Predictive maintenance of actuators in linear systems: A receding horizon set-theoretic approach

Francesco Tedesco | Waseem Akram | Mehdi Forouzanfar | Alessandro Casavola | Domenico Famularo

1 Dipartimento di Ingegneria Informatica, Modellistica, Elettronica e Sistemistica (DIMES), Università della Calabria, Rende, CS, Italy
2 Department of Electrical Engineering, Islamic Azad University, Ahvaz Branch, Ahvaz, Iran

Correspondence
Francesco Tedesco, Dipartimento di Ingegneria Informatica, Modellistica, Elettronica e Sistemistica (DIMES), Università della Calabria, Via Pietro Bucci, Cubo 42-c, 87036 Rende, CS, Italy. Email: francesco.tedesco@unical.it

Funding information
Ministero dello Sviluppo Economico, Grant/Award Number: B31B19000670008

Abstract
This work is focused on a model predictive control (MPC) based approach for the regulation of systems whose actuators are subject to loss of effectiveness. Such a degradation process, whose evolution is assumed to be measurable and predictable, can lead to actuators breakdown whenever certain thresholds are exceeded. Within this context, if the control problem is defined with ad hoc operational constraints and/or running costs, the intrinsic MPC capability of mitigating faulty events arises. To this end, the proposed control scheme consists of two modules: the former is in charge of performing a prognostic activity on actuators’ health, while the second one reconfigures the control law on the basis of actuators’ degradation information. The core of the proposed method relies on modeling healthy and faulty plant configurations via a switching systems paradigm that is instrumental to offline determine sequences of precomputed inner approximations of one-step ahead controllable sets. Such regions are online selected by a switching logic in order to determine a control signal properly weighted on the basis of the measured actuators degradation level.

KEYWORDS
fault tolerant control, model predictive control, predictive maintenance, switching systems

1 INTRODUCTION

The degree of complexity of industrial control systems has been progressively increased so that their management may include ad hoc predictive maintenance tasks in order to preserve the overall integrity. Within this context, the notion of just-in-time predictive maintenance is of interest here and refers to the capability of optimizing the assets repair at the requested time instant. Repairs performed too soon or too late could incur in added expenses and/or severe component failures. In order to guarantee the above mentioned properties, it is essential to develop effective supervision and diagnosis methods providing resiliency and fault tolerance.

Abbreviations: FTC, fault tolerant control; MPC model predictive control
According to the variety and severity of faults that may affect a given plant, different levels of performance have to be considered in several fault scenarios. Moving from safe to dangerous regions, degraded performance is often acceptable. In addition, in order to ensure that the closed-loop system is able to track a command input or a reference model/trajectory even in the event of faults, reconfigurable control strategies need to be synthesized to achieve safety and satisfactory performance.4

Specific attention is here dedicated to the actuators’ role which is crucial within a feedback control system. In fact, the actuator capability to deliver the demanded control action can be affected by degradation phenomena resulting in a best case performance reduction or complete plant fatal breakdown if the stability of the system is lost.

For these reasons, prognostics and health monitoring (PHM) for actuators are gaining interest among researchers.3,5,6 Among them, a particular focus is related to the determination of the actuators’ healthy status in order to estimate their time-to-failure or remaining-useful-lifetime (RUL).7 The latter quantity can be exploited in a maintenance plan to schedule future interventions to prevent undesired monitored device crash.5 In a control perspective, the RUL or other PHM information can be used to compensate for the degradation effects of the actuators by smartly balancing the control effort over them.2,9,10 This is achieved by reconfiguring the control actions so as to preserve the desired dynamic and static performance of the system, as well as its stability, while protracting the life of the actuators until maintenance operations are carried out.

Within this context the model predictive control (MPC) approach seems to be a perfect candidate to properly regulate a plant while smartly distributing control effort on the actuators to achieve fault-tolerant capabilities.11,12 Such an aspect can be handled in a generic and systematic manner in the MPC design. For this reason, such a strategy has attracted the attention of many researchers focusing on MPC-based FTC schemes, see References 13-16.

The first contribution13 deals with the thermal damages reduction involving a boiler–turbine system. In this case, the MPC cost contains a term related to the dynamics of the degradation that is described by means of a linearized model. As a result, a substantial reduction in the accumulated damage was observed during a step response simulation, at the cost of some loss of performance. However, the damages depend on the cost function weights, as well as the step magnitude in the control task.

In the second contribution,14 RUL estimates of increasingly degrading electromechanical actuators have been adopted for an MPC strategy. In order to mitigate the accumulated damage, the predictive controller was in charge of modifying the reference position to an internal control loop with the aim of limiting the transient actuator current. Moreover, the RUL constraint is managed via a soft approach where predicted violations are penalized in the MPC cost function. Anyway, there is no a priori guarantee that the actual constraint on the RUL value is enforced. As in Reference 13, the damage results depend on the tuning of the controller.

The third one15 takes into consideration mixed logical dynamic expressions to represent hybrid systems. Using this approach, a hybrid model of the system to be controlled is obtained, which includes inherent hybrid phenomena and possible logical modes caused by faults occurrence. This allows one to adapt the system model on-line by taking into account the fault information provided by a fault diagnosis and isolation module. In this way, the controller can cope with the considered faults.

Finally, in Reference 16, the actuator degradation evolution is assumed to have a progress rate proportional to the control effort. The loss of effectiveness occurs when the degradation level overcomes an intermediate threshold. Within this scenario, an MPC control law is adopted that needs to solve a mixed-integer programming problem at each sampling step to deal with binary deviations along with the predictions.

