Data-driven fault diagnosis and robust control: Application to PEM fuel cell systems

Carlos Ocampo-Martinez[1], Ricardo Sánchez-Peña[2], Fernando D. Bianchi[3] and Ari Ingimundarson[4]

[1]Universitat Politècnica de Catalunya,
Institut de Robòtica i Informàtica Industrial, CSIC-UPC,
Llorens i Artigas 4-6, 08028 Barcelona, Spain
[2]CONICET and Instituto Tecnológico de Buenos Aires (ITBA),
Av. Madero 399, (C1106ACD) Buenos Aires, Argentina
[3]Catalonia Institute for Energy Research, IREC,
Jardins de les Dones de Negre 1, 08930 Sant Adrià de Besòs, Barcelona, Spain
[4]Mannvit hf, Grensásvegur 1, 108, Reykjavík, Iceland

Abstract

A data-driven methodology that includes the unfalsified control concept in the framework of fault diagnosis and isolation (FDI) and fault-tolerant control (FTC) is presented. The selection of the appropriate controller from a bank of controllers in a switching supervisory control setting is performed by using an adequate FDI outcome. By combining simultaneous on-line performance assessment of multiple controllers with the fault diagnosis decision from structured hypothesis tests (SHT), a diagnosis statement regarding what controller is most suitable to deal with the current (nominal or faulty) mode of the plant is obtained. Switching strategies that use the diagnosis statement are also proposed. This approach is applied to a non-linear experimentally validated model of the breathing system of a polymer electrolyte membrane (PEM) fuel cell. The results show the effectiveness of this FDI-FTC data-driven methodology.

Keywords: Fault diagnosis; fault-tolerant control; unfalsified control; fuel cells

1 Introduction

Within the scientific community, there is nowadays a unified agreement indicating that hydrogen (H_2), as an energy vector generated from alternative energy sources, represents a viable option to mitigate problems associated with hydrocarbon combustion. In this context, the change from the current energy system to a new system with a stronger involvement of H_2 requires the introduction of fuel cells as elements of energy conversion. However, several problems have to be faced in order to efficiently manage these complex systems and, so far, some classical control solutions have been proposed. Several control problems remain unsolved due to the fact that there is still a diversity of variables to regulate and indexes to optimise, which should be further determined and described. In particular, a key issue to address consists in introducing optimisation concepts for different operating modes of the system and fault tolerant

control strategies capable to cope with non-linear uncertain behaviours. This is an unexplored area in the automation of polymer electrolyte membrane (PEM) fuel cells — PEMFC — and requires tailored solutions based on advanced control strategies.

An important aspect when controlling real systems in general is concerned with the occurrence of component faults and their influence over the whole system performance. In fact, faults and model/sensor /actuator uncertainty might play similar roles, then the distinction among them gives rise to conceptual differences between active[1] and passive[2] fault-tolerant control (FTC) design approaches [1]. In the framework of fuel cells and assuming an active FTC architecture, several approaches for fault detection and isolation (FDI) have been proposed. Model-based FDI for PEMFC systems based on consistency relations for the detection and isolation of predefined faults has been proposed in [2], while in [3], a comparison of both model-based and data-driven fault detection methods for fuel cells is addressed. The work in [4] proposes a methodology to use the electrical model for fuel cell system diagnosis, while in [5], a fault diagnosis and accommodation system based on fuzzy logic has been developed as an effective complement for a closed-loop scheme. Regarding FTC, Feroldi [6] proposes an MPC scheme for adding fault tolerance capabilities to a two-actuator PEMFC system.

An important research trend 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, e.g., [7, 8, 9, 10], among others. A conceptually suitable technique to implement a decision block is by means of unfalsified control (UC), see [11], since it is able to discard large number of controllers from a given set without inserting them into the feedback loop. The use of UC for fault tolerance was previously presented in [12], but not many application papers have been presented regarding UC and its use for FTC [13, 14]. Notice that UC aims at excluding controllers according to their closed-loop performance. Alternative approaches reported in [15, 16] performs model (in)validation by introducing the *model falsification concept*, acting as the *dual* of the UC approach. The main difference between these techniques relies on the way the fault is determined and used: while the model falsification finds the model that matches the fault situation by using *set-valued observers*, UC seeks the best closed-loop performance by testing several pre-computed controllers.

The objective of this work is to integrate the use of robust data-driven controllers, in particular those based on the UC approach, to achieve fault tolerance within the framework of the *structured hypothesis tests* (SHTs) proposed by [17] for PEMFC-based systems. Figure 1 shows how FDI and FTC blocks can be integrated and consolidated in a single UC-based block, which combines tasks of both supervision and execution levels to be made almost simultaneously. 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. The only online evaluation (instead of diagnosis) is based on the ultimate goal of any practical control system: *performance*, and on real-time input/output data streams from the PEMFC sensors.

The FDI-FTC architecture integrating UC 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 modular fashion, where controllers are added to the bank to handle specified/unspecified faults or covering/rejecting system disturbance effects. This framework was presented in a previous work by two of the authors for fuel cell systems [18], being also applicable to a wide range of FTC problems. In addition, an implementation of the UC approach has been also reported by three of the authors but considering the UC as the supervisory controller and testing its fault tolerance capabilities [19]. Here the UC is integrated into the FDI-FTC topology, which makes this paper the evolution of the work in [19] into the fault-tolerant

[1] Active FTC strategies aim at adapting the control loop based on the information provided by a fault diagnosis and isolation (FDI) module within the fault-tolerant architecture.

[2] In passive FTC strategies, a single-control law is used in both faultless and faulty operation, assuming a certain degree of performance degradation.

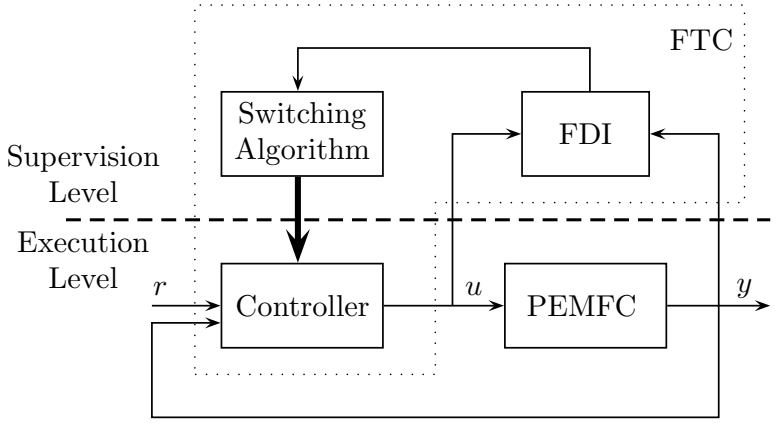

Figure 1: General FDI-FTC architecture in PEMFC.

framework.

The remainder of the paper is organized as follows. In Section 2, the UC and the hypothesis testing backgrounds are presented. Sections 3 and 4 introduce the main results, which combine the SHT and the diagnosis and control strategies. These are combined in an algorithm presented in Section 5. The case study description and the main simulation results on the experimentally validated simulator are presented and discussed in Section 6. Finally, the most relevant conclusions are drawn in Section 7.

