INTERNATIONAL JOURNAL OF ADAPTIVE CONTROL AND SIGNAL PROCESSING
Int. J. Adapt. Control Signal Process. 2008; **22**:142–160
Published online 22 August 2007 in Wiley InterScience (www.interscience.wiley.com). DOI: 10.1002/acs.987

Safety verification and adaptive model predictive control of the hybrid dynamics of a fuel cell system

M. Fiacchini*,†, T. Alamo, I. Alvarado and E. F. Camacho

Departmento de Ingenieria de Sistemas y Automatica, Escuela Superior de Ingenieros, University of Seville, Seville, Spain

SUMMARY

The problem of safety verification of a fuel cell (FC) system is addressed in this paper. The aim of safety verification is to check whether the oxygen ratio can reach dangerous values or not. Assuming that the compressor voltage is controlled by means of a feedforward control, two algorithms for safety verification are formulated and applied to the PWA model of the FC. An improved behavior is obtained using an adaptive predictive controller to determine the voltage to be applied to the compressor. An admissible robust control invariant set for the PWA model of the system is computed. The control action of the predictive controller is obtained in such a way that the state is always included in the safe region provided by the admissible robust control invariant set. This guarantees that the proposed controller always provides safe evolutions of the system. Copyright © 2007 John Wiley & Sons, Ltd.

Received 19 November 2006; Revised 12 April 2007; Accepted 7 June 2007

KEY WORDS: verification; model predictive control; PWA systems; fuel cell system

1. INTRODUCTION

In recent years, many research efforts have been directed to the study of hybrid systems [1–6]. These systems exhibit discrete and continuous dynamics simultaneously. The presence of the two types of dynamics leads to the substantial inapplicability of both the classical systems theory and the automata theory.

Many of the research efforts in hybrid systems have been motivated to verify the behavior of safety-critical system components. The problem of safety verification is to verify whether some non-safe regions can be reached or not by a given controlled hybrid system. Verification techniques

*Correspondence to: M. Fiacchini, Departmento de Ingenieria de Sistemas y Automatica, Escuela Superior de Ingenieros, University of Seville, Seville, Spain.
†E-mail: mirko@cartuja.us.es

Contract/grant sponsor: European Commission
Contract/grant sponsor: MEC

are usually based on computation of the reachable set of a hybrid automaton representing the system under study, or an approximation of that set. An alternative method employs the concepts of abstraction and refinement for computing that approximated set; iteratively, a simplified hybrid model is generated (abstraction), an evolution violating the safety condition is searched and eventually used for refining the abstraction. Important contributions to this research area are presented in [7–11]. Finally, some computational tools for model checking of hybrid systems must be mentioned, such as *Uppaal*, *Hytech* and *CheckMate*.

In this paper, the problem of safety verification of a fuel cell (FC) plant is addressed. The FC, located in the laboratory of the Departamento de Ingenieria de Sistemas y Automatica of the University of Seville, generates electricity from the chemical reaction between oxygen and hydrogen. The plant is composed of different sub-systems. In this safety verification problem, it is assumed that the voltage of the compressor is given by the feedforward control presented in [12]. Under this assumption, a simple discrete-time PWA model of the plant is obtained. The obtained model has a switching nature that depends on the slope of the current input. Two verification algorithms are proposed for such class of PWA models.

In order to improve the behavior, an adaptive model predictive controller for the compressor voltage is presented. The proposed controller relies on the use of an admissible robust control invariant set. The computation of an admissible robust control invariant sets for hybrid systems has been addressed in [4]. The computation of the maximal robust control invariant set for a PWA system is in many situations computationally unaffordable. Using the particular characteristics of the obtained PWA system, we are able to present an efficient algorithm for the computation of an admissible robust control invariant set for the FC system. The presented adaptive model predictive controller incorporates a constraint that forces the evolution to be confined in the obtained admissible robust control invariant set. This guarantees that, in spite of the simplifications assumed to obtain an implementable adaptive predictive controller, the evolution of the system always remains within the safe region.

The paper is organized as follows. In the next section, a brief description of an FC is given. In Section 3, the problem of safety verification for the FC is formulated and a PWA model of the system is presented. In Section 4, two verification algorithms are applied to the PWA model. Section 5 presents a synthesis-oriented model of the system. The computation of the admissible robust control invariant set is detailed in Section 6. The adaptive predictive controller, along with different numerical results are presented in Section 7. The paper concludes with Section 8.

2. DESCRIPTION OF FUEL CELLS

An FC is a device that generates electricity from hydrogen and oxygen. This is achieved by converting chemical energy of the fuel directly into electricity. An FC is a class of galvanic cell based on oxidation–reduction reaction composed by three main parts:

1. *Anode*: where the electrons and ions are produced. The anode reaction is $H_2 \rightarrow 2H^+ + 2e^-$.
2. *Cathode*: where the ions and electrons are combined. The cathode reaction is $\frac{1}{2}O_2 + 2H^+ + 2e^- \rightarrow H_2O$.
3. *Electrolyte*: it is the electric insulator able to conduct ions. The electrolyte of the proposed FC is a proton exchange membrane (PEM) made of a polymer (Nafion).

DOI: 10.1002/acs

The overall reaction is $H_2 + \frac{1}{2}O_2 \rightarrow H_2O + \text{Electricity} + \text{Heat}$. See that the secondary products are merely water and heat. The rate of the reaction is determined by the electricity consumption of the external load. The elementary FC is assembled forming a membrane electrode assembly (MEA) where the PEM is sandwiched between the anode, the cathode and the flow field plates. The anode and cathode are made of carbon fiber paper and a platinum catalyst. An elementary FC can provide 1.2 V although the typical value is 0.6 V. In order to obtain a larger voltage, FCs are stacked.

The FC system considered in this paper is a PEM FC, which operates with pure hydrogen and air and an external humidifier. This provides up to 1200 W of unregulated DC power at a nominal output voltage of 26 V. The FC is now connected to a resistive load which can be manipulated manually and will allow the simulation of different loads. The system is basically divided into five parts: (1) *The Cell stack*: it is the part of the system where the electricity is produced. (2) *The electric load*: simulates a real consumer of the produced electricity. (3) *Air supply and humidity exchanger*: the FC is supplied by air with a required humidity. The air is filtered and accelerated by a controlled compressor and humidified in an humidity exchanger. The necessary water is obtained from the water product of the reaction. (4) *Hydrogen storage and supply*: the hydrogen pressure and flow are regulated in the operating conditions. (5) *Cooling system*: the heat produced by the generation of the electricity is refrigerated by a fan which moves air through the stack, controlling the temperature of the plant.

Despite the efficiency of the cell stack being about 60%, the efficiency of the whole FC system is typically 35% due to the external devices. A detailed dynamic model of the FC has been developed by Arce and del Real using existing knowledge taken from the literature (see [13]). This model has been validated on the real plant. A technical report illustrating such model can be found at page http://www.esi2.us.es/∼bordons. A journal version of this technical report will be available in the *Journal of Power Sources* [12].

3. HYBRID MODEL FOR THE VERIFICATION OF THE FUEL CELL

The oxygen ratio is a very important variable to consider when the model is analyzed in terms of safety verification due to the *oxygen starvation* phenomenon. The system is said to be in the starvation mode when the ratio between the oxygen input flow and the reacting one is less than 2. When it occurs, the current oxygen flow cannot maintain the process and this can damage the membrane and therefore destroy the FC. It is clear that the importance of monitoring the ratio to guarantee the system never enters in a starvation mode. Hence, the safety condition is

$$\lambda_{O_2} = \frac{W_{O_2,\text{in}}}{W_{O_2,\text{reacted}}} \geqslant 2 \tag{1}$$

where $W_{O_2,\text{in}}$ is the oxygen input flow and $W_{O_2,\text{reacted}}$ is the oxygen reacting in the cell.