In this article, an MPC strategy with FTC capabilities is proposed to take care of possible loss of actuator effectiveness due to degradation progress. As in Reference 16, the degradation rate is assumed to be proportionally related to the control effort and a modification (gain reduction) of the input map of the plant occurs when a specified threshold is overcome by the deterioration level. Unlike Reference 16, online mixed-integer programming is avoided and most of the computational effort is offline moved by resorting to one-step ahead controllable set concepts developed for a hybrid system paradigm. In particular, a group of system models is derived by considering all possible actuator faults configurations. Then, for each model, a family of one-step ahead controllable sets is determined. Such sets are used during the online operations in a receding horizon strategy aimed at steering the state toward the origin. Moreover, when the plant deviates with respect to its normal behavior, due to the degradation effects, the new corresponding configuration along with the related family of controllable sets is adopted for control purposes. The resulting FT scheme is based on the interactions between two interconnected modules: a PHM unit, being responsible for monitoring the actuator degradation level and a reconfigurable controller that is designed to adapt its action on the basis of the information conveyed by the PHM block. The main improvement with respect to Reference 16 relies on its reduced computational burdens since, as previously
stated, any mixed-integer optimization is avoided. Furthermore, feasibility retention can be proved even during the recovery phase occurring when a faulty actuator is repaired/replaced. Finally, it is formally proved that the proposed strategy is able to ensure a minimum guaranteed RUL before a complete actuators’ failure. Preliminary results of this work have been presented in Reference 17 that is here extended in several directions and by adding further contents. In particular,

1. The problem to be solved is introduced in a more formal and exhaustive way.
2. Relevant details are revealed about each stage of the working logic of the proposed control architecture.
3. All the theoretical results include a formal proof and have been presented in a more comprehensive fashion.
4. The simulation section has been enriched by presenting more detailed descriptions.

The article is organized as follows: in Section 2, the problem to be solved is formulated. Section 3 presents the proposed control architecture along with its main property. In Section 4, a simulative example is included to assess the presented methods. Finally, some conclusions end the article.

2 | PROBLEM FORMULATION

Let us consider plants that can be modeled as

\[ x(t+1) = Ax(t) + B(\rho(t))u(t) + B_d d(t), \]  

(1)

where \( x(t) \in \mathbb{R}^n \) denotes the state, \( u(t) \in \mathbb{R}^m \) the input, \( \rho(t) = [\rho_1(t), \ldots, \rho_m(t)] \in \mathbb{R}^m \) collects the degradation values of each actuators evolving as

\[ \rho_i(t+1) = \rho_i(t) + \alpha_i |u_i(t)|, \quad i = 1, \ldots, m \]  

(2)

and \( d(t) \in \mathbb{R}^d \) represents the process disturbance assumed to be confined into the compact set \( D \) containing the origin. Moreover the plant actuator input is subject to some saturation constraints

\[ u(t) \in U^c, \quad \forall t \geq 0, \quad U^c := \{ u \in \mathbb{R}^m : |u_i| \leq u_{\text{max}} \}. \]  

(3)

with \( u_{\text{max}} > 0 \) and \( U^c \) a compact subset of \( \mathbb{R}^m \) containing the origin as an interior point.

It is evident from (2) that the actuator deterioration increases for nonzero control inputs. Moreover, the impact of the degradation process on the \( i \)th input matrix column \( B_i(\rho_i(t)) \in \mathbb{R}^n \) is modeled as follows

\[ B_i(\rho_i) = \begin{cases} B_i & \text{if } \rho_i < \rho_{\text{lim},i}, \\ \gamma_i B_i & \text{if } \rho_{\text{lim},i} \leq \rho_i \leq \rho_{\text{max},i}, \\ 0 & \text{if } \rho_i > \rho_{\text{max},i}. \end{cases} \]  

(4)

Here \( B_i \) denotes the nominal input column matrix and the real valued coefficient \( \gamma_i, 0 < \gamma_i < 1 \), quantifies the loss of \( i \)th actuator effectiveness when the degradation reaches the threshold \( \rho_{\text{lim},i} \). In this respect, the following three operative scenarios arise:

1. **Normal phase**: \( \rho_i < \rho_{\text{lim},i} \), the actuator is healthy and is able to work under nominal conditions.
2. **Maintenance required phase**: \( \rho_{\text{lim},i} \leq \rho_i \leq \rho_{\text{max},i} \), in this scenario most of the efficiency of the actuator is lost, anyway the stabilizability of the system is guaranteed.
3. **Actuator breakdown**: \( \rho_i > \rho_{\text{max},i} \), the vector \( \rho_{\text{max},i} \in \mathbb{R} \) represents the maximum degradation level that can be tolerated without total breakdown of the actuators. In this situation the stabilizability of the system is not any longer guaranteed.

