Proceeding of the 2004 American Control Conference
Boston, Massachusetts June 30 - July 2, 2004

A Simultaneous Stabilization Approach to (Passive) Fault Tolerant Control

Jakob Stoustrup

Department of Control Engineering
Institute of Electronic Systems
Aalborg University
DK-9220 Aalborg
Denmark

E-mail: jakob@control.aau.dk
URL: www.control.aau.dk/~jakob/

Vincent D. Blondel

Department of Mathematical Engineering
Université catholique de Louvain
Avenue Georges Lemaître, 4
B-1348 Louvain-la-Neuve
Belgium

E-mail: blondel@inma.ucl.ac.be
URL: www.inma.ucl.ac.be/~blondel/

***Abstract*— This paper discusses the problem of designing fault tolerant compensators that stabilize a given system both in the nominal situation, as well as in the situation where one of the sensors or one of the actuators has failed. It is shown that such compensators always exist, provided that the system is detectable from each output and that it is stabilizable. The proof of this result is constructive. A family of second order systems is described that requires fault tolerant compensators of arbitrarily high order.**

I. Introduction

The interest for using fault tolerant controllers is increasing. A number of theoretical results as well as application examples has now been described in the literature, see e.g. [1], [2], [3], [4], [5], [6], [7], [8], [9], [10] to mention some of the relevant references in this area.

The approaches to fault tolerant control can be divided into two main classes: *Active* fault tolerant control and *passive* fault tolerant control. In active fault tolerant control, the idea is to introduce a fault detection and isolation block in the control system. Whenever a fault is detected and isolated, a supervisory system takes action, and modifies the structure and/or the parameters of the feedback control system. In contrast, in the passive fault tolerant control approach, a fixed compensator is designed, that will maintain (at least) stability if a fault occurs in the system.

This paper will only discuss the passive fault tolerant control approach, also sometimes referred to as *reliable* control. This approach has mainly two motivations. First, designing a fixed compensator can be made in much simpler hardware and software, and might thus be admissible in more applications. Second, classical reliability theory states that the reliability of a system decreases rapidly with the complexity of the system. Hence, although an active fault tolerant control system might in principle accomodate specific faults very efficiently, the added complexity of the overall system by the fault detection system and the supervisory system itself, might in fact sometimes deteriorate plant reliability.

In [11], a fault tolerant control problem has been addressed for systems, where specific sensors could potentially fail such that the corresponding outputs were unavailable for feedback, whereas other outputs were assumed to be available at all times.

In [12, Sec. 5.5], the question of fault tolerant parallel compensation has been discussed, i.e. whether it is possible to design two compensators such that any of them alone or both in parallel will internally stabilize the closed loop system.

The existence results given in [11], [12] mentioned above, can be considered to be special cases of the main results of this paper.

In this paper, we shall consider systems for which any sensor (or in the dual case any actuator) might fail, and we wish to determine for which systems such (passive) fault tolerant compensators exist. The main results state that the only precondition for the existence of solutions to this fault tolerant control problem is just stabilizability from each input and detectability of the system from each output.

II. Notation

Throughout the paper, $\mathcal{RP}^{p\times m}$ shall denote the set of proper, real-rational functions taking values in $\mathcal{C}^{p\times m}$, and $\mathcal{RSP}^{p\times m}$ shall denote the set of strictly proper, real-rational functions taking values in $\mathcal{C}^{p\times m}$. $\mathcal{RH}_\infty^{p\times m}$ shall denote the set of stable, proper, real-rational functions taking values in $\mathcal{C}^{p\times m}$. The notation $\{s \in \mathcal{R}_{+\infty} : B(s) = 0\}$ will be used as shorthand for zeros of $B(\cdot)$ on the positive real line. The set includes the point at infinity if $\lim_{s\to\infty} B(s) = 0$. For matrices A,B,C,D of compatible dimensions, the expression

$$G(s) = \left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right)$$

will be used to denote the transfer function $G(s) = C(sI - A)^{-1}B + D$. Real-rational functions will be indicated by their dependency of a complex variable s (as in $G(s)$, $K(s)$), although the dependency of s will be suppressed in the notation (as in G, K), where no misunderstanding should be possible.