The aim of safety verification analysis is to check that the current reference does not lead to starvation or, alternatively, to formulate conditions over the reference signal to ensure that the phenomenon does not take place. As detailed in the following sections, a discrete-time PWA model obtained using the model derived in [12], can be used to efficiently address the safety verification problem.

DOI: 10.1002/acs

3.1. Discrete-time PWA model of the fuel cell

Consider that, to prove safety, it is necessary to evaluate all the possible evolutions of the system for a given set of initial conditions. The continuous-time complete model cannot be used for verification purposes because of the following:

1. The complexity of the system: non-linearities and high-order dynamics.
2. The dynamical variables are strongly coupled.
3. Different time scales: the presence of different physics phenomena lead to very different time constants.

In this section, a simplified discrete-time PWA model is presented. Obviously, that model has to capture the main dynamical features of the original one. The current load I_{st} is initially considered as the input and the oxygen ratio λ_{O_2} as the output. The temperature is considered constant; the ambient temperature is fixed in 298 K and the FC one in 333 K. This assumption is practically equivalent to impose the system in a normal operational state, that is, neither in the starting nor in the stopping phase. Under this assumption, the effect of the variation of temperature is negligible.

The employed sampling time is $t = 0.2$s, which is appropriate to capture the main dynamics of the system and coincides with the sample time of a digital filter present in the air pump block. A low-order model consisting of a four poles transfer function has been considered. The least square criterion is employed to obtain the corresponding parameters. The admissible current load goes from 10 to 40 A, since this is the range in which the model is valid.

Some simulations are executed applying steps as input, that is, varying instantaneously the current load from a value to another. This kind of input signal has been used since we assume the electrical loads to be able to switch suddenly from a constant value to another. Different discrete-time linear models can be obtained for each different input steps. In this way, a PWA model in which the regions are determined by the input is obtained.

The obtained responses showed that the system reacts immediately to an input variation, that is, the system is not strictly proper. In Figure 1, the input and output signals are represented. It can be seen that the input variation leads to a jump of the output to an unsafe value close to 1.5. This is due to the fact that electrochemical dynamics have little time constant compared with the sampling time. Also, note that the oxygen ratio, after the transitory due to the step input, recovers its initial value. This is due to the feedforward control implemented in the compressor of the FC.

The transfer function to identify is parameterized as

$$y(k) = \left[c + \frac{b_1 z^{-1} + \cdots + b_m z^{-m}}{1 + a_1 z^{-1} + \cdots + a_n z^{-n}} \right] u(k) \tag{2}$$

where $u \in \mathbb{R}$ is the input, the current load, and $y \in \mathbb{R}$ denotes the deviation of the oxygen ratio with respect to the steady value. Given a step input, the initial deviation from the steady value is determined by the product of c and the size of the step. Therefore, it is concluded that the different values of the constant c obtained at different operating conditions can be used to fully characterize the input steps that lead to the violation of the safety restriction (1). However, this analysis characterizes the starvation phenomenon only under step inputs. A much more evolved analysis is required to address the verification problem under arbitrary inputs.

DOI: 10.1002/acs

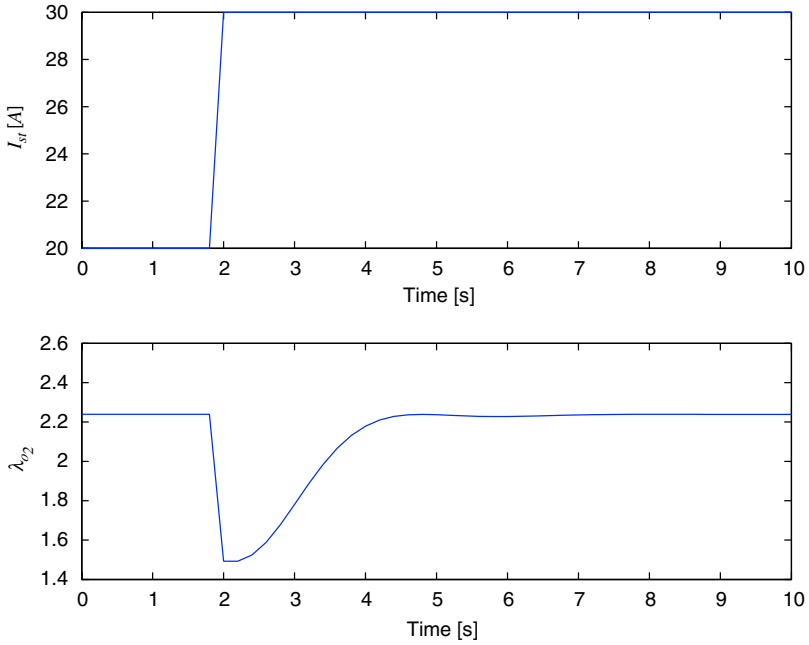

Figure 1. Simulation with a step input.

In order to gain more insight into the nonlinear dynamics of the system, ramp signals were also used for identifying the plant. Simulations lead to some conclusions:

1. The system steady-state output does not depend on the constant input, that is, if the input is maintained constant, the oxygen ratio is $\lambda_{O_2} \cong 2.2391$. This is due to the feedforward control implemented in the compressor, which drives the system to this steady state when the input current reaches a constant value.
2. The system depends not linearly on the slope value of the current input. In other words, the deviation of λ_{O_2} with respect to the steady-state value depends in a nonlinear way on the rate of change of the input.
3. Surprisingly, the output depends only on the ratio between the variation of the current and the current. That is, defining $\Delta I_{\mathrm{st}}(k) = I_{\mathrm{st}}(k) - I_{\mathrm{st}}(k-1)$, the output of the plant is basically determined by

$$r(k) = \frac{\Delta I_{\mathrm{st}}(k)}{I_{\mathrm{st}}(k)} \tag{3}$$

regardless on the particular values $\Delta I_{\mathrm{st}}(k)$ and $I_{\mathrm{st}}(k)$.

From the aforementioned observations, it is concluded that an appropriate strategy to obtain a PWA model of the system involves considering the ratio (3) as the excitation input and the oxygen