In view of the above envisaged scenarios, it is worth observing that the degradation process is itself not reversible. Anyway, an external fix procedure is nevertheless possible for the generic \( i \)th actuator during the system operations that basically resets its \( \rho_i \) degradation value to be lower than \( \rho_{\text{lim},i} \).
Moving from these considerations, we can define the following specific state space configurations of the original plant (1), each one related to fault occurrences of a subset of actuators $A_j \subset \{1, m\}$

$$x(t + 1) = Ax(t) + B_j u(t) + B_d d(t),$$

where $B_j = B \cdot \text{diag}(\{a_1^j, \ldots, a_m^j\})$, with $a_i^j \in \{0, \gamma, 1\}$. Moreover, it is assumed that for each realization of $B_j$, $(A, B_j)$ is a stabilizable pair. Model (5) represents a particular system configuration where a single or multiple actuators are partially available so that only the remaining healthy input devices belonging to $\{1, m\} \setminus A_j$ and associated with the input map $B_j$ are in charge of driving the plant. In this way, all admissible system configurations can be abstractly collected into a switching system where a logical rule that orchestrates the switching among $3^m - \nu$ subsystems (5):

$$\Sigma_\nu : \{ x(t + 1) = Ax(t) + B_j u(t) + B_d d(t).$$

$B_0 \equiv B$ being the nominal input matrix (where all the actuators are healthy) and $\nu$ denoting the number of possible subsystems configuration where $(A, B_j)$ is not a stabilizable pair (such a pairs are excluded from the $\Sigma_\nu$ configurations). The switching mechanism among these subsystems can be defined by a switching logic that generates a proper signal described through classes of piecewise constant sequences $\sigma : \mathbb{Z}_+ \rightarrow I$, $|I| = 3^m - \nu$ where the index $j = \sigma(t)$ denotes the active mode at the time instant $t$. Now we have all the ingredients to formulate the problem at hand as follows:

**Maintenance oriented-fault tolerant control (MOFTC) problem.** Given the plant (1), at each time instant $t$ compute a control input that, on the basis of the current degradation status of the actuators $\rho(t)$, is able to asymptotically stabilize the plant (1) while satisfying constraints (3) and preserving actuators reliability as much as possible regardless of any disturbance occurrence.

Remark 1. Faulty model (4) is used in particular to model stuck faults, see, for example, Reference 18. In a more general case, the switching rule (4) can be seen as a workaround to approximate by quantization a continuous (and possibly nonlinear) loss of effectiveness fault generated by increasing the degradation level of the actuators. Better approximations could be achieved by using additional quantization levels, at the cost of an increase in the number of subsystem configurations $(A, B_j)$.

3 | **THE FAULT TOLERANT CONTROL SCHEME FOR PREDICTIVE MAINTENANCE OPERATIONS (PM-FTC)**

The proposed solution for MOFTC problem is based on set-theoretic ideas (see Reference 19 for a comprehensive tutorial) tailored to a control framework in order to deal with faulty occurrence. The main design step is at offline determining for each mode $j$ of the switching system (6) a family of one-step ahead controllable sets. Then, during the online operations, whenever the prognostic module detects a loss of effectiveness in the actuators and the related $j$th mode is selected, the model-based controller exploits the related sets family to compute a command input via the receding horizon strategy developed in Reference 20. While the discrimination task among the given $I := 3^m - \nu$ systems mode is quite easy, because the degradation signals $\rho_i$ is assumed to be perfectly known, the control reconfiguration task is quite critical as it involves a switching $(j \rightarrow h, j \neq h)$ in the model exploited by the control law and as a consequence the closed-loop stability and constraints fulfillment could be invalidated if proper operations are not correctly performed.

To deal with such an issue, we proposed the control architecture presented in Figure 1 and composed by two modules: (1) a prognostic module where $m$ detector units are in charge of monitoring actuators health and a switching logic that defines the current system mode $(\sigma(\cdot))$ on the basis of actuators status and the operating scenario $(s(\cdot))$ for the controller, respectively; (2) a reconfigurable control unit that determines a control input $u(t)$ on the basis of the system configuration $\sigma(t)$ and one of the operating status $s(t) \in \{\text{HEALTHY, FAULTY, RECOVERY}\}$ to be clarified in next sections.

3.1 | **Controllable set sequences for switching systems**

The crucial task in the design of the proposed strategy is concerned with the determination of families of one-step ahead controllable sets for each system configuration (6) $j$, that is, $\{ T_k \}_{k=0}^N$, $j = 0, 1, \ldots, I$, with $N \in \mathbb{Z}_+$ denoting the last level for the sequence growth (please refer to Reference 19 for detailed notation).
Such a notion in the present context needs to be generalized to take into account possible safe transitions from healthy to faulty configuration and vice versa. To this end, it is worth observing that at each time instant $t$, the control input $u(t)$ is computed by using the active mode $j = \sigma(t)$ and the related sets family $\{T^i_k\}_{k=0}^N$. In this situation, if a system configuration modification $j \leftarrow h$ occurs, because of faulty/recovery event, the application of this command could produce one-step ahead state evolution $x(t+1)$ not belonging to any element of the sequences $\{T^h_k\}_{k=0}^N$, $j = 0, 1, \ldots, l$. The above stated considerations motivate the determination of controllable set sequences as follows:

$T^i_k := \{x \in \mathbb{R}^n : \exists u \in U, u_i \in \mathcal{U}, \forall i \in A_j : \forall d \in D, \{Ax + Bj u + Bd d\} \in T^j_{k-1}\}, \quad j = 1, \ldots, l. \tag{7}$

$T^0_k := \{x \in \mathbb{R}^n : \exists u \in U : \forall d \in D, \{Ax + B_0 u + B_d d\} \in T^0_{k-1}, \{Ax + B_j u + B_d d\} \in T^j_{N}, j = 1, \ldots, l\}, \tag{8}$

where $U_i := \{u_i \in \mathbb{R} : |u_i| \leq \bar{a}_i\}$, with $0 < \bar{a}_i < u_{\max}$.