III. Problem Formulation

Consider a system of the form:

$$\begin{aligned} \dot{x} &= Ax + Bu \\ y_1 &= C_1 x \\ y_2 &= C_2 x \\ &\vdots \\ y_p &= C_p x \end{aligned} \tag{1}$$

where $x \in \mathcal{R}^n$, $u \in \mathcal{R}^m$, $y_i \in \mathcal{R}$, $i = 1 \dots, p$ and $A, B, C_i, i = 1 \dots, p$ are matrices of compatible dimensions. Each of the p measurements y_i, $i = 1, \dots, p$, is the output of a sensor, which can potentially fail.

In this paper, we will determine whether it is possible to design a feedback compensator that is guaranteed to stabilize a given system, in case *any* sensor could potentially fail. To be more precise, we are looking for a dynamic compensator $u = K(s)y$, $K \in \mathcal{RP}^{m\times p}$, with the property, that each of the following feedback laws:

$$u = K(s)\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_p \end{pmatrix},$$

$$u = K(s)\begin{pmatrix} 0 \\ y_2 \\ \vdots \\ y_p \end{pmatrix}, \quad u = K(s)\begin{pmatrix} y_1 \\ 0 \\ \vdots \\ y_p \end{pmatrix},$$

$$\dots, \quad u = K(s)\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ 0 \end{pmatrix} \tag{2}$$

are internally stabilizing, i.e. that both the nominal system as well as each of the systems resulting from one of the sensors failing are all stabilized by $K(s)$.

It is obvious, that the answer to this question immediately provides the answer to the corresponding dual question: i.e. whether is is possible to design a compensator, that works in the nominal situation, but also if any of the actuators would fail.

IV. Preliminaries

We remind the reader - see e.g. [13, Theorem 5.9, Page 127] - that a doubly coprime factorization of a strictly proper plant and a stabilizing compensator

$$\begin{aligned} G(s) &= N(s)M^{-1}(s) = \tilde{M}^{-1}(s)\tilde{N}(s) \\ K(s) &= U(s)V^{-1}(s) = \tilde{V}^{-1}(s)\tilde{U}(s) \end{aligned}$$

where

$$\begin{aligned} &G \in \mathcal{RSP}^{p\times m}, \quad N \in \mathcal{RH}_\infty^{p\times m}, \quad M \in \mathcal{RH}_\infty^{m\times m}, \\ &\qquad \tilde{M} \in \mathcal{RH}_\infty^{p\times p}, \quad \tilde{N} \in \mathcal{RH}_\infty^{p\times m}, \\ &K \in \mathcal{RP}^{m\times p}, \quad U \in \mathcal{RH}_\infty^{m\times p}, \quad V \in \mathcal{RH}_\infty^{p\times p}, \\ &\qquad \tilde{V} \in \mathcal{RH}_\infty^{m\times m}, \quad \tilde{U} \in \mathcal{RH}_\infty^{m\times p} \end{aligned}$$

can be found from an observer based controller by the formulae:

$$\begin{aligned} \begin{pmatrix} M & U \\ N & V \end{pmatrix} &= \left(\begin{array}{c|cc} A+BF & B & -L \\ \hline F & I & 0 \\ C & 0 & I \end{array}\right) \\ \begin{pmatrix} \tilde{V} & \tilde{U} \\ \tilde{N} & \tilde{M} \end{pmatrix} &= \left(\begin{array}{c|cc} A+LC & B & L \\ \hline -F & I & 0 \\ C & 0 & I \end{array}\right) \end{aligned} \tag{3}$$

where A, B, C are parameters for a (minimal) state space representation for $G(s)$, i.e. matrices of smallest, compatible dimensions such that

$$G(s) = \left(\begin{array}{c|c} A & B \\ \hline C & 0 \end{array}\right)$$

F is an arbitrary stabilizing state feedback gain and L is an arbitrary stabilizing observer gain, i.e. F and L are matrices of compatible dimensions such that both $A+BF$ and $A+LC$ have characteristic polynomials which are Hurwitz.

The eight matrices defined by (3) satisfy the double Bezout identity:

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

We also remind the reader, that a *unit* is an element of a ring, which has an inverse in that ring. In particular, a unit in the ring of stable proper rational functions, is simply a stable proper function with a stable proper inverse.

