will be included all the time. This mean that Q will be included as an open loop transfer function in the nominal system and in a feedback loop in the faulty system. The advantage by this passive FTC architecture is that delays due to fault isolation is removed from the FTC loop.

5. Fault Tolerant Control

Just as in connection with fault diagnosis, the fault tolerant control problem will depend strongly on the type of faults that can appear in the system. In this paper, the various fault tolerant control design problems will be described for the three different model structures given in Section 2. Especially in connection with FTC for systems with structural changes, the solution (the selected controller structure, type etc.) will depend strongly on the specific case. There does not exist any general method with explicit design formulae that can handle the general case. Much better design results can be obtained by using dedicated design methods.

5.1. FTC for Systems with Additive Faults

In a large number of systems, faults are described as additive faults. In connection with FTC, this might not be very useful. The reason is that the additive faults can be considered as external input signals to the system, at least if they are assumed to be uncorrelated with the system states. External input signals will not cause any changes in the system dynamics. Specifically, they are not able to change the stability of the closed-loop system, see e.g.[42]. Consider for example faults on an actuator. Such faults will in general affect the stability margins of the closed-loop system. FTC for systems with additive faults is therefore only relevant if the faults that can appear enter the system outside the closed loop. Consider the general 2×2 system setup with additive faults given by (3). Closing the system by a stabilizing controller $K(s)$ given by (2) gives the following closed loop transfer function:

$$e = (G_{ed} + G_{eu}K(I - G_{yu}K)^{-1}G_{yd})d + (G_{ef} + G_{eu}K(I - G_{yu}K)^{-1}G_{yf})f \tag{20}$$

From (20), it is clear that bounded additive faults can not affect the closed-loop stability - only the performance of the system will be affected. The main FTC problem as defined formally in [17] is not meaningful in this case. Instead the design of a feedback controller needs to be done with respect to minimizing the effect from additive faults on the closed loop transfer function, i.e. a fault tolerant control problem with mild performance reduction, please refer to [17] for a formal definition. This problem is equivalent with a disturbance rejection problem.

The design of the controller can be done in two steps. First a nominal controller $K_0(s)$ is designed such that the nominal performance is satisfied. In the second step, the Youla-Kucera parameterized controller $K(Q)$ given by (9) or (10) is applied, based on the nominal controller $K_0(s)$. Using $K(Q)$ as the feedback controller for the system given by (3) result in the following closed-loop system:

$$\begin{aligned} e &= (G_{ed} + G_{eu}U\tilde{M}G_{yd} + G_{eu}MQ\tilde{M}G_{yd})d + (G_{ef} + G_{eu}U\tilde{M}G_{yf} + G_{eu}MQ\tilde{M}G_{yf})f \\ &= (T_{1d} + T_2QT_{3d})d + (T_{1f} + T_2QT_{3f})f \end{aligned} \tag{21}$$

From the above closed loop transfer function, it is clear that the FTC problem, i.e. the design of Q, is equivalent with a disturbance rejection problem. Standard optimization methods can be applied directly for the design of a stable Youla-Kucera parameter Q. Using a standard method for the design of Q, the closed loop transfer function in (21) can be written as an LFT given by:

$$e = \mathcal{F}_l(P_{add}, Q)\begin{pmatrix} d \\ f \end{pmatrix} \tag{22}$$

where

$$P_{add} = \begin{pmatrix} \begin{pmatrix} T_{1d} & T_{1f} \end{pmatrix} & T_2 \\ \begin{pmatrix} T_{3d} & T_{3f} \end{pmatrix} & 0 \end{pmatrix}$$

The standard setup design problem is shown in Figure 4.

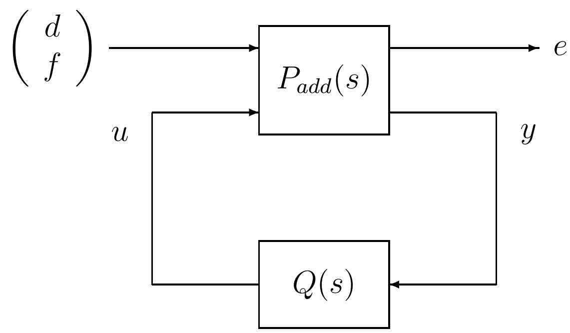

Fig. 4. The standard setup for design of Q for systems with additive faults

Based on the standard setup for the design of Q, we have the following design problem for Q.