It is worth noticing that recursions (8) relate to the computations of the set sequence associated to the healthy condition ($j = 0$) and take into account all the possible fault occurrences in order to guarantee healthy-to-faulty transitions. In other words, starting from a generic state $x \in T^0_k$ and by applying the corresponding computed command input $u(x)$, the requirements in (8) guarantee that the one-step state evolution $x(t+1)$ will belong to $T^0_{k-1}$ or to some of $T^j_{k-1}$ under a fault occurrence: this essentially ensures a healthy-to-faulty transition. In this respect, Figure 2 depicts for better clarification an illustrative scenario of healthy-to-faulty transitions of two systems configurations. There, the state estimate $x$ belongs to $T^0_2$ and the command input $u$ is computed on the basis of the healthy model configuration ($\sigma = 0$). When $u$ is applied to (1), two situations could occur:

(i) **No damages** (Figure 2 continuous path): The model configuration of (1) is not modified so that the one-step state evolution $x(t+1)$ is driven to $T^0_1$ thanks to the set-membership requirement:

$\{Ax + B_0 u + B_d d\} \in T^0_{k-1}$

of (8).

(ii) **Fault 1 occurrence** (Figure 2 red-dashed path): The plant (1) assumes the model configuration (6) with $j = 1$. Then, $x(t+1) \in T^1_1$ because of the requirement in (8)

$\{Ax + B_1 u + B_d d\} \in T^1_{k-1}$. 
On the other hand, faulty-to-healthy transition will take place in a safe way thanks to following set inclusions

\[ T_k^0 \subset T_N^j, \quad \forall j = 1, \ldots, l, \quad \text{and} \quad \forall k = 0, \ldots, N. \] (9)

that hold true by construction thanks to the structure of both recursions (8) and (7). Then, when a recovery from the \( j \)th fault configuration occurs, the computed command \( u(t) \) will drive the state evolution \( x(t) \) toward \( T_0^j \). Then, (9) guarantees that, in a finite time \( \tilde{t}, \tilde{t} \geq 1, x(t + \tilde{t}) \) will belong to \( T_N^j \cap T_k^0 \) for some \( k \geq 0 \) so the controller can be reconfigured to compute command input by exploiting the nominal sets family \( \{ T_0^k \}_{k=0}^N \). Furthermore, it is worth noticing that in recursions (7) the damaged actuators \( u_i, i \in A_j \) are further constrained to belong to the restricted set \( U_j \) in order to guarantee a minimum and fixed remaining useful time\(^{21} \) within the \( j \)th system configuration. The following proposition specifies this aspect in a more formal way.

**Proposition 1.** Let the degradation laws (2) be given within the maintenance phase, that is, \( \rho_i(t') \geq \rho_{\text{lim},i} \) for some \( t' > 0 \). Then, if the control input \( u_i(t) \) for the \( i \)th actuator is maintained within \( U_i \) for \( t \geq t' \), the minimum guaranteed remaining lifetime before a total breakdown is given by

\[ \text{MGRUL}_i := \frac{(\rho_{\text{max},i} - \rho_{\text{lim},i})}{\alpha_i \bar{u}_i}. \] (10)

**Proof.** The proof is trivial and consists of determining the time instant \( k' \) needed to reach \( \rho_{\text{max},i} \) starting from \( \rho_{\text{lim},i} \) when applying a constant input \( u_i(t) \equiv \bar{u}_i \) (maximum magnitude), then

\[ \rho_i(k') = \rho_{\text{lim},i} + \sum_{h=0}^{k'-1} \alpha_i \bar{u}_i = \rho_{\text{lim},i} + k' \alpha_i \bar{u}_i. \]

From the latter equation, by imposing that \( \rho_i(k') = \rho_{\text{max},i} \), one obtains

\[ k' = \frac{(\rho_{\text{max},i} - \rho_{\text{lim},i})}{\alpha_i \bar{u}_i}. \]

Then, the proposition statement directly follows. \( \blacksquare \)

Finally, the determination to be performed offline of the terminal regions \( T_0^j, j = 0, 1, \ldots, l \), with related control gains \( K_j, j = 0, 1, \ldots, l \), are here introduced by considering the system dynamics (6). It can be performed by exploiting switching stability arguments and technicalities proposed in References 22 and 23.
Proposition 2. Given the switching system (6), there exist pairs \((T^j_0, K_j)\), \(j = 0, 1, \ldots, l\), with \(T^j_0 \neq \emptyset\) robustly invariant sets with associated \(K_j\) stabilizing state feedback control laws for each model configuration of (6) complying with the input constraints (3), if the following set-valued inclusions are satisfied:

\[
(A + B_j K_j) T^j_0 + B_d D \subseteq T^j_0, \quad j = 1, \ldots, l, \tag{11}
\]

\[
K_j T^j_0 \subseteq U, \quad j = 1, \ldots, l, \tag{12}
\]

and

\[
(A + B_0 K_0) T^0_0 + B_d D \subseteq T^0_0, \tag{13}
\]

\[
T^0_0 \subseteq T^j_0, \quad j = 1, \ldots, l, \tag{14}
\]

\[
K_j T^0_0 \subseteq U, \quad j = 1, \ldots, l. \tag{15}
\]

Proof. See the Appendix. □

3.2 Prognostic module

The logic underlying the prognostic module depicted in Figure 1 is here presented. A bank of \(m\) monitoring devices provides the degradation signals of the actuators to a switching logic that exploits such information to perform the task of determining the active mode \(\sigma(t)\) of the system (6) and establish the operating status \(s(t)\) for the control unit. In this way, at the control level, a family of controllable set sequences \(\{T^j_k\}_{k=0}^N\) can be properly selected in order to compute an admissible control action. In particular the switching signal \(\sigma(t)\) is given by

\[
\sigma(t) = j, \text{ if } A_j \text{ collects damaged actuators only} \tag{16}
\]

and the intrinsic switching logic follows the semantic of the state automata depicted in Figure 3 that is hereinafter outlined:

- Whenever one or more actuators are damaged, that is, \(\rho_i(t) > \rho_{\text{lim}, i}\) for some \(i \in \{1, m\}\), a transition from healthy status to faulty status takes place. In this scenario, according to Proposition 1 a complete breakdown of some actuators can occur after at least MGRUL\(_i\) time instants. Then, any repairing procedure should be accomplished within this time interval.