DOI: 10.1002/acs

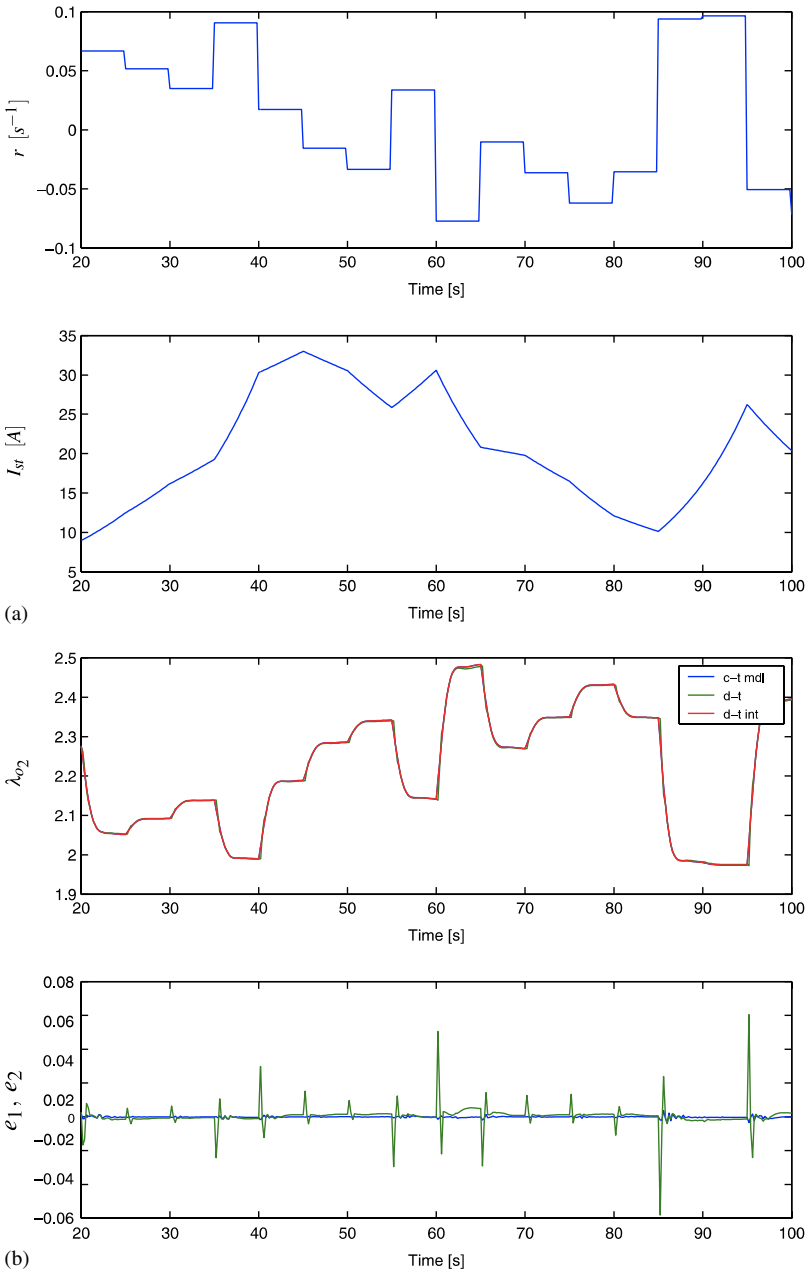

Figure 2. Evaluation of the identified PWA models under random ratio input. The maximal error of the PWA model with the integrator is about 30 times greater than the one of the PWA model identified without imposing the presence of an integrator: (a) random ratio and input and (b) oxygen ratios y errors.

DOI: 10.1002/acs

ratio λ_{O_2}, normalized around the steady-state value, as the output. The proposed PWA model is the following:

$$y(k) = G_i(z)u(k) \quad \text{if } u(k) \in R_i \tag{4}$$

where the input is $u(k) = r(k)$ and n_i regions R_i, $i = 1, \ldots, n_i$ are considered. Note that the different regions are characterized only by the input $r(k)$. For the identification, two different models have been considered:

1. A 3 zeros–3 poles model with a discrete integrator:

$$y(k) = \frac{z^{-1}}{1 - z^{-1}} \frac{b_0^i + b_1^i z^{-1} + b_2^i z^{-2} + b_3^i z^{-3}}{1 + a_1^i z^{-1} + a_2^i z^{-2} + a_3^i z^{-3}} u(k) \tag{5}$$

2. A 4 zeros–4 poles model without imposing the presence of a discrete integrator:

$$y(k) = \frac{b_1^i z^{-1} + b_2^i z^{-2} + b_3^i z^{-3} + b_4^i z^{-4}}{1 + a_1^i z^{-1} + a_2^i z^{-2} + a_3^i z^{-3} + a_4^i z^{-4}} u(k) \tag{6}$$

The identification algorithm is applied computing a linear system for each ratio between -0.1 and $0.1\ \mathrm{s}^{-1}$ and variation of $0.01\ \mathrm{s}^{-1}$, that is, $r_i = -0.1, -0.09, \ldots, 0.09, 0.1\ \mathrm{s}^{-1}$, $i = 1, \ldots, n_i$ with $n_i = 21$. Two PWA systems, composed of a family of transfer functions, one for each ratio, are obtained.

In Figure 2(a) and (b), the results of the identification are displayed. Figure 2(a) shows the input; in the upper plot a random ratio input is represented, in the lower one the corresponding current load is displayed. In Figure 2(b), the evolutions corresponding to the complex continuous-time model [12] and the identified time-discrete PWA models are represented in the upper plot. In the lower plot, the prediction errors corresponding to both PWA models are shown. The error is greater than 0.06 for the model with an integrator. However, for the other model, the error never reaches values greater than 0.002. The outputs of the continuous-time model and those of the PWA discrete-time corresponding to the transfer function without integrator are practically equal.

4. SAFETY VERIFICATION USING THE PWA MODEL

The identification procedure illustrated in the previous section provides two discrete-time PWA linear systems, good approximations of the continuous-time nonlinear one. In this section, the PWA model is employed for evaluating if the system is safe. Moreover, since the PWA model without the integrator provides a better approximation, this one is considered.

First, it is opportune to reformulate each PWA model in state-space representation. For that purpose, it is necessary to define a state vector. We consider the state vector $x(k) = [y(k), y(k-1), y(k-2), y(k-3), u(k-1), u(k-2), u(k-3)]^{\mathrm{T}}$. Dynamical system (6) can be re-written as

$$x(k+1) = A_i x(k) + B_i u(k) \quad \text{if } u(k) \in R_i \tag{7}$$

DOI: 10.1002/acs

where

$$A_i = \begin{bmatrix} -a_1^i & -a_2^i & -a_3^i & -a_4^i & b_2^i & b_3^i & b_4^i \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \qquad (8)$$

$$B_i = [b_1^i \quad 0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0]^{\mathrm{T}}$$

for $i = 1, \ldots, n_i$. In the following, we will consider $u(k) = r(k)$.

Due to the PWA nature of the model, each transfer function is considered valid for a neighborhood of a nominal ratio r_i. The considered nominal values are $r_i = -0.1, -0.09, \ldots, 0.09, 0.1$, $i = 1, \ldots, n_i$, where $n_i = 21$ is the number of different regions. The distance between them is $\delta_r = 0.01$. It is concluded that the PWA regions are

$$R_i = \{r \in (-0.105, 0.105) : |r - r_i| \leqslant 0.5\delta_r\} \qquad (9)$$

for $i = 1, \ldots, n_i$. Note that it has been supposed that the ratio cannot exceed the value of 0.105 in magnitude. Clearly, if $u(k) \in R_i$ then $\Delta_r(k) = r_i - u(k)$ satisfies $|\Delta_r(k)| \leqslant 0.5\delta_r = 0.005$.

Moreover, denote with w the additive uncertainty due to the difference between the complex continuous-time model given in [12] and the identified PWA one, excited by the same input, that is $w(k) = \lambda_{O_2}(k) - y(k)$. Various simulations have confirmed that the error can be considered bounded, that is $|w(k)| \leqslant \delta_w = 0.002$.

Hence, the following PWA model will be considered for validation purposes:

$$x(k+1) = A_i x(k) + B_i r_i + B_i \Delta_r(k) + E w(k) \quad \text{if } r(k) = r_i + \Delta_r(k) \in R_i \qquad (10)$$

where $E = [1\ 0\ 0\ 0\ 0\ 0\ 0]^{\mathrm{T}}$, $|w(k)| \leqslant 0.002$ and $i = 1, \ldots, n_i$.

Suppose, without loss of generality, that the input and the output are bounded in two polyhedral sets: $y(k) \in Y = \{y \in \mathbb{R} : 1 \leqslant y \leqslant 3\}$, $u(k) \in U = \{u \in \mathbb{R} : -0.105 \leqslant u \leqslant 0.105\}$. Such bounds do not exclude any interesting state. These bounds on the values of $y(k)$ and $u(k)$ imply that the state space $x(k)$ is assumed to belong to a bounded polyhedron $X \subset \mathbb{R}^7$, which can be easily obtained from Y and U. Moreover, the safety condition can be expressed in the polyhedral form, that is, the state x is said to satisfy the safety condition if it belongs to the polyhedron $S = \{x \in \mathbb{R}^7 : H_s x \leqslant K_s\} \subseteq X$.