We will need the following result (see [14, Theorem 5.2, Page 106] or [12, Corollary 6, Page 118]) on the strong stabilization problem, i.e. the problem of finding a stable stabilizing compensator:

Lemma 1: Let $A(s), B(s)$ be stable proper transfer functions. Then there exists a stable proper transfer function $Q(s)$ such that the function

$$A(s) + B(s)Q(s)$$

is a unit in the ring of stable proper rational functions, if and only if

$$A(z_{\text{ip}})$$

has constant sign for all $z_{\text{ip}} \in \{s \in \mathcal{R}_{+\infty} : B(s) = 0\}$.

V. Main Results

In this section we shall present our main results which state that for systems with several outputs, it is always possible to find a compensator, that both stabilizes the nominal situation, as well as the situation where any of the sensors fails. In a similar fashion, it is shown, that it is always possible to design a fault tolerant feedback compensator for a system with several actuators. The only precondition to these results, is in the first case that all unstable modes for the system are observable by each sensor and in the second (dual) case, that all modes are controllable by each actuator.

Theorem 1: Consider a system given by a state space model of the form (1). Assume, that the pair (A,B) is stabilizable, and that each of the pairs $(C_i,A)\,,i=1,\ldots,p$, is detectable. Then, there exists a dynamic compensator $K(s)$ such that each of the $p+1$ control laws (2) internally stabilizes the system (1).

The proof will be constructive, and we shall give some comments on practical computations in the sequel of the proof.

Proof: First, let us note that it suffices to prove the result in the case where $m=1$ and $p=2$. To see that $m=1$ can be assumed without loss of generality, one can just consider the system

$$\begin{array}{rclcl} \dot{x} & = & Ax & + & \bar{B}\bar{u} \\ y_1 & = & C_1 x & & \\ y_2 & = & C_2 x & & \\ & \vdots & & & \\ y_p & = & C_p x & & \end{array} \tag{4}$$

where $\bar{B}=Bv, v\in\mathcal{R}^{m\times 1}, \bar{u}\in\mathcal{R}$, and v is any vector such that the pair $(A,\bar{B})$ is also stabilizable. This is always possible, see e.g. [15, Corollary 1.1, Page 43]. Thus, if $\bar{u}=\bar{K}(s)y$ is a fault tolerant feedback law for (4), then $u=K(s)\underline{y}$ is a fault tolerant feedback law for (1) with $K(s)=v\bar{K}(s)$.

Next, if

$$K(s)=\begin{pmatrix} K_1(s) & K_2(s) \end{pmatrix} \tag{5}$$

is a fault tolerant feedback compensator for this system:

$$\begin{array}{rclcl} \dot{x} & = & Ax & + & Bu \\ y_1 & = & C_1 x & & \\ y_2 & = & C_2 x & & \end{array} \tag{6}$$

then

$$K(s)=\begin{pmatrix} K_1(s) & K_2(s) & 0 & \ldots & 0 \end{pmatrix} \tag{7}$$

is a fault tolerant feedback compensator for the system (1). Indeed, in the nominal situation or if one of the sensors corresponding to $y_i, i=3,\ldots,p$ fails, the control signal generated by (7) will be the same as the control signal generated by (5) in the nominal situation. If $y_i, i=1,2$ fails, (7) will still generate the same control signal as (5) which is known to stabilize the shared dynamics of the two systems.

Thus, without loss of generality, we will assume that the system in consideration has the form

$$\begin{array}{rclcl} \dot{x} & = & Ax & + & Bu \\ y_1 & = & C_1 x & & \\ y_2 & = & C_2 x & & \end{array} \tag{8}$$

where B is a single column matrix, $C_i, i=1,2$ are single row matrices, $u,y_i\in\mathcal{R}, i=1,2$. Thus, it will be assumed that the transfer functions from u to each of the outputs are scalar.

