Proceedings of the 17th World Congress
The International Federation of Automatic Control
Seoul, Korea, July 6-11, 2008

Using the Unfalsified Control Concept to achieve Fault Tolerance ⋆

Ari Ingimundarson * **Ricardo S. Sánchez Peña** *,**

* *Advanced Control Systems (SAC), Technical University of Catalonia (UPC), Rambla de Sant Nebridi, 10, 08222 Terrassa, Spain (e-mail: ari.ingimundarson@upc.edu)*
** *Institució Catalana de Recerca y Estudis Avançats, Barcelona, Spain (e-mail: ricardo.sanchez-pena@upc.edu)*

Abstract: The paper investigates the use of the unfalsified control concept in the area of fault tolerant control. No fault diagnosis system is required but rather by a simultaneous on-line performance assessment of multiple controllers in a bank of controllers, the best one for the plant at each time can be selected. A controller does not need to form part of the feedback loop for its performance to be assessed. Strategies to construct the bank of controllers are discussed and a switching strategy for fault tolerant control is presented. No previous models of system or faults are necessary, only real-time input/output data streams. Finally the investigated methodology is put to the test by applying it to a non-linear model of the breathing system of a PEM fuel cell.

Keywords: Unfalsified Control, Fault Tolerant Control, Fuel Cells

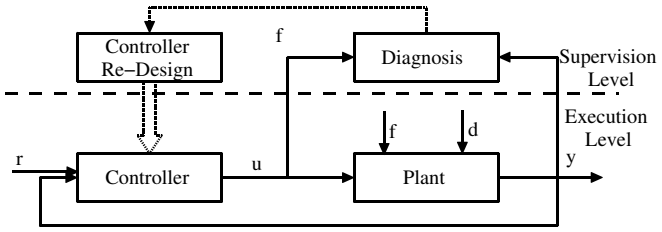

Fig. 1. General architecture of fault tolerant control.

1. INTRODUCTION

Systematic methods to achieve Fault Tolerant Control (FTC) have been an active research topic the last decade, see Blanke et al. (2003). The typical architecture presented as a mean to achieve FTC is shown in Fig. 1. The role of the diagnosis block is to characterize the fault occurring in the plant so that the control-redesign block can adjust the controller to maintain or at least gracefully degrade the control performance when faults occur.

There are several inherent difficulties with this structure, see Zhang and Jiang (2006). Faults are seldom diagnosed without uncertainty and diagnosis delays can occur due to convergence times. Even if it would be assumed that the fault diagnosis information is perfect, predicting what controller performs best is not a trivial problem when a real plant is considered.

Also from a wide-angle perspective, faults and (model, sensor, actuator) uncertainty play similar roles, and the conceptual distinction between them represents a "gray" area. In some sense this distinction should be placed by the designer at the initial stage, and as a consequence he would be forced to design a robust controller to cope with the assumed uncertainties selected (global, dynamic, structured, parametric) and a FTC for the faults, based on this preliminary distinction.

These problems are very difficult and hopes of a standard methodology emerging to solve them are perhaps small, specially considering how related fields such as adaptive control have developed. The adaptive control field has not converged to a standard solution even though research in the field goes back 40 years.

An important trend in research in adaptive control is focusing on the use of multi model techniques and switching supervisory control where a bank of controllers is designed and a decision block decides which controller is most suitable at each moment to achieve the performance specifications according to the measurements of the plant, see Fekri et al. (2006). A frequently mentioned technique to implement the decision block is to use unfalsifed control (UC). Some of the properties that make UC interesting for the FTC field are for example better transient response when changes occur in the plant, see Safonov and Tsao (1997). The reason being that UC can eliminate efficiently large classes of controllers from consideration without inserting them into the feedback path. The use of unfalsified control for fault tolerance was previously presented in Yamé and Kinnaert (2004), but not many application papers have been presented regarding UC and none regarding its use for FTC.

The objective of this work is to use the unfalsified control concept (see Safonov and Tsao (1997)) to achieve fault tolerance in control systems. As mentioned before, UC is

⋆ This work was supported in part by the Research Commission of the *Generalitat de Catalunya* (ref. 2005SGR00537), and by the Spanish CICYT (ref. DPI2005-04722) and (ref. DPI2005-05415).

a recent methodology strongly related to adaptive control that offers some interesting properties for FTC. At heart, UC is a learning mechanism that allows efficient, simultaneous and fast exclusion of unsuitable controllers from a previously defined set of controllers without the use of models to do so. The only online evaluation (instead of diagnosis) is based on the ultimate goal of any practical control system: **performance** [1], and on real-time input/output data streams.