Problem 1 *For a given number $\gamma > 0$, $\alpha \in \{2, \infty\}$,* ***the $\mathcal{H}_\alpha$ suboptimal fault tolerant control problem with performance recovery for system with additive faults*** *is defined as the problem of designing, if existent, a feedback controller Q_α, such that the closed loop transfer function $T_{e,add}$ is stable and the $\mathcal{H}_\alpha$ norm of $T_{e,add}$ is less than or equal to γ, where $T_{e,add}$ is given by*

$$T_{e,add} = \mathcal{F}_l(P_{add}, Q_\alpha)$$

and P_{add} is given by

$$P_{add} = \begin{pmatrix} \begin{pmatrix} G_{ed} + G_{eu}U\tilde{M}G_{yd} & G_{ef} + G_{eu}U\tilde{M}G_{yf} \end{pmatrix} & G_{eu}M \\ \begin{pmatrix} \tilde{M}G_{yd} & \tilde{M}G_{yf} \end{pmatrix} & 0 \end{pmatrix}$$

It should also be pointed out that the exact, the almost exact and the optimal design problems for Q have been considered in details in [25].

Combining FTC with a fault isolation method gives a possibility to design a number of Q-controllers, every single one dedicated to a single fault case. When faults appear in the system, the specified Q-controller to the given fault case can then be selected. It is also important to note that the Q controller needs to be decoupled when there is no faults in the system, else the closed loop transfer function will be modified, see (21). It is clear that the FTC problem in this case is a performance problem and the closed loop stability will not be affected by the additive faults (modeled as bounded external signals).

5.2. FTC for Systems with Parametric Faults

In this case, the closed-loop stability can be affected by the parametric faults, if G_{yu} depend on the parametric faults. As in Section 5.1, a Youla-Kucera parameterized controller $K(Q)$ is applied, where the nominal controller $K(0) = K_0$ is designed for the nominal system. The Youla-Kucera parameter is then applied for obtaining FTC, i.e. Q needs to stabilize the closed-loop system when a fault has appeared in the system. The stability of the closed loop system require stability of the nominal closed-loop system and closed-loop stability of a loop where both Q and the parametric faults θ is included, [35]. The stability of the closed-loop system is satisfied by the design of the nominal feedback controller $K(0)$. The other closed-loop system that needs to be stable is given by

$$\tilde{S}(Q) = (I - QS(\theta))^{-1} \tag{23}$$

where $S(\theta)$ is the dual Youla-Kucera parameter, depending on the parametric faults θ.

It is required that S is stable to guarantee closed-loop stability. Combining the Youla-Kucera parameterization with the dual Youla-Kucera parameterization, it is not a condition that Q and S need to be stable to guarantee closed-loop stability. Q and S just need to satisfy that the closed-loop system given by (23) is stable, [35]. In the general case, $S(\theta)$ take the following form:

$$S(\theta) = \tilde{M}G_{yw}\theta(I - [G_{zw} + G_{zu}U\tilde{M}G_{yw}]\theta)^{-1}G_{zu}M \tag{24}$$

In connection with (24), it is important to note that the stability condition of S and/or of $\tilde{S}(Q)$ in (23) for satisfying that the faulty closed loop system is stable, is only valid if the faulty system is still detectable and stabilizable from the specified input signals u and output signals y. This is a standard condition in connection with FTC systems. If the faulty system is not detectable and/or stabilizable, additional actuators and/or sensors need to be included in the system to satisfy these two conditions.

It is important to note that if S is stable, we do not need a Q-parameter to stabilize the system. In this way, S can be used for analyzing which faults are admissible and how large they can be before the closed-loop system will become unstable.

Based on the general equation for $S(\theta)$ given by (24), we have the following FTC design problem.

Problem 2 ***The fault tolerant control problem for system with parametric faults*** *is defined as the problem of designing, if existent, a feedback controller Q, such that $\tilde{S}(Q)$ given by*

$$\tilde{S}(Q) = (I - QS(\theta))^{-1}$$

is stable, where S is given by

$$S(\theta) = \tilde{M}G_{yw}\theta(I - [G_{zw} + G_{zu}U\tilde{M}G_{yw}]\theta)^{-1}G_{zu}M$$