2 Background

2.1 The Unfalsified Control Concept

The UC core is based on ideas from Popper [20] about the philosophy of science. Learning (i.e., singling out the appropriate controller) is achieved by using experimental data to falsify hypotheses. Basically, UC is a selection algorithm that seeks the best controller K from a predefined set $\mathcal{K}$ at each time instant, in a general feedback configuration. The controller selection relies on evaluating the closed loop performance achieved by each $K \in \mathcal{K}$ from the input-output data.

UC consists in testing the intersection of three sets. The behaviour of the system up to the current time is given by the time data records of the reference r, the input u and the output y (see Figure 1). This measurement information gives a partial knowledge about the plant and is represented by the set $\mathbf{P}_{data}$, which is the set of triples (r, y, u) consistent with past measurements of (u, y). A controller $K_i \in \mathcal{K}$ defines another set

$$\mathbf{K}_i \stackrel{\triangle}{=} \{(r, y, u), \mid u = K_i(r, y)\},$$

which represents the behaviour of such a controller K_i. Finally, the performance specifications can also be expressed as a set $\mathbf{T}_{spec}$ in the triple (r, y, u), e.g.,

$$\mathbf{T}_{spec} \stackrel{\triangle}{=} \{(r, y, u), \mid V(r, u, y) < \eta\},$$

where $V(\cdot)$ is a cost function and $\eta > 0$.

With the previous definitions, a controller is said to be *falsified* by measurement information $\mathbf{P}_{data}$ if this information is sufficient to deduce that the performance specification $(r, y, u) \in \mathbf{T}_{spec}$ would be violated if that controller would be in the feedback loop. Otherwise the controller is said to be *unfalsified*. That is, a controller K_i is unfalsified if the statement

$$\mathbf{P}_{data} \cap \mathbf{K}_i \cap \mathbf{T}_{spec} \neq \emptyset \tag{1}$$

holds. This implies that the controller is falsified if there is no triple (r, y, u) consistent with the past measures and the control mapping K_i fulfilling the performance specification established by $\mathbf{T}_{spec}$.

One of the main advantages of the UC formulation is that the set $\mathbf{P}_{data} \cap \mathbf{K}_i$ can be characterized even though the controller K_i does not integrate the feedback loop. When the controller is causally left invertible[3] in terms of r given u and y and when the performance specifications depend only on behaviours measured at observation instances, a *fictitious reference* signal r_f can be calculated as follows

$$r_{f,i} = y + K_i^{-1}\, u,$$

where, in this context, K_i^{-1} denotes the inverse mapping, producing the input of the controller corresponding to the measured system input u. This fictitious reference signal is the signal that would have generated the data $\mathbf{P}_{data}$ if controller K_i would have been placed in the closed loop.

With $r_{f,i}$ associated to the controller K_i, the performance specification set $\mathbf{T}^i_{spec}$ is given by a cost function

$$V(r_{f,i}, u, y, t) = \max_{\tau \leq t} \frac{||W_e \ * \ (r_{f,i} - y)||_\tau^2 + ||W_u \ * \ u||_\tau^2}{||r_{f,i}||_\tau^2 + \alpha}, \tag{2}$$

where $\alpha \in \mathbb{R}_{>0}$ is a small constant to avoid numerical problems when $r_{f,i}$ is close to zero and W_e and W_u are weights related to the error $e \triangleq r_{f,i} - y$, and the control signal, respectively. The selection of these weights is done in a similar way than in mixed-sensitivity optimal control, i.e., penalising certain frequency content of the signals in order to reach a trade-off between tracking and control effort. In particular, the weight W_e penalises the tracking error in low frequencies and W_u penalises the control signal in high frequencies. Moreover, the notation $\|x(t)\|_\tau = \sqrt{\int_0^\tau x(t)^T x(t) dt}$ denotes the truncated L_2-*norm* of a signal $x(t)$ and $*$ is the convolution operator.

In addition, UC theory requires a *detectable* cost function in order for the system to be stable, see page 20, Remark 2.2 in [21]. This cost function and the set of controllers guarantee that instabilities will be detected even though the physical system is initially unknown. The proposed cost function in (2) has this property.

Being K_j the controller active at the present time and $M + 1$ the total number of controllers in the bank, the controller to be inserted in the loop in the next sampling time that satisfies (1) can be tested online following Algorithm 1. In this context, M denotes the cardinality of a set of controllers designed for facing faulty behavioural modes.

2.2 Problem Definition

The design of an active FTC architecture implies the suitable functioning of an FDI module. This section deals with the way FDI is achieved, taking into account performance features related to the closed-loop PEMFC system. For this purpose, the SHT framework for fault diagnosis presented in [17] and further developed in [22] is adopted. As pointed out in the Introduction, this framework has many advantages that make it interesting for FTC. Within this framework, this paper shows how the UC copes with the

[3]This assumption can be avoided by using matrix fraction descriptions, as indicated in Section 2.4. of [21].

Algorithm 1 UC Controller Computation

for $i = 0$ to M **do**
    compute $r_{f,i} = y + K_i^{-1}(u, y)$
    compute $V(r_{f,i}, u, y)$
end for
set $\hat{i} \leftarrow \arg\min_i V(r_{f,i}, u, y)$
if $V(r_{f,\hat{i}}, u, y) \leq V(r_{f,j}, u, y) + \eta$ **then**
    set $K_j \leftarrow K_{\hat{i}}$
else
    set $K_j \leftarrow K_j$
end if

closed-loop performance in the form of hypothesis sub-statement. For the purpose of brevity, several simplifications of the framework are made and only subtle issues are omitted.

Remark 1 *SHT may be seen as a generalization of the well known structured residual method in fault detection and isolation discussed in [23]. It has the additional advantage of being theoretically grounded in classical hypothesis testing and propositional logic. For decision making purposes, statistical tests [24] would take into account probabilities and hopes while the proposed SHT-based method is supported by (diagnosis) statements, which can be measured/inferred from the real process.*

With the aim to control a PEMFC system P that can be found in several behavioural modes (nominal or faulty), a bank of controllers

$$\mathcal{K} = \{K_0, K_1, K_2, \ldots, K_M\} \tag{3}$$

may be stated. Let $\mathcal{F}$ be defined as the set of behavioural modes

$$\mathcal{F} = \{F_0, F_1, F_2, \ldots F_N,\ F_u\}, \tag{4}$$

where F_0 is the nominal behavioural mode (no fault) and F_i, with $i = 1, \ldots, N$, are faulty modes. Moreover, $F_u = F_{N+1}$ (unknown fault) denotes all abnormal behaviour that can not be explained by the other fault modes. Now, the first $N + 1$ elements of the set $\mathcal{F}$ contain all behavioural modes that have been considered sufficiently important so that a dedicated controller design to manage them has been performed; F_{N+1} is excluded. The design can be motivated by the existence of redundancy, probability of fault or any other reason that motivates an FTC strategy. The cardinality of both sets[4] $|\mathcal{F}| = N + 2$ and $|\mathcal{K}| = M + 1$ are, in principle, unrelated. Nevertheless, from the practical point of view, there should be at least one controller for each fault mode, i.e., $M \geq N$. It could also happen that several controllers may handle a particular failure and *vice versa*, a single controller could handle several fault situations.