FTC using UC can be performed without a fault diagnosis routine and does not depend on assumptions concerning how many faults can affect the system at a time, nor system or fault models. The unfalsified FTC system is implemented in a switching supervisory controller setting by the creation of a bank of controllers. This allows the construction of the FTC system in a very modular fashion where controllers are added to the bank to handle specified or unspecified faults.

The current paper extends the ideas in Yamé and Kinnaert (2004) by providing a more realistic and practical example. The test of UC for fault tolerance is applied to a serious and relevant control problem: the breathing system of a PEM fuel cell stack where a high fidelity model was used to test the algorithms. Furthermore, a switching strategy tailored to the fault tolerant control problem is presented. As a FTC goal is to take advantage of system redundancy, controllers with different input/output structures were used in the current paper. The algorithms were tested in simulation only as the faults provoked in the system would have easily caused irrevocable damage. In this way a proof of concept would be archived and new research directions could be discovered.

The paper is organized as follows. Section 2 presents the basic concepts on FTC and UC and their connections. Section 3 presents the practical example and section 4, the results obtained after applying several faults to the Hi-Fi simulator. Final conclusions and future research directions are discussed in section 5.

2. FAULT TOLERANCE THROUGH UNFALSIFIED CONTROL

2.1 The unfalsified control concept

The core of unfalsified control is based on ideas of Popper (Popper (1963)) on the philosophy of science. Learning (i.e. controller identification) is achieved by using experimental data to falsify hypothesis. To explain what unfalsified control is, we begin by repeating from Safonov and Tsao (1997) the definition of what is meant by a falsified controller.

[1] At this point, one could be tempted to consider *robust performance* instead of performance as the specification test, and in that case already make a clear distinction between uncertainty and faults. This is not correct due to the fact that the input/output signals measured in real time are already representative of the actual plant. Instead, robust performance (or robust stability) considers a model set that "covers" the actual plant beforehand in order to have certain guarantees of performance (or stability). Therefore performance of the actual plant, through the actual input/output signals are the only necessary information needed to verify in real time applications.

Definition 1. A controller is said to be *falsified* by measurement information if this information is sufficient to deduce that the performance specification $(r, y, u) \in \mathbf{T}_{spec}\ \forall\, r \in \mathbf{R}$ would be violated if that controller would be in the feedback loop. Otherwise the controller is said to be *unfalsified*.

$\mathbf{T}^i_{spec}$ is the performance specification set for controller i. If $(r, y, u) \in \mathbf{T}^i_{spec}$ then the performance is acceptable for signals (r, y, u) in terms of specifications for controller i. The other sets that are used to falsify a controller are:

(1) $\mathbf{K}^i$ denotes the set of triples (r, y, u) satisfying the equations that define the behavior of a controller K^i
(2) $\mathbf{P}_{data}$ denotes the set of triples (r, y, u) consistent with past measurements of (u, y)

A controller i is falsified if it is proven that

$$\mathbf{P}_{data} \cap \mathbf{K}^i \subset \mathbf{T}^i_{spec} \tag{1}$$

is false.

One of the principal advantages of this unfalsified viewpoint is that the set $\mathbf{P}_{data} \cap \mathbf{K}^i$ can be characterized even though the controller K^i does not form part of the feedback loop. An important special case occurs when the controller is causally left invertible in terms of r given u and y. Then given data u, y a *fictitious reference* signal $\tilde{r}_i$ can be calculated. The fictitious reference signal is the reference signal that would have generated the data (u, y) if controller K^i would have been in the loop.

Once obtained, the signal triple (r, y, u) can be inserted into a cost function reflecting the desired performance of the controller in question. Further practical details of how this is done can be found in Safonov and Tsao (1997); Yamé and Kinnaert (2004). In Jun and Safonov (1999) it is demonstrated how PID controllers can be falsified, something that will be later explored in the current article.

2.2 Using the unfalsified control concept for fault tolerance

We limit ourselves to the supervisory switching control settings, see Fig. 2, and consider therefore a finite set of controllers, $\mathcal{K} = \{K_0, K_1, K_2, \ldots K_N\}$. Several strategies are possible to select $\mathcal{K}$. It is assumed that K_0 is the nominal controller, designed to work in the fault free case. For the fault tolerant control setting the rest of the set should be selected with two things in mind, the possible faults that can occur and the redundancy in the system. The bank of controllers can also be complemented with controllers designed with maximum robustness while satisfying some minimal performance criteria with the aim to cover a wide spectrum of unspecified faults and maintain the system operational but with degraded performance. This again attains the distinction between fault and uncertainty which has been commented in the introduction.

Notice that to falsify a controller, its input/output signals need to be measured online. Controllers that use back-up components (actuators or sensors) not used in normal operation, can not be falsified and are discarded from consideration here. If backup components are available it is assumed they are used only when all controllers K_i have been falsified.

