VERSITA

*Int. J. Appl. Math. Comput. Sci., 2012, Vol. 22, No. 1, 211–223*
DOI: 10.2478/v10006-012-0016-7

amcs

# ROBUST MULTISENSOR FAULT TOLERANT MODEL–FOLLOWING MPC DESIGN FOR CONSTRAINED SYSTEMS

ALAIN YETENDJE, MARIA M. SERON, JOSÉ A. DE DONÁ

Centre for Complex Dynamic Systems and Control (CDSC)
School of Electrical Engineering and Computer Science
University of Newcastle, Callaghan, NSW 2308, Australia
e-mail: alain.yetendjelemegni@uon.edu.au

In this paper, a robust fault-tolerant control strategy for constrained multisensor linear systems, subject to sensor faults and in the presence of bounded state and output disturbances, is proposed. The scheme verifies that, for each sensors–estimator combination, suitable residual variables lie inside pre-computed sets and selects a more appropriate combination based on a chosen criterion. An active fault tolerant output feedback controller yields an MPC-based control law and, by means of the notion of a "tube" of trajectories, we ensure robust closed-loop exponential stability and good performance in the fault-free case and under the occurrence of abrupt sensor faults.

**Keywords:** fault tolerant control, constraints, robustness, invariant sets.

## 1. Introduction

Almost all real world control systems have an associated set of constraints. For example, inputs always have minimum and maximum values and states are usually required to lie within certain ranges (Goodwin *et al*., 2005). A correct controller design will ensure that the constraints are satisfied. However, even with such a design, when some plant components such as sensors fail, the constraints could be violated. Therefore, it is important to take into account constraints in fault-tolerant control design.

Model Predictive Control (MPC) is one of the most successful approaches for designing non-linear controllers for linear systems with constraints. The idea of developing Fault Tolerant Control (FTC) approaches based on MPC control has been discussed in the last few years within the research community. In the work of Maciejowski (1999), the foundations of a possible theory were discussed and simulations on an aircraft system showed that MPC offers the possibility to achieve fault tolerance by reconfiguring the controller in response to a fault.

Further on, it was shown (Maciejowski, 2002) that when knowledge of the fault is available one can increase fault tolerance by modifying parameters of the optimisation problem which is solved at each sampling instant in MPC. Faults that affect the internal model or system constraints can be incorporated into an MPC controller in a straightforward way. When a fault occurs in one element of the system (e.g., actuators) and makes the control objective unattainable, it is possible to discard that control item by removing the corresponding output from the optimisation cost function (Maciejowski, 2002). Other possibilities consist of degrading the control objective by changing the constraints in order to represent certain kind of faults, and/or modifying the internal system model used by the MPC controller.

Maciejowski (1999) claims that the inclusion of the knowledge of the fault in an MPC controller relies on the presence of an efficient and dependable FDI unit, on the capacity of updating automatically the model of the system, and on the control objectives defined for the MPC controller which can be left unchanged after the fault. Patwardhan *et al*. (2006) developed a model predictive and fault tolerant control scheme using an innovative form of state space model derived purely from data using system identification techniques. An FTC approach using fuzzy techniques for FDI and MPC for fault accommodation is presented by Mendonça *et al*. (2006). In the work of Mhaskar (2006), a fault tolerant scheme using the explicit characterisation of the stability region, together with the constraint handling capabilities and optimality properties of MPC, is proposed for nonlinear systems subject to uncertainty, constraints, and faults in the control actu-

ators. Pranatyasto and Qin (2001) considered a principal component-based FTC system controlling a simulated fluid catalytic cracking unit using MPC. Sheng-Qi *et al*. (2008) proposed an active fault tolerant control scheme based on MPC and FDI using a two-stage Kalman filtering algorithm.

Ocampo-Martinez and Puig (2008) embedded an active fault-tolerant scheme based on MPC within the hybrid system framework. A hybrid model of the system to be controlled including faulty modes is proposed, and then a fault-tolerant hybrid MPC controller is designed. In the work of Mhaskar *et al*. (2006), the problem of achieving fault tolerance in the presence of uncertainty was addressed, where a robust hybrid predictive controller was used to characterise the stability region under each control configuration.

Most of these approaches tackle the problem of FDI and reconfiguration separately and are usually carried out on simulation examples, experimental systems, or real applications, but very few of them provide analytical proofs that guarantee fault tolerance for constrained systems.

In this paper we consider a sensor FDI strategy which employs a bank of sensors–estimator combinations and verifies that, for each of these combinations, the updated estimation tracking errors lie inside pre-computed "healthy" sets. Those combinations for which the latter set-containment property holds are considered within a chosen selection criterion (e.g., switching of sensors-estimator combinations (Seron *et al*., 2008; Yetendje *et al*., 2010), sensors–estimation fusion (De Doná *et al*., 2009; Yetendje *et al*., 2011)) to be used by the controller.

We propose an active fault-tolerant control scheme based on the output feedback problem for constrained linear discrete-time systems subject to state and measurement disturbances (Mayne *et al*., 2006). The output feedback controller yields a "tube", whose center is generated by using conventional MPC with tighter constraints on the nominal system, and whose size is restricted by using a local feedback that attempts to steer all trajectories of the uncertain system to the central trajectory (Rawlings and Mayne, 2009).

Proofs of fault tolerance of the resulting closed-loop system and robust exponential stability of a robust invariant set are given under a set of conditions on the system parameters (disturbance bounds, reference offsets and bounds, etc.) in the fault-free case and under the occurrence of sensor faults. We consider both sensor bias and the loss of effectiveness (including total outage). In that sense, we extend the approach initiated by the authors in the preliminary conference paper (Yetendje *et al*., 2010) to consider the loss of effectiveness by an *unknown amount* and the likely case of *sensor bias*, and we include *integral action* in the stabilising tube MPC controller.

The remainder of the paper proceeds as follows. Section 2 outlines the proposed FTC scheme, together with a description of the plant, as well as a formulation of the tracking objective. In Section 3 we describe the measurement system and detail the sensor fault model. Section 4 shows the estimator design, followed by a description of the estimate reconfiguration in Section 5. In Section 6 we introduce the robust tube-MPC controller and tracking errors. In Section 7 we derive invariant sets for the closed-loop system dynamics. Section 8 describes the nominal optimal MPC design for the reference system. In Section 9 we describe the fault detection and identification principle and establish the stability and fault tolerance properties of the overall scheme. Finally, Section 10 illustrates with an example the effectiveness of the proposed fault tolerant constrained control scheme.

## 2. FTC scheme structure, plant and tracking objective

**2.1. General FTC scheme structure.** Figure 1 depicts the proposed robust fault tolerant multisensor MPC scheme, whose elements are described in the subsequent sections.

**2.2. Plant description and tracking objective.** Consider the discrete-time linear time-invariant plant

$$x^+ = Ax + Bu + Ew, \tag{1a}$$

$$y^* = C^* x, \tag{1b}$$

where $x \in \mathbb{R}^n$ is the system state, $u \in \mathbb{R}^m$ is the control input, $x^+ \in \mathbb{R}^n$ is the successor state, $w \in \mathbb{R}^r$ is an unknown but bounded state disturbance and $y^* \in \mathbb{R}^q$ is a system performance output[1] not affected by faults (typically, measurements that the system cannot afford to lose without affecting detectability). $A \in \mathbb{R}^{n\times n}$, $B \in \mathbb{R}^{n\times m}$, $E \in \mathbb{R}^{n\times r}$, $C^* \in \mathbb{R}^{q\times n}$ are constant matrices, and the pair $(A, B)$ is assumed to be controllable. We assume that $w \in \mathbb{W} \subset \mathbb{R}^r$, where $\mathbb{W}$ is a known C-set[2].

The control objective is for the performance output $y^*$ to track a setpoint $y_s = C^* x_s$ where $x_s$ satisfies

$$x_s = Ax_s + Bu_s \tag{2}$$

for some vector $u_s$ and such that the controlled plant (1) fullfils hard constraints $x - x_s \in \mathbb{X}$, $u - u_s \in \mathbb{U}$, where $\mathbb{X} \subset \mathbb{R}^n$ is a closed set that contains the origin in its interior and $\mathbb{U} \subset \mathbb{R}^m$ is a compact set that contains the origin in its interior.