In this section, we show that the particular structure adopted for the PWA model of the system allows us to propose two algorithms for checking whether the system is safe or not. In particular, the fact that the PWA region active at each instant depends only on the input and not on the state, strongly simplifies the verification analysis. This is illustrated in the following sections.

An instrumental proposition is introduced before further analysis.

Proposition 1

Consider PWA system (10) and a polyhedral set $P = \{x \in \mathbb{R}^7 : Hx \leqslant K\}$. The set of states mapped inside the set P by means of the ith PWA model, regardless of the input $r(k) \in R_i$ and the

DOI: 10.1002/acs

admissible uncertainty $w \in W$, is equal to

$$Q = \{x \in \mathbb{R}^7 : HA_i x \leqslant K - HB_i r_i - 0.5|HB_i \delta_r| - |HE\delta_w|\} \tag{11}$$

where $|HB_i \delta_r|$ and $|HE\delta_w|$ are the vectors whose entries are the absolute values of the elements of $HB_i \delta_r$ and $HE\delta_w$, respectively.

Proof
In order to prove the result, the following equality should be proved:

$$Q = \{x \in \mathbb{R}^7 : H(A_i x + B_i r + Ew) \leqslant K, \forall r \in R_i, \forall w \in W\}$$

Denoting with H_k the kth row of matrix H, with K_k the kth element of vector K and with n_k the number of rows of H and K, it follows

$$\begin{aligned}
Q &= \{x \in \mathbb{R}^7 : H(A_i x + B_i r + Ew) \leqslant K, \forall r \in R_i, \forall w \in W\} \\
&= \left\{x \in \mathbb{R}^7 : \max_{r \in R_i, w \in W} \{H_k(A_i x + B_i r + Ew)\} \leqslant K_k, \forall k = 1, \ldots, n_k\right\} \\
&= \left\{x \in \mathbb{R}^7 : H_k A_i x + \max_{r \in R_i, w \in W} \{H_k(B_i r + Ew)\} \leqslant K_k, \forall k = 1, \ldots, n_k\right\} \\
&= \left\{x \in \mathbb{R}^7 : H_k A_i x + \max_{r \in R_i} \{H_k B_i r\} + \max_{w \in W} \{H_k E w\} \leqslant K_k, \forall k = 1, \ldots, n_k\right\}
\end{aligned} \tag{12}$$

Noting that

$$\max_{r \in R_i} \{H_k B_i r\} = H_k B_i r_i + 0.5|H_k B_i \delta_r| \quad \forall k = 1, \ldots, n_k$$

$$\max_{w \in W} \{H_k E w\} = |H_k E \delta_w| \quad \forall k = 1, \ldots, n_k$$

we obtain $Q = \{x \in \mathbb{R}^7 : HA_i x + HB_i r_i + 0.5|HB_i \delta_r| + |HE\delta_w| \leqslant K\}$. □

Consider the ith linear model and suppose that the input does not exit from the ith region, that is, $r(k) \in R_i$ or equivalently $r(k) = r_i + \Delta_r(k)$, with $|\Delta_r(k)| \leqslant 0.5\delta_r$, for every $k \geqslant 0$. Denote S^i_j the set of initial states $x(0)$ such that the trajectories generated by the ith linear model remain inside the safe region during at least the first j samples, regardless of the uncertainty $w(k) \in W$ and the ratio $r(k) \in R_i$, for all $k = 0, \ldots, j$. Note that, by definition $S^i_0 = S$. Suppose that the set S^i_j is a polyhedron, that is, it can be expressed as $S^i_j = \{x \in \mathbb{R}^n : H^i_j x \leqslant K^i_j\}$. Then, the set S^i_{j+1} is given by

$$S^i_{j+1} = \{x \in S : H^i_j(A_i x + B_i r + Ew) \leqslant K^i_j, \forall r \in R_i, \forall w \in W\} \tag{13}$$

for all $i = 1, \ldots, n_i$. This implies that the sequence S^i_j, for $j \geqslant 0$, can be computed iteratively. It is clear that $S^i_{j+1} \subseteq S^i_j$ and that the sequence converges to a set S^i_∞. That is, $\lim_{j \to \infty} S^i_j = S^i_\infty$, which is the desired safe set (assuming that the input r belongs always to R_i). The following proposition provides a way for computing the set S^i_{j+1} given S^i_j.

DOI: 10.1002/acs

Proposition 2
Consider the set S^i_{j+1} defined in (13). Define

$$T^i_{j+1} = S \cap \{x \in \mathbb{R}^7 : \tilde{H}^i_{j+1} x \leqslant \tilde{K}^i_{j+1}\}$$

where $\tilde{H}^i_{j+1} = H^i_j A_i$ and $\tilde{K}^i_{j+1} = K^i_j - H^i_j B_i r_i - 0.5|H^i_j B_i \delta_r| - |H^i_j E \delta_w|$. Note that $|H^i_j B_i \delta_r|$ and $|H^i_j E \delta_w|$ denote the vectors whose entries are the absolute values of the elements of $H^i_j B_i \delta_r$ and $H^i_j E \delta_w$, respectively. Then $T^i_{j+1} = S^i_{j+1}$.

Proof
The proof stems directly from Equation (13) and Proposition 1:

$$\begin{aligned} S^i_{j+1} &= S \cap \{x \in \mathbb{R}^7 : H^i_j (A_i x + B_i r + E w) \leqslant K^i_j, \forall r \in R_i, \forall w \in W\} \\ &= S \cap \{x \in \mathbb{R}^7 : H^i_j A_i x \leqslant K^i_j - H^i_j B_i r_i - 0.5|H^i_j B_i \delta_r| - |H^i_j E \delta_w|\} = T^i_{j+1} \end{aligned}$$ □

Note that by construction, if S^i_j is a polyhedral set then S^i_{j+1} is polyhedral. Hence, from this and the fact that by definition $S^i_0 = S$ is polyhedral, it follows that every set S^i_j is polyhedral. This result can be employed to design two algorithms to determine the set of initial conditions that guarantee a safe evolution of the plant. These two algorithms for the safety verification of the PWA model are detailed in the following.

1. The first algorithm provides a necessary condition for safety. It is based on the following idea: consider individually each linear model and, for each of them, suppose that the system remains in the related region. This is equivalent to impose that the ratio remains always in a unique region R_i. Then, under this assumption, the possible trajectories are a subset of the admissible ones. Hence, if one or more linear systems yield unsafety, the whole PWA system is unsafe. The benefit of this algorithm is that it has a low computational burden when compared with the second one which can be avoided if the system results unsafe.

Then, for each region R_i, for $i=1, \ldots, n_i$, apply

Algorithm 1

(a) Given the admissible region $S = \{x \in \mathbb{R}^7 : H_s x \leqslant K_s\}$, set $H^i_0 = H_s$ and $K^i_0 = K_s$. Make $T^i_0 = S$ and $j = 1$.
(b) $T^i_j = S \cap \{x \in \mathbb{R}^7 : \tilde{H}^i_j x \leqslant \tilde{K}^i_j\}$, where

$$\tilde{H}^i_j = H^i_{j-1} A_i, \quad \tilde{K}^i_j = K^i_{j-1} - H^i_{j-1} B_i r_i - 0.5|H^i_{j-1} B_i \delta_r| - |H^i_{j-1} E \delta_w|$$

(c) Obtain a non-redundant set of linear constraints $H^i_j x \leqslant K^i_j$ such that the obtained set T^i_j is rewritten as $T^i_j = \{x \in \mathbb{R}^7 : H^i_j x \leqslant K^i_j\}$.
(d) If $T^i_j = T^i_{j-1}$, or T^i_j is empty then stop. Else, set $j = j + 1$ and return to step b.