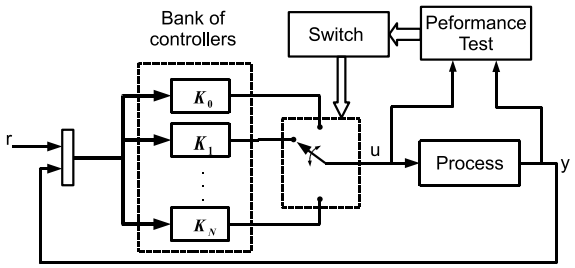

Fig. 2. Schematic diagram of control structure.

When a fault occurs it is important to switch to the correct controller as soon as possible as transients during switching can have undesirable effects. Furthermore, if no controller can handle the fault, backup systems need to be started or a system shutdown needs to be performed. A *switching strategy* is now presented to minimize the number of switches to find the correct controller when a fault occurs.

The set of considered faults is denoted $F = \{F_1, F_2, \dots F_M\}$. It is assumed that a controller K_i is available for each fault. A single fault might be handled by more than one controller. An example is a sensor fault that only affects controllers that use that sensor. A controller can also be designed to handle more than one fault. The set of faults controller K_i is expected to handle is denoted $\mathcal{F}_{K_i}$. It is also assumed that a priority order exists between the controllers in $\mathcal{K}$.

It is assumed that each fault is equally probable to occur. When a fault occurs, this causes the performance to deteriorate so that a new controller needs to be selected. As there should always be an unfalsified controller in the set of controllers for each fault, the choice should be trivial. But this rests on the assumption that falsification occurs instantly when a fault occurs which is not necessarily the case. It could be that at the time of switching, the fault effect has not yet falsified all the controllers in $\mathcal{K}$ that it should.

Denote $\mathcal{K}_f \subset \mathcal{K}$ the set of falsified controllers at the time of switching. Related to that set is a set of faults $\mathcal{F}_f$ given by

$$\mathcal{F}_f = \bigcup_{K_i \in \mathcal{K}_f} \mathcal{F}_{K_i}$$

This is the set of faults that can be excluded from consideration as their designated controller has been falsified. The set of possible faults at the time of switching is denoted $\mathcal{F}_f^c$ and is given by the remaining faults when $\mathcal{F}_f$ is removed from $\mathcal{F}$.

The controller that should be selected is the one that handles the maximum number of faults in $\mathcal{F}_f^c$. This is the controller with the maximum number of element in $\mathcal{F}_{K_i} \bigcap \mathcal{F}_f^c$. If two controllers handle the same number of faults, the controller with higher priority is selected. To demonstrate the switching strategy an example is presented.

Example 2. Assume 4 faults are possible and to handle them, 3 controllers have been designed. The sets $\mathcal{F}_{\mathcal{K}_i}$ are given as

$$\mathcal{F}_{K_1} = \{F_1\} \quad \mathcal{F}_{K_2} = \{F_2, F_3\} \quad \mathcal{F}_{K_3} = \{F_4\}$$

Assume that when the nominal controller is falsifed, K_1 is falsified as well. Then $\mathcal{F}_f^c = \{F_2, F_3, F_4\}$ and the controller which handles most faults in $\mathcal{F}_f^c$ is K_2. If $\mathcal{F}_{K_3}$ would have been $\{F_3, F_4\}$ then the controller would be selected according to the priority between K_2 and K_3.

The static switching strategy presented can be improved if probability of occurrence of each fault is known. Furthermore, switching strategy are often implemented with timed automata to be able to remember the switching order and to control the time spent using each controller.

3. UNFALSIFIED FTC APPLIED TO FUEL CELL BREATHING CONTROL

3.1 PEM fuel cell breathing control

Fuel cell stacks are highly complex systems with many physical phenomena involved. Generally, when referring to the control problems involved in operating fuel cell stacks, a division is made into the control of reactant flow and the control of operating conditions such as temperature and humidity. The current article is focused on fault tolerant control of the fuel cell breathing (see Pukrushpan et al. (2004b) for the general control problem) or more specifically the control of air flow to the fuel cell stack.

The model of the fuel cell stack that is used in this study was presented in Pukrushpan et al. (2004a) and its Simulink implementation is available online at the home page of that reference and has been used in a number of investigations on the fuel cell breathing problem. The model of the air supply subsystem is repeated here for completeness.

3.2 Air supply system model

The model is based on lumping together the cathode volume as well as the the volumes of the tubes before and after the cathode, as illustrated in Fig. 3. Thus, the compressor is driven by an electrical motor, supplying air to the inlet manifold where it later flows to the cathode volume. The air that is not reacted and water vapor from the reaction then leave through the return manifold. To control the fuel fell breathing, the tension to the motor (v_{cm}) which drives the compressor is manipulated. Measured variables are typically compressor airflow W_{cp}, inlet manifold pressure P_{im} and stack voltage V_{st}. These signals are shown in Fig. 3.