[1] We use "performance output" to distinguish it from the measured outputs defined further in Section 3. This gives us more design freedom in the sense that one may be measuring particular combinations of states but require performance properties (e.g., tracking) for some other combination of states.

[2] A C-set is a compact, convex set that contains the origin in its (non-empty) interior.

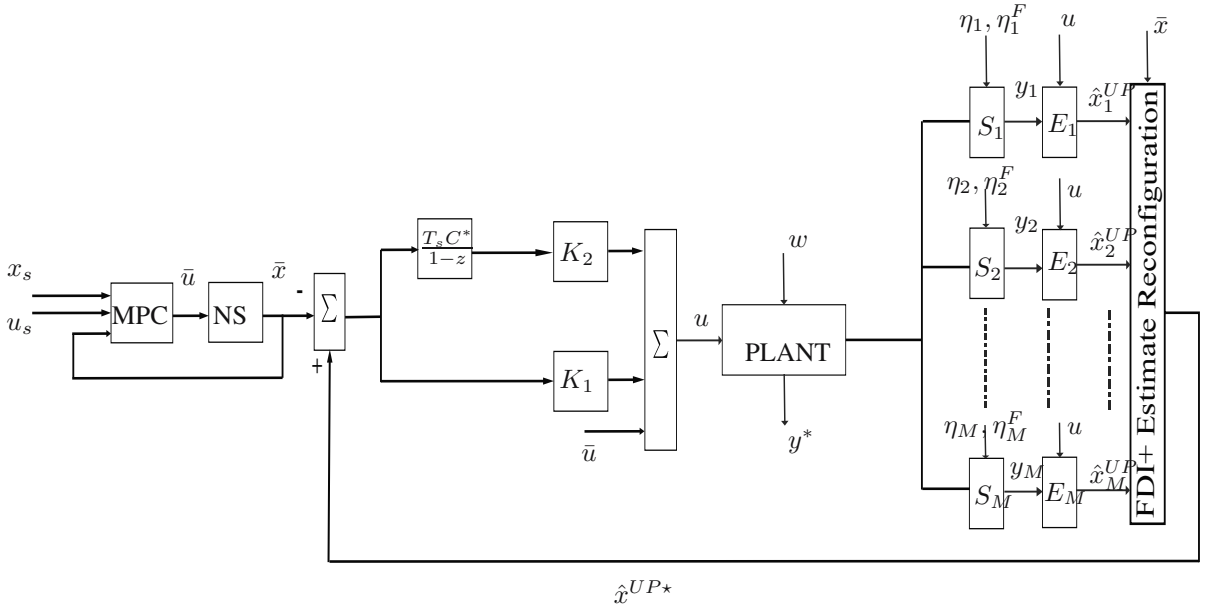



Fig. 1. FTC scheme (NS: Nominal System (17)).

## 3. Measurement system and sensor fault model

We consider a bank of output equations which, when all sensors are healthy, combine several sensor measurements as follows:

$$y_i = C_i x + \eta_i$$

for $i = 1, \ldots, M$, where $y_i \in \mathbb{R}^{p_i}$ is the measured output of the $i$-th group of sensors $S_i$ (see Fig. 1), $\eta_i \in \mathbb{R}^{p_i}$ is an unknown but bounded measurement noise, $C_i \in \mathbb{R}^{p_i \times n}$ are constant matrices. The measurement noise $\eta_i$ is known to the extent that it lies in the C-set $\mathbb{N}_i \subset \mathbb{R}^{p_i}$, that is, $\eta_i \in \mathbb{N}_i$, for $i = 1, \ldots, M$. We observe that the above measurement framework allows the same physical sensor to belong to more than one group, and different groups of sensors can measure the same or different state variables. We require the following assumption.

**Assumption 1.** The pairs $(A, C_i)$ are observable, for $i = 1, \ldots, M$. To model sensor faults, we will expand the above measurement equation to contemplate the sensor loss of effectiveness and bias in the following form:

$$y_i = \Pi_i(C_i x + \eta_i) + (I_{p_i} - \Theta_i)\eta_i^F, \tag{3}$$

where $\eta_i^F \in \mathbb{R}^{p_i}$ are unknown but bounded measurement noises, and $I_{p_i}$ is the $p_i \times p_i$ identity matrix.

In the forecoming analysis, the "under-fault" noise $\eta_i^F$ will be considered to lie in the following compact, convex set:

$$\mathbb{N}_i^F(\bar{\eta}_i) = \{\eta_i \in \mathbb{R}^{p_i} : \quad |\eta_i - \bar{\eta}_i| \leq \tilde{\eta}_i^F\}, \tag{4}$$

where $\bar{\eta}_i$ is a constant vector that models bias in the $i$-th group of sensors and $\tilde{\eta}_i^F$ is a non-negative vector.

The *fault matrices* $\Pi_i \in \mathbb{R}^{p_i \times p_i}$, $\Theta_i \in \mathbb{R}^{p_i \times p_i}$ in (3) and the vector $\bar{\eta}_i \in \mathbb{R}^{p_i}$ in (4) characterise the sensor fault situation, and are described as follows:

- **Fault free situation** (all sensors are healthy):

$$\Pi_i = \Theta_i = I_{p_i}. \tag{5}$$

- **Loss of effectiveness:**

$$\Pi_i = \operatorname{diag}\{\pi_{i1}, \ldots, \pi_{ip_i}\}, \quad \Theta_i = \Pi_i, \quad \bar{\eta}_i = 0, \tag{6}$$

where $\pi_{ij} \in [0, 1]$, for $j = 1, \ldots, p_i$. From (3), $\pi_{ij} < 1$ signifies that the $j$-th sensor of the $i$-th sensor group has lost effectiveness. In particular, $\pi_{ij} = 0$ indicates an outage of the sensor.

- **Sensor bias:**

$$\Pi_i = I_{p_i}, \quad \Theta_i = \operatorname{diag}\{1, \ldots, \overset{j}{\underset{\downarrow}{0}}, \ldots, 1\}, \quad \bar{\eta}_i = [0, \ldots, \bar{\eta}_{ij}, \ldots, 0]' \tag{7}$$

with $\bar{\eta}_{ij} \neq 0$, where the above choices of the combination $(\Pi_i, \Theta_i, \bar{\eta}_i)$ indicate bias in the $j$-th sensor of the $i$-th group.

## 4. Estimators

In accordance with the measurement equations (3), we consider a bank of $M$ estimators $E_1, \ldots, E_M$ (see Fig. 1),

where each estimator is associated with one group of sensors and is designed in order to estimate the states of the system (1). The estimators are described by the following equations, for $i = 1, \ldots, M$:

$$\hat{x}_i^+ = A\hat{x}_i + Bu + L_i[y_i - C_i\hat{x}_i], \tag{8}$$

$$\hat{x}_i^{UP} = \hat{x}_i + G_i[y_i - C_i\hat{x}_i], \tag{9}$$

where $\hat{x}_i \in \mathbb{R}^n$ is the current state estimate and $\hat{x}_i^{UP} \in \mathbb{R}^n$ is the *updated* state estimate. The estimator gains $L_i \in \mathbb{R}^{n\times p_i}$ are such that

$$A_{L_i} \triangleq A - L_iC_i \tag{10}$$

are Schur[3] matrices, for $i = 1, \ldots, M$ (this is always possible by Assumption 3). The update gains $G_i \in \mathbb{R}^{n\times p_i}$ are arbitrary real matrices of appropriate dimensions.[4]

Provided the $i$-th group of sensors is "healthy" (i.e., $\Pi_i = \Theta_i = I_{p_i}$), the estimated states $\hat{x}_i$ satisfy, using (3) and (8),

$$\hat{x}_i^+ = A\hat{x}_i + Bu + L_iC_i\tilde{x}_i + L_i\eta_i \tag{11}$$

with the state estimation error

$$\tilde{x}_i \triangleq x - \hat{x}_i \tag{12}$$

satisfying

$$\tilde{x}_i^+ = A_{L_i}\tilde{x}_i + (Ew - L_i\eta_i)\,. \tag{13}$$

## 5. Estimate reconfiguration

Every estimator (8) and (9) independently estimates the states of the system (1) and gives the updated state estimate $\hat{x}_i^{UP}$ to be evaluated by an FDI mechanism. Only "healthy" updated estimates, as diagnosed by the FDI unit (described in Section 9), are used at the reconfiguration stage, which will then provide an adequate "reconfigured" updated estimate for use by the feedback controller.