- If no actuators are damaged, that is, \(\rho_i(t) \leq \rho_{\text{lim}, i}\) for all \(i \in \{1, m\}\) and if the current state \(x(t)\) belongs to some set of the family \(\{T^j_k\}_{k=0}^N\), then a transition from faulty to healthy status can be triggered. This rule can be fully understood in view of the fact that in healthy mode, the control unit determines the control actions by means of the nominal sets family \(\{T^0_k\}_{k=0}^N\). Anyway, since in the faulty status the control unit is instructed to maintain the state \(x(t)\) into the controllable set sequence \(\{T^j_k\}_{k=0}^N\), there is not guarantee that the current state set-membership belong to any set of \(\{T^0_k\}_{k=0}^N\) when the involved actuators belonging to \(A_j\) are repaired and their degradation signals are resumed to default values. So, in this scenario the switching logic reconfigures the control unit in order to work in the recovery status until condition

\[
x(t) \in T^N_0 \tag{17}
\]

becomes true.

- A transition to healthy status is triggered from the recovery status after positive checking of condition (17). Nevertheless, a transition to faulty status is still possible if a new actuator is damaged.
3.3 | MPC based control unit design

The operations of the control unit depicted in Figure 1 are here described in the following algorithm that takes as input the pair \((\sigma(t), s(t))\) conveyed by the prognostic module and implements the receding horizon control approach based on the arguments presented in Section 3.1.

Please notice that the running costs used in the previous algorithm are chosen according to the following prescriptions:

- \(J_0(u) := \|u\|_{Q_0}^2\) is adopted to safeguard the actuators health while steering the state into the successor set \(T_{k(t)}^0\).
- \(J_j^i(u) := \|u\|_{Q_i}^2\), \(i \in A_j\), is used in order to postpone as much as possible further damages in healthy actuators not belonging in \(A_j\) while steering the state into the successor set \(T_{k(t)}^j\). Observe that, according to Proposition 1, constraints (21) ensure a certain amount of time MGRUL before a complete failure of at least one damaged actuators in \(A_j\).
- \(J^k(x, u) := \|Ax(t) + Bu\|_{Q_k}^2\), in order to speed up the steering process of \(x(t)\) into \(T_N^0\) so that the healthy status can be activated.

Remark 2. The degradation process (2) is the same considered in Reference 16 and evolves whenever the control input is nonzero in a way that depends on its amplitude only. However, more sophisticated degradation laws can be considered with slight modifications of the solution control scheme. In this respect, it is important to remark that the proposed control strategy does not strictly depend on this specific degradation model but it can be adapted to generic monotonically increasing degradation signal.

3.4 | Properties

The main properties of the PM-AFTC algorithm are summarized in the following proposition.

**Proposition 3.** Let \(\{T_k^j\}_{k=0}^N\) be a family of non-empty set sequences and \(x(0) \in \bigcup_{j=0}^l T_N^j\). Then, the PM-AFTC scheme is able to solve MOFTC problem by guaranteeing closed-loop asymptotic stability and constraints fulfillment.
**Algorithm 1. Control unit**

INPUT: $\sigma(t)$, $s(t)$  
OUTPUT: $u(t)$

1: goto label $s(t)$  
2: HEALTHY:  
3: if $k(t) = 0$ then  
4: \hspace{1em} $u(t) \leftarrow K_0 x(t)$  
5: else  
6: \hspace{1em} $u(t) \leftarrow \text{arg min } J_0(\mu)$  
7: \hspace{2em} s.t. $Ax(t) + B_0 u \in T^{0}_{k(t)-1}$, $u \in U$;  
8: end if  
9: goto 22  
10: FAULTY:  
11: if $k(t) = 0$ then  
12: \hspace{1em} $u(t) \leftarrow K_\sigma x(t)$  
13: else  
14: \hspace{2em} $u(t) \leftarrow \text{arg min } J^F(x(t), u)$  
15: \hspace{2em} s.t. $Ax(t) + B_\sigma u \in T^{\sigma(t)}_{k(t)-1}$, $u \in U, u_i \in U_i, i \in A_{\sigma(t)}$;  
16: end if  
17: goto 22  
18: RECOVERY:  
19: if $i(t) = 0$ then  
20: \hspace{1em} $u(t) \leftarrow K_{\sigma(t)} x(t)$  
21: else  
22: \hspace{2em} $u(t) \leftarrow \text{arg min } J^R(x(t), u)$  
23: \hspace{2em} s.t. $Ax(t) + B u \in T^{\sigma(t)}_{k(t)-1}$, $u \in U$;  
24: end if  
25: goto 22  
26: apply $u(t)$ to the plant (1);  
27: set $t \leftarrow t + 1$;  
28: goto 1