Each fault mode can contain a wide set of behaviours. For example, the plant can be fully operational in a mode that represents a fault in a redundant sensor but only if the controller currently in the loop does not depend on that sensor. It is not specially assumed that models exist for all faulty modes. On the other hand, notice that the design of a controller based on an adequate control-oriented model (COM) for a specific fault mode improves the closed-loop performance with respect to a non dedicated controller.

Moreover, when the system is undergoing a particular fault mode, a controller can be designed to cope with it, assuming the necessary sensors and actuators have been taken into account. Therefore, previous to the implementation, a set of controllers have been designed, each tuned to a particular fault dynamics, see also [25]. On the other hand, if these controllers have a certain degree of robustness they can possibly

[4] In the sequel, the notation $|A|$ denotes the cardinality of the set A.

cope with *neighbour* dynamics for which they were not designed[5]. From these two facts:

- If the controller is falsified, the dynamics taking place are not the ones for which the controller was initially tuned for.
- A controller, which has been tuned to a particular fault, might perform *reasonably well* for another fault (or even for the nominal) if these dynamics are not far away from the initial fault it was designed for.

In this paper, a controller $K_j \in \mathcal{K}$ designed to manage or handle each fault mode $F_i \in \mathcal{F}$ is assumed, although F_i might be also handled by more than one controller. In addition, a priority order may be assigned to controllers related to a certain fault F_i, e.g., according to the number of faults handled by the controller K_j. On the other hand, the set of faults that the controller K_i is expected to handle is denoted $\mathcal{F}_{K_i}$ and contains one or more fault modes. The F_{N+1} mode is never included in any $\mathcal{F}_{K_i}$. Therefore, $1 \leq |\mathcal{F}_{K_i}| < N+1$.

The bank of controllers can 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, e.g., $F_u = F_{N+1}$, and maintain the system operational but with degraded performance[6].

To test whether a controller fulfils its design specifications, its input/output signals need to be measurable online. Controllers that consider back-up components (actuators or sensors) not used in normal operation are therefore discarded here. If backup components are available, it is assumed they are used only when all controllers in $\mathcal{K}$ have been falsified.

3 Using the Structured Hypothesis Tests

3.1 SHT for Fault Diagnosis

When the currently used controller is falsified, additional hypothesis tests using *a priori* data related to the possible system behaviour can be created to aid in switching to the correct controller. Consider F_p as the fault mode present in the system. The aim would be to reduce the set of which F_p could be a member at the time of switching.

In this framework, several hypothesis regarding the present behavioural mode are continuously tested on-line. The set of hypothesis tests is denoted

$$\mathcal{H} = \{H_0, H_1, \dots H_L\}. \tag{5}$$

Here, the SHT is a function of the experimental data u and y. The null hypothesis for the k-th hypothesis test H_k^0 is when the active fault mode belongs to a set of faults Z_k. The alternative hypothesis H_k^1 is when the actual fault mode does not belong to Z_k. Therefore, if H_k^0 is rejected, H_k^1 is accepted, and the actual fault mode does not belong to Z_k (and belongs to its complement Z_k^C).

[5] In addition, a broad robust controller, which will possibly provide low performance, is designed in case the system is in the unknown mode F_u. This covers all possible cases.

[6] Here, it is assumed for the problem to be tractable that either the system is in F_i, $i = 0, ..., N$ or in the unknown situation F_u. But in the sequel, the maximum robustness controller should be able to provide at least stability, with a low performance, to the closed-loop system. Otherwise, there is no way around the problem. This condition is in accordance with the usual assumptions in UC.

For the k-th hypothesis test, the null hypothesis and its alternative can be written as follows:

$$H_k^0 : F_p \in Z_k \quad \text{“some fault mode in } Z_k \text{ can explain the data } (u, y)\text{”},$$
$$H_k^1 : F_p \in Z_k^C \quad \text{“no fault mode in } Z_k \text{ can explain the data } (u, y)\text{”}.$$

The convention regarding the hypothesis and its complement is as follows. When H_k^0 is rejected, it is assumed that H_k^1 is true, but when H_k^0 is not rejected, nothing should be assumed. Therefore, the following fact holds.

Fact 1 *If H_k^0 holds (H_k is not rejected), then $F_p \in S_{H_k}^0$. If H_k^1 holds (H_k is rejected), then $F_p \in S_{H_k}^1$.* $\triangledown$

Here, $S_{H_k}^0$ and $S_{H_k}^1$ are *diagnosis sub-statements* containing fault modes in $\mathcal{F}$. In what follows, it will be assumed that $S_{H_k}^0 = \mathcal{F}$, which means that if the k-th hypothesis is not rejected, this test gives no information about F_p. Moreover, $S_{H_k}^1$ always contains F_u. For further discussion about how $S_{H_k}^0$ and $S_{H_k}^1$ can be constructed, see [17]. For the purpose of this paper, this section allows to define the output of a *Statement Diagnoser* module within a FDI-FTC structure, which is defined as *diagnosis statement* and denoted as S. This decision is made by processing several module inputs defined beforehand as diagnosis sub-statements (see Section 5).

3.2 SHT for Controller Performance

In particular, the closed-loop performance can also be taken into account when designing the FDI module. Specifically, the UC acts within this framework as a diagnosis sub-statement by considering (1) as the hypothesis

$$H_{UC} \triangleq H_0 : \mathbf{P}_{data} \cap \mathbf{K}_i \cap \mathbf{T}_{spec} \neq \emptyset. \tag{6}$$

Therefore, a controller K_i is unfalsified if (6) is not invalidated. The following notation is applied:

$$H_0^0 : \mathbf{P}_{data} \cap \mathbf{K}_i \cap \mathbf{T}_{spec} \neq \emptyset \quad \text{(performance is achieved)},$$
$$H_0^1 : \mathbf{P}_{data} \cap \mathbf{K}_i \cap \mathbf{T}_{spec} = \emptyset \quad \text{(fails performance, } K_i \text{ is falsified)}.$$

Here, the terms falsified, rejected and invalidated will be used as synonyms. In other words, the hypothesis H_0, which stands for K_i controlling the current feedback loop, is rejected when this controller is falsified. Hence, the following fact holds.

Fact 2 *When H_0^1 holds (H_0 is rejected), the controller is falsified and therefore $F_p \notin \mathcal{F}_{K_i}$. Otherwise, if H_0^0 holds (H_0 not invalid), nothing can be said, i.e., $F_p \in \mathcal{F}$.* $\triangledown$

A bank of controllers is created to handle specific fault modes. Fact 2 applies when this task has been adequately performed. Notice that, by convention, H_0 is considered as the first hypothesis statement of the set $\mathcal{H}$ in (5).

4 Combining Diagnosis and Control Strategies

4.1 The Diagnosis Statement

The information about the present fault mode obtained from the set of falsified controllers and the diagnosis sub-statements are combined to form a *diagnosis statement* S, which is the conclusion reached by the set of hypothesis tests.