We consider two different methodologies for the reconfiguration stage. The first methodology *switches* between the available sensors–estimator combinations by means of a suitable criterion (Yetendje *et al*., 2010). In the second methodology, employed by De Doná *et al*. (2009), the estimates deemed "healthy" by means of the FDI test are *fused* based on an optimal fusion steady-state Kalman filter.

Each methodology, the switching or fusion of estimates, has its own merits. The fusion estimate is *optimal* in the linear minimum variance sense and hence, in that sense, it is regarded as the best estimate possible. On the other hand, the switching strategy is computationally very simple to implement since, at each time instant, only one sensor (or one group of sensors) is selected based on a trivial optimisation problem. The choice of the reconfiguration technique is left at the user discretion. Therefore, for the remainder of the paper, the "reconfigured" updated estimate provided by either technique is generically denoted by

$$\hat{x}^{UP*} = \sum_{\ell\in\mathbb{H}} \lambda_\ell \hat{x}_\ell^{UP} \tag{14}$$

with $\mathbb{H}$ defined as

$$\mathbb{H} \triangleq \{\ell \in \{1, \ldots, M\} : \text{sensor group } \ell \text{ is diagnosed as healthy}\} \tag{15}$$

and $\sum_{\ell\in\mathbb{H}} \lambda_\ell = I_n$.

We will later explain in Section 9 how the set $\mathbb{H}$ is constructed and updated at each time step by the FDI unit. For details on how the coefficients $\lambda_\ell$, $\ell \in \mathbb{H}$, are computed, see the works of Yetendje *et al*. (2010) for switching, and De Doná *et al*. (2009) as well as Yetendje *et al*. (2011) for fusion. For each possible $\mathbb{H} \in \mathbb{P}_M$ (the set of all subsets of $\{1, \ldots, M\}$), the corresponding coefficients $\lambda_\ell, \forall \ell \in \mathbb{H}$, can be precomputed and stored so that the online reconfiguration task simply amounts to employing the pre-stored set of coefficients corresponding to the current index set $\mathbb{H}$.

For future reference, we define the "reconfigured" updated state estimation error as

$$\tilde{x}^{UP*} \triangleq x - \hat{x}^{UP*} = \sum_{\ell\in\mathbb{H}} \lambda_\ell \left[(I_n - G_\ell C_\ell)\,\tilde{x}_\ell - G_\ell\eta_\ell\right], \tag{16}$$

where we used (3) (with $\Pi_\ell = \Theta_\ell = I_{p_\ell}$), (9), (12), and (14).

## 6. Robust tube-MPC controller and tracking errors

Following Rawlings and Mayne (2009), we view as the "reference model" as the *nominal* system obtained from (1) by neglecting $w$,

$$\bar{x}^+ = A\bar{x} + B\bar{u}, \tag{17}$$

where $\bar{x} \in \mathbb{R}^n$ denotes the nominal system state and $\bar{u} \in \mathbb{R}^m$ is the input to the nominal system. Choosing an initial state $\bar{x} = \bar{x}(0)$ and a nominal control sequence $\bar{\mathbf{u}} \triangleq \{\bar{u}(0), \bar{u}(1), \ldots\}$ yields a nominal state sequence solution $\bar{\mathbf{x}} \triangleq \{\bar{x}(0), \bar{x}(1), \ldots\}$ of (17), which constitutes the center of a *tube*. In Section 8 we will elaborate more on the implementation of this nominal system with a constrained MPC design, once we have all the necessary elements (in particular, the invariant sets described in Section 7).

Since the real system is disturbed, the future trajec-

[3] A Schur matrix has eigenvalues of magnitude less than one.

[4] If the estimators are steady-state Kalman filters, then $L_i$ and $G_i$ are obtained via an algebraic Riccati equation (see, e.g., Sun and Deng, 2008).

tory of the disturbed plant will differ from the nominal prediction. To counteract the effect of the disturbances, we use the methodology of Rawlings and Mayne (2009, Ch. 3) to force the trajectory to lie as close as possible to the nominal one by combining in the control $u$ a feed-forward part, given by the tube-based model predictive controller, and a feedback part with integral action:

$$u = \bar{u} + K_1(\hat{x}^{UP*} - \bar{x}) + K_2\sigma, \tag{18}$$

where $\sigma \in \mathbb{R}^q$ denotes the integral action state, defined by

$$\sigma^+ = \sigma + T_s C^*(\bar{x} - \hat{x}^{UP*}) \tag{19}$$

with $T_s > 0$ an arbitrary constant (typically the sampling interval) and $C^*$ the performance output matrix as in (1b).

**Assumption 2.** (*Controller gain*) The gain $K = \begin{bmatrix} K_1 & K_2 \end{bmatrix}$ is computed off-line such that

$$A_K = \begin{bmatrix} A + BK_1 & BK_2 \\ -T_s C^* & I_q \end{bmatrix}$$

is a Schur matrix.

Note that the above is a standard assumption in reference tracking applications (see, e.g., Jemaa and Davison (2003)) for an equivalent condition in terms of the original system (1a) and integral action (19)).

Further, in Section 8, we will explain how the control action $\bar{u}$ is obtained by means of MPC.

We define the plant tracking error, $z$, the integrator-augmented plant tracking error, $\xi$, the estimation tracking errors, $e_i$, the augmented estimation tracking errors, $\upsilon_i$, and the updated estimation tracking errors, $e_i^{UP}$, for $i = 1, \ldots, M$, as

$$z \triangleq x - \bar{x}, \tag{20}$$

$$\xi = \begin{bmatrix} z' & \sigma' \end{bmatrix}', \tag{21}$$

$$e_i \triangleq \hat{x}_i - \bar{x}, \tag{22}$$

$$\upsilon_i = \begin{bmatrix} e_i' & \sigma' \end{bmatrix}', \tag{23}$$

$$e_i^{UP} \triangleq \hat{x}_i^{UP} - \bar{x} = e_i + \gamma_i, \tag{24}$$

where, from (9),

$$\gamma_i \triangleq G_i[y_i - C_i\hat{x}_i]. \tag{25}$$

(Note, in particular, that the tracking error of the integrator state is computed relative to its reference which is zero.)

Using (12), and substituting (3) (with $\Pi_i = \Theta_i = I_{p_i}$) in (25), we have that, under healthy operation of the $i$-th group of sensors,

$$\gamma_i = G_i C_i \tilde{x}_i + G_i \eta_i. \tag{26}$$

Also, using (16) and (20), the "reconfigured" updated estimate tracking error $e^{UP*}$ satisfies

$$e^{UP*} \triangleq \hat{x}^{UP*} - \bar{x} = z - \tilde{x}^{UP*}. \tag{27}$$

Then, from (1), (16)–(21) and (27), we can express the dynamics of the augmented plant tracking error as

$$\xi^+ = A_K \xi + \begin{bmatrix} -BK_1 & E \\ T_s C^* & 0 \end{bmatrix} \begin{bmatrix} \tilde{x}^{UP*} \\ w \end{bmatrix}. \tag{28}$$

Using (18) and (27) in (11), the closed-loop estimator states $\hat{x}_i$ corresponding to healthy sensors satisfy

$$\begin{aligned} \hat{x}_i^+ = {} & A\hat{x}_i + B\bar{u} + BK_1\left(z - \tilde{x}^{UP*}\right) \\ & + BK_2\sigma + L_i C_i \tilde{x}_i + L_i \eta_i. \end{aligned} \tag{29}$$

Using (12), (17), (19), (20), (22), (23), (27) and (29), each augmented estimation tracking error $\upsilon_i$ satisfies the difference equation

$$\begin{aligned} \upsilon_i^+ = {} & A_K \upsilon_i + \begin{bmatrix} BK_1 + L_i C_i \\ -T_s C^* \end{bmatrix} \tilde{x}_i \\ & + \begin{bmatrix} -BK_1 \\ T_s C^* \end{bmatrix} \tilde{x}^{UP*} + \begin{bmatrix} L_i \\ 0 \end{bmatrix} \eta_i. \end{aligned} \tag{30}$$

## 7. Invariant sets for the closed-loop system dynamics

In this section, we derive invariant sets for the closed-loop system dynamics. In this analysis, we will assume that the FDI unit (described in Section 9) correctly identifies the faulty groups of sensors, so that the "reconfigured" updated estimate (14) is only formed by estimates corresponding to healthy groups of sensors. Later, in Section 9, we will validate this analysis by providing conditions that guarantee that the FDI unit correctly discards faulty groups of sensors.