In the general case, the equation for $S(\theta)$ given above is quite complicated. $S(\theta)$ needs to be derived explicitly in every single case in order to reduce the complexity of $S(\theta)$. Consider two simple cases, where the parametric faults are placed at either the input to the system (actuator faults) or at the output to the system (sensor faults), i.e. the system given by (4) takes the following form

$$\begin{pmatrix} G_{ed}(\theta) & G_{eu}(\theta) \\ G_{yd}(\theta) & G_{yu}(\theta) \end{pmatrix} = \begin{pmatrix} G_{ed} & G_{eu} + G_{eu}\theta \\ G_{yd} & G_{yu} + G_{yu}\theta \end{pmatrix} \tag{25}$$

for parametric faults at the input. The system given by (4) takes the following form for parametric faults at the output

$$\begin{pmatrix} G_{ed}(\theta) & G_{eu}(\theta) \\ G_{yd}(\theta) & G_{yu}(\theta) \end{pmatrix} = \begin{pmatrix} G_{ed} & G_{eu} \\ G_{yd} + \theta G_{yd} & G_{yu} + \theta G_{yu} \end{pmatrix} \tag{26}$$

The dual Youla-Kucera parameter S is then given by:

$$S(\theta) = \tilde{N}_u\theta(I - U\tilde{N}_u\theta)^{-1}M \tag{27}$$

for parametric faults at the input and

$$S(\theta) = \tilde{M}_u\theta(I - N_u\tilde{U}\theta)^{-1}N_u \tag{28}$$

for parametric faults at the output.

The two FTC design problems for parametric faults at the input and the output are given as follows.

Problem 3 ***The fault tolerant control problem for system with parametric input faults*** *is defined as the problem of designing, if existent, a feedback controller Q, such that $\tilde{S}(Q)$ given by*

$$\tilde{S}(Q) = (I - QS(\theta))^{-1}$$

is stable, where S is given by

$$S(\theta) = \tilde{N}_u\theta(I - U\tilde{N}_u\theta)^{-1}M$$

Problem 4 ***The fault tolerant control problem for system with parametric output faults*** *is defined as the problem of designing, if existent, a feedback controller Q, such that $\tilde{S}(Q)$ given by*

$$\tilde{S}(Q) = (I - QS(\theta))^{-1}$$

is stable, where S is given by

$$S(\theta) = \tilde{M}_u\theta(I - N_u\tilde{U}\theta)^{-1}N_u$$

So far, the stability part with respect to parametric faults has been treated. This is the most important part of the FTC. However, it will also in some cases be possible to design the FTC controller (the Q controller) with respect to both closed-loop stability as well as closed-loop performance. Closing the loop of the system in (4) with the feedback controller $K(Q)$, we get the following closed loop transfer function:

$$e = T_{ed}(s)d \tag{29}$$

where

$$T_{ed}(s) = G_{ed}(\theta) + G_{eu}(\theta)(U + MQ)((V - G_{yu}(\theta)U) + (N_u - G_{yu}(\theta)M)Q)^{-1}G_{yd}(\theta)$$

and

$$\begin{pmatrix} G_{ed}(\theta) & G_{eu}(\theta) \\ G_{yd}(\theta) & G_{yu}(\theta) \end{pmatrix} = \begin{pmatrix} G_{ed} + G_{ew}\theta(I - G_{zw}\theta)^{-1}G_{zd} & G_{eu} + G_{ew}\theta(I - G_{zw}\theta)^{-1}G_{zu} \\ G_{yd} + G_{yw}\theta(I - G_{zw}\theta)^{-1}G_{zd} & G_{yu} + G_{yw}\theta(I - G_{zw}\theta)^{-1}G_{zu} \end{pmatrix}$$

Again, using a standard setup, shown in Figure 5, for the design of the feedback controller Q, we have the following design problems for FTC with mild performance reduction.

Problem 5 *For a given number $\gamma > 0$, $\alpha \in \{2, \infty\}$,* ***the $\mathcal{H}_\alpha$ suboptimal fault tolerant control problem with performance recovery for system with parametric faults*** *is defined as the problem of designing, if existent, a feedback controller Q_α, such that the closed loop transfer function $T_{ed,m}$ is stable and the $\mathcal{H}_\alpha$ norm of $T_{ed,m}$ is less than or equal to γ, where $T_{ed,m}$ is given by*

$$T_{ed,m} = \mathcal{F}_l(P_m, Q_\alpha)$$

and P_m is given by

$$P_m = \begin{pmatrix} G_{ed}(\theta) + G_{eu}(\theta)U(V - G_{yu}(\theta)U)^{-1}G_{yd}(\theta) & G_{eu}(M - U(V - G_{yu}(\theta)U)^{-1}(N_u - G_{yu}(\theta)M)) \\ (V - G_{yu}(\theta)U)^{-1}G_{yd}(\theta) & -(V - G_{yu}(\theta)U)^{-1}(N_u - G_{yu}(\theta)M) \end{pmatrix}$$