Each falsified controller excludes from consideration the fault modes $\mathcal{F}_{K_i}$ the controller is designed to handle. Denote the set of falsified controllers as $\mathcal{K}_f \subseteq \mathcal{K}$. Using Fact 2, the information about the current fault mode obtained from the set of falsified controllers is that the considered fault mode belongs to set $\mathcal{F}_f^c$ obtained by removing all fault modes related to the falsified controllers, i.e.,

$$\mathcal{F}_f^c = \mathcal{F} \setminus \bigcup_{K_i \in \mathcal{K}_f} \mathcal{F}_{K_i}, \tag{7}$$

where $\setminus$ is the notation for set complement. Notice that (7) provides the information concerning the final decision of the control performance sub-statement, facing the selection of the appropriate controller from the set of the unfalsified ones. According to Fact 1, each rejected hypothesis test H_k limits the current fault mode F_p to belong to the sub-diagnosis statement $S^1_{H_k}$. Denote the set of rejected hypothesis tests as $\mathcal{H}_f \subset \mathcal{H}$. Then, combining the information of rejected hypothesis tests yields the set $S_{\mathcal{H}_f}$ to which F_p should belong to, i.e.,

$$S_{\mathcal{H}_f} = \bigcap_{H_i \in \mathcal{H}_f} S^1_{H_i}, \qquad i = 1, \ldots, L. \tag{8}$$

In this case, (8) provides the evaluation of the remainder set of sub-statements (excluding the sub-statement of control performance already evaluated in (7)). Notice that the information for individually evaluating these sub-statements comes from signals measured from the system, which should not be necessarily those used for the control performance sub-statement module (UC-based controller selection). Hence, outputs y and z can be measured from the system, where z are not necessarily controlled.

Combining (7) and (8) yields the diagnosis statement S of the combined hypothesis tests to which F_p should belong to, i.e.,

$$S = \mathcal{F}_f^c \cap S_{\mathcal{H}_f}. \tag{9}$$

Notice that S is never empty as it will always include F_u. Also note that by defining $H_{UC} \triangleq H_0$ as before and including it in (8), then $S^1_{H_0} \triangleq \mathcal{F}_f^c$ holds and (9) can be included in the general framework, i.e., (8) holds for all $i = 0, \ldots, L$.

4.2 Controller Switching Strategy

When a fault occurs, it is important to switch to the correct controller as soon as possible in order to avoid further performance degradation. Furthermore, this paper considers that there will exist a controller $K_\star \in \mathcal{K}$ of low performance and high robustness that will be used in case that the $M+1$ controllers in $\mathcal{K}$ are not selected. Hence, $K_\star$ ensures that the system keeps working despite of this situation. It also implies $|\mathcal{K}| = M + 2$.

In this section, a *switching strategy* is presented, which takes advantage of the combined diagnosis statement given by (9). Two possible situations can trigger switching. Firstly, if the controller currently in the feedback loop is falsified and the sub-statements different from the one related to the control performance produce the corresponding output, a switch is performed. Secondly, if a controller with

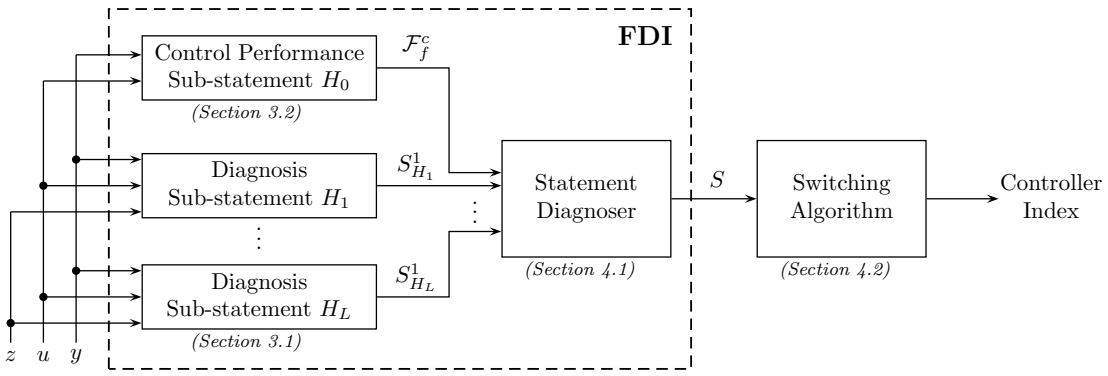

Figure 2: Scheme of the proposed integration of UC into the SHT framework. Here, L different diagnosis sub-statements have been considered.

higher priority (according to pre-established criteria) than the controller currently in the feedback loop becomes unfalsified and again the other sub-statements allow to, then a switch is performed as well. In both cases, the set S and the controller priority definition determine both the possible fault and the controller to handle it. It means that the controller falsification performed by the UC strategy is not the unique factor that determines the switching. Information about the status of other components within the loop and acting as indicators of the current behavioural mode determine the output S^1_H and hence the decision S.

Among many priority criteria that may be used to distinguish among controllers handling faults within the set S, the following can be enumerated:

1. The number of failure modes a controller can handle.
2. The ruggedness of sensors and actuators a controller is connected to.
3. The best performance according to a particular cost function, e.g., (2).
4. The amount of uncertainty a controller can handle (in cases a conservative design is sought). This criterion confronts the previous one, therefore a compromise should be met.
5. The controller that achieves the least number of switching, e.g., a slight loss of performance could be tolerated if the actual controller in the loop is kept, in order to avoid switching transients.

5 The Overall Proposed SHT Strategy

Different procedures described in previous sections are then merged to determine the suitable controller according to the fault model currently affecting the system. Hence, Figure 2 depicts the entire proposed approach and the corresponding outcomes, while Algorithm 2 summarizes the whole FDI-FTC procedure. In order to clearly explain how the approach works, Example 1 is presented.

Example 1 *Assume four faults are possible and three controllers have been designed to handle them. The sets $\mathcal{F}_{K_i}$ are:*

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

Algorithm 2 FDI-FTC Procedure

Require: $\mathcal{F}_{K_0}, \ldots, \mathcal{F}_{K_M}, S_{H_1}, \ldots, S_{H_L}$

loop
  take u and y from the system
  evaluate sub-statement H_0 (control performance)
  compute $\mathcal{F}_f^c = \mathcal{F} \setminus \bigcup_{K_i \in \mathcal{K}_f} \mathcal{F}_{K_i}$ ▷ with $\mathcal{F}$ in (4)
  for $i = 1$ to L **do**
    evaluate sub-statement H_i (diagnosis)
  end for
  compute $S_{\mathcal{H}_f} = \bigcap_{H_i \in \mathcal{H}_f} S^1_{H_i}$
  compute the statement $S = \mathcal{F}_f^c \cap S_{\mathcal{H}_f}$
  determine the controller index $j \in \{0, 1, \ldots, M\}$ ▷ by using criteria outlined in Section 4.2
  insert the controller $K_j \in \mathcal{K}$ into the closed loop ▷ with $\mathcal{K}$ in (3)
end loop

In addition, assume that hypothesis H_1 relates faults $\{F_2, F_3\}$ with the break-down of a particular sensor and H_2 with a short circuit in an actuator that relates with faults $\{F_1, F_4\}$. Controllers are prioritized according to the number of faults they can manage (criteria (1) in Section 4.2). During the closed-loop operation, both the nominal and the K_1 controllers have been falsified and the sensor is broken. Therefore, $S^1_{H_0} = \mathcal{F}_f^c = \{F_2, F_3, F_4\}$, and $\mathcal{H}_f = \{H_1\}$, and thus $S^1_{H_1} = \{F_2, F_3\}$ and $S = \mathcal{F}_f^c \bigcap S_{\mathcal{H}_f} = \{F_2, F_3\}$. As a consequence, controller K_2 is selected because it handles more faults in S, i.e., $\{F_2, F_3\}$ vs. F_3 handled by K_3.