The model of the motor and compressor is based on Newton's second law:

$$J_{cp}\frac{d\omega_{cp}}{dt} = \tau_{cm} - \tau_{cp} \tag{2}$$

where τ_{cp} is the load torque and τ_{cm} is the compressor motor (cm) torque which is calculated based on a static motor equation

$$\tau_{cm} = \eta_{cm}\frac{k_t}{R_{cm}}(v_{cm} - k_v\omega_{cp}) \tag{3}$$

where k_t, R_{cm} and k_v are constants, η_{cm} is the mechanical efficiency, and ω_{cp} the velocity of the compressor and

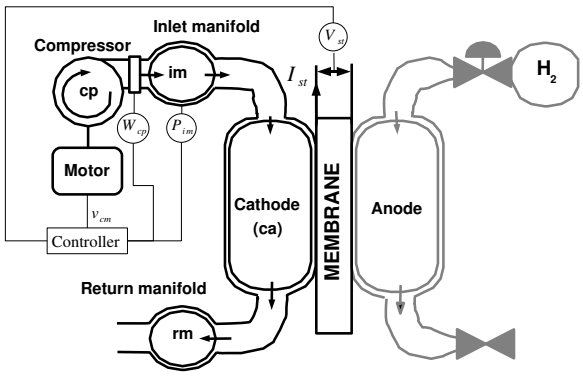

Fig. 3. Scheme of the FC reactant supply system with lumped volumes (on the basis of Pukrushpan et al. (2004a))

motor. The torque required to drive the compressor is based on the thermodynamic equation:

$$\tau_{cp} = \frac{C_p}{\omega_{cp}} \frac{T_{atm}}{\eta_{cp}} \left[\left(\frac{p_{im}}{p_{atm}} \right)^{(\gamma-1)/\gamma} - 1 \right] W_{cp} \tag{4}$$

where γ is the ratio of the specific heats of air, C_p is the constant-pressure specific heat capacity of air, η_{cp} is the compressor efficiency, p_{im} is the pressure inside the inlet manifold and p_{atm} and T_{atm} are the atmospheric pressure and temperature, respectively. A static compressor map, $W_{cp}(\omega_{cp}, p_{cp}/p_{atm})$ is used to determine the air flow rate W_{cp} through the compressor.

The inlet manifold behavior is governed by energy and mass conservation equations:

$$\frac{dm_{im}}{dt} = W_{cp} - W_{im}, \tag{5}$$

$$\frac{dp_{im}}{dt} = \frac{\gamma R}{M_a^{atm} V_{im}} (W_{cp} T_{cp} - W_{im} T_{im}), \tag{6}$$

where R is the universal gas constant, γ is the ratio of the specific heat capacities of air, M_a^{atm} is the molar mass of atmospheric air, V_{im} is the manifold volume, and

$$T_{im} = \frac{p_{im} V_{im} M_a^{atm}}{R m_{im}}$$

is the inlet manifold gas temperature. The flow out of the inlet manifold (W_{im}) is considered proportional to the pressure difference between the inlet manifold and the cathode, $W_{im} = k(P_{im} - P_{ca})$. The same assumption is made for the flow out of the cathode into the return manifold (W_{ca}). The state equation of the return manifold pressure is

$$\frac{dp_{rm}}{dt} = \frac{R T_{st}}{M_a^{ca} V_{rm}} (W_{ca} - W_{rm}), \tag{7}$$

which is actually a mass conservation equation as it is assumed that there is no temperature difference between cathode and return manifold. Finally the flow out of the return manifold is governed by an orifice relation.

$$W_{rm} = \frac{A_T p_{rm}}{\sqrt{R T_{rm}}} (p_r)^{1/\gamma} \left\{ \frac{2\gamma}{\gamma - 1} \left[1 - (p_r)^{1-1/\gamma} \right] \right\}^{1/2}$$

where $p_r = p_{ca}/p_{atm}$ and A_T is effective area of the orafice.

The full model of the fuel cell stack has 8 states. Input variables are stack current I_{st} and compressor voltage v_{cm}. Output variables or measured variables are stack voltage V_{st}, inlet manifold pressure P_{im} and compressor air flow W_{cp}.

3.3 The fuel cell breathing control problem

The purpose of the stack is to respond to a variable power load applied to it. The load of the stack is changed by changing the current that flows through it. When the current is changed the reactant flows need to be adjusted. The current is thus considered an exogenous variable in the breathing control problem (see Pukrushpan et al. (2004b)).