**7.1. Estimation errors analysis.** The difference equation (13) can be rewritten in the form

$$\tilde{x}_i^+ = A_{L_i}\tilde{x}_i + \tilde{\delta}_i, \quad \tilde{\delta}_i \triangleq Ew - L_i\eta_i. \tag{31}$$

Each "disturbance" $\tilde{\delta}_i$ lies in the C-set $\tilde{\Delta}_i \triangleq E\mathbb{W} \oplus (-L_i\mathbb{N}_i)$ (where the symbol $\oplus$ denotes the Minkowski sum of sets).

Since $A_{L_i}$ are Schur matrices, there exist a C-set $\tilde{\mathbb{S}}_i$ that is finite time computable and RPI[5] for the system (31) and the constraint set $\left(\mathbb{R}^n, \tilde{\Delta}_i\right)$ (Rawlings and Mayne, 2009).

[5]A set $\Omega \in \mathbb{R}^n$ is Robust Positively Invariant (RPI) for $x^+ = f(x, w)$ and the constraint set $(\mathbb{X}, \mathbb{W})$, if $\Omega \subset \mathbb{X}$ and $f(x, w) \in \Omega$, for $x \in \Omega$, and $w \in \mathbb{W}$. If $f(x, w) = Ax + w$, then the set $\Omega$ satisfies $A\Omega \oplus \mathbb{W} \subseteq \Omega$. In addition, if $x(0) \in \Omega$, then $x(k) \in \Omega$, for all $k \geq 0$.

Using (16), we can compute the C-set $\tilde{\mathbb{S}}^{UP*}$, where $\tilde{x}^{UP*}$ lies whenever each estimation error $\tilde{x}_\ell \in \tilde{\mathbb{S}}_\ell$, $\ell \in \mathbb{H}$, as

$$\tilde{\mathbb{S}}^{UP*} \triangleq \text{Conv.hull}\Big( \cup_{\mathbb{H}\in\mathbb{P}_M} \big( \oplus_{\ell\in\mathbb{H}} \lambda_\ell \big[ (I_n - G_\ell C_\ell)\tilde{\mathbb{S}}_\ell \oplus (-G_\ell)\,\mathbb{N}_\ell \big] \big) \Big), \tag{32}$$

where 'Conv.hull' denotes the convex hull and $\mathbb{P}_M$ is the set of all subsets of $\{1,\dots,M\}$ (see Section 5).

**Remark 1.** Notice that, since the set $\tilde{\mathbb{S}}^{UP*}$ in (32) is obtained over all possible combinations of healthy sensor groups, a valid alternative would be to compute $\tilde{\mathbb{S}}^{UP*}$ only for the current combination of healthy sensors. However, employing (32) makes the FDI algorithm simpler since the sets used in the corresponding tests are fixed for any possible fault situation. Alternatively, at the expense of more calculations, one could update the FDI algorithm by recomputing the relevant sets after a fault occurs, possibly resulting in a less conservative overall approach.

**7.2. Augmented plant tracking error analysis.** The dynamics of the augmented plant tracking error $\xi$ given in (28) can be rewritten in the form

$$\xi^+ = A_K\xi + \delta_\xi, \quad \delta_\xi = \begin{bmatrix} -BK_1 & E \\ T_sC^* & 0 \end{bmatrix} \begin{bmatrix} \tilde{x}^{UP*} \\ w \end{bmatrix}, \tag{33}$$

where $\tilde{x}^{UP*}$ and $w$ are bounded respectively by $\tilde{\mathbb{S}}^{UP*}$ and $\mathbb{W}$. Here $\delta_\xi$ lies in the set $\Delta_\xi$ defined by

$$\Delta_\xi = \begin{bmatrix} -BK_1 \\ T_sC^* \end{bmatrix} \tilde{\mathbb{S}}^{UP*} \oplus \begin{bmatrix} E \\ 0 \end{bmatrix} \mathbb{W}. \tag{34}$$

Since $A_K$ is a Schur matrix, there exists a C-set $\Xi$ that is finite time computable and RPI for the system (33) and the constraint set $(\mathbb{R}^{n+q}, \Delta_\xi)$. In the sequel, $\Xi_z$ and $\Xi_\sigma$ represent respectively the projection of $\Xi$ on its components $z$ and $\sigma$.

**7.3. Estimation and updated estimation tracking errors analysis in the case of healthy sensors.** The dynamics of the augmented estimation tracking errors $\upsilon_i$ (under healthy operation of the $i$-th group of sensors) given in (30) can be rewritten in the form

$$\begin{aligned} \upsilon_i^+ &= A_K\upsilon_i + \delta_i, \\ \delta_i &\triangleq \begin{bmatrix} BK_1 + L_iC_i \\ -T_sC^* \end{bmatrix} \tilde{x}_i + \begin{bmatrix} -BK_1 \\ T_sC^* \end{bmatrix} \tilde{x}^{UP*} + \begin{bmatrix} L_i \\ 0 \end{bmatrix} \eta_i, \end{aligned} \tag{35}$$

where each $\delta_i$ lies in the set $\Delta_i$ defined by

$$\Delta_i \triangleq \begin{bmatrix} BK_1 + L_iC_i \\ -T_sC^* \end{bmatrix} \tilde{\mathbb{S}}_i \oplus \begin{bmatrix} -BK_1 \\ T_sC^* \end{bmatrix} \tilde{\mathbb{S}}^{UP*} \oplus \begin{bmatrix} L_i \\ 0 \end{bmatrix} \mathbb{N}_i. \tag{36}$$

Since $A_K$ is a Schur matrix, there exists a C-set $\Upsilon_i$ that is finite time computable and RPI for the system (35) and the constraint set $(\mathbb{R}^{n+q}, \Delta_i)$. In particular, the set $\mathbb{S}_i$, projection of the set $\Upsilon_i$ on the first component $e_i$, is associated to the estimation tracking error of the $i$-th group of sensors.

Using (27), we can compute the C-set $\mathbb{S}^{UP*}$, where the "reconfigured" updated estimation tracking error $e^{UP*}$ lies whenever $z \in \Xi_z$ and $\tilde{x}^{UP*} \in \tilde{\mathbb{S}}^{UP*}$, with $\tilde{\mathbb{S}}^{UP*}$ defined in (32), as

$$\mathbb{S}^{UP*} \triangleq \Xi_z \oplus \big( -\tilde{\mathbb{S}}^{UP*} \big). \tag{37}$$

We conclude this section with a result that establishes the existence of and characterises the invariant tubes where the system trajectories lie.

**Theorem 1.** (Tube for system trajectories) *Assume the system initial state, $x(0)$, the integral action initial state, $\sigma(0)$, the nominal system initial state, $\bar{x}(0)$, and the initial value of the estimators associated with healthy groups of measurements, $\hat{x}_i(0)$, for $i \in \mathbb{H}$ satisfy*

$$\begin{aligned} \tilde{x}_i(0) &= x(0) - \hat{x}_i(0) \in \tilde{\mathbb{S}}_i, \\ \xi(0) &= \begin{bmatrix} x(0) - \bar{x}(0) \\ \sigma(0) \end{bmatrix} \in \Xi, \\ \upsilon_i(0) &= \begin{bmatrix} \hat{x}_i(0) - \bar{x}(0) \\ \sigma(0) \end{bmatrix} \in \Upsilon_i. \end{aligned}$$

*Let*

$$u(k) = \bar{u}(k) + K_1(\hat{x}^{UP*}(k) - \bar{x}(k)) + K_2\sigma$$

*$\forall\, k \geq 0$, where $\hat{x}^{UP*}$ is defined in* (14)*. Then for every $k \geq 0$, we have*

*(i)* $\tilde{x}^{UP*}(k) \in \tilde{\mathbb{S}}^{UP*}$,

*(ii)* $\xi(k) \in \Xi$, $z(k) \in \Xi_z$ *and* $x(k) \in \{\bar{x}(k)\} \oplus \Xi_z$,

*(iii)* $\upsilon_i(k) \in \Upsilon_i$ *and, in particular,* $e_i(k) \in \mathbb{S}_i$*. In addition,* $e^{UP*}(k) \in \mathbb{S}^{UP*}$.