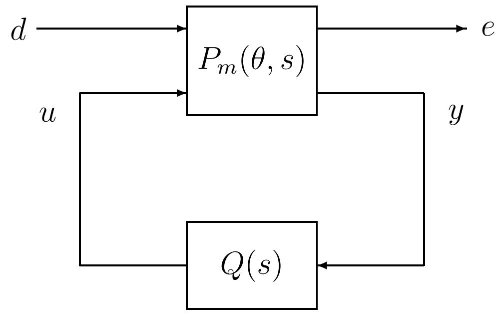

Fig. 5. The standard setup for design of Q for systems with parametric faults

At last, let us again consider the two cases with parametric input faults and output faults. The general system in (4) is then given by (25) and (26), respectively. The general closed loop transfer function in (29) is then given by

$$\begin{aligned} T_{ed}(\theta) &= G_{ed} + G_{eu}(I+\theta)(U+MQ)((V-G_{yu}(I+\theta)U)+(N_u-G_{yu}(I+\theta)M)Q)^{-1}G_{yd} \\ &= G_{ed} + G_{eu}(I+\theta)(U+MQ)(I-\tilde{N}_u\theta(U+MQ))^{-1}\tilde{M}G_{yd} \end{aligned} \tag{30}$$

for parametric faults at the input and

$$\begin{aligned} T_{ed}(\theta) &= G_{ed} + G_{eu}(U+MQ)((V-(I+\theta)G_{yu}U)+(\tilde{N}_u-(I+\theta)G_{yu}M)Q)^{-1}(I+\theta)G_{yd} \\ &= G_{ed} + G_{eu}M(\tilde{U}+Q\tilde{M})\tilde{M}(I-\theta N_u(\tilde{U}+Q\tilde{M}))^{-1}(I+\theta)G_{yd} \end{aligned} \tag{31}$$

for parametric faults at the output, respectively.

Using a standard setup formulation, we get the following open loop transfer functions for the design of the Q controller in the two cases (see Figure 5 for the standard setup). For the input fault case, we have

$$\begin{aligned} P_{m,i}(\theta) &= \begin{pmatrix} \bar{G}_{ed}(\theta) & \bar{G}_{eu}(\theta) \\ \bar{G}_{yd}(\theta) & \bar{G}_{yu}(\theta) \end{pmatrix} \\ &= \begin{pmatrix} G_{ed} + G_{eu}(I+\theta)U(I-\tilde{N}_u\theta U)^{-1}\tilde{M}G_{yd} & G_{eu}(I+\theta)(I-U\tilde{N}_u\theta)^{-1}M \\ (I-\tilde{N}_u\theta U)^{-1}\tilde{M}G_{yd} & (I-\tilde{N}_u\theta U)^{-1}\tilde{N}_u\theta M \end{pmatrix} \end{aligned} \tag{32}$$

and for the output fault case, we have

$$\begin{aligned} P_{m,o}(\theta) &= \begin{pmatrix} \bar{G}_{ed}(\theta) & \bar{G}_{eu}(\theta) \\ \bar{G}_{yd}(\theta) & \bar{G}_{yu}(\theta) \end{pmatrix} \\ &= \begin{pmatrix} G_{ed} + G_{eu}M\tilde{U}(I-\theta N_u\tilde{U})^{-1}(I+\theta)G_{yd} & G_{eu}M(I-\tilde{U}\theta N_u)^{-1} \\ \tilde{M}(I-\theta N_u\tilde{U})^{-1}(I+\theta)G_{yd} & \tilde{M}\theta N_u(I-\tilde{U}\theta N_u)^{-1} \end{pmatrix} \end{aligned} \tag{33}$$

respectively.

As in the additive fault case, it is possible to combine fault tolerant control with fault isolation. It is then possible to design a number of Q controllers, one for every single fault case and then select a specific Q controller when a fault appear in the system. A system setup including a FTC controller for 3 potential parametric faults is shown in Figure 2, where Q_{FTC} are the FTC part and $Q_{FDI,i}$ are the residual generators for the fault isolation part.

5.3. FTC for Systems with Structural Changes

This is the most relevant problem in connection with FTC. From a feedback point of view, a fault in a closed-loop system will in most cases change the structure of the system. However, in many cases, these structural changes can be described by using LFTs as considered in the parametric fault case.