Define $C=\begin{pmatrix} C_1 \\ C_2 \end{pmatrix}$ and let $K_0(s)$ be an internally stabilizing compensator for the system (8), which has the transfer function $G(s)=C(sI-A)^{-1}B$. Introduce a doubly coprime factorization of $G(s)$ and $K_0(s)$, i.e. stable proper functions $M,N,\tilde{V}_0,\tilde{U}_0$:

$$G(s)=N(s)M^{-1}(s)=\begin{pmatrix} N_1(s) \\ N_2(s) \end{pmatrix} M^{-1}(s)$$

$$K_0(s)=\tilde{V}_0^{-1}(s)\tilde{U}_0(s)=\tilde{V}_0^{-1}(s)\begin{pmatrix} \tilde{U}_{0,1}(s) & \tilde{U}_{0,2}(s) \end{pmatrix}$$

satisfying the Bezout identity

$$\tilde{V}_0 M-\tilde{U}_0 N=\tilde{V}_0 M-\tilde{U}_{0,1}N_1-\tilde{U}_{0,2}N_2=1 \tag{9}$$

This can always be done - explicit formulae are given by (3).

Next, we note that replacing in (9) the triplet

$$\begin{pmatrix} \tilde{V}_0 & \tilde{U}_{0,1} & \tilde{U}_{0,2} \end{pmatrix} \quad \text{by} \quad \begin{pmatrix} \tilde{V} & \tilde{U}_1 & \tilde{U}_2 \end{pmatrix}$$

where

$$\begin{array}{rcl} \tilde{V} & = & \tilde{V}_0-Q_2N_1-Q_3N_2 \\ \tilde{U}_1 & = & \tilde{U}_{0,1}-Q_1N_2-Q_2M \\ \tilde{U}_2 & = & \tilde{U}_{0,2}+Q_1N_1-Q_3M \end{array}$$

also provides a solution to (9), as this simple calculation shows:

$$\begin{aligned} &\tilde{V}M-\tilde{U}_1N_1-\tilde{U}_2N_2 \\ &=\left(\tilde{V}_0-Q_2N_1-Q_3N_2\right)M-\left(\tilde{U}_{0,1}-Q_1N_2-Q_2M\right)N_1 \\ &\qquad-\left(\tilde{U}_{0,2}+Q_1N_1-Q_3M\right)N_2 \\ &=\tilde{V}_0M-\tilde{U}_{0,1}N_1-\tilde{U}_{0,2}N_2 \\ &=1 \end{aligned}$$

Consequently, any transfer function of the form:

$$\begin{aligned} &\tilde{V}^{-1}\begin{pmatrix} \tilde{U}_1 & \tilde{U}_2 \end{pmatrix} \\ &=\left(\tilde{V}_0-Q_2N_1-Q_3N_2\right)^{-1} \\ &\qquad\times\begin{pmatrix} \tilde{U}_{0,1}-Q_1N_2-Q_2M & \tilde{U}_{0,2}+Q_1N_1-Q_3M \end{pmatrix} \end{aligned} \tag{10}$$

where Q_1,Q_2,Q_3 are all stable proper rational functions, is also a stabilizing compensator.

In the sequel, we shall demonstrate, that Q_1,Q_2,Q_3 can be chosen such that $\tilde{V}^{-1}\begin{pmatrix} \tilde{U}_1 & \tilde{U}_2 \end{pmatrix}$ stabilizes both the nominal and the faulty systems.

If the sensor corresponding to one of the outputs fails, the controller $\tilde{V}^{-1}\begin{pmatrix} \tilde{U}_1 & \tilde{U}_2 \end{pmatrix}$ has to stabilize a system of the form:

$$G=\begin{pmatrix} N_1(s) \\ 0 \end{pmatrix} \qquad \text{or} \qquad G=\begin{pmatrix} 0 \\ N_2(s) \end{pmatrix}$$

which means that stability is obtained if and only if the compensator (10) satisfies the two equations:

$$\begin{aligned}
&\left(\tilde{V}_0 - Q_2N_1 - Q_3N_2\right)M \\
&- \begin{pmatrix} \tilde{U}_{0,1} - Q_1N_2 - Q_2M & \tilde{U}_{0,2} + Q_1N_1 - Q_3M \end{pmatrix} \begin{pmatrix} N_1 \\ 0 \end{pmatrix} \\
&= \tilde{V}_0M - Q_2N_1M - Q_3N_2M \\
&\quad - \tilde{U}_{0,1}N_1 + Q_1N_2N_1 + Q_2MN_1 \\
&= \tilde{V}_0M - \tilde{U}_{0,1}N_1 + Q_1N_2N_1 - Q_3N_2M = u_1 \qquad (11)
\end{aligned}$$

and

$$\begin{aligned}
&\left(\tilde{V}_0 - Q_2N_1 - Q_3N_2\right)M \\
&- \begin{pmatrix} \tilde{U}_{0,1} - Q_1N_2 - Q_2M & \tilde{U}_{0,2} + Q_1N_1 - Q_3M \end{pmatrix} \begin{pmatrix} 0 \\ N_2 \end{pmatrix} \\
&= \tilde{V}_0M - \tilde{U}_{0,2}N_2 - Q_1N_1N_2 - Q_2N_1M = u_2 \qquad (12)
\end{aligned}$$

where u_1, u_2 are units in the ring of stable proper rational functions.