**Proof.** The proof is aimed at showing that while the state $x(t)$ is into $x(0) \in \bigcup_{j=0}^{J} T^j_N$, a solution at time $t + 1$ is always ensured to exist through the resolution of one of the optimization problems in steps 6, 13, and 20 of Algorithm 1. To this end, it is worth to discriminate four possible scenarios: (i) if at the generic instant $t$, $s(t) = \text{healthy}$ and the state $x(t) \in T^{0}_{k(t)}$, an input vector $u$ complying with constraints (3) ensuring $Ax(t) + Bu$ belongs to $T^{0}_{k(t)-1}$ can be selected by solving the optimization program in step 6 of Algorithm 1, that in this case is feasible by construction of (8); (ii) if a $j$th configuration fault occurs, $s(t)$ is modified to $\text{faulty}$ and by construction of the sequence $T^j_k$ the state evolution $Ax(t) + Bu$ will belong to $T^j_{k(t)-1}$ thanks to the input computed via step 13 of Algorithm 1; (iii) if $s(t) = \text{faulty}$ and $x(t) \in T^{\sigma(t)}_{k(t)}$, recursions (7) guarantee optimization problem in step 20 of Algorithm 1 leads to the computation of input $u$ such that $Ax(t) + B_\sigma u \in T^{\sigma(t)}_{k(t)-1}$;
(iv) A further possible situation is represented by the case where \( s(t) = \text{recovery}, \sigma(t) = 0 \) and \( x(t) \notin \mathcal{T}^0_N \). Even in this case recursions (7) guarantee the existence of a command vector \( u \) such that \( Ax(t) + Bu \in \mathcal{T}_{k(t) - 1}^j \) or to \( \mathcal{T}^0_N \).

4 | ILLUSTRATIVE EXAMPLE

In order to assess the proposed approach, we consider a discrete-time unstable system having the same structure (1) and identified by the following matrices

\[
A = \begin{bmatrix} 1.0203 & 0.0081 \\ 0.0162 & 1.0101 \end{bmatrix}, \quad B_d = \begin{bmatrix} 1 \\ 1 \end{bmatrix},
\]

where

\[
B(\rho) = \begin{cases} B_0 = \begin{bmatrix} 0.0008 \\ 0.2010 \end{bmatrix} & \text{if } \rho \leq \rho_{\text{lim}}, \\
B_1 = \gamma B_0 & \text{if } \rho > \rho_{\text{lim}}, \end{cases}
\]

with the sampling time is \( T_s = 0.02 \text{s} \). The degradation process involving the unique actuator is modeled as in (2) with \( \alpha = 0.019 \) and \( \rho_{\text{lim}} = 0.7 \). It is assumed that the loss of actuator effectiveness entails a 90% reduction of the gain, that is, \( \gamma = 0.1 \).

Within the simulation, the goal is to steer the state to the origin from the given initial condition \( x(0) = [-1.3, 4.2]^T, \rho(0) = 0.48, \) under the following constraints: \( |u(t)| \leq 5, |d(t)| \leq 0.05, \rho(\tau_k) \leq \rho_{\text{max}} = 1 \).

The PM-AFTC algorithm has been initialized according to the prescriptions of Section 3, in particular:

- The state-feedback laws and related terminal regions have been determined via the BMI optimization procedure included in the proof of Proposition 2 presented in the Appendix, in particular we obtained \( K_0 = [-191.15, -38.22]^T \) and \( K_1 = [-9.86, -1.19]^T \).
- Two families of one-step state ahead controllable sets, say it \( \mathcal{T}^0_k \) \( \{ 60 \} \) and \( \mathcal{T}^1_k \) \( \{ 118 \} \), have been computed for the healthy and faulty configuration, respectively, with \( \bar{u}_1 = 1 \), that ensures a minimum remaining lifetime MGRL\(_1\) = 0.38 s.

All the simulations have been carried on an Apple MacBook Pro M1 8-core with Matlab using the Gurobi optimization solver.

4.1 | Case study 1

In order to emphasize the benefits of the proposed approach, a comparison has been performed with similar RHC schemes not owning fault-tolerant capabilities and designed in the following way:

- MPC\(_1\): This is a predictive controller that does not consider neither the degradation dynamics nor any fault occurrence. It consists on the control unit designed in Section 3 and online operated with constant switching signals \( \sigma(t) \equiv 0 \) and \( s(t) = \text{healthy} \). The solved control problem coincides with (19) with running cost \( J^R(x, \mu) \).
- MPC\(_2\): In this case, the predictive controller takes into account degradation dynamics in the cost only but it is not able to explicitly deal with fault occurrences. It consists on the control unit designed in Section 3 and online operated with constant switching signals \( \sigma(t) \equiv 0 \) and \( s(t) = \text{healthy} \). The solved control problem coincides with (19) with running cost \( J^R(\mu) \).

Simulation results are depicted through Figures 4–6. From these figures, it is evident that the considered counterpart schemes are not able to accomplish the control goals. In fact the MPC\(_1\) presents an aggressive behavior (Figure 5 (top)). Then, the actuator degradation growth reaches the \( \rho_{\text{lim}} \) value in a very short time (Figure 5 (middle)) and there is no way
FIGURE 4  State evolutions

FIGURE 5  Behavior of MPC$_1$ and MPC$_2$ schemes: Computed input (top), degradation signal (middle), set-membership signals (down)
**Figure 6** Behavior of PM-AFTC scheme: (A) Computed input, (B) degradation signal, (C) set-membership signal, (D) controller status

**Figure 7** Comparison with Reference 16: Domain of attraction
for the controller to keep the state inside its domain of attraction (DoA) $T^60_0$, as depicted in Figure 4, even if the actuator were repaired because the feasibility of the scheme is irreversibly lost. As a consequence, the simulation is stopped.