In the following, let us just consider the system given by transfer functions described by (5). It is further assumed that the system can only be in the normal (nominal) mode and in one abnormal mode. The abnormal mode is given by:

$$\Sigma_S : \begin{pmatrix} \tilde{G}_{ed} & \tilde{G}_{eu} \\ \tilde{G}_{yd} & \tilde{G}_{yu} \end{pmatrix} \tag{34}$$

The closed loop transfer function for the nominal system Σ and Σ_S when the feedback controller in (2) is applied are given by

$$\begin{array}{rcl} T_{ed,nom}(s) & = & G_{ed} + G_{eu}K(I - G_{yu}K)^{-1}G_{yd} \\ T_{ed,S}(s) & = & \tilde{G}_{ed} + \tilde{G}_{eu}K(I - \tilde{G}_{yu}K)^{-1}\tilde{G}_{yd} \end{array} \tag{35}$$

Following the line from the above section, we can again calculate S as a function of the system changes and use this for obtaining FTC. The structural changes of G_{yu} can be described in the following way:

$$\begin{array}{rcl} \tilde{G}_{yu} & = & G_{yu} + (\tilde{G}_{yu} - G_{yu}) \\ & = & G_{yu} + \theta \end{array}$$

From Table 1, we have that

$$S = \tilde{M}\theta(I - U\tilde{M}\theta)^{-1}M \tag{36}$$

Using $\theta = \tilde{G}_{yu} - G_{yu}$ in S, we get directly

$$S = (\tilde{M}\tilde{G}_{yu} - \tilde{N}_u)(\tilde{V} - \tilde{U}\tilde{G}_{yu})^{-1}$$

If S given by (36) is unstable, the controller needs to be modified by using the Q feedback controller for stabilizing the system in the abnormal mode. Based on this fact, we have the following FTC design problem for systems with structural changes.

Problem 6 ***The fault tolerant control problem for system with structural changes*** *is defined as the problem of designing, if existent, a feedback controller Q, such that $\tilde{S}(Q)$ given by*

$$\tilde{S}(Q) = (I - QS)^{-1}$$

is stable, where S is given by

$$S = \tilde{M}\theta(I - U\tilde{M}\theta)^{-1}M$$

with $\theta = \tilde{G}_{yu} - G_{yu}$.

Now, let us consider the closed loop transfer function from d to e given by (35). Let the system given in the abnormal mode be described as additive changes of the nominal transfer functions, i.e.

$$\begin{pmatrix} \tilde{G}_{ed} & \tilde{G}_{eu} \\ \tilde{G}_{yd} & \tilde{G}_{yu} \end{pmatrix} = \begin{pmatrix} G_{ed} & G_{eu} \\ G_{yd} & G_{yu} \end{pmatrix} + \begin{pmatrix} \theta_{ed} & \theta_{yd} \\ \theta_{eu} & \theta_{yu} \end{pmatrix} \tag{37}$$

In the general case, the θ parameters defined in (37) will be function of a single θ parameter, i.e.

$$\begin{pmatrix} \theta_{ed} & \theta_{yd} \\ \theta_{eu} & \theta_{yu} \end{pmatrix} = \begin{pmatrix} \theta_{ed}(\theta) & \theta_{yd}(\theta) \\ \theta_{eu}(\theta) & \theta_{yu}(\theta) \end{pmatrix}$$

due to the fact that every system change is caused by a single fault. The closed loop transfer function $T_{ed,S}(s)$ is given by is the given by

$$\begin{aligned} T_{ed,S}(s) &= \tilde{G}_{ed} + \tilde{G}_{eu}K(I - \tilde{G}_{yu}K)^{-1}\tilde{G}_{yd} \\ &= (G_{ed} + \theta_{ed}) + (G_{eu} + \theta_{eu})K(I - (G_{yu} + \theta_{yu})K)^{-1}(G_{yd} + \theta_{yd}) \end{aligned} \tag{38}$$

In the special case where G_{yu} does not change in the abnormal mode, i.e. $T_{ed,S}(s)$ in (38) is given by

$$T_{ed,S}(s) = (G_{ed} + \theta_{ed}) + (G_{eu} + \theta_{eu})K(I - G_{yu}K)^{-1}(G_{yd} + \theta_{yd})$$

In this case, the stability of the closed loop system will not be affected by the system change. The system change will only affect the performance of the closed loop system. This is equivalent with the additive fault case, where the design of Q turns out to be an open loop design problem. Note that a change in G_{ed} and/or G_{eu} might not be detectable from the measurement signal y, which can make it impossible to do any compensation for the fault in the system. This case will not be discussed further.