Thus, the existence of a fault tolerant controller has now been shown to be inferred from the existence of stable proper rational functions Q_1, Q_2, Q_3, such that u_1, u_2 become units. We will prove this existence by first choosing Q_1 appropriately. Subsequently, (11) and (12) will be considered as equations for Q_3 and Q_2 which are no longer coupled, and show that each has an admissible solution.

To that end, first note that it is possible to determine a stable proper function Q_1, such that:

$$Q_1(s)N_1(s)N_2(s) - \tilde{U}_{0,1}(s)N_1(s)\Big|_{s=z_{\text{ip}}} = \frac{1}{2} \qquad (13)$$

for all positive real zeros of M, $z_{\text{ip}} \in \{z \in \mathcal{R}_{+\infty} : M(z) = 0\}$, since $N_1(z_{\text{ip}})N_2(z_{\text{ip}})$ can not be zero for $M(z_{\text{ip}}) = 0$ due to coprimeness of M and N_1 and of M and N_2. To determine Q_1 satisfying (13) in practice can be done by a standard rational interpolation.

Now, for a fixed Q_1, (11) can be recognized as a strong stabilization problem in the variable Q_3. It is known from Lemma 1 that such Q_3 exists if and only if

$$\tilde{V}_0M - \tilde{U}_{0,1}N_1 + Q_1N_2N_1\Big|_{s=z_{\text{ip}}}$$

has constant sign for every value of

$$z_{\text{ip}} \in \{z \in \mathcal{R}_{+\infty} : M(z) = 0 \quad \text{or} \quad N_2(z) = 0\}$$

For $M(z_{\text{ip}}) = 0$ we obtain:

$$\begin{aligned}
&\tilde{V}_0(s)M(s) - \tilde{U}_{0,1}(s)N_1(s) + Q_1(s)N_2(s)N_1(s)\Big|_{s=z_{\text{ip}}} \\
&\quad = -\tilde{U}_{0,1}(s)N_1(s) + Q_1(s)N_2(s)N_1(s)\Big|_{s=z_{\text{ip}}} = \frac{1}{2} \qquad (14)
\end{aligned}$$

from (13). For $N_2(z_{\text{ip}}) = 0$, we get:

$$\begin{aligned}
&\tilde{V}_0(s)M(s) - \tilde{U}_{0,1}(s)N_1(s) + Q_1(s)N_2(s)N_1(s)\Big|_{s=z_{\text{ip}}} \\
&\quad = \tilde{V}_0(s)M(s) - \tilde{U}_{0,1}(s)N_1(s)\Big|_{s=z_{\text{ip}}} = 1 \qquad (15)
\end{aligned}$$

where (9) has been applied. This proves the existence of an admissible function Q_3. To determine Q_3 in practice, one approach is first to find u_1 that interpolates the constraints (14) and (15), and subsequently to determine Q_3 as a solution to (11). If u_1 in addition is chosen to interpolate all constraints arising from zeros of M and N_2 in the right half plane (not just the positive half line), Q_3 can be computed by:

$$Q_3 = \frac{\tilde{V}_0M - \tilde{U}_{0,1}N_1 + Q_1N_2N_1 - u_1}{N_2M} \qquad (16)$$