6 PEMFC Simulation Results

6.1 System Description

The system considered consists of a PEMFC test bench station, which mainly comprises a main fuel-cell stack and ancillary units. A schematic diagram of the system is depicted in Figure 3, and the main subsystems are briefly described below [26].

- Air Compressor: 12 V DC oil-free diaphragm vacuum pump. The input voltage V_{cp} of this device is used as the control action.
- Hydrogen and oxygen humidifiers and line heaters: these are used to maintain proper humidity and temperature conditions inside the cell stack, an important issue for PEM membranes. Cellkraft® membrane exchange humidifiers are used in the current set-up. Decentralized PID controllers ensure adequate operation values.
- Fuel cell stack: an ZBT® 8-cell stack with Nafion 115® membrane electrode assemblies (MEAs) is used, 50 cm^2 of active area and 150 W power.

A full-validated dynamic model of the overall PEMFC-based system, specially developed for control purposes, is presented and deeply discussed in [27, 26]. This model retains parameters with physical significance and adequately describes the interaction between the different subsystems (fuel cell stack, reactant supply system and humidity management unit). Every subsystem has been modelled in terms of

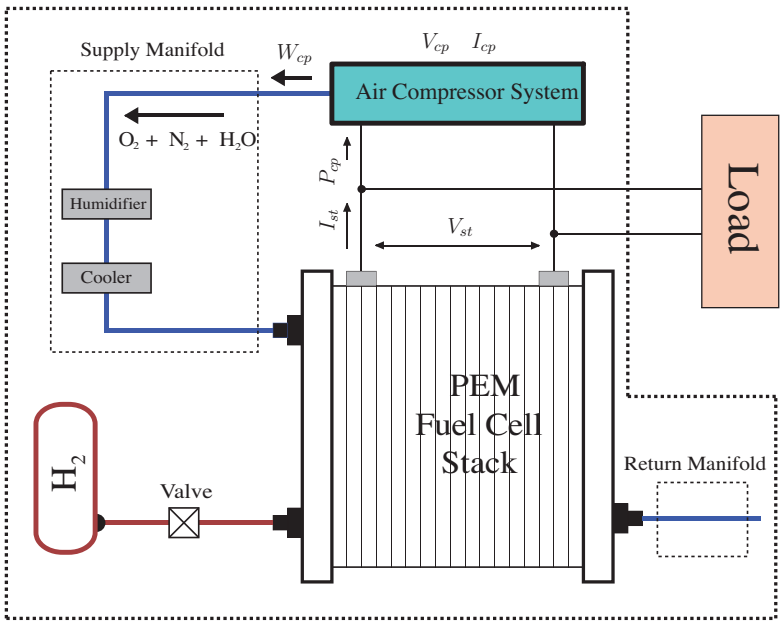

Figure 3: Schematic diagram of the PEMFC-based system

physical laws for the posterior adjustment of some specific parameters, combining a theoretical approach, together with empirical analysis based on experimental data.

Accordingly, the system can be represented by the following continuous-time state-space model:

$$\dot{x}(t) = f\left(x(t)\right) + g(x(t))\, u(t), \tag{10a}$$

$$y(t) = h(x(t)), \tag{10b}$$

where $x \in \mathbb{R}^7$ is the state vector, whose variables are defined as

- $\tilde{x}_1 = \omega_{cp}$: motor shaft angular velocity;
- $\tilde{x}_2 = m_{hum,ca}$: air mass inside the cathode humidifier;
- $\tilde{x}_3 = m_{O_2,ca}$: oxygen mass in the cathode channels;
- $\tilde{x}_4 = m_{N_2,ca}$: nitrogen mass in the cathode channels;
- $\tilde{x}_5 = m_{v,ca}$: vapour mass in the cathode channels;
- $\tilde{x}_6 = m_{H_2,an}$: hydrogen mass in the anode channels;
- $\tilde{x}_7 = m_{v,an}$: vapour mass in the anode channels.

Besides, $u \in \mathbb{R}$ is the control input corresponding to the compressor voltage denoted V_{cp} and $y \in \mathbb{R}$ in the system output corresponding to the inlet stoichiometry of the PEMFC cathode, namely λ_{O_2}. Additionally, $f : \mathbb{R}^7 \to \mathbb{R}^7$, $g : \mathbb{R}^7 \to \mathbb{R}^7$, $h : \mathbb{R}^7 \to \mathbb{R}$ are nonlinear mapping functions of the states, inputs and output, respectively. The system is affected by the external disturbance $I_{st} \in \mathbb{R}$ (through the mapping

functions), which corresponds to the stack current. The objective of a nominal control design consists in tracking λ_{O_2} such that

$$\lim_{t\to\infty}(\lambda_{O_2,\text{ref}} - \lambda_{O_2}(t)) = 0, \tag{11}$$

while rejecting the effect of changes in I_{st} (disturbance), where $\lambda_{O_2,\text{ref}}$ corresponds with a given stoichiometry reference.

The reason for presenting this mathematical model under a data-driven controller design is twofold. First, it allows to have a simulation-oriented model (SOM) used as the virtual reality for the simulations. On the other hand, it is possible to obtain control-oriented models from the SOM such that the bank of controllers used within the UC framework can be obtained. Notice that there is an offline part of the design where the nominal behaviour of the system is known so that not only COM but also fault models/scenarios can be established.

6.2 System Status Scenarios

In this paper, two faults are explicitly considered:

- *Fault 1 (F_1):* This fault is related to the capacity of the air supply from the compressor connected to the PEMFC cathode. This fault is induced in the model by modifying the combined inertia of the compressor motor and the compression device, denoted by J [27]. Basically, this fault implies that the air feeding to the fuel cell is reduced, which implies that the stoichiometry is directly affected, a fact that in turn produces harmful effect over the membrane.

- *Fault 2 (F_2):* This fault is related to the cathode output flow, which is restricted in order to induce the fault. In this case, the fault causes the increment of the internal pressure of the system, which in turn affects the proton exchange and reduces the stack current that feeds the load. The latter is reached by conveniently modifying the cathode output constraint K_{ca} of the PEMFC model [27].

The reason for considering these particular faults in this case study is twofold. First, this faults make sense from the practical viewpoint, therefore they can happen suddenly in a PEMFC-based system. Second, since the faults can be reproduced in a real experiment, their simulation is quite interesting in order to know the potential consequences for a future implementation over an available testbench.