The MPC$_2$ controller behaves in a similar way (see Figures 4 and 5). Anyway, in this case, the degradation growth is significantly delayed thanks to the modified running cost. On the contrary, a different scenario arises when the proposed PM-AFTC scheme is adopted. In particular, the control goals are successfully achieved and the state is steered toward the origin (Figure 4) despite of fault events occurring at time instants $t = 0.68$ s, $t = 2.21$ s. Moreover, from Figure 6 it is possible to observe that after the first fault occurrence (Figure 6B), the state is steered along the sets of the family $\{ T^1_k \}_{k=0}^{118}$, successor to $T^5_1$ (Figure 6C). The same controllable set sequence is used even after the repair/replace occurrence at time $t = 0.99$[s] (Figure 6B) because the state $x(0.99)$ does not belong to $T^0_60$ (Figure 6C). Then, few time instants are spent into the recovery status (Figure 6D) in order to steer $x(t)$ into $T^0_60$ so that the healthy status is activated at time instant $t = 1.04$. Then, a second fault occurs after 1.14 seconds and even in this case the switch to the faulty status is performed. Also in this case, after the actuator reparation, the healthy status is instantly activated because the state $x(2.64)$ is already contained into $T^0_60$.

### 4.2 Case study 2

A second comparison has been performed with the RHC scheme of Vieira et al.\textsuperscript{16} that explicitly takes into account in the online optimization problem the degradation on the input matrix $B$ in Equation (5) by means of mixed-integer slack variables. In Figure 7, the DoA of such a scheme is compared, for different values of the prediction horizon $N$, with our proposed scheme obtained by considering the sets union depicted in Figure 4. The significantly “lower size” of the DoA of the contrasted method is mainly due to the presence of a terminal constraints imposing that the final predicted state is equal to 0. A further reason is that this approach is not able to manage a recovery phase of the broken actuator.

The comparison analysis has been carried out also in terms of control performance by simulating our approach and the Vieira et al.\textsuperscript{16} method, $N = 20$ case, starting from an admissible initial condition $x(0) = [-0.26, 2.89]^T$, $\rho(0) = 0.2$. In this respect, the simulation results can be observed in Figure 8. Clearly, the method of Vieira et al.\textsuperscript{16} outperforms our method as it is able to steer the state to 0 in a shorter time without exceeding the fault threshold $\rho_{lim,i}$. Anyway, such performance require a significant computational burden (see Table 1) that makes this method impractical in many applications. On the
contrary, the PM-AFTC, although behaving in a worse way, needs a very low amount of CPU time to perform the online computations.

5 | CONCLUSIONS

In this work, a receding-horizon-based control strategy has been presented for dealing with loss of actuators effectiveness. To this end, the degradation effect of actuators has been assumed to be proportional to the control effort. Within this context, the loss of effectiveness occurs when the deterioration level overcomes a threshold placed between nominal working range and complete actuator breakdown. A fault-tolerant control strategy with reconfiguration capabilities has been proposed for linear discrete-time systems subject to input constraints. The key idea was at exploiting set-invariance notions to design a control architecture to properly manage actuator fault occurrences. The numerical results are encouraging in terms of efficiently preventing occurrences of critical scenarios. Future works will be focused on the application of the proposed strategy to a practical case study in Oil & Gas domain and autonomous surface/underwater vehicles.

ACKNOWLEDGMENTS

This research is based upon work partially supported by the industrial research project PON 01-01517, entitled “PIM (Pipeline Integrity Management) 4.0,” granted by the Italian Ministry of Economic Development (MISE), Fondo per la Crescita Sostenibile – Sportello “Fabbrica Intelligente,” PON I&C 2014-2020. Open Access Funding provided by Universita della Calabria within the CRUI-CARE Agreement. [Correction added on 18 May 2022, after first online publication: CRUI funding statement has been added.]

CONFLICT OF INTEREST

All authors declare that they have no conflicts of interest.

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are available from the corresponding author upon reasonable request.

ENDNOTE

*http://www.gurobi.com

ORCID

Francesco Tedesco https://orcid.org/0000-0001-5876-3711
Mehdi Forouzanfar https://orcid.org/0000-0002-6440-5731
Domenico Famularo https://orcid.org/0000-0003-0185-2611

REFERENCES

1. Galar D, Sandborn P, Kumar U. Maintenance Costs and Life Cycle Cost Analysis. CRC Press; 2017.
2. Zhang Y, Jiang J. Bibliographical review on reconfigurable fault-tolerant control systems. Annu Rev Control. 2008;32:229-252.
3. Bougacha O, Varnier C, Zerhouni N. A review of post-prognostics decision-making in prognostics and health management. Int J Prognost Health Manag. 2020;11(15):31.
4. Khelassi A, Weber P, Theilliol D. Reconfigurable control design for over-actuated systems based on reliability indicators. Proceedings of the 2010 Conference on Control and Fault-Tolerant Systems (SysTol); 2010:365-370.
5. Bougacha O, Varnier C, Zerhouni N. Impact of decision horizon on post-prognostics maintenance and missions scheduling: a railways case study. Int J Rail Transp. 2021. doi:10.1080/23248378.2021.1940329
6. Zagorowska M, Wu O, Ottewill JR, Reble M, Thornhill NF. A survey of models of degradation for control applications. Annu Rev Control. 2020;50:150-173.
APPENDIX. PROOF OF PROPOSITION 1