*Proof.* (Part 1) Since $\tilde{\mathbb{S}}_i$ is an RPI set, the assumption on the initial conditions $\tilde{x}_i(0) \in \tilde{\mathbb{S}}_i$ implies $\tilde{x}_i(k) \in \tilde{\mathbb{S}}_i$, $\forall k \geq 0$. Therefore, from (16) and (32), $\tilde{x}^{UP*}(k) \in \tilde{\mathbb{S}}^{UP*}$, $\forall k \geq 0$.

(Part 2) Since $\tilde{x}^{UP*}(k) \in \tilde{\mathbb{S}}^{UP*}$, then $\delta_\xi(k) \in \Delta_\xi$ in (33)–(34), $\forall k \geq 0$. Combining this result with the assumption $\xi(0) \in \Xi$, together with the invariance of $\Xi$, we have $\xi(k) \in \Xi$, $\forall k \geq 0$. In particular, $z(k) \in \Xi_z$

(see Section 7.2). Moreover, from (20), we have that $x = \bar{x} + z$, and it follows that the system state, $x(k)$, satisfies $x(k) \in \{\bar{x}(k)\} \oplus \Xi_z, \forall k \geq 0$.

(Part 3) Since $\tilde{x}_i(k) \in \tilde{\mathbb{S}}_i$ and $\tilde{x}^{UP*}(k) \in \tilde{\mathbb{S}}^{UP*}$, we have that $\delta_i \in \Delta_i$ in (35) and (36), $\forall k \geq 0$. With the assumption on the initial condition $\upsilon_i(0) \in \Upsilon_i$, and the invariance of $\Upsilon_i$, it follows that $\upsilon_i(k) \in \Upsilon_i$, $\forall k \geq 0$. In particular, $e_i(k) \in \mathbb{S}_i$. Moreover, $z(k) \in \Xi_z$, and $\tilde{x}^{UP*}(k) \in \tilde{\mathbb{S}}^{UP*}$, $\forall k \geq 0$ imply, from (27) and (37), that $e^{UP*}(k) \in \mathbb{S}^{UP*}$, $\forall k \geq 0$. ■

The assumption made in Theorem 1 above, that the initial values are in the corresponding invariant sets, is satisfied if, e.g., enough time elapses at the beginning of system operation without a change in the fault situation (a reasonable initialisation assumption), since those sets are attractive and convergence in finite time is ensured.

## 8. Nominal MPC design

We define the nominal optimal control problem for the reference system (17) to track the setpoint $(x_s, u_s)$ as

$$\begin{aligned}&\bar{\mathbb{P}}_N(\bar{x}, x_s, u_s):\\ &V_N^0(\bar{x}, x_s, u_s) \triangleq \min_{\bar{\mathbf{u}}} \{V_N(\bar{x}, \bar{\mathbf{u}}, x_s, u_s) | \bar{\mathbf{u}} \in \vartheta_N(\bar{x}, x_s)\},\end{aligned} \tag{38}$$

where $N$ is the prediction horizon, $\bar{x} = \bar{x}(0)$ is the initial condition of the nominal system (17) at the current time, and the cost $V_N(\bar{x}, \bar{\mathbf{u}}, x_s, u_s)$ is defined by[6]

$$\begin{aligned}&V_N(\bar{x}, \bar{\mathbf{u}}, x_s, u_s)\\ &\quad \triangleq \sum_{k=0}^{N-1} \big[ \|\bar{x}(k) - x_s\|_Q^2\\ &\qquad + \|\bar{u}(k) - u_s\|_R^2 \big] + \|\bar{x}(N) - x_s\|_P^2\end{aligned} \tag{39}$$

where $Q$, $R$ and are $P$ positive definite weighting matrices.

The constraint set $\vartheta_N(\bar{x}, x_s)$ is defined by[7]

$$\begin{aligned}&\vartheta_N(\bar{x}, x_s)\\ &\quad \triangleq \big\{\bar{\mathbf{u}} | \bar{u}(k) - u_s \in \mathbb{U} \ominus (K_1 \mathbb{S}^{UP*} \oplus K_2 \Xi_\sigma),\\ &\quad \bar{x}(k) - x_s \in \mathbb{X} \ominus \Xi_z, \forall k \in \{0, 1, \ldots, N-1\},\\ &\quad \bar{x}(N) - x_s \in \mathbb{X}_f\big\},\end{aligned} \tag{40}$$

where $\mathbb{X}_f \subset \mathbb{X} \ominus \Xi_z$ is the terminal constraint set. Note that $\bar{u}$ is forced to satisfy the tighter constraint $\bar{u} - u_s \in \mathbb{U} \ominus (K_1 \mathbb{S}^{UP*} \oplus K_2 \Xi_\sigma)$, which from (18), (27) and (iii) Theorem 1), ensures $u - u_s \in \mathbb{U}$. Similarly, in order to ensure that the unknown state $x = \bar{x} + z$ (see (20) and Theorem 1, Item 2)) satisfies the state constraint $x - x_s \in \mathbb{X}$, we must ensure that $\bar{x} - x_s \in \mathbb{X} \ominus \Xi_z$.

The solution of $\bar{\mathbb{P}}_N(\bar{x}, x_s, u_s)$ is

$$\begin{aligned}&\bar{\mathbf{u}}^0(\bar{x}, x_s, u_s)\\ &\quad = \arg\min_{\bar{\mathbf{u}}} \{V_N(\bar{x}, \bar{\mathbf{u}}, x_s, u_s) | \bar{\mathbf{u}} \in \vartheta_N(\bar{x}, x_s)\},\end{aligned} \tag{41}$$

and the model predictive control law $\kappa_N$ is obtained as

$$\bar{u} = \kappa_N(\bar{x}, x_s, u_s) \triangleq \bar{u}^0(0; \bar{x}, x_s, u_s), \tag{42}$$

where $\bar{u}^0(0; \bar{x}, x_s, u_s)$ is the first element in the sequence $\bar{\mathbf{u}}^0(\bar{x}, x_s, u_s)$.

We next establish the stability properties of the above nominal controller. We start by imposing the following assumption that requires the disturbances and noises to be "small enough", which suffices for the sets in the conditions defining the constraint set (40) to be non-empty (see Rawlings and Mayne, 2009).

**Assumption 3.** *(Tighter sets for constraint satisfaction)* The disturbance sets $\mathbb{W}$, $\mathbb{N}_i$, for $i = 1, \ldots, M$, are sufficiently small to ensure that $\Xi_z \subset \mathbb{X}$ and $K_1 \mathbb{S}^{UP*} \oplus K_2 \Xi_\sigma \subset \mathbb{U}$.

We will next select the cost function and the terminal constraint set in the following way, standard in MPC, (Rawlings and Mayne, 2009).

**Assumption 4.** *(Cost function and terminal set)* The matrices $Q$, $R$, $P$ in (39) satisfy the discrete algebraic Riccati equation

$$A'PA - P - (A'PB)(R + B'PB)^{-1}(B'PA) + Q = 0.$$

The terminal constraint set $\mathbb{X}_f$ given in (40) is chosen to be the maximal positively invariant constraint admissible set for the system $\bar{x}^+ = A\bar{x} + B\bar{u}$ under the tighter constraints $\bar{x} - x_s \in \mathbb{X} \ominus \Xi_z$ and $\bar{u} - u_s \in \mathbb{U} \ominus (K_1 \mathbb{S}^{UP*} \oplus K_2 \Xi_\sigma)$. Let

$$\bar{\mathbb{X}}_N(x_s) \triangleq \{\bar{x} \,|\, \vartheta_N(\bar{x}, x_s) \neq \emptyset\}, \tag{43}$$

where $\vartheta_N(\bar{x}, x_s)$ is the constraint set defined in (40). We then have the following result.

**Lemma 1.** (Exponential stability of the nominal system) *Consider the system* (17) *where $\bar{u}$ is the nominal MPC law* (42). *Suppose that $\bar{\mathbb{X}}_N(x_s)$ defined in* (43) *is compact.*[8] *Then, the setpoint $x_s$ is exponentially stable with a region of attraction $\bar{\mathbb{X}}_N(x_s)$ for the system* (17) *and* (42).