At the end of the procedure, if the set is empty then there exists at least an unsafe trajectory and the system is unsafe. By construction, and from Proposition 2, which states that $T^i_j = S^i_j$, the

DOI: 10.1002/acs

set T_j^i is the set of initial conditions $x(0)$ such that the first j steps of the trajectories generated by the ith model, $x(k)$, for $k=0,\ldots,j$, are contained in the safe region S, regardless of the uncertainty and for all the possible ratios belonging to the ith region, $r(k)\in R_i$, $k=0,\ldots,j$. This means that, if T_j^i is empty at the end of the algorithm, no safe initial condition can be maintained indefinitely inside the safe region or, equivalently, that for all the initial condition $x(0)\in S$ there is an input sequence $r(k)\in R_i$ and an uncertainty sequence $w(k)\in W$, $k=0,\ldots,j$, such that the considered initial condition evolves in the unsafe region. Note that repeating the algorithm for all $i=1,\ldots,n_i$ imply to consider only the set of input sequences that do not switch from a region to another, which is a subset of all the admissible input sequences. Hence, an unsafe trajectory for the restricted analysis, in which no switchings between regions is allowed, is admissible also for the PWA model. This proves that if the algorithm terminates with an empty set then the system is unsafe.

However, in order to guarantee safety with respect to the considered uncertain PWA model, the following algorithm is required.

2. In the second algorithm, all the possible trajectories of the system are considered. Therefore, the complexity is higher. However, it determines in an exact way the initial conditions that lead to safe trajectories regardless of the uncertainty and the input.

Algorithm 2

(a) Given the admissible region $S=\{x\in\mathbb{R}^7 : H_s x\leqslant K_s\}$, set $H_0=H_s$ and $K_0=K_s$. Make $T_0=S$ and $j=1$.

(b) $T_j=S\cap\{x\in\mathbb{R}^7 : \tilde{H}_j x\leqslant\tilde{K}_j\}$ where

$$\tilde{H}_j=\begin{bmatrix} H_{j-1}A_1\\ H_{j-1}A_2\\ \cdots\\ H_{j-1}A_{n_i}\end{bmatrix},\quad \tilde{K}_j=\begin{bmatrix} K_{j-1}-H_{j-1}B_1r_1-0.5|H_{j-1}B_1\delta_r|-|H_{j-1}E\delta_w|\\ K_{j-1}-H_{j-1}B_2r_2-0.5|H_{j-1}B_2\delta_r|-|H_{j-1}E\delta_w|\\ \cdots\\ K_{j-1}-H_{j-1}B_{n_i}r_{n_i}-0.5|H_{j-1}B_{n_i}\delta_r|-|H_{j-1}E\delta_w|\end{bmatrix}$$

(c) Obtain a non-redundant set of linear constraints $H_j x\leqslant K_j$ such that the obtained set T_j is rewritten as $T_j^i=\{x\in\mathbb{R}^7 : H_j x\leqslant K_j\}$.

(d) If $T_j=T_{j-1}$, or T_j is empty then stop. Else, set $j=j+1$ and return to step b.

As it is justified below, if the algorithm stops with an empty set T_j then the set of initial conditions yielding safe trajectories is empty. On the other hand, if the algorithm finishes providing a non-empty set T_j, then this set equals the set of initial conditions that correspond to a safe operation regardless of the uncertainty $w(k)$ and the input $r(k)$.

Consider the polyhedral set T_{j-1} and denote n_{j-1}^r the number of rows of matrices H_{j-1} and K_{j-1}. Hence, matrices H_j and K_j defined in step b of Algorithm 2 have $n_i\cdot n_{j-1}^r$ rows. Following the same lines as for Algorithm 1 (see Proposition 2), it is concluded that the first n_{j-1}^r rows of H_j and K_j determine the set of states which are mapped inside T_{j-1} by every $r(k)\in R_1$ and every $w\in W$, the rows from n_{j-1}^r+1 to $2n_{j-1}^r$ determine the set of points mapped inside T_{j-1} for every $r(k)\in R_2$ and every $w\in W$, and so on and so forth. Hence, H_j, K_j determine the subset of S that is mapped inside T_{j-1} regardless of $r(k)$ and $w\in W$. From this and $T_0=S$, it can be proved that the set T_j is the set of initial conditions such that all the trajectories generated by the

DOI: 10.1002/acs

PWA model remain inside the safe region at least for the next j steps regardless of the input $r(k)$ and the uncertainty $w(k)$.

4.1. Safety verification of the fuel cell: results

Executing the first algorithm for the FC PWA model, the result is that some inputs yield to unsafety. In particular if $r_i = 0.1,\ 0.09,\ 0.08$ then the output can reach the threshold of 2. Note that the result agrees with the simulation; from Figure 2(a) and (b), and from other simulations not shown here, it is concluded that if the ratio is maintained at values close to 0.09 or larger, then the oxygen ratio decreases to values lower than 2. It is concluded that if the ratio is greater than or equal to 0.08, then the process is not at a safe operation. This means that in order to avoid the starvation, ratio inputs greater than 0.08 should be avoided. In order to check if the system operates in a safe way for ratios smaller than 0.08, the regions corresponding to ratios greater than or equal to 0.08 are not considered when running the second algorithm. Once eliminated the unsafe inputs $0.08, 0.09$ and 0.1, the second algorithm terminates with a non-empty set, which corresponds to the set of initial conditions that correspond to a safe operation of the plant (provided that the input ratio does not enter into the regions corresponding to ratios $0.08, 0.09$ and 0.1).

5. A SYNTHESIS-ORIENTED MODEL

In the FC system, the control of the air compressor is a crucial task as it is responsible for a safe operation of the system. In previous sections, we assume that the control of the air compressor is the feedforward control law, as detailed in [12]. This control maintains the output λ_{O_2} at a safe value for constant currents. As the variations on the compressor voltage have an important effect on the dynamics of λ_{O_2}, this voltage will be considered as the control input for the system. The idea is to obtain, by means of an adaptive predictive controller, a control correction signal that added to the original feedforward control improves the performance of the system while guaranteeing that the unsafe transients are avoided. This adaptive strategy provides better results than the ones obtained with the original feedforward control, regulating the output to the desired stable value and guaranteeing that the safe constraints are fulfilled.

In the model described in the previous sections, the controller for the air compressor is the aforementioned feedforward law. In order to control the air compressor, a new model of the system is required. This new model should describe the evolution of λ_{O_2} as a PWA model. In this section, we present a synthesis-oriented PWA model consisting of two inputs: the current load (or its ratio) and the variations of compressor voltage. The ratio $r(k)$ will be considered as an external signal defining the system dynamics, that is, the active linear model of the PWA at each instant. That signal will be used in the adaptive model predictive control for selecting the linear model to employ for computing the prediction. The predictive controller provides a correction signal that is added to the feedforward law. The main objective is to compute the correction signal in such a way that it robustly avoids the unsafe starvation region.

For this aim and knowing that the dynamics of the system depend on the ratio $r(k)$, the synthesis-oriented PWA model has been identified applying two pseudorandom binary signal (PRBS): the first on the current ratio, around the nominal value r_i, and the second as voltage variation added to the compressor voltage.

DOI: 10.1002/acs

In other words, for each nominal ratio $r_i \in \{-0.1,\ -0.09, \ldots,\ 0.09,\ 0.1\}$, the ratio excitation is

$$r(k) = r_i + r_{\mathrm{PRBS}}(k) \tag{14}$$

where $r_{\mathrm{PRBS}}(k) = \{+\frac{\delta_r}{2}, -\frac{\delta_r}{2}\}$ is the value of the PRBS.

The other excitation signal is the variation of the compressor voltage:

$$v_{\mathrm{cmp}}(k) = v_{\mathrm{FF}}(I_{\mathrm{st}}(k)) + v_{\mathrm{c}}(k) \tag{15}$$

where the nominal voltage $v_{\mathrm{FF}}(I_{\mathrm{st}}(k))$ is the one provided by the feedforward control and it depends only on the current, $v_{\mathrm{c}}(k) = \{-1, +1\}$ is the added PRBS signal and the compressor voltage $v_{\mathrm{cmp}}(k)$ is given by their sum.