We will suppose that the structure of the terminal set is

\[ T_0^j = \left\{ x \in \mathbb{R}^n \mid x^T P_0^j x \leq 1 \right\} \tag{A1} \]

and we want to derive a set of matrix inequalities under which the state invariance condition

\[ (A + B_d K_j) T_0^j + B_d D \subset T_0^j, \quad j = 0, 1, \ldots, l, \tag{A2} \]

the sets inclusion

\[ T_0^0 \subset T_0^j, \quad j = 1, \ldots, l \tag{A3} \]
and input constraints condition

\[ K_j T_{0j}^j \subset U^r, \quad j = 0, 1, \ldots, l, \]  

(A4)

are verified. The condition (A2) translates into the following implication

\[
\begin{cases}
  x^T P_0^j x \leq 1 \\
  \tilde{d}^T d \leq \tilde{d}
\end{cases} \Rightarrow (x^+)^T P_0^j x^+ \leq 1,
\]

(A5)

where

\[ x^+ = (A + B_j K_j)x + B_d d. \]

In terms of the vector \([x^T \quad d^T]^T\), the right-hand side of (A5) can be rewritten as

\[
1 - \begin{bmatrix} x^T & d^T \end{bmatrix} \begin{bmatrix} (A + B_j K_j)^T \\ B_d^T \end{bmatrix} \begin{bmatrix} P_0^j \\ B_d^T \end{bmatrix} \begin{bmatrix} (A + B_j K_j)^T \\ B_d^T \end{bmatrix}^T \begin{bmatrix} x \\ d \end{bmatrix} \geq 0.
\]

(A6)

The same can be done for the left hand term inequalities of (A5)

\[
1 - \begin{bmatrix} x^T \quad d^T \end{bmatrix} \begin{bmatrix} I_n & 0 \\ 0 & I_d \end{bmatrix} \begin{bmatrix} P_0^j \\ 0 \end{bmatrix} \begin{bmatrix} I_n & 0 \\ 0 & I_d \end{bmatrix}^T \begin{bmatrix} x \\ d \end{bmatrix} \geq 0.
\]

(A7)

\[
\tilde{d} - \begin{bmatrix} x^T \\ d^T \end{bmatrix} \begin{bmatrix} 0 & 0 \\ I_d & I_d \end{bmatrix} \begin{bmatrix} x \\ d \end{bmatrix} \geq 0.
\]

(A8)

Thanking to S-procedure arguments, the validity of (A6)–(A8) reduces to the satisfaction of

\[
1 - \tau_1 - \tau_2 \tilde{d} + \begin{bmatrix} x^T \\ d^T \end{bmatrix} \begin{bmatrix} I_n & 0 \\ 0 & I_d \end{bmatrix} \begin{bmatrix} P_0^j \\ 0 \end{bmatrix} \begin{bmatrix} I_n & 0 \\ 0 & I_d \end{bmatrix} \begin{bmatrix} x \\ d \end{bmatrix} + \tau_2 \begin{bmatrix} I_d \\ I_d \end{bmatrix} \begin{bmatrix} 0 \\ 0 \end{bmatrix} \geq 0.
\]

which turns to be satisfied if the following LMIs hold true

\[
\begin{bmatrix}
  \tau_1 P_0^j & 0 & (A + B_j K_j)^T \\
  0 & \tau_2 I_d & B_d^T \\
  A + B_j K_j & B_d & P_0^{j-1}
\end{bmatrix} \geq 0.
\]

(A9)

Finally, the inequality (A9) can be turn into

\[
\begin{bmatrix}
  \tau_1 P_0^j & 0 & (A + B_j K_j)^T P_0^j \\
  0 & \tau_2 I_d & B_d^T P_0^j \\
  P_0^j (A + B_j K_j) & P_0^j B_d & P_0^j
\end{bmatrix} \geq 0
\]

via standard congruence transformation.
The sets inclusion condition (A3) can be managed quite easily due to the ellipsoidal structure of \( \mathcal{T}_0, j = 0, \ldots, l \). By considering the related shaping matrices \( P_0^j \) we have

\[
P_0^0 \succeq P_0^j, \quad j = 1, \ldots, l.
\] (A10)

Let us now consider the input constraints inequality (A4) which is equivalent to the following implication

\[
x^T P_0^j x \leq 1 \Rightarrow |K_j^j x| \leq u_{\text{max}} \Rightarrow x^T (K_j^j)^T K_j^j x \leq u_{\text{max}}^2, \quad j = 1, \ldots, l, \quad i = 1, \ldots, m,
\] (A11)

where \( K_j^j \) denotes the \( j \)th row of \( K_j \) and, via S-procedure arguments, we have

\[
u_{\text{max}}^2 - \tau_{2+i} + x^T \left( \tau_{2+i} P_0^j - K_j^j K_j^j \right) x \geq 0, \quad j = 1, \ldots, l, \quad i = 1, \ldots, m
\] (A12)

that are satisfied if

\[
u_{\text{max}}^2 - \tau_{2+i} \geq 0, \quad i = 1, \ldots, m
\] (A13)

and

\[
\begin{bmatrix}
\tau_{2+i} P_0^j & (K_j^j)^T \\
K_j^j & I
\end{bmatrix} \succeq 0, \quad j = 1, \ldots, l, \quad i = 1, \ldots, m.
\] (A14)

Finally, by choosing \( \tau_{2+i} = u_{\text{max}}^2, j = 1, \ldots, l, i = 1, \ldots, m \) in (A13), (A14) becomes

\[
\begin{bmatrix}
u_{\text{max}}^2 P_0^j & K_j^j \\
K_j^j & I
\end{bmatrix} \succeq 0, \quad j = 1, \ldots, l, \quad i = 1, \ldots, m.
\] (A15)