The main performance variable in the breathing control problem is the oxygen excess ratio λ defined as

$$\lambda = \frac{W_{ca,in,O_2}}{W_{reacted}} \tag{8}$$

where W_{ca,in,O_2} is the oxygen entering the cathode and $W_{reacted}$ is the oxygen reacted, which in turn is proportional to the current drawn from the stack:

$$W_{reacted} = M_{O_2} \frac{n I_{st}}{4F} \tag{9}$$

where M_{O_2} is the molar mass of O_2, n is the number of cells in the stack, I_{st} is the stack current while F is the Faraday number ($F = 96485[C]$).

The oxygen excess ratio reflects mainly two things. First of all, if it is low, oxygen starvation can take place which can damage the stack permanently. If λ is too large, as the energy required to run the compressor is the principal parasitic loss of the stack, the stack could be operated more economically with a lower λ. In terms of sensitivity to faults, it is clear that a decrease in λ can have much worse consequences than an increase. For the model in question it was shown in Pukrushpan et al. (2004a) that a suitable value of λ was equal to 2.

On the other hand λ can not be measured directly as W_{ca,in,O_2} is not measurable. A related variable, the compressor airflow W_{cp} is measured instead. As oxygen content in air is constant (21%) and by using Eq. (8), a reference value for W_{cp} can be calculated as proportional to stack current I_{st}, $W_{cp}^{ref} = \alpha I_{st}$. The performance variable for the controller was thus the error between the reference airflow and compressor airflow:

$$e_{W_{cp}} = W_{cp}^{ref} - W_{cp} \tag{10}$$

3.4 The control structure

A supervisory control structure based on a bank of controllers was used in the article to achieve fault tolerance. A schematic diagram of the structure is shown in Fig. 2

The nominal controller is a LQG design similar to the one presented in Pukrushpan et al. (2004b). The LQG controller used all measurements $y = [W_{cp}\ p_{im}\ V_{st}]$, and an integrator was implemented for the error $e_{W_{cp}}$. By using both dynamic and static feed-forward, a satisfactorily response of λ could be obtained in the nominal case. This response is shown in Fig. 4 for the load profile demonstrated in the same figure. What is shown is the set point W_{cp}^{ref} and the set point after the feed forward

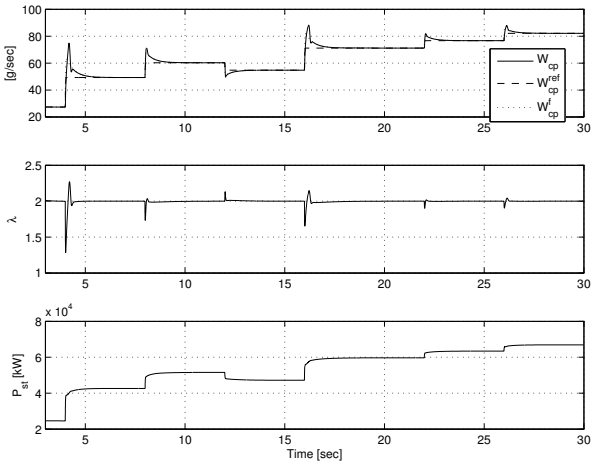

Fig. 4. Airflow, λ and Power

Table 1. Fault scenarios

Fault	Effect on the System
	Parametric faults
1	compressor efficiency η_{cp} is decreased
2	mechanical efficiency η_{cm} is decreased
3	compressor motor torque τ_{cm} is decreased
4	outflow area of outlet manifold A_T decreased
5	cathode exit flow area decreased
6	limit upper range of compressor
	Dynamic faults
7	measured signal W_{cp} filtered through low pass filter
8	measured signal W_{cp} delayed
9	measured signal p_{im} filtered through low pass filter
10	measured signal p_{im} delayed
	Sensor faults
11	sensor signal measuring W_{cp} is increased/decreased
12	white Gaussian noise is added to W_{cp}
13	sensor signal measuring p_{im} is increased/decreased

filter, W_{cp}^f. The stack in question is supposed to be able to supply 70 kW of power and thus it is seen that the load profile spans the whole range of stack power. Fig. 4 shows that λ recovers to a value above 1.9 within a period of 0.1 seconds when load changes are performed.

3.5 Fault scenarios

Several fault scenarios of various degrees of severity were tested by simulation (see Table 1). Notice that as only one actuator was available in the plant, severe actuator faults generally caused the test quantities of all controllers to surpass their alarm limits.

The types of faults considered in this study could be divided into three main groups, parameter faults, changes in the dynamical behavior of the system and sensor faults. Parameter faults were implemented by modifying in an abrupt manner some of the parameters presented in the model in Section 3. System or loop faults where implemented by adding to the loop transfer function dynamical behavior so that open loop responses were slowed down by a low pass filter or delayed with a time delay. Finally, sensor faults were implemented where the measured signals either acquired a strong increase in their noise characteristics or the sensor signals were modified proportionally either up or down.