As a closing of this section, we will give the $\mathcal{H}_\alpha$, $\alpha \in \{2, \infty\}$ fault tolerant control design problem with mild performance reduction for system with structural changes. For doing this, $K(Q)$ is applied. It is further assumed that $\theta_{yu}(\theta) = \theta$. This assumption is without loss of generality. We then have the following design problem.

Problem 7 *For a given number $\gamma > 0$, $\alpha \in \{2, \infty\}$,* ***the $\mathcal{H}_\alpha$ suboptimal fault tolerant control problem with performance recovery for system with structural changes*** *is defined as the problem of designing, if existent, a feedback controller Q_α, such that the closed loop transfer function $T_{ed,s}$ is stable and the $\mathcal{H}_\alpha$ norm of $T_{ed,s}$ is less than or equal to γ, where $T_{ed,s}$ is given by*

$$T_{ed,s} = \mathcal{F}_l(P_s, Q_\alpha)$$

and P_s is given by

$$P_s = \begin{pmatrix} (G_{ed} + \theta_{ed}) + (G_{eu} + \theta_{eu})U\tilde{M}(I - \theta U\tilde{M})^{-1}(G_{yd} + \theta_{yd}) & (G_{eu} + \theta_{eu})(I - U\tilde{M}\theta)^{-1}M \\ \tilde{M}(I - \theta U\tilde{M})^{-1}(G_{yd} + \theta_{yd}) & \tilde{M}\theta(I - U\tilde{M}\theta)^{-1}M \end{pmatrix}$$

6. A Passive Fault Tolerant Controller Architecture

In the above section, the applied architecture for the fault tolerant controllers is based on a fault detection/isolation followed by a connection of a dedicated FTC controller Q, see e.g. Figure 2. The fault detection/isolation will introduce a time delay from a fault appear in the system until a fault tolerant controller can be connected to the system. However, it can not in all cases be accepted that a time delay is included between a fault appear in the system until a fault tolerant controller is active. One way to remove this time delay in the FTC architecture is to let the fault tolerant controller be active all the time. As a consequence of this, the fault tolerant controller Q needs to be designed with respect to both the performance of the nominal system as well as with respect to closed loop stability of the faulty system. This approach is known as *passive* fault tolerant control.

Since passive fault tolerant control is based on one fixed controller, this approach is intimately related to robust control. One of the differences is that in robust control, all plants in the uncertainty set are given equal weight in the design process. In contrast, in passive fault tolerant control, usually the nominal model will be given much higher weight than the faulty situations. In a typical design case, only a minor detuning of the nominal controller can be accepted, which means that the faulty situations will lead to a relatively larger performance degradation. In its extreme version, this is known as a 'limb home strategy'.

Using the Youla-Kucera architecture shown in Figure 1 as the architecture for a passive fault tolerant controller, we get the following transfer function for the performance of the nominal closed loop system:

$$T_{ed} = G_{ed} + G_{eu}U\tilde{M}G_{yd} + G_{eu}MQ\tilde{M}G_{yd} \tag{39}$$

Further, let the dual Youla-Kucera parameter for the faulty system be given by S. Then the FTC design problem is to design Q such that

$$\tilde{S} = (I - QS)^{-1} \in \mathcal{RH}_\infty \tag{40}$$

Design of a Q controller that will minimize (or at least make smaller than some admissible bound) a suitable norm of the closed loop transfer function given in (39) and also satisfy the stability condition in (40) is a multi objective design problem. Further and more important, it is required that Q is open loop stable, because Q appears in an open loop in T_{ed} in (39). This means that the faulty system must be stabilizable by a stable Q controller, i.e. it must be strongly stabilizable.

It should also be pointed out that this passive FTC approach has the disadvantage that it can only handle a single fault or a few faults in the system. Further, another problem is a possible reduction of the performance of the nominal system by including Q in the closed loop system.

Lets close this section with the design problem for passive fault tolerant controllers.

Problem 8 *For a given number $\gamma > 0$, $\alpha \in \{2, \infty\}$, **the passive fault tolerant control problem** is defined as the problem of designing, if existent, a feedback controller $Q_\alpha, \in \mathcal{RH}_\infty$, such that the $\mathcal{H}_\alpha$ norm of the nominal closed loop transfer function T_{ed} is less than or equal to γ, and stabilize the faulty system, i.e.*

$$\tilde{S} = (I - Q_\alpha S)^{-1} \in \mathcal{RH}_\infty$$

where T_{ed} is given by

$$T_{ed} = G_{ed} + G_{eu}U\tilde{M}G_{yd} + G_{eu}MQ\tilde{M}G_{yd}$$

7. Conclusion

An architecture for fault tolerant control has been proposed. This architecture relies on a common framework for fault modeling based on linear fractional transformations, which facilitates modeling of additive faults, parametric faults, as well as faults that change the model structure.