*Proof.* If Assumptions 1–4 are satisfied for the optimal control problem $\bar{\mathbb{P}}_N(\bar{x}, x_s, u_s)$, and $\bar{\mathbb{X}}_N(x_s)$ is compact, then there exist constants $c_1$ and $c_2$ such that

[6] For a given matrix $F$, $\|x\|_F$ denotes $\|x\|_F = \sqrt{x'Fx}$.

[7] The symbol $\ominus$ denotes the Minkowski (Pontryagin) set difference.

[8] If $\mathbb{X}$ in (40) is not compact, the compactness of $\bar{\mathbb{X}}_N(x_s)$ can be ensured by substituting $\mathbb{X}$ in (40) by its intersection with an arbitrarily large bounded box.

the value function $V_N^0(\bar{x}, x_s, u_s)$ satisfies (Rawlings and Mayne, 2009)

$$\begin{aligned} V_N^0(\bar{x}, x_s, u_s) &\geq c_1|\bar{x} - x_s|^2, && \forall \bar{x} \in \bar{\mathbb{X}}_N(x_s), \\ \Delta V_N^0(\bar{x}, x_s, u_s) &\leq -c_1|\bar{x} - x_s|^2, && \forall \bar{x} \in \bar{\mathbb{X}}_N(x_s), \\ V_N^0(\bar{x}, x_s, u_s) &\leq c_2|\bar{x} - x_s|^2, && \forall \bar{x} \in \bar{\mathbb{X}}_N(x_s), \end{aligned} \tag{44}$$

where

$$\Delta V_N^0(\bar{x}, x_s, u_s) = V_N^0(\bar{x}^+, x_s, u_s) - V_N^0(\bar{x}, x_s, u_s).$$

Hence $x_s$ is exponentially stable for the nominal system $\bar{x}^+ = A\bar{x} + B\kappa_N(\bar{x}, x_s, u_s)$ with a region of attraction $\bar{\mathbb{X}}_N(x_s)$, i.e., there exist constants $c \geq 0$ and $\gamma \in (0, 1)$ such that $|\bar{x}(k) - x_s| \leq c|\bar{x}(0) - x_s|\gamma^k, \forall k \geq 0$ (Rawlings and Mayne, 2009). ■

**Corollary 1.** The nominal state $\bar{x}$ in (17) is bounded such that $\bar{x} \in \bar{\mathbb{X}} \triangleq \{x \in \mathbb{R}^n : |x - x_s| \leq \bar{x}_{\max}\}$, for some vector $\bar{x}_{\max} \in \mathbb{R}^n$.

*Proof.* It is straightforward to see from the proof of Lemma 1 that taking $\bar{x}_{\max} = c|\bar{x}(0) - x_s|$ ensures that the nominal state $\bar{x}$ is bounded as claimed. ■

Later, in Section 9.2, we will show exponential stability of the fault tolerant output MPC scheme based on the above nominal controller results.

## 9. Fault detection and identification

In this section we describe the proposed fault detection and identification principle. The principle is based on the separation of "healthy" sets, where the updated estimation tracking errors (24) remain under healthy operation, from "under-fault" sets, towards which the updated estimation tracking errors jump when abrupt sensor faults occur in one or more groups of sensors. In contrast with other schemes, (see, e.g., Larson *et al.*, 2002) which use stochastic arguments for fault detection and control reconfiguration, the approach followed here is very simple computationally since, once the required conditions are satisfied by design (off-line), the on-line system complexity only depends on the number of different fault situations considered.

**9.1. Condition for fault tolerance.** Suppose that the $j$-th group of sensors is healthy and such that its associated estimation error, $\tilde{x}_j$, defined in (12), and the estimation tracking error, $e_j$, defined in (22), satisfy $\tilde{x}_j \in \tilde{\mathbb{S}}_j$ and $e_j \in \mathbb{S}_j$, where $\tilde{\mathbb{S}}_j$ and $\mathbb{S}_j$ are the RPI sets defined in Sections 7.1 and 7.3, respectively. Using (24) and (26), we can then compute the C-set

$$\mathbb{S}_j^{UP} \triangleq \mathbb{S}_j \oplus (G_j C_j)\tilde{\mathbb{S}}_j \oplus G_j \mathbb{N}_j, \tag{45}$$

to which the updated estimation tracking error $e_j^{UP}$ belongs whenever $e_j \in \mathbb{S}_j$, $\tilde{x}_j \in \tilde{\mathbb{S}}_j$, $\eta_j \in \mathbb{N}_j$. We know from (iii) of Theorem 1, that this condition will hold for as long as the $j$-th group of sensors remains healthy

Consider next a fault in the $j$-th group of sensors, characterised by a change of the fault matrices $\Pi_j$ and/or $\Theta_j$ in (3) from the identity matrix (the healthy case, see (5)) to a new "under fault" value (see (6) and (7) for some cases of fault situations that can be contemplated in the present framework). At the time of the fault, substituting (3) into (24) and (25) and using (12) and (22) we have that the "under fault" updated estimation tracking error, $e_j^{UP,F}$, satisfies

$$\begin{aligned} e_j^{UP,F} = &\left[I_n + G_j\left(\Pi_j - I_{p_j}\right)C_j\right] e_j \\ &+ G_j\left(\Pi_j - I_{p_j}\right)C_j\bar{x} + G_j\Pi_j C_j\tilde{x}_j \\ &+ G_j\left[\Pi_j\eta_j + \left(I_{p_j} - \Theta_j\right)\eta_j^F\right]. \end{aligned} \tag{46}$$

Since, at the time of the fault, the estimation tracking error $e_j$ still belongs to $\mathbb{S}_j$ and the estimation error $\tilde{x}_j$ is still in $\tilde{\mathbb{S}}_j$, the updated estimation tracking error $e_j^{UP,F}$ at the time of the fault will belong to the set

$$\begin{aligned} &\mathbb{S}_j^{UP,F}(\Pi_j, \Theta_j, \bar{\eta}_j) \\ &\quad = \left[I_n + G_j\left(\Pi_j - I_{p_j}\right)C_j\right]\mathbb{S}_j \\ &\qquad \oplus G_j\left(\Pi_j - I_{p_j}\right)C_j\bar{\mathbb{X}} \oplus G_j\Pi_j C_j\tilde{\mathbb{S}}_j \oplus G_j\Pi_j\mathbb{N}_j \\ &\qquad \oplus G_j\left(I_{p_j} - \Theta_j\right)\mathbb{N}_j^F(\bar{\eta}_j), \end{aligned} \tag{47}$$

where $\bar{\mathbb{X}}$ is as in Corollary 1, and the measurement noise sets $\mathbb{N}_j$, $\mathbb{N}_j^F(\bar{\eta}_j)$ are defined in Section 3.

In order to ensure effective fault detection and identification, we have to verify that the sets $\mathbb{S}_j^{UP}$ and $\mathbb{S}_j^{UP,F}(\Pi_j, \Theta_j, \bar{\eta}_j)$ are separated.

**Assumption 5.** The condition $\mathbb{S}_j^{UP} \cap \mathbb{S}_j^{UP,F}(\Pi_j, \Theta_j, \bar{\eta}_j) = \emptyset$ holds for all $j = 1, \ldots, M$, for any of the possible values of the combination $(\Pi_j, \Theta_j, \bar{\eta}_j)$ characterising the examined fault situations for the $j$-th group of sensors.

**Remark 2.** The scheme will be ensured to be fault tolerant for each value of the fault combination $(\Pi_j, \Theta_j, \bar{\eta}_j)$ that satisfies Assumption 5. Depending on the problem characteristics, more than one value (usually a continuous range) of this combination can be considered for the $j$-th group of sensors. For example, one can test the range of fault tolerance against the loss of effectiveness of a particular $i$-th sensor of the $j$-th group by considering $\Pi_j = \Theta_j = \mathrm{diag}\{1, \ldots, \pi_{ji}, \ldots, 1\}$, $\bar{\eta}_j = 0$, and testing the separation condition of Assumption 5 for all $\pi_{ji} \in [0, \pi_{ji}^*]$, for some $\pi_{ji}^* \in [0, 1)$. The range of fault tolerance against bias in a particular $i$-th sensor of the $j$-th group can be tested similarly by considering the values of the combination $(\Pi_j, \Theta_j, \bar{\eta}_j)$ given in (7) (with the indices $i$ and $j$ interchanged) and verifying the validity of

Assumption 5 for all $|\bar{\eta}_{ji}| \in [\bar{\eta}^*_{ji}, \infty)$, for some $\bar{\eta}^*_{ji} > 0$. More generally, depending on the topology of the sets involved, one can test more complex fault scenarios such as simultaneous bias and loss of effectiveness, simultaneous failure of one or more sensors in each group, etc.