Table 2. Bank of controllers.

	Type	y	Design criteria
K_0	LQG	$[W_{cp}\ p_{im}\ V_{st}]$	Nominal controller.
K_1	PID	$[W_{cp}]$	Maximum robustness. Dynamic and parameter faults.
K_2	PID	$[p_{im}]$	Maximum robustness. Fault in the W_{cp} sensor.

3.6 Backup controllers

Two controllers were designed to serve as back up controllers when the performance of the nominal one would be unsatisfactory. Firstly, a PID controller using W_{cp} as the controlled variable and W_{cp}^{ref} as set point was designed, primarily with robustness in mind while satisfying some minimal performance requirements. The faults this controller was supposed to handle were dynamic and parametric faults that could deteriorate the performance of the nominal controller. Secondly, a PID controller controlling the pressure in the inlet manifold (P_{im}) was designed in case of faults in the sensor measuring W_{cp}. The set point for this controller was calculated by finding an approximate linear relation of pressure p_{im} as a function of W_{cp} and using W_{cp}^{ref}. This controller was also designed with robustness in mind while satisfying some minimal performance requirements. The controllers present in the bank of controllers are summarized in Table 2. Controller K_1 was given higher priority than K_2 in the implementation of the switching strategy.

3.7 Characterizing the performance specification set

Membership of (r, y, u) in the performance specification set T_{spec}^i was tested by verifying positivity of a test quantity given by

$$J_i = \|r\|_\tau^2 - \|w_1^i * (y - r)\|_\tau^2 - \|w_2^i * u\|_\tau^2 + \sigma_i \qquad (11)$$

where $y - r$ is the error signal and $*$ is the convolution operator. When J_i is calculated for a controller i not in the feedback loop, the virtual reference value $\tilde{r}_i$ is used for r. To calculate $\tilde{r}_i$, the control laws are inverted as shown in Jun and Safonov (1999) and Yamé and Kinnaert (2004). See also *cost detectable* performance criteria in van Helvoort et al. (2007); Manuelli et al. (2007); Wang et al. (2007).

A similar test quantity was used in Jun and Safonov (1999) and Safonov and Tsao (1997). As pointed out in Safonov and Tsao (1997) this test reflects an $\mathcal{H}_\infty$-weighted mixed-sensitivity performance criterion

$$\left\| \begin{matrix} W_1 S \\ W_2 K S \end{matrix} \right\| < 1$$

where the $S = 1/(1 + KP)$ is the sensitivity function. The starting point for the design of the weights W_1^i and W_2^i was the control design performed for each controller. The weights, as well as σ_i, were tuned so that when the plant was controlled over all operating regions with satisfactory performance, the controller would not be falsified. Furthermore, faults that did not have severe influence on the performance variables should not falsify controllers either. The selection of W_1^i and W_2^i as well as σ_i required some design effort and tuning to make them work satisfactorily.

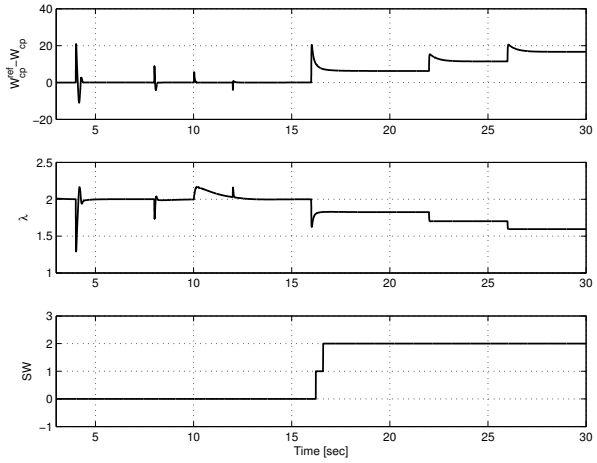

Fig. 5. Scenario 1. Bold line: switching implemented.

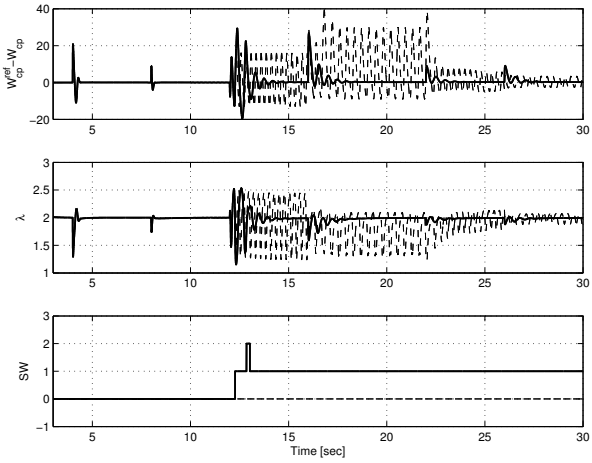

Fig. 6. Scenario 2. Bold line: switching implemented. Dashed line: nominal controller only.