The proof of existence of an admissible Q_2 is completely analogous to the proof of existence of Q_3. The interpolation constraints for (12) corresponding to $M(z_{\text{ip}}) = 0$ amounts to:

$$\begin{aligned}
&\tilde{V}_0(s)M(s) - \tilde{U}_{0,2}(s)N_2(s) - Q_1(s)N_1(s)N_2(s)\Big|_{s=z_{\text{ip}}} \\
&= -\tilde{U}_{0,2}(s)N_2(s) - Q_1(s)N_1(s)N_2(s)\Big|_{s=z_{\text{ip}}} \\
&= 1 - \tilde{V}_0(s)M(s) + \tilde{U}_{0,1}(s)N_1(s) - Q_1(s)N_1(s)N_2(s)\Big|_{s=z_{\text{ip}}} \\
&= 1 - \frac{1}{2} = \frac{1}{2} \qquad (17)
\end{aligned}$$

where (9) and (13) has been exploited. For $N_1(z_{\text{ip}}) = 0$ we obtain the constraints:

$$\begin{aligned}
&\tilde{V}_0(s)M(s) - \tilde{U}_{0,2}(s)N_2(s)\Big|_{s=z_{\text{ip}}} \\
&\quad = \tilde{V}_0(s)M(s) - \tilde{U}_{0,2}(s)N_2(s) - Q_1(s)N_1(s)N_2(s)\Big|_{s=z_{\text{ip}}} \\
&\quad = 1 \qquad (18)
\end{aligned}$$

from (9). Q_2 can now be found as a solution to (12), and the resulting u_2 will interpolate the conditions (17) and (18). Again, Q_2 might be computed by first finding u_2 interpolating all constraints arising from zeros of M and N_1 in the right half plane (not just (17) and (18)), and then computing Q_2 as:

$$Q_2 = \frac{\tilde{V}_0M - \tilde{U}_{0,2}N_2 - Q_1N_1N_2 - u_2}{N_1M} \qquad (19)$$

Thus, one possible fault tolerant compensator is:

$$\begin{aligned}
K = &\left(\tilde{V}_0 - Q_2N_1 - Q_3N_2\right)^{-1} \\
&\times \begin{pmatrix} \tilde{U}_{0,1} - Q_1N_2 - Q_2M & \tilde{U}_{0,2} + Q_1N_1 - Q_3M \end{pmatrix} \qquad (20)
\end{aligned}$$

which stabilizes the system given by (8) in the nominal case, as well as in the case, where one of the two sensors fail. ■

We again stress that every step in the proof is constructive. A worked example based on a procedure based on this proof can be found in [16].

A corresponding result for actuator failures follows trivially from Theorem 1 by duality:

Theorem 2: Consider a system given by a state space model of the form:

$$\begin{aligned}
\dot{x} &= Ax + B_1u_1 + \ldots + B_mu_m \\
y &= Cx
\end{aligned} \qquad (21)$$

where $x \in \mathcal{R}^n$, $u_i \in \mathcal{R}$, $i = 1\ldots,m$, $y \in \mathcal{R}^p$ and $A, B_i, i = 1\ldots,m$, C are matrices of compatible dimensions. Assume, that each of the pairs (A,B_i), $i = 1,\ldots,m$, is stabilizable and that the pair (C,A) is detectable. Then, there exists a dynamic compensator $K(s)$ such that the nominal control law:

$$u = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_m \end{pmatrix} = K(s)y$$

as well as each of the m control laws

$$u = \begin{pmatrix} 0 \\ u_2 \\ \vdots \\ u_m \end{pmatrix}, \quad u = \begin{pmatrix} u_1 \\ 0 \\ \vdots \\ u_m \end{pmatrix}, \quad \ldots, \quad u = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ 0 \end{pmatrix}$$

internally stabilizes the system (21).

Proof: Follows by transposing the system and the compensator. ■

It is interesting to note that it might be necessary to resort to arbitrarily high controller orders even for a system of low order. As an example, consider for $\varepsilon > 0$:

$$G_\varepsilon(s) = \begin{pmatrix} \frac{s-1}{(s-(1+\varepsilon))(s+1)} \\ \frac{s-1}{(s-(1+\varepsilon))(s+1)} \end{pmatrix} \tag{22}$$

with the following coprime factorization

$$G_\varepsilon(s) = N(s)M(s)^{-1} = \begin{pmatrix} \frac{s-1}{(s+1)^2} \\ \frac{s-1}{(s+1)^2} \end{pmatrix} \left(\frac{s-(1+\varepsilon)}{s+1} \right)^{-1}$$

for which the fault tolerant control problem is equivalent to finding $K(s) = \tilde{V}^{-1} \begin{pmatrix} \tilde{U}_1 & \tilde{U}_2 \end{pmatrix}$ such that