By applying the (primary) Youla-Kucera parameterization, an additional controller parameter has been introduced as the main tool to achieve fault tolerance. A feature of the Youla-Kucera parameterization is that it automatically includes a diagnostic signal.

Systematic design procedures to obtain numerical values for the correction parameter have been indicated, which rely on optimization based control design techniques.

In order to quantify the fault tolerance of a given configuration, the dual Youla-Kucera parameterization has been introduced. The magnitude of the corresponding parameter reflects the magnitude of faults that can be handled by the FTC system without losing e.g. stability or performance.

Although faults leading to structural changes of a system in principle calls for ad hoc solutions, it has still been possible to give general formulae for fairly rich and important classes of structural changes.

References

[1] Anderson B.: From Youla-Kucera to identification, adaptive and nonlinear control. *Automatica*, vol. 34, no. 12, pp. 1485–1506, 1998.

[2] Basseville M., Nikiforov I.: *Detection of abrupt changes - theory and application*. Prentice Hall 1993.

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

[4] Blanke M., Staroswiecki M., Wu E.: Concepts and methods in fault-tolerant control. *Proceedings of the American Control Conference, ACC-2001*, pp. 2606–2620, Washington DC, USA 2001.

[5] Boskovic J., Mehra R.: A multiple model-based reconfigurable flight control system design. *Proceedings of the 37th IEEE Conference on Decision and Control*, pp. 4503 –4508, 1998.

[6] Boskovic J., Yu S., Mehra R.: Stable adaptive fault-tolerant control of overactuated aircraft using multiple models, swithcing and tuning. *Proceedings the AIAA Guidance, Navigation and Control Conference*, pp. 3612–3617, 1998.

[7] Boyd S., Balakrishnan V., Barratt C., Khraishi N., Li X., Meyer D., Norman S.: A new CAD method and associated architectures for linear controllers. *IEEE Transactions on Automatic Control*, vol. 33, no. 3, pp. 268–283, 1988.

[8] Boyd S., Barratt C.: *Linear controller design - limits of performance*. Prentice Hall 1991.

[9] Chen J., Patton R.: *Robust model-based fault diagnosis for dynamic systems*. Kluwer Academic Publishers 1998.

[10] Dahleh M., Diaz-Bobillo I.: *Control of Uncertain systems*. Prentice Hall 1995.

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

[12] Ganguli S., Marcos A., Balas G.: Reconfigurable LPV control design for Boeing 747-100/200 longitudinal axis. *Proceedings of the American Control Conference*, vol. 5, pp. 3612–3617, 2002.

[13] Gertler J.: *Fault detection and diagnosis in engineering systems*. Marcel Dekker 1998.

[14] Grimble M.: *Robust industrial control - Optimal design approach for polynomial systems*. Prentice Hall 1994.

[15] Niemann H., Stoustrup J.: Passitive fault tolerant control of an inverted double pendulum - A case study example, 2002, submitted for publication.

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

[17] Niemann H., Stoustrup J.: An architecture for fault tolerant controllers. *International Journal of Control*, vol. 78, no. 14, pp. 1091–1110, 2005.

[18] Niemann H., Stoustrup J.: Passive fault tolerant control of a double inverted pendulum - a case study. *Control Engineering Practice*, vol. 13, no. 8, pp. 1047–1059, 2005.

[19] Niemann H., Stoustrup J., Abrahamsen R.: A note on implementation of multivariable controllers, 2002, submitted for publication, journal paper.

[20] Odgaard P., Stoustrup J., Andersen P., Vidal E.: Computing decoupled residuals for compact disc players. *Proceedings of the 6th IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes*, Beijing, PRC 2006.

[21] Odgaard P., Stoustrup J., Andersen P., Vidal E.: Accommodation of repetitive sensor faults - applied to surface faults on compact discs. *IEEE Transactions on Control Systems Technology*, vol. 16, pp. 348 – 355, 2008.

[22] Odgaard P., Stoustrup J., Andersen P., Wickerhauser M.: Wavelet packet based detection of surface faults on compact discs. *Proceedings of the 6th IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes*, Beijing, PRC 2006.

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

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

[25] Saberi A., Stoorvogel A.A., Sannuti P.: Exact, almost, and optimal input decoupled (delayed) observers. *International Journal of Control*, vol. 73, no. 7, pp. 552–582, 2000.