Moreover, the system is initially at the equilibrium given by $v_{\mathrm{cmp}}(k) = v_{\mathrm{FF}}(I_{\mathrm{st}}(k))$ and the constant current $I_{\mathrm{st}}(k) = I_{\mathrm{st}}$. The output considered for identification is the value $y(k) = \lambda_{\mathrm{O}_2} - 2.2391$ and it has been employed to identify the linear model valid around the nominal ratio r_i. The least squares criterion has been applied jointly with the four-pole model:

$$\begin{aligned} y(k) = & \frac{b_1^i z^{-1} + b_2^i z^{-2}}{1 + a_1^i z^{-1} + a_2^i z^{-2} + a_3^i z^{-3} + a_4^i z^{-4}} r(k) \\ & + \frac{c_1^i z^{-1} + c_2^i z^{-2}}{1 + a_1^i z^{-1} + a_2^i z^{-2} + a_3^i z^{-3} + a_4^i z^{-4}} v_{\mathrm{c}}(k) \end{aligned} \tag{16}$$

for $i = 1, \ldots, n_i$. Note that the model is given by the sum of two transfer functions whose four poles are the same. This structure provides good identification results and is very useful for computing a robust control invariant set due to its simplicity.

The model can be rewritten in the form of regressor function, that is,

$$y(k) = \phi(k)^{\mathrm{T}} \theta_i \tag{17}$$

for $i = 1, \ldots, n_i$ and where $\phi(k)$ is the regressor composed of the last values of output and inputs and the parameter vector is $\theta_i = [-a_1^i, -a_2^i, -a_3^i, -a_4^i, b_1^i, b_2^i, c_1^i, c_2^i]^{\mathrm{T}}$. It is easy to compute the parameter vector θ_i solution of the least squares problem.

Then, for each admissible nominal ratio, a linear model is computed. As a further level of simplification, we consider a PWA model composed of $n_i = 9$ linear models, that is, the related to $r_i \in \{-0.1, -0.075, 0.05, \ldots, 0.075, 0.1\}$, with $n_i = 9$ number of regions. Hence, the active linear model is the ith if $r(k) = r_i + \Delta_r(k)$, with $|\Delta_r(k)| \leqslant 0.5\delta_r$, where $\delta_r = 0.025$ and $i = 1, \ldots, n_i$. The choice of a lower number of regions, $n_i = 9$ in spite of the 21 employed for the safety verification PWA model, relies on practical reasons. Indeed, the computation of the robust control invariant set, presented in the following, generates a sequence of polyhedra whose complexity grows with the number of regions. Hence, we decided to reduce the number of regions at the expense of greater uncertainties affecting the precision of the model. The number of regions $n_i = 9$ represented a good trade-off between the complexity of the generated sets and the precision of the model needed to obtain an appropriate non-empty control invariant set.

DOI: 10.1002/acs

6. ROBUST CONTROL INVARIANT SET

The first step to design the adaptive model predictive controller is to find an admissible robust control invariant set for the PWA model. This requires the computation of a region of the state space in which there exists an admissible input such that the next state is contained in that set, regardless of the uncertainty and the active linear model. First, the PWA model (16) is formulated in state-space form. Define the state-space PWA model as

$$x(k+1) = A_i x(k) + B_i^R r(k) + B_i^{V_c} v_c(k) + E w(k) \quad \text{if } r(k) \in R_i \tag{18}$$

where

$$A_i = \begin{bmatrix} -a_1^i & -a_2^i & -a_3^i & -a_4^i & b_2^i & c_2^i \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad B_i^R = \begin{bmatrix} b_1^i \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \quad B_i^{V_c} = \begin{bmatrix} c_1^i \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \quad E = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \tag{19}$$

for $i = 1, \ldots, n_i$. The state, normalized around the steady-state value of 2.2391, is $x(k) = [\lambda_{O_2}(k) - 2.2391, \lambda_{O_2}(k-1) - 2.2391, \lambda_{O_2}(k-2) - 2.2391, \lambda_{O_2}(k-3) - 2.2391, r(k-1), v_c(k-1)]^T$. The active model of the PWA model is determined by the current value of the ratio $r(k)$: the ith model is valid at time k if $r(k) \in R_i$. As the value of $r(k)$ is accessible, at each instant it is possible to know which of the nine linear models determines the dynamics of the system.

The additive uncertainty $w(k)$ represents the error due to the difference between the PWA model and the nonlinear model presented in [12]. As it has been checked by a sufficient large number of simulations, this uncertainty never reaches amplitudes greater than 0.015. Thus, the constraint $w(k) \in W = \{w(k) \in \mathbb{R} : |w(k)| \leqslant \delta_w = 0.02\}$ provides an appropriate conservative bound. The control input is bounded too: $v_c(k) \in V = \{v(k) \in \mathbb{R} : |v_c(k)| \leqslant 10\}$.

The safety condition, namely $\lambda_{O_2} \geqslant 2$, bounds the admissible region of the state space. The admissible region for the first four states, which are the past values of $\lambda_{O_2} - 2.2391$, is given by

$$2 - 2.2391 \leqslant x_j(k) \leqslant 3 - 2.2391, \quad j = 1, \ldots, 4 \tag{20}$$

where the upper bound is a trivial bound never reached by λ_{O_2} (λ_{O_2} never reaches values higher than 3). This bound has been added to avoid eventual computational problems related to managing unbounded polyhedra. The fifth state is the past value of the ratio. As we restrict to ratios included between $-0.1 - 0.5\delta_r$ and $0.1 + 0.5\delta_r$, it results that x_5 must satisfy

$$-0.1125 \leqslant x_5(k) \leqslant 0.1125 \tag{21}$$

The sixth state, which is the past compressor voltage, has to fulfill

$$-10 \leqslant x_6(k) \leqslant 10 \tag{22}$$

These linear inequalities define a safe polyhedron of the state space which can be expressed as $X = \{x \in \mathbb{R}^6 : Mx \leqslant N\} \subseteq \mathbb{R}^6$.

DOI: 10.1002/acs

Define the set C_k as the set of states x for which there is an adaptive robust control policy that guarantees that the sequence $x(0), x(1), \ldots, x(k)$ belongs to the admissible set X regardless of the uncertainty and the ratio input. It is clear that $C_k \subseteq C_{k-1}$, $\forall k$. Moreover, standard arguments for invariant set allows one to affirm that the set

$$\lim_{k\to\infty} C_k = C_\infty$$

constitutes an admissible robust control invariant set.

Define, as an extended state, the vector composed by the state x and the input v_c, that is: $x^e(k) = [x(k)^T, v_c(k)^T]^T \in \mathbb{R}^7$. Given the polyhedral representation of C_k in the state-space $\mathbb{R}^6$, $C_k = \{x \in \mathbb{R}^6 : M_k x \leqslant N_k\}$, the set C_{k+1} is given by

$$C_{k+1} = \bigcap_{i=1}^{n_i} \mathrm{Proj}_x(P_{k+1}^i) \tag{23}$$

where

$$P_{k+1}^i = \{x^e \in X \times V : M_k(A_i x + B_i^{V_c} v_c + B_i^R r + E w) \leqslant N_k, \forall r \in R_i, \forall w \in W\} \tag{24}$$

and $\mathrm{Proj}_x(P_{k+1}^i)$ indicates the projection of the set $P_{k+1}^i \subseteq \mathbb{R}^7$ on the subspace $\mathbb{R}^6$ related to state x.