Note that the healthy updated estimation tracking error sets $\mathbb{S}_j^{UP}$ defined in (45) are centred at 0 (this is so because the sets $\tilde{\mathbb{S}}_j$ associated with the dynamics (31), $\mathbb{S}_j$ associated with the dynamics (35), and $\mathbb{N}_j$ defined in Section 3, are all centred at 0). The set $\mathbb{S}_j^{UP,F}(\Pi_j, \Theta_j, \bar{\eta}_j)$ defined in (47), on the other hand, is offset around a centre point $c_j(\Pi_j, \Theta_j, \bar{\eta}_j)$ given by

$$c_j(\Pi_j, \Theta_j, \bar{\eta}_j) = G_j(\Pi_j - I_{p_j})C_j x_s + G_j(I_{p_j} - \Theta_j)\bar{\eta}_j, \tag{48}$$

where $x_s$ and $\bar{\eta}_j$ are respectively the center points of $\bar{\mathbb{X}}$ and $\mathbb{N}_j^F(\bar{\eta}_j)$, as expressed in Corollary 1 and (4). Thus, the reference offset $x_s$ and the bias constant $\bar{\eta}_j$ (which in turn shift the centre $c_j(\Pi_j, \Theta_j, \bar{\eta}_j)$ in (48)) are instrumental to the set separation condition of Assumption 5. The former is determined by the required operation point of the system (as given by the setpoint $y_s$, cf. Section 2.2). The latter is given by the type of faults the sensors are subjected to.

We require the following assumption, which describes the initialisation condition of the FTC scheme.

**Assumption 6.** Before the occurrence of the first sensor fault, the system has been operating under a healthy condition for a sufficiently long time such that all the estimation error trajectories are inside the RPI sets $\tilde{\mathbb{S}}_i$ defined in Section 7.1, for $i = 1, \ldots, M$, and the estimation tracking errors are inside the RPI sets $\mathbb{S}_i$ defined in Section 7.3. Moreover, we assume that at least one group of sensors is healthy at all times.

**Remark 3.** Notice that Assumption 6 guarantees that when the fault in the $j$-th sensor group occurs at some time instant $k$, $\tilde{x}_j(k)$ is in $\tilde{\mathbb{S}}_j$ and $e_j(k)$ is in $\mathbb{S}_j$. Hence we have, at the time of the fault, $e_j^{UP,F} \in \mathbb{S}_j^{UP,F}(\Pi_j, \Theta_j, \bar{\eta}_j)$. Combining this condition with Assumption 5, we conclude that the $j$-th group of sensors, for $j \in \{1, \ldots, M\}$, is healthy at any time $k$ (and thus can be combined and used for reconfiguration in (14)) if $e_j^{UP}(k) \in \mathbb{S}_j^{UP}$, and that the moment $e_j^{UP}(k)$ leaves the set $\mathbb{S}_j^{UP}$ allows us to detect a fault in that sensor group which, in consequence, must be discarded.

Based on the above developments, the fault diagnosis criterion proposed for the FDI unit is as follows:

**Criterion 1.** (FDI) At each time step $k$, for each $i = 1, \ldots, M$, if the updated estimation tracking error satisfies $e_i^{UP}(k) \in \mathbb{S}_i^{UP}$, with $\mathbb{S}_i^{UP}$ defined in (45), then the $i$-th group of sensors is deemed healthy and considered for reconfiguration in (14)–(15). If $e_i^{UP}(k) \notin \mathbb{S}_i^{UP}$, then the $i$-th group of sensors is deemed faulty and discarded for all future times.

**9.2. Stability analysis.** The tube MPC controller (18) steers the trajectories of the uncertain system (1) toward the central trajectory $\bar{x}$ generated by the nominal system (17). The following theorem uses the properties of this nominal system to establish closed-loop stability of the overall fault tolerant control scheme based on the tube MPC controller reconfigured with the use of the FDI Criterion 1.

**Theorem 2.** *Consider the system* (1)*, where $u$ is computed as in* (18)–(19)*, with $\bar{u}$ given by* (42)*, $\hat{x}^{UP*}$ given by* (14)*, and $\bar{x}$ generated by the nominal system* (17) *and* (42)*. Suppose the conditions stated in Assumptions 3, 4, 5 and 6 hold. Then we have what follows:*

1. *The system* (1) *reconfigured with the use of the FDI Criterion 1 to select the index set $\mathbb{H}$ in* (15) *(used to compute the "reconfigured" updated estimates* (14)*) preserves exponential stability with a region of attraction $\bar{\mathbb{X}}_N(x_s) \oplus \Xi_z$, whenever the $j$-th group of sensors fails with fault combination $(\Pi_j, \Theta_j, \bar{\eta}_j)$.*

2. *The state of the system* (1)*, $x$, converges robustly and exponentially fast to $\{x_s\} \oplus \Xi_z$ while satisfying the state and control hard constraints $x - x_s \in \mathbb{X}$ and $u - u_s \in \mathbb{U}$.*

*Proof.* As explained in Remark 3, Assumptions 5 and 6 guarantee that the FDI Criterion 1 only selects healthy groups of sensors to compute the "reconfigured" updated estimates (14) used in the control law (18).

While $\tilde{x}_\ell \in \tilde{\mathbb{S}}_\ell, \forall \ell \in \mathbb{H}$, we have $\tilde{x}^{UP*} \in \tilde{\mathbb{S}}^{UP*}$ and hence $z \in \Xi_z$ (see Theorem 1, Parts (i) and (ii)). The proposed choices for the cost function and the terminal constraint set $\mathbb{X}_f$ in Assumption 4 guarantee that the result in Lemma 1 holds. As explained in the latter lemma, the region of attraction for $\bar{x}$ is the feasibility region of the optimisation problem $\bar{\mathbb{X}}_N(x_s)$. Since $x = \bar{x} + z$, the domain of attraction for $x$ is $\bar{\mathbb{X}}_N(x_s) \oplus \Xi_z$. Therefore, the system is exponentially stable with a region of attraction $\bar{\mathbb{X}}_N(x_s) \oplus \Xi_z$, and $x$ converges robustly and exponentially fast to $\{x_s\} \oplus \Xi_z$. In addition, using the fact that $x = \bar{x} + z$, $\bar{x} - x_s \in \mathbb{X} \ominus \Xi_z$ and $z \in \Xi_z$, yields $x - x_s \in \mathbb{X}$. Similarly, using (18)–(19), (27), $\bar{u} - u_s \in \mathbb{U} \ominus (K_1 \mathbb{S}^{UP*} \oplus K_2 \Xi_\sigma)$, and $e^{UP*} \in \mathbb{S}^{UP*}$, we have that $u - u_s \in \mathbb{U}$. The proof is thus complete. ■

## 10. Illustrative example

We consider the automotive longitudinal control problem under a *stop-and-go scenario*, discussed by Martínez and de Wit (2004), to illustrate the effectiveness of the proposed fault tolerant constrained control approach. In this

problem, the vehicle interdistance dynamics are typically represented by discretisation of a double integrator plant which, for a sampling period $T_s = 0.01$ s, satisfies (1) with

$$A = \begin{bmatrix} 1 & 0.1 \\ 0 & 1 \end{bmatrix}, \quad B = E = \begin{bmatrix} 0 \\ 0.1 \end{bmatrix},$$

where the first state represents the interdistance [m] and the second state its time derivative [m/s]. The process disturbance $w$ represents an error in the estimation of the leader vehicle acceleration and belongs to the C-set $\mathbb{W} \triangleq \{w \in \mathbb{R}^2 : |w| \leq 0.01\}$. The vehicle interdistance can be measured using sensors of different nature, accuracy and noise levels (e.g., automotive lasers, radars, stereo-vision), which lead to having the same output matrix with different noise characteristics. To illustrate this point, we consider four distance sensors $S_i$, with the following characteristics in the measurement equations (3): $C_i = \begin{bmatrix} 1 & 0 \end{bmatrix}$ for $i = 1, \ldots, 4$, and the measurement noises have the associated C-sets $\mathbb{N}_1 \triangleq \tilde{\mathbb{N}}_1^F \triangleq \{\eta \in \mathbb{R} : |\eta| \leq 0.001\}$, $\mathbb{N}_p = \mathbb{N}_p^F \triangleq \{\eta \in \mathbb{R}, |\eta| \leq 0.1\}, p = 2, 3, 4$. Sensor $S_1$ exhibits a low noise level, while the remaining sensors exhibit a higher noise level. We will consider that a bias appears in sensor $S_1$ at time $t_f = 17$ s, characterised by $\Pi_1 = 1$, $\Theta_1 = 0$ in (7), and the magnitude of the bias in (4) is any value such that $|\bar{\eta}_1| \in [0.85, \infty)$. The state, and control constraint sets are $\mathbb{X} \triangleq \{x \in \mathbb{R}^2 : |x_2| \leq 6\}$ and $\mathbb{U} \triangleq \{u \in \mathbb{R} : |u| \leq 25\}$.