$$\begin{array}{cccccccc} \tilde{V}\frac{s-(1+\varepsilon)}{s+1} & - & \tilde{U}_1\frac{s-1}{(s+1)^2} & - & \tilde{U}_2\frac{s-1}{(s+1)^2} & = & u_1 \\ \tilde{V}\frac{s-(1+\varepsilon)}{s+1} & - & 0 & - & \tilde{U}_2\frac{s-1}{(s+1)^2} & = & u_2 \\ \tilde{V}\frac{s-(1+\varepsilon)}{s+1} & - & \tilde{U}_1\frac{s-1}{(s+1)^2} & - & 0 & = & u_3 \end{array} \tag{23}$$

where u_1, u_2, u_3 are all units in the ring of stable proper functions.

Evaluating these equations at $s = 1$ at $s = \infty$, we notice that

$$u_1(1) = u_2(1) = u_3(1) \quad \text{and} \quad u_1(\infty) = u_2(\infty) = u_3(\infty)$$

On the other hand, we also have

$$u_1(1+\varepsilon) = u_2(1+\varepsilon) + u_3(1+\varepsilon)$$

Let us define the units $v_2 = u_2/u_1$ and $v_3 = u_3/u_1$. Then we have:

$$v_2(1) = v_3(1) = 1\,, \quad v_2(\infty) = v_3(\infty) = 1$$

and

$$v_2(1+\varepsilon) + v_3(1+\varepsilon) = 1$$

From this last equation, we infer that either $v_2(1+\varepsilon) \leq \frac{1}{2}$ or $v_3(1+\varepsilon) \leq \frac{1}{2}$. Assume without loss of generality that $v_2(1+\varepsilon) \leq \frac{1}{2}$. Then v_2 is a unit such that

$$v_2(1) = 1\,, \quad \gamma := v_2(1+\varepsilon) \leq \frac{1}{2}\,, \quad \text{and} \quad v_2(\infty) = 1$$

The constraint at infinity, means that we can assume v_2 to be of the form:

$$v_2(s) = \frac{s^n + \alpha_1 s^{n-1} + \ldots + \alpha_n}{s^n + \beta_1 s^{n-1} + \ldots + \beta_n} \tag{24}$$

for some n, which leads to the conditions:

$$1 + \alpha_1 + \ldots + \alpha_n = 1 + \beta_1 + \ldots + \beta_n \tag{25}$$

and

$$\begin{aligned} &(1+\varepsilon)^n + (1+\varepsilon)^{n-1}\alpha_1 + \ldots + \alpha_n \\ &\quad = \gamma(1+\varepsilon)^n + \gamma(1+\varepsilon)^{n-1}\beta_1 + \ldots + \gamma\beta_n \end{aligned} \tag{26}$$

Subtracting (25) from (26) gives:

$$\begin{aligned} &(1+\varepsilon)^n - 1 + \left((1+\varepsilon)^{n-1} - 1\right)\alpha_1 \\ &\quad + \ldots + ((1+\varepsilon) - 1)\,\alpha_{n-1} \\ &= (\gamma(1+\varepsilon)^n - 1) + \left(\gamma(1+\varepsilon)^{n-1} - 1\right)\beta_1 \\ &\quad + \ldots + (\gamma - 1)\beta_n \end{aligned} \tag{27}$$

We remind the reader, that a necessary condition for (24) to be a unit is that $\alpha_i > 0, \beta_i > 0, i = 1,\ldots,n$. Thus, all the terms on the left hand side of (27) are positive. This means, however, that (27) can only be true if

$$(1+\varepsilon)^n > \frac{1}{\gamma} \geq 2$$

or, equivalently

$$n > \frac{\log 2}{\log(1+\varepsilon)} \to \infty \quad \text{for} \quad \varepsilon \to 0_+$$