4. RESULTS

The simulation results of selected but representative fault scenarios are now presented. In Figs. 5, 6 and 7 the error $e_{W_{cp}}$ and λ are demonstrated as well as the switching signal (SW) which indicates what controller was selected at each time (0 corresponds to K_0, 1 to K_1 and 2 to K_2).

Scenario 1. Drop in compressor efficiency. The fault caused a 40% decrease in the thermodynamical efficiency of the compressor at time 10. At that time the nominal controller demonstrates sufficient robustness so that the occurrence of the fault has little or no effect on performance. The integral action quickly compensates the effect of the fault and the system continues unaffected until a higher load is applied to it at time 16. Then the motor can not supply the required torque to achieve the required airflow.

It can be seen in the figure that at time 16 the λ value drops sharply and the error increases and settles at a stationary value. Immediately the nominal controller was falsified and at time 16.5 the two backup controllers. Shortly afterwards the limit of the actuator was reached so that the closed loop was broken. The values of J_i for the backup controllers started to rise at time 16 before they were switched into the feedback loop.

Similar behavior was observed when other parameter faults affecting the compressor, motor or the flow path were applied. In these cases, as there is only one actuator available, for a certain value of fault amplitude, the compressor motor would saturate and the required airflow could not be delivered. The effect of these faults was generally only noticed at higher loads and not necessary when the fault was applied.

Scenario 2. Dynamic fault. In this case the sensor signal W_{cp} was filtered through a first order transfer function with a time constant of 0.05 seconds and unitary gain at time 10. This fault has no effect on stationary behavior and thus would be difficult to detect with FDI methods that depend on differences in steady state behavior. This fault in particular could have been included as uncertainty in the design of the nominal controller. But as mentioned in the introduction, this is a tradeoff question between performance and robustness that the designer has to address in the beginning.

It can be seen in the figure that the addition of this dynamics in the loop seriously affects the performance of the nominal controller as λ starts to oscillate at time 12, again later than when the fault is applied. When switching is allowed it is observed that backup controller 1 takes over at that time 12 and backup controller 2 shortly afterwards. Then, backup controller 1 is selected again as it is unfalsified after a short time interval. λ is stabilized around 2 with this controller and performance is deteriorated but remains acceptable for the rest of the scenario. The undesirable effect of the fault was avoided by the FTC mechanism.

Scenario 3. Fault in W_{cp} sensor. In this case the W_{cp} signal is reduced to 20% of its value at time 10. The behavior in the nominal case is not surprising as the fault breaks the feedback loop causing the signals to diverge quickly. Notice that the PID-W_{cp} controller evidently depends on the faulty signal W_{cp} as well and it should therefore be quickly unfalsified. But it takes longer time than the nominal controller because it is designed to be more robust and therefore tolerate worse performance. In either case, in less than a second the correct controller is switched in and prolonged oxygen starvation is avoided.

5. CONCLUSIONS AND FURTHER RESEARCH TOPICS

Using the unfalsified control concept and switching supervisory control, but without the use of a fault diagnosis system, a fault tolerant control system for the breathing control problem of a PEM fuel cell stack was designed, implemented and tested in simulation. In several scenarios, some of which were presented in the result section, oxygen starvation in the stack was reduced or avoided by the use of the strategy. Sensor redundancy could be effectively taken advantage of by including controllers that depended on distinct sensor as shown in Scenario 3.

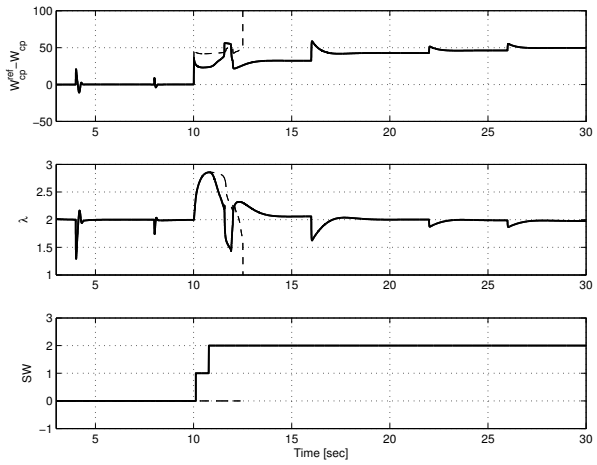

Fig. 7. Scenario 3. Bold line: switching implemented. Dashed line: nominal controller only.