Therefore, taking both faults into account, three scenarios are defined according to the system status: the nominal scenario (F_0), where the system shows no faults, and the F_1 and F_2 scenarios, considering the corresponding faults. Hence, in this case $M = 2$. Notice that the approach presented in this paper handles single-fault situations. However, the extension to multiple simultaneous faults just implies the inclusion of more scenarios and controllers.

6.3 FDI-FTC Setup

As mentioned in Section 3.1, the design of the entire FDI-FTC architecture combines different pre–established hypothesis from the system behaviour and the operation of its devices. In this case, several hypotheses are considered:

- *Hypothesis related to the UC criteria:* This hypothesis, denoted H_0, is based on the decision taken by the UC controller according to (1). To this end, three $\mathcal{H}_\infty$ controllers (K_0, K_1, K_2) have been

designed such that

$$\begin{aligned}\mathcal{F}_{K_0} &= \{F_0, F_2\},\\ \mathcal{F}_{K_1} &= \{F_1\},\\ \mathcal{F}_{K_2} &= \{F_2\}.\end{aligned} \tag{12}$$

- *Hypotheses related to a membrane voltage drop alarm:* The setup contains an alarm that indicates a faulty operation of the PEMFC in relation with the stack voltage. This alarm turns on when either Fault 1 or 2 hold. Hence, two hypotheses are defined

$$\begin{aligned}H_1 &= \{\text{alarm OFF}\},\\ H_2 &= \{\text{alarm ON}\}.\end{aligned}$$

  When H_1 is rejected, i.e., H_1^1 holds, then $S_{H_1}^1 = \{F_1, F_2\}$. In turn, when H_2 is rejected, i.e., H_2^1 holds, then $S_{H_2}^1 = \{F_0\}$.

Regarding the UC controller, the performance for each K_i is based on the cost function in (2), with $W_e = 10$, $W_u = 8$ and $\alpha = 10^{-3}$. These weights provide a tradeoff between performance and robustness. The controllers are designed with standard tools from the Robust Control framework ($\mathcal{H}_\infty$ optimal control) and computed by means of a Linear Matrix Inequality (LMI) optimization procedure [28]. Each $\mathcal{H}_\infty$ controller has been designed based on a model that corresponds to the faultless (F_0) case, and for the two faults described previously (F_1 and F_2). For each case, the complete nonlinear model has been linearised at different loads, i.e. $I_{st} = 2, 4, 6, 8$ A, hence 12 linear models have been obtained. In each F_i, $i = 0, 1, 2$, four resultant models have been combined in a nominal model $G_i(s)$ and an uncertainty weight W_{unc}^i is set in order to produce a robust controller. Finally, three $\mathcal{H}_\infty$ controllers $K_i(s)$, for $i = 0, 1, 2$, have been designed for all cases. It turns out that the nominal controller K_0 works adequately not only for the faultless case but also for the second fault F_2, i.e., $\mathcal{F}_{K_0} = \{F_0, F_2\}$. According to the discussion presented in Section 4.2, there should exist a controller $K_\star \in \mathcal{K}$ that ensures the coverage of the possible behavioural mode F_u. In this case, no other controller different from $K_i(s)$, for $i = 0, 1, 2$ was considered. Therefore, the F_u mode is handled here by using $K_0(s)$. The switching among controllers is based on the decision of the FDI module (evaluation of sub-statements including the one related to the control performance handled by the UC approach) and the switching strategy explained previously (Section 4.2). The controller state-space matrices can be found in the Appendix.

6.4 Results and Discussion

The example considers a load perturbation of $I_{st} = 6$ A, which is a quite common assumption for stationary applications. Notice that different values of I_{st} can be taken into account by increasing the bank of designed controllers according to new system models. However, this paper considers a reduced number of cases, seeking for the simplicity and clarity of the presentation. All three controller designs are based on the linearised models corresponding to this current in the nominal, Fault 1 and Fault 2 scenarios, respectively. In addition, a small amount of model uncertainty around each of these operation points has been considered in order to have a minimum robustness margin and a high level of performance. The desired stoichiometry is $\lambda_{O_2,\text{ref}} = 3$ for all cases.

Figure 4 shows the curves obtained from the proposed simulation. The top graph corresponds to the different scenarios associated with the system status. They induce the behaviour of the system reflected in its output. Moreover, the status of the alarm associated to the stack voltage is presented in the fifth plot. Taking into account the system output λ_{O_2} and the control signal V_{cp} (related to the current controller K_i), the UC procedure provides the index of the most suitable controller according to the cost function