Note that P_{k+1}^i is the set of $x^e = [x^T, v_c^T]^T$ such that the state x is mapped inside C_k, by means of the control action v_c, when the model is the ith and regardless of the admissible values of r and w. Then, projecting P_{k+1}^i on the subspace of x, the result is the set of states for which there exists at least an admissible value of v_c such that the successor state is mapped inside C_k for all $r \in R_i$ and $w \in W$. Hence, the intersection of the projections provides the set of states that can be maintained in the safe region $k+1$ steps. Note that the previous statement relies on the fact that the value of $r(k)$ is assumed to be measurable.

The following proposition provides a way for computing P_{k+1}^i given C_k. This, and Equation (23) allows one to compute C_{k+1}.

Proposition 3
Consider the set P_{k+1}^i defined in (24). For any $i = 1, \ldots, n_i$, define

$$F_{k+1}^i = \{x^e \in X \times V : M_k A_i x + M_k B_i^{V_c} v_c \leqslant N_k - M_k B_i^R r_i - 0.5|M_k B_i^R \delta_r| - |M_k E \delta_w|\} \tag{25}$$

where $|M_k B_i^R \delta_r|$ indicates the vector whose entries are the absolute values of the elements of $M_k B_i^R \delta_r$. The same for $|M_k E \delta_w|$. Then $P_{k+1}^i = F_{k+1}^i$.

Proof
The result stems directly from the definition of P_{k+1}^i and Proposition 1:

$$\begin{aligned} P_{k+1}^i &= (X \times V) \cap \{x^e \in \mathbb{R}^7 : M_k(A_i x + B_i^{V_c} v_c + B_i^R r + E w) \leqslant N_k, \forall r \in R_i, \forall w \in W\} \\ &= (X \times V) \cap \{x^e \in \mathbb{R}^7 : M_k(A_i x + B_i^{V_c} v_c) + M_k B_i^R r_i + 0.5|M_k B_i^R \delta_r| + |M_k E \delta_w| \leqslant N_k\} \\ &= F_{k+1}^i \end{aligned}$$

□

DOI: 10.1002/acs

The following algorithm provides a way to compute an admissible robust control invariant set.

Algorithm 3

1. Set the initial region $C_0 = X = \{x \in \mathbb{R}^6 : M_0 x \leqslant N_0\}$ and $j = 0$.
2. For each region R_i, for $i = 1, \ldots, n_i$, define

$$F_{j+1}^i = \{x^e \in C_0 \times V : M_j A_i x + M_j B_i^{V_c} v_c \leqslant N_j - M_j B_i^R r_i - 0.5|M_j B_i^R \delta_r| - |M_j E \delta_w|\}$$

3. Compute

$$C_{j+1} = \bigcap_{i=1}^{n_i} \mathrm{Proj}_x(F_{j+1}^i)$$

4. Obtain a non-redundant set of linear constraints $M_{j+1} x \leqslant N_{j+1}$ such that $C_{j+1} = \{x \in \mathbb{R}^6 : M_{j+1} x \leqslant N_{j+1}\}$.
5. If $C_{j+1} = C_j$, or C_j is empty then stop. Else, set $j = j + 1$ and return to step 2.

The algorithm has been applied to the PWA model of the FC and it converged after 19 iterations to a non-empty polyhedron $\hat{C} = \{x \in X : \hat{M} x \leqslant \hat{N}\}$. This polyhedron represents a robust control invariant set for the uncertain PWA system that can be used to implement the adaptive model predictive control proposed in the following section.

7. ADAPTIVE MODEL PREDICTIVE CONTROL

The admissible robust control invariant set $\hat{C}$ is used to guarantee that the proposed controller provides a safe operation of the FC. Every control strategy forcing the state $x(k)$ to remain inside the admissible robust control invariant set ensures that the system remains in the safe region. We employ an adaptive model predictive control strategy which minimizes a quadratic cost and guarantees that the state remains in the safe region. The model used for the prediction depends on the current ratio.

PWA model (18) has been used for designing the model predictive control. The inputs of the controller are the measurement of $\lambda_{O_2}(k)$ and of the current $I_{st}(k)$. At each instant the ratio $r(k)$ is computed from the current input:

$$r(k) = \frac{I_{st}(k) - I_{st}(k-1)}{I_{st}(k)} \tag{26}$$

and the state $x(k)$ of PWA model (18) is updated.

The active linear model is given by the value of $r(k)$ as previously described. Moreover, we assume that the ratio is maintained constant at N steps, where N is the control (and prediction) horizon. Note, however, that, if in the prediction the current reaches the extremal values of 9 V or 41 V, then the ratio is set to zero for the rest of the prediction horizon. The original nonlinear system is valid for a range of current between 9 and 41 A, then we used an opportune saturation (ratio equal to zero) when these extreme values are attained. Thus, in the case that the predicted current reaches the saturated region, the considered ratio is $r(k + j) = 0$ and the related system is

DOI: 10.1002/acs

employed. Hence, the ratio in the prediction horizon is

$$r(k+j)=\begin{cases} r(k) & \text{if } I_{\mathrm{st}}(k+j)\in[9,41] \\ 0 & \text{otherwise} \end{cases} \tag{27}$$

and $I_{\mathrm{st}}(k+j)$ is computed from $I_{\mathrm{st}}(k)$ and using Equation (26).

Through a set of linear constraints, we imposed that the first predicted state belongs to the admissible robust control invariant set $\hat{C}$ despite the uncertainties. This guarantees that the evolution of the system always remains in $\hat{C}$. An additional set of constraints imposes that the predicted nominal state does not violate the safety condition ($\lambda_{\mathrm{O}_2}>2$).

The proposed model predictive control is the following:

$$\begin{aligned} \min_{v_{\mathrm{c}}(k),\ldots,v_{\mathrm{c}}(k+N-1)} \quad & \left\{ \sum_{j=0}^{N-1} (x(k+j|k)^{\mathrm{T}} Q_{\mathrm{MPC}} x(k+j|k) + v_{\mathrm{c}}(k+j)^{\mathrm{T}} R_{\mathrm{MPC}} v_{\mathrm{c}}(k+j)) \right. \\ & \left. + x(k+N|k)^{\mathrm{T}} P_{\mathrm{MPC}} x(k+N|k) \right\} \\ \text{s.t.} \quad & x(k|k)=x(k) \\ & x(k+j+1|k)=A_i x(k+j|k)+B_i^R r(k+j)+B_i^{V_{\mathrm{c}}} v_{\mathrm{c}}(k+j) \\ & \quad \text{if } r(k+j)\in R_i, \quad j=0,\ldots,N-1 \\ & \hat{M}(A_i x(k)+B_i^R r(k)+B_i^{V_{\mathrm{c}}} v_{\mathrm{c}}(k))+|\hat{M}E\delta_w|\leqslant \hat{N} \quad \text{if } r(k)\in R_i \\ & x_1(k+j|k)\geqslant(2-2.2391), \quad j=1,\ldots,N \end{aligned} \tag{28}$$

The prediction horizon has been fixed to $N=8$, for practical reasons. In fact, we tested the adaptive MPC for different values of N, and we found that beyond this value, the MPC control does not provide substantial improvement with respect to horizon 8. The cost is quadratic in the predicted state $x(k+j|k)$ and in the control input $v_{\mathrm{c}}(k+j)$, $j=1,\ldots,N$. The considered output is $y(k)=Cx(k)=[1,0,0,0,0,0]x(k)=\lambda_{\mathrm{O}_2}(k)-2.2391$ and the weighting matrices are $Q_{\mathrm{MPC}}=10\ C^{\mathrm{T}}C$ and $R_{\mathrm{MPC}}=0.1$.

Note that the optimization problem which has to be solved at each sampling time is a quadratic programming problem. The sequence of predicted ratios, defined in Equations (26) and (27), is used for computing the state and the set of constraints, depending on the ratios as well as the initial state $x(k)$ and the initial voltage $v_{\mathrm{c}}(k)$.