From (23) we obtain:

$$\begin{aligned} v_2 = \frac{u_2}{u_1} &= \frac{\tilde{V}\frac{s-(1+\varepsilon)}{s+1} - \tilde{U}_2\frac{s-1}{(s+1)^2}}{\tilde{V}\frac{s-(1+\varepsilon)}{s+1} - \tilde{U}_1\frac{s-1}{(s+1)^2} - \tilde{U}_2\frac{s-1}{(s+1)^2}} \\ &= \frac{(s-(1+\varepsilon))(s+1) - (s-1)\tilde{V}^{-1}\tilde{U}_2}{(s-(1+\varepsilon))(s+1) - (s-1)\tilde{V}^{-1}\tilde{U}_1 - (s-1)\tilde{V}^{-1}\tilde{U}_2} \end{aligned}$$

Since the order of the left hand side of this equation tends to infinity as ε tends to zero, clearly also the order either of $\tilde{V}^{-1}\tilde{U}_1$ or of $\tilde{V}^{-1}\tilde{U}_2$ has to tend to infinity.

Thus, the order of the resulting controller can be required to be of arbitrarily high order even for this family of second order systems.

VI. Conclusions

In this paper, we have proved the existence for any given system of a fault tolerant compensator, which stabilizes the system during its normal operating conditions, but also in the case that one of the sensors or actuators would fail. Only complete failures of sensors or actuators were considered, i.e. the case where the signals of the failing sensor/actuator become zero or at least uncorrelated with the expected signal.

The proof given was constructive, and it was demonstrated for a simple example that carrying out the steps of the proofs can lead to a fault tolerant compensator. It should be stated, however, that the design process is not easy. Also, in practice, the issue of performance should be addressed, which can, unfortunately, not easily be done in the framework suggested here.

It was also shown that the dynamical order of any fault tolerant compensator for some systems even of order two might have to be considerably large, due to intrinsic properties of the system.

A subject of future research is to clarify whether the same results hold for systems in which several sensors and actuators (but not all of either kind) can fail simultaneously.

VII. Acknowledgements

The authors did the research on which this paper is based during a stay at the Institut Mittag-Leffler, Stockholm, Sweden, in the spring of 2003, under a program entitled *Mathematical Control and Systems Theory*. The authors would like to thank the organizers of this Mittag-Leffler program for inviting both authors.

References

[1] M. Blanke, M. Kinnaert, J. Lunze, and M. Staroswiecki, *Diagnosis and Fault-Tolerant Control*. Springer, 2003.

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

[3] H. Niemann and J. Stoustrup, “An architecture for fault tolerant controllers,” submitted for publication.

[4] ——, “Passive fault tolerant control of an inverted double pendulum - A case study example,” in *Proceedings of IFAC SAFEPROCESS 2003*, Washington, DC, USA, 2003, p. 6.

[5] ——, “Reliable control using the primary and dual Youla parameterization,” in *Proceedings of the 41st IEEE Conference on Decision and Control*, Las Vegas, NV, USA, 2002, pp. 4353–4358.

[6] R. Patton, “Fault tolerant control: The 1997 situation,” in *Proceedings of the IFAC Symposium SAFEPROCESS’97*, Hull, England, 1997, pp. 1033–1055.

[7] J. Stoustrup and H. Niemann, “Fault tolerant feedback control using the youla parameterization,” in *Proceedings of the 6th European Control Conference*, Porto, Portugal, Sept. 2001.

[8] N. Wu, Y. Zhang, and K. Zhou, “Detection, estimation and accommodation of loss of control effectiveness,” *International Journal of Adaptive Control and Signal Processing*, vol. 14, pp. 775–795, 2000.

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

[10] K. Zhou and Z. Ren, “A new controller architecture for high performance robust, and fault-tolerant control,” *IEEE Transactions on Automatic Control*, vol. 46(10), pp. 1613–1618, 2001.

[11] A. Alos, “Stabilization of a class of plants with possible loss of outputs or actuator failures,” *IEEE Transactions on Automatic Control*, vol. 28, no. 2, pp. 231–233, Feb. 1983.

[12] M. Vidyasagar, *Control System Synthesis: A Factorization Approach*. Cambridge, Massachusetts: The MIT Press, 1987.

[13] K. Zhou, J. Doyle, and K. Glover, *Robust and Optimal Control*. Prentice Hall, 1996.

[14] V. Blondel, *Simultaneous Stabilization of Linear Systems*, ser. Lecture Notes in Control and Information Sciences. Heidelberg: Springer-Verlag, 1994, no. 191.

[15] W. Wonham, *Linear Multivariable Control: A Geometric Approach*. Springer-Verlag, 1979.

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