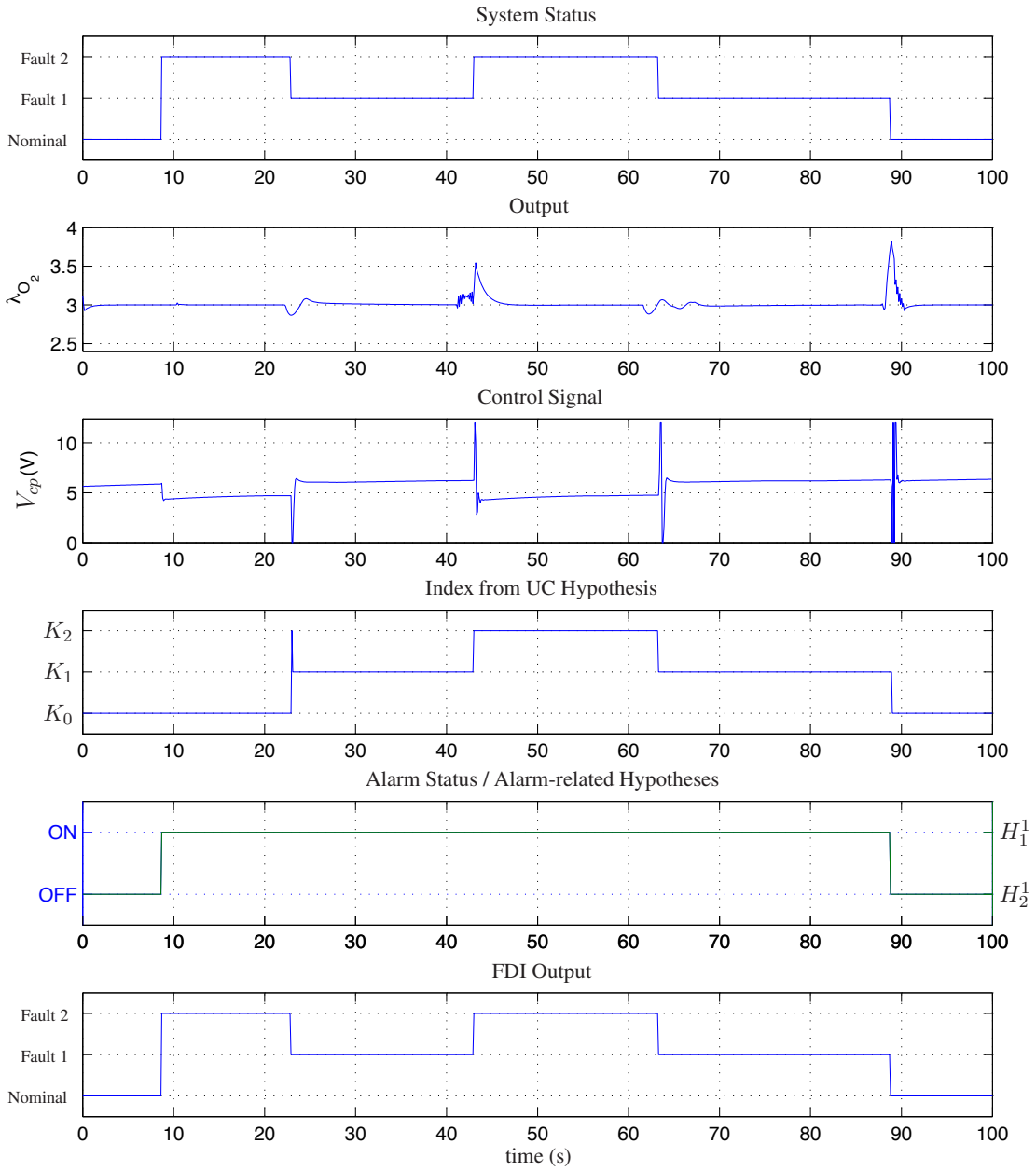

Figure 4: Case study simulation results.

selected. This decision, related to the hypothesis test H_0, is combined with the alarm status in order to determine the fault currently affecting the system.

In the proposed simulation, all hypotheses contribute in obtaining the FDI output. Considering the situation from $t = 9\,\text{s}$ up to $t = 23\,\text{s}$, the UC hypothesis H_0 determines no controller switching even though the system status changes from the nominal scenario to the F_2, due to the fact that K_0 also

handles F_2. However, the hypotheses related to the alarm status (ON) combined with the priority criterion, based on the maximum number of fault handling that minimizes controller switching, are instrumental in selecting the proper FDI outcome. Here, $\mathcal{K}_f = \{K_1\}$ and $\mathcal{F}_f^c = \{F_0, F_2\}$. In addition, H_1^1 holds and $S_{H_1}^1 = \{F_1, F_2\}$, therefore according to (9) yields

$$S = \mathcal{F}_f^c \cap S_{\mathcal{H}_1}^1 = \{F_2\}. \tag{13}$$

The last part of the simulation scenario where $t \in (89, 100]$ follows the previous discussion but considering that H_2^1 holds (alarm OFF).

From $t = 24\,\text{s}$ up to $t = 89\,\text{s}$, since H_1^1 holds (alarm ON), the proper FDI output is based on the intersection in (9):

- The UC-related index indicates K_1, therefore $\mathcal{F}_f^c = \{F_1\} \rightarrow S = \{F_1\}$.
- The UC-related index indicates K_2, hence $\mathcal{F}_f^c = \{F_0, F_2\}$ and $S_{H_2}^1 = \{F_1, F_2\}$. Therefore $S = \{F_2\}$.

During the elapsed time from t = 9 s up to t = 89 s (corresponding with alarm ON), the only sub-statement that changes is $\mathcal{F}_f^c$, which corresponds with the falsification of controllers performed by the UC strategy (in this case, the result of the SHT of $\mathcal{H}_0$). According to the fourth graph of Figure 4, the index changes as the proper controller is chosen, which implies the falsification of the rest of controllers. This falsification procedure follows the design established in (12). The outcome of this example illustrates that the combination of the diagnosis sub-statements with the UC procedure determines the correct choice of the fault scenario, i.e., the coincidence between the first and last plots in Figure 4.

7 Conclusions and Future Research

This paper proposes and discusses the integration of the robust unfalsified control (UC) strategy with the fault diagnosis and isolation scheme based on structured hypothesis testing, inserted in a fault-tolerant control scheme for its use in the management of PEMFC-based systems. Here, UC acts as a real-time learning mechanism that efficiently excludes unsuitable controllers without the use of PEMFC models. The FTC scheme works in a modular fashion: a fault affecting the system just implies the addition of a new controller into a bank of controllers to cope with it. The approach has been tested with a realistic simulator of the breathing system for a PEMFC-based system, obtaining successful results when different faults affected the system. The case of multiple simultaneous faults and their effect in system performance will be the matter of future research and the implications in the design of the controllers of the bank. Moreover, the dynamic influence of the controller currently placed in the closed loop and the falsification/unfalsification of the rest of controllers is another topic of future interest. Moreover, the implementation of the proposed approach to the real test bench the SOM was obtained from, is also a challenge to reach in the coming future.

References

[1] Blanke M, Kinnaert M, Lunze J, Staroswiecki M. *Diagnosis and Fault-Tolerant Control*. Springer-Verlag Berlin Heidelberg, 2006.

[2] Rosich A, Sarrate R, Nejjari F. On-line model-based fault detection and isolation for PEM fuel cell stack systems. *Applied Mathematical Modelling* 2014; **38**(11-12):2744 – 2757.

[3] Lowery N, Vahdati M, Potthast R, Holderbaum W. Classification and fault detection methods for fuel cell monitoring and quality control. *Journal of Fuel Cell Science Technology* 2013; **10**(2):1–8.

[4] Hernandez A, Hissel D, Outbib R. Modeling and fault diagnosis of a polymer electrolyte fuel cell using electrical equivalent analysis. *IEEE Transactions on Energy Conversion* 2010; **25**(1):148–160.

[5] Yang W, Lee K, Junker S, Ghezel-Ayagh H. Fuzzy fault diagnosis and accommodation system for hybrid fuel-cell/gas-turbine power plant. *IEEE Transactions on Energy Conversion* 2010; **25**(4):1187 – 1194.

[6] Feroldi D. Fault diagnosis and fault tolerant control of PEM fuel cell systems. *PEM Fuel Cells with Bio-Ethanol Processor Systems*. Springer Verlag, 2012; 185 – 206.

[7] Fekriy S, Athans M, Pascoal A. Issues, progress and new results in robust adaptive control. *International Journal of Adaptive Control Signal Processing* 2006; **20**:519–579.

[8] Baldi S, Battistelli G, Mosca E, Tesi P. Multi-model unfalsified adaptive switching control: Test functionals for stability and performance. *International Journal of Adaptive Control and Signal Processing* 2011; **25**(7):593–612.

[9] Giovanini L. Robust adaptive control using multiple models, switching and tuning. *IET Control Theory &Applications* 2011; **5**(18):2168–2178.

[10] Rosa P, Silvestre C. Multiple-model adaptive control using set-valued observers. *International Journal of Robust and Nonlinear Control* 2014; **24**(16):2490–2511.

[11] Safonov MG, Tsao TC. The unfalsified control concept and learning. *IEEE Transactions On Automatic Control* 1997; **42**:843–847.

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

[13] Jain T, Yame JJ, Sauter DD. Synergy of canonical control and unfalsified control concept to achieve fault tolerance. *Proceedings of the 18th IFAC World Congress*, Milano (Italy), 2011; 14 832–14 837.

[14] Jain T, Yamé J, Sauter D. Model-free reconfiguration mechanism for fault tolerance. *International Journal of Applied Mathematics and Computer Science* 2012; **22**(1):125–137.