Note that, in practice, the ratio is not indefinitely maintained at a non-zero value. As a matter of fact, in normal operation, the ratio will be close to zero. Only during the transitory due to a change from a current load to another, the ratio will take values different from zero. Hence, we consider the system corresponding to ratio zero for computing the matrix P_{MPC}. The final cost matrix P_{MPC} is the one corresponding to the LQR obtained using the same weighting matrices.

The employment of different linear models depending on the current ratio provides the adaptive nature to the control strategy. This, jointly with the safety constraint $x(k+1)\in\hat{C}$, allows one to ensure safeness avoiding the use of more conservative strategies, such as the min–max predictive controller.

DOI: 10.1002/acs

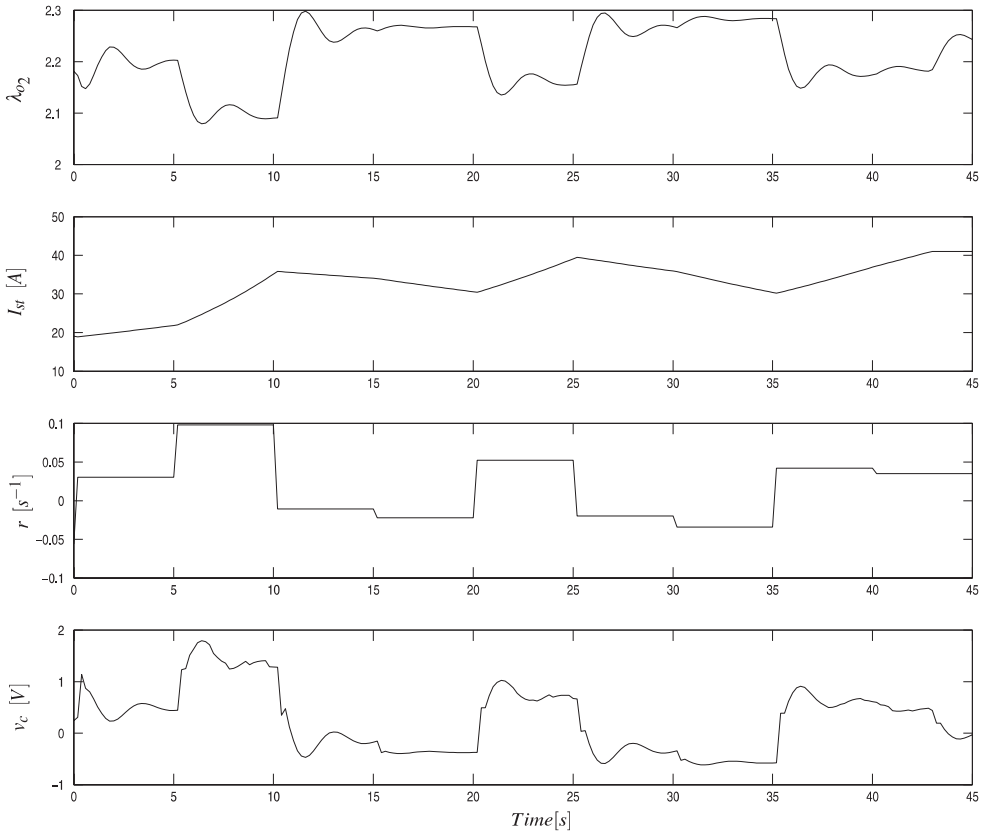

Figure 3. Evolution with MPC and a random varying $r(k)$.

In Figure 3, it is shown the result of the application of the MPC to the nonlinear system. The ratio $r(k)$ is constant during each interval of 5 s and it takes random values. The current I_{st} reaches a wide range of admissible values. The control action is smooth and it has an amplitude smaller than 2 V. Note that the value of λ_{O_2} never reaches the unsafe values, not even between 5 and 10 s, when the ratio is maintained at a value which would have caused unsafety in the absence of the proposed adaptive control strategy.

8. CONCLUSIONS

In this paper, the problem of safety verification of an FC plant has been addressed. The safety verification for the FC consists in checking whether the oxygen ratio reaches values lower than 2 or not, under variation of the current load. A simple discrete-time model in the PWA form has been obtained. Specific algorithms to check the safe operation of the plant have been provided. An adaptive model predictive controller has been proposed. Such a controller relies on the computation of an admissible robust control invariant set. The controller forces the system to remain in a safe set.

DOI: 10.1002/acs

ACKNOWLEDGEMENTS

The authors would like to acknowledge A. Arce and A. J. del Real for supplying the detailed fuel cell model, the European Commission and the MEC for funding this work in the framework of the NoE HYCON FP6-IST-511368 and the project DPI2005-04568.

REFERENCES

1. Heemels WPMH, De Schutter B, Bemporad A. Equivalence of hybrid dynamical models. *Automatica* 2001; **37**:1085–1091.
2. Bemporad A, Borrelli F, Morari M. Optimal controllers for hybrid systems: stability and piecewise linear explicit forms. *Proceedings of the 39th IEEE Conference on Decision and Control*, vol. 2(2), Sydney, Australia, 2000; 1810–1815.
3. Grieder P, Kvanisca M, Baotic M, Morari M. Stabilizing low complexity feedback control of constrained piecewise affine systems. *Automatica* 2005; **41**:1683–1694.
4. Rakovic S, Grieder P, Kvasnica M, Mayne D, Morari M. Computation of invariant sets for piecewise affine discrete time systems subject to bounded disturbances. *Proceedings of the 43rd IEEE Conference on Decision and Control*, Atlantis, Paradise Island, Bahamas, 2004; 1418–1423.
5. Lazar M, Heemels W, Weiland S, Bemporad A. Stabilization conditions for model predictive control of constrained PWA systems. *Proceedings of the 43rd IEEE Conference on Decision and Control*, Atlantis, Paradise Island, Bahamas, 2004; 4595–4600.
6. Bemporad A, Borrelli F, Morari M. Piecewise linear optimal controllers for hybrid systems. *Proceedings of the American Control Conference*, vol. 2, Chicago, IL, U.S.A., 2000; 1190–1194.
7. Alur R, Dang T, Ivancic F. *Hybrid Systems*: *Computation and Control*: *5th International Workshop*, *HSCC 2002*, Stanford, CA, U.S.A. Springer: Berlin, Heidelberg, 25–27 March 2002; 35.
8. Alur R, Dang T, Ivancic F. *Tools and Algorithms for the Construction and Analysis of Systems*: *9th International Conference*, *TACAS 2003*, *Held as Part of the Joint European Conferences on Theory and Practice of Software*, *ETAPS 2003*, Warsaw, Poland. Springer: Berlin, Heidelberg, 7–11 April 2003; 208–223.
9. Alur R, Dang T, Ivancic F. *Hybrid Systems*: *Computation and Control*: *6th International Workshop*, *HSCC 2003*, Prague, Czech Republic. Springer: Berlin, Heidelberg, 3–5 April 2003; 4–19.
10. Alur R, Henzinger T, Laferriere G, Pappas GJ. Discrete abstraction of hybrid systems. *Proceedings of the IEEE* 2000; **88**(7):971–984.
11. Lafarriere G, Pappas GJ, Sastry S. O-minimal hybrid systems. *Mathematics of Control*, *Signals*, *and Systems* (*MCSS*). Springer: London, 2000; 1–21.
12. del Real AJ, Arce A, Bordons C. Development and experimental validation of a PEM fuel cell dynamic model. *Journal of Power Sources* 2007; DOI: 10.1016/j.jpowsour.2007.04.06.
13. Prukushpan JT, Stefanopoulou AG, Peng H. *Control of Fuel Cell Power Systems*: *Principles*, *Modeling and Analysis and Feedback Design*. Springer: Berlin, 2004.