[26] Skogestad S., Postlethwaite I.: *Multivariable feedback control - Analysis and design*. John Wiley & Sons 1996.

[27] Soltani S., Izadi-Zamanabadi R., Stoustrup J.: Parametric fault detection based on H-infinity optimization in a satellite launch vehicle. *Proceedings of the 2008 IEEE Multi-conference on Systems and Control*, San Antonio, Texas, USA 2008.

[28] Staroswiecki M.: On reconfigurability with respect to actuator failures. *Proceedings of the IFAC World Congress*, Barcelona, Spain 2002.

[29] Staroswiecki M., Hoblos G., Aïtouche A.: Fault tolerance analysis of sensor systems. *Proceedings of the 38th IEEE Conference on Decision and Control*, Phoenix, Arizona 1999.

[30] Stoustrup J., Blondel V.: Fault tolerant control: A simultaneous stabilization result. *IEEE Transactions on Automatic Control*, vol. 49, no. 2, pp. 305–310, 2004.

[31] Stoustrup J., Niemann H.: Fault tolerant feedback control using the youla parameterization. *Proceedings of the 6th European Control Conference*, pp. 1970–1974, Porto, Portugal 2001.

[32] Stoustrup J., Niemann H.: Fault estimation - a standard problem approach. *International Journal of Robust and Nonlinear Control*, vol. 12, pp. 649–673, 2002.

[33] Stoustrup J., Niemann H.: Fault isolability conditions for linear systems with additive faults. *Proceedings of the 2006 American Control Conference*, Minneapolis, Minnesota, USA 2006.

[34] Stoustrup J., Zhou K. (eds.): *Robustness Issues in Fault Diagnosis and Fault Tolerant Control*. Hindawi Publishing Corp US SR 2007, ISBN-10: 9774540255, ISBN-13: 978-9774540257, 168 pages.

[35] Tay T., Mareels I., Moore J.: *High performance control*. Birkhäuser 1997.

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

[37] Wu N.: Reconfigurable control design: Achieving stability robustness and failure tracking. *Proceedings of the 32nd Conference on Decision and Control*, pp. 2278–2283, San Antonio, Texas, USA 1993.

[38] Wu N., Chen T.: Feedback design in control reconfigurable systems. *International Journal of Robust and Nonlinear Control*, vol. 6, no. 6, pp. 561–570, 1996.

[39] Wu N., Zhou K., Salomon G.: Control reconfigurability of linear time-invariant systems. *Automatica*, vol. 36, pp. 1767–1771, 2000.

[40] Youla D., Bongiorno J., Jabr H.: Modern Wiener-Hopf design of optimal controllers - Part I: The single-input-output case. *IEEE Trans. Automatic Control*, vol. 21, no. 1, pp. 3–13, 1976.

[41] Youla D., Jabr H., Bongiorno J.: Modern Wiener-Hopf design of optimal controllers - Part II: The multivariable case. *IEEE Trans. Automatic Control*, vol. 21, no. 3, pp. 319–338, 1976.

[42] Zhou K., Doyle J., Glover K.: *Robust and optimal control*. Prentice Hall 1995.

[43] Zhou K., Ren Z.: A new controller architecture for high performance robust, and fault-tolerant control. *IEEE Transactions on Automatic Control*, vol. 46, no. 10, pp. 1613–1618, 2001.

FAULT DIAGNOSIS AND FAULT TOLERANT CONTROL: AN OPTIMIZATION BASED APPROACH

J. Stoustrup*

*Automation & Control, Department of Electronic Systems, Aalborg University, Fr. Bajers Vej 7C, Denmark. Email: jakob@es.aau.dk, URL: es.aau.dk/staff/jakob

FAULT DIAGNOSIS AND FAULT TOLERANT CONTROL: AN OPTIMIZATION BASED APPROACH. A general architecture for fault tolerant control is proposed. The architecture is based on the (primary) Youla-Kucera parameterization of all stabilizing compensators, and uses the dual Youla-Kucera parameterization to quantify the performance of the fault tolerant system.

The approach suggested can be applied for additive faults, parametric faults, and for system structural changes. The modeling for each of these fault classes are described.

The method allows to design for passive as well as for active fault handling. Also, the related design method can be fitted either to guarantee stability or to achieve graceful degradation in the sense of guaranteed degraded performance.

A number of fault diagnosis problems, fault tolerant control problems, and feedback control with fault rejection problems are formulated/considered, mainly from a fault modeling point of view.