[15] Rosa P, Casau P, Silvestre C, Tabatabaeipour S, Stoustrup J. A set-valued approach to FDI and FTC: Theory and implementation issues. *Proceedings of the 8th IFAC Safeprocess*, Mexico City (Mexico), 2012; 1281–1286.

[16] Rosa P, Silvestre C, Athans M. Model falsification using set-valued observers for a class of discrete-time dynamic systems: a coprime factorization approach. *International Journal of Robust and Nonlinear Control* 2014; **24**(17):2928–2942.

[17] Nyberg M. Model based fault diagnosis: Methods, theory, and automotive engine applications. PhD Thesis, Linköpings Universitet June 1999.

[18] Ingimundarson A, Sánchez-Peña R. Using the unfalsified control concept to achieve fault tolerance. *IFAC World Congress*, Seoul (Korea), 2008; 1236–1242.

[19] Bianchi F, Ocampo-Martinez C, Kunusch C, Sánchez-Peña R. Fault-tolerant unfalsified control for PEM fuel cell systems. *IEEE Transactions on Energy Conversion* 2015; **30**(1):307–315.

[20] Popper KR. *Conjectures and Refutations: The Growth of Scientific Knowledge.* Routhledge: London, 1963.

[21] Stefanovic M, Safonov M. *Safe Adaptive Control*. Springer: London, 2011.

[22] Gelso E, Castillo S, Armengol J. *Artificial Intelligence Research and Development*, *Frontiers in Artificial Intelligence and Applications*, vol. 184, chap. An interval-based approach for fault isolation and identification in continuous dynamic systems. IOS Press, 2008; 421 – 429.

[23] Gertler J. Analytical redundancy methods in fault detection and isolation; survey and synthesis. *Proceedings of the IFAC Fault Detection, Supervision and Safety for Technical Processes*, Baden-Baden (Germany), 1991; 9–21.

[24] Hazewinkel M ((ed.)). *Verification of statistical hypotheses*. Encyclopedia of Mathematics, Springer, 2001.

[25] Sánchez-Peña RS, Colmegna P, Bianchi F. Unfalsified control based on the $\mathcal{H}_\infty$ controller parameterisation. *International Journal of Systems Science* 2015; **46**(15):2820–2831.

[26] Kunusch C, Puleston P, Mayosky M. *Sliding-Mode Control of PEM Fuel Cells*. Springer London Ltd: London, UK, 2012.

[27] Kunusch C, Puleston P, Mayosky M, Husar A. Control oriented modelling and experimental validation of a PEMFC generation system. *IEEE Transactions on Energy Conversion.* 2011; **6**(3):851–861.

[28] Gahinet P, Apkarian P. An LMI approach to $\mathcal{H}_\infty$ control. *International Journal of Robust and Nonlinear Control* 1994; **4**(8):421–448.

A Appendix

The state-space matrices for all three controllers used in the example are presented below.

$\boxed{K_0}$

$$
\begin{aligned}
A &= \begin{bmatrix}
-6.7829 & -0.0037 & 0.0001 & 3.9715 & -220.3413 & -59.0786 & 179.7676 \\
0.0050 & -0.0064 & -0.0000 & -0.0000 & 0.0023 & 0.0008 & -0.0023 \\
0.0391 & -0.0002 & -0.0072 & -0.0015 & 0.0155 & 0.0055 & -0.0167 \\
-4.7632 & -0.0001 & -0.0023 & -0.0339 & -2.7012 & -0.8747 & 2.6597 \\
216.2607 & -0.0039 & -0.0388 & 3.7455 & -27.4785 & 1.3811 & -3.9073 \\
-96.3049 & 0.0033 & 0.0177 & -3.5833 & 116.4761 & 19.6490 & -61.0929 \\
-330.0259 & 0.0080 & 0.0600 & -7.2706 & 123.8101 & 46.4117 & -137.5476
\end{bmatrix}, \\
B &= \begin{bmatrix} -92.7 & 0 & 0 & -1.3 & -1.7 & -1694.7 & -2041.1 \end{bmatrix}^T \\
C &= \begin{bmatrix} -45.8786 & 0.0040 & -0.0000 & -4.2879 & 237.4097 & 63.6404 & -193.6486 \end{bmatrix}, \\
D &= 99.8065.
\end{aligned}
$$

$\boxed{K_1}$

$$
\begin{aligned}
A &= \begin{bmatrix}
-2.6940 & 13.5819 & -0.0167 & -0.4572 & -6.4127 & -10.5250 & 37.0514 \\
-15.5808 & -0.3058 & 0.0004 & 0.0108 & 0.1174 & -0.6021 & 1.9980 \\
0.0123 & 0.0004 & -0.0066 & -0.0001 & -0.0001 & 0.0010 & -0.0033 \\
0.3318 & 0.0099 & -0.0002 & -0.0082 & -0.0015 & 0.0294 & -0.0960 \\
3.8733 & 0.1247 & -0.0001 & -0.0010 & -0.0671 & 0.3651 & -1.2173 \\
12.8354 & -0.9643 & 0.0012 & 0.0323 & 0.5091 & -6.6624 & 21.7635 \\
-90.6640 & 39.4620 & -0.0487 & -1.3259 & -19.0496 & 32.3284 & -99.5904
\end{bmatrix}, \\
B &= \begin{bmatrix} -81 & -4.4 & 0 & 0.2 & 2.7 & -53.1 & -2391 \end{bmatrix}^T \\
C &= \begin{bmatrix} -56.3643 & -16.3028 & 0.0199 & 0.5470 & 7.6641 & 12.5496 & -44.1792 \end{bmatrix}, \\
D &= 96.6336.
\end{aligned}
$$

$\boxed{K_2}$

$$
\begin{aligned}
A &= \begin{bmatrix}
-3.9146 & 0.0046 & -0.5139 & 6.3732 & 134.0345 & -33.6667 & -93.5428 \\
-0.0000 & -0.0281 & 0.0000 & -0.0001 & 0.0014 & -0.0007 & -0.0018 \\
0.3972 & 0.0000 & -0.0302 & 0.0169 & -0.0233 & 0.0362 & 0.0996 \\
-6.1935 & -0.0003 & 0.0206 & -0.1885 & -0.2688 & -0.2997 & -0.8257 \\
-132.9598 & -0.0023 & 0.1958 & -2.1387 & -21.2025 & -2.9375 & -7.7631 \\
24.4698 & 0.0016 & -0.1317 & 1.7434 & 25.6023 & -19.1737 & -49.9312 \\
217.0745 & 0.0068 & -0.6228 & 7.4867 & 108.2153 & -34.9274 & -92.5914
\end{bmatrix}, \\
B &= \begin{bmatrix} -74 & 0 & 0.1 & -0.7 & -6 & -89.6 & 2052.6 \end{bmatrix}^T \\
C &= \begin{bmatrix} -60.0003 & -0.0062 & 0.6918 & -8.5838 & -180.3063 & 45.2286 & 125.6666 \end{bmatrix}, \\
D &= 99.3740.
\end{aligned}
$$