The construction of a FTC system using unfalsified control can be done in a modular manner by adding controllers for specific faults to the bank of controllers or by adding specially robust controllers expected to handle a wide spectrum of unknown faults. This stands in contrast to traditional FTC where it can be difficult to predict the behavior of the diagnosis system when unknown faults occur. Furthermore, the occurrence of multiple faults has no significance for the unfalsified FTC while traditional FDI often rests on a "one fault" assumption. Particularly for most space applications this is part of the specifications, e.g. NASA, ESA.

A switching strategy was presented for unfalsified FTC where the aim was to minimize the number of switches to reach the designated controller. Switching among controllers is an item by itself, with several alternatives based on Lyapunov theory, which can be used to guarantee stable switching among LTI systems, converting the bank of controllers into a single LPV controller (Becker and Packard (1994); Gahinet and Apkarian (1995)) with a measured parameter based on the performance alarm, or even LPV switching (Lu and Wu (2004)).

The results demonstrate the importance of on-line performance assessment for FTC. In Scenarios 1 and 2 it was shown that switching to backup controllers occurred only when the effect of the fault caused performance problems for the nominal controller and not when the fault occurred. Achieving similar behavior without performance assessment could be difficult as it would involve inferring controller performance from uncertain fault information for a real plant.

The main design effort in the current study was spent on designing the test quantities that test membership in the performance specification set. Some authors have addressed that problem (see Mosca and Agnoloni (2002)) but often the plant is assumed to be SISO and linear for the results to be coherent with the assumptions. Special attention has to be given to situations when the performance tests are not valid, for example when the actuators reach their saturations limits, in which case the feedback loop is broken.

An experimental setup is in preparation at UPC and future physical tests will be performed on it.

REFERENCES

G. S. Becker and A. Packard. Robust performance of LPV systems using parametrically-dependent linear feedback. *Systems and Control Letters*, 23:205–215, 1994.

M. Blanke, M. Kinnaert, J. Lunze, and M. Staroswiecki. *Diagnosis and Fault-Tolerant Control*. Springer-Verlag Berlin Heidelberg, 2003. ISBN 3-540-01056-4.

S. Fekri, M. Athans, and A. Pascoal. Issues, progress and new results in robust adaptive control. *Int. J. Adapt. Control Signal Process.*, 20:519–579, 2006.

P.l Gahinet and P. Apkarian. A convex characterization of gain-scheduled $\mathcal{H}_\infty$ controllers. *IEEE Transactions on Automatic Control*, 40(5):853–864, 1995.

M. Jun and M. G. Safonov. Automatic PID Tuning: An Application of Unfalsified Control. In *Proceedings of the 1999 IEEE International Symposium on Computer Aided Control System Design*, pages 328–333, Hawai USA, 1999.

B. Lu and F. Wu. Switching LPV control designs using multiple parameter-dependent Lyapunov functions. *Automatica*, 40(11):1973–1980, 2004.

C. Manuelli, S. G. Cheong, E. Mosca, and M. G. Safonov. Stability of unfalsified adaptive control with non-SCLI controllers and related performance under different prior knowledge. In *European Control Conference*, Kos, Greece, 2007.

E. Mosca and T. Agnoloni. Switching supervisory control based on controller falsification and closed-loop performance inference. *Journal of Process Control*, 12:457–466, 2002.

K. R. Popper. *Conjectures and Refutations: The Growth of Scientific Knowledge.* Routhledge, London, 1963.

J. T. Pukrushpan, A. G. Stefanopoulou, and H. Peng. *Control of Fuel Cell Power Systems Principles, Modeling, Analysis and Feedback Design.* Advances in Industrial Control. Springer, 2004a.

J. T. Pukrushpan, A. G. Stefanopoulou, and H. Peng. Control of fuel cell breathing. *Control Systems Magazine*, pages 30–46, 2004b.

M. G. Safonov and T.-C. Tsao. The unfalsified control concept and learning. *IEEE Transactions On Automatic Control*, 42:843–847, 1997.

J. van Helvoort, B. de Jager, and M. Steinbuch. Data-driven multivariable controller design using ellipsoidal unfalsified control. In *American Control Conference*, pages 510–515, 2007.

R. Wang, A. Paul, M. Stefanovic, and M. G. Safonov. Cost-detectability and stability of adaptive control systems. *International Journal of Robust and Nonlinear Control*, 17(5-6):549–561, 2007.

J.J. Yamé and M. Kinnaert. A fault accomodation strategy based on closed-loop performance monitoring. In *43rd IEEE Conference on Decision and Control*, pages 5242–5247, Atlantis, Paradise Island, Bahamas, 2004.

Y. Zhang and J. Jiang. Issues on integration of fault diagnosis and reconfigurable control in active fault-tolerant control systems. In *Proceedings of SAFEPROCESS 2006*, 2006.