The tube MPC controller is required to steer the nominal system from the locally stable initial state $\bar{x} = \bar{x}(0) = \begin{bmatrix} 0 & 0 \end{bmatrix}$ at time 0, to, alternatively (following a square-like wave pattern), the setpoints $x_s = x_{s_2} = [2 \quad 0]'$ and $x_s = x_{s_{10}} = [10 \quad 0]'$, with a horizon $N = 30$. The matrices $Q$, $R$, $P$ in (39) are computed as explained in Assumption 4, with $Q = I_2$, $R = 10^{-5}$ and

$$P = \begin{bmatrix} 11.5134 & 1.0523 \\ 1.0523 & 1.1063 \end{bmatrix}.$$

Moreover, the feedback part of the tube MPC controller uses the stabilising gain $K = \begin{bmatrix} 6.3608 & 8.0362 & -0.8830 \end{bmatrix}$ computed using LQR.

With the above data, we computed the domains of attraction $\bar{\mathbb{X}}_N(x_{s_2})$, $\bar{\mathbb{X}}_N(x_{s_{10}})$ of the nominal system under tighter constraints as depicted in Fig. 2 associated, respectively, with the setpoints $x_{s_2}$ and $x_{s_{10}}$. The constant setpoints $x_{s_2}$, $x_{s_{10}}$ (dot markers), the terminal constraint sets, respectively $\mathbb{X}_f(x_{s_2}) \triangleq \{x_{s_2}\} \oplus \mathbb{X}_f$, $\mathbb{X}_f(x_{s_{10}}) \triangleq \{x_{s_{10}}\} \oplus \mathbb{X}_f$, together with the initial state $\bar{x}$ (square marker) are also plotted on the same figure. Note that $x_{s_2} \in \text{int}(\mathbb{X}_f(x_{s_2}))$, $x_{s_{10}} \in \text{int}(\mathbb{X}_f(x_{s_{10}}))$ and starting from the initial condition $\bar{x}$, the states of the nominal system can be steered to the respective terminal constraint set in $N$ steps while satisfying the tighter control constraints.

The estimators (8) and (9) are designed as steady state Kalman estimators whose equations can be found in, e.g., the work of Sun and Deng (2008). We chose the following parameters in those equations:

$$G_1 = \begin{bmatrix} 0.9991 \\ 0.9503 \end{bmatrix}, \quad G_2 = G_3 = G_4 = \begin{bmatrix} 0.6875 \\ 0.6250 \end{bmatrix},$$
$$L_i = AG_i, \quad \forall i \in \{1, \ldots, 4\}.$$

The "reconfigured" updated estimate $\hat{x}^{UP*}$ presented in Section 5 is obtained by using an optimal fusion steady state Kalman filter technique, as explained by De Doná *et al*. (2009).

Using the procedure of Kofman *et al*. (2007), we compute the RPI sets described in Section 7 as well as the "healthy" and "faulty" sets (45) and (47). As can be inferred from Fig. 3, the separation condition of Assumption 5 holds for the range of bias considered for sensor $S_1$, in particular for $\bar{\eta}_1 = \{\pm 0.85, \pm 2.95\}$.

When a fault occurs in sensor $S_1$, the corresponding updated estimation tracking error trajectories jump from the RPI set $\mathbb{S}_1^{UP}$ defined in (45) to the "shifted" RPI sets $\mathbb{S}_1^{UP,F}(\Pi_1, \Theta_1, \bar{\eta}_1)$ defined in (47), making fault diagnosis possible. According to Theorem 2, we can conclude that the system preserves exponential stability with respective regions of attraction $\bar{\mathbb{X}}_N(x_{s_2}) \oplus \Xi_z$ and $\bar{\mathbb{X}}_N(x_{s_{10}}) \oplus \Xi_z$ whenever $S_1$ fails. At time $t_F - T_s$, $e_1^{UP}$ belongs to $\mathbb{S}_1^{UP}$, and at the time of the fault, $t_F$, $e_1^{UP}$ jumps to the sets $\mathbb{S}_1^{UP,F}(\Pi_1, \Theta_1, \bar{\eta}_1)$. Figure 4 shows the effectiveness of the fault tolerant constrained scheme (for the purpose of this temporal simulation, we used a constant bias $\bar{\eta}_1 = 2.95$). The first subplot displays the reference signal (dash-dotted line) which is tracked by the actual vehicle interdistance (dotted line) under the fault situation considered. The second subplot depicts the reference and the system velocity which satisfy, respectively, the tighter bounds $[-4.707 \quad 4.707]'$ and the constraints previously defined. Finally, as shown in the third subplot, the reference and the system acceleration (control action) satisfy, respectively, the tighter bounds $[-7.438 \quad 7.438]'$ and the input constraints previously defined.

## 11. Conclusion

We have proposed a robust fault tolerant control scheme for constrained multisensor linear systems subject to sensor faults and in the presence of bounded state and output disturbances. An FDI unit provides a mechanism where the updated estimation tracking error of each sensor-estimator combination is tested for containment in a precomputed healthy set. An active fault tolerant output feedback MPC controller guarantees robust closed-loop exponential stability of the system in normal operation and under abrupt faults in some of the sensors, including loss of effectiveness (total outage as an extreme case) and sensor bias, in both cases by unknown amounts. An illustrative

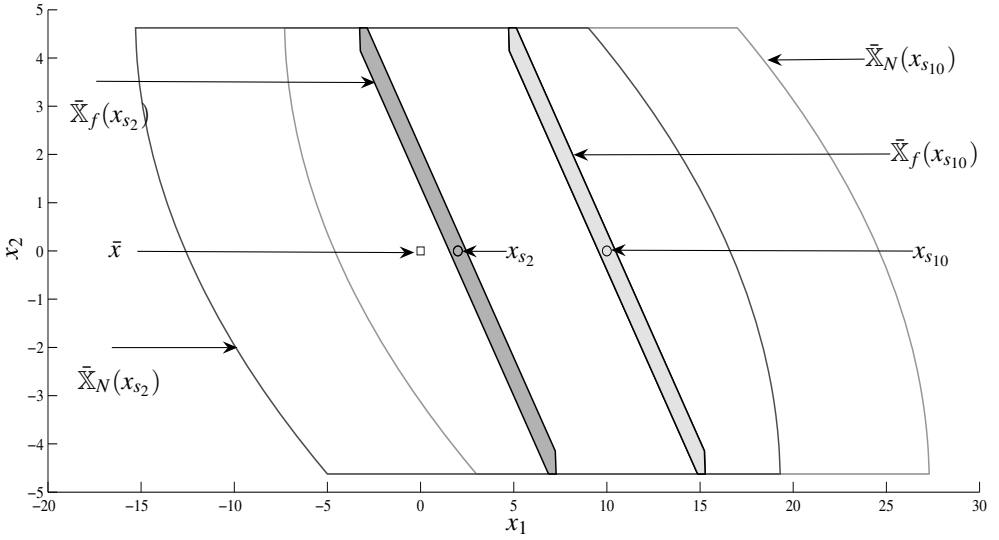



Fig. 2. Domain of attraction and terminal constraint sets for the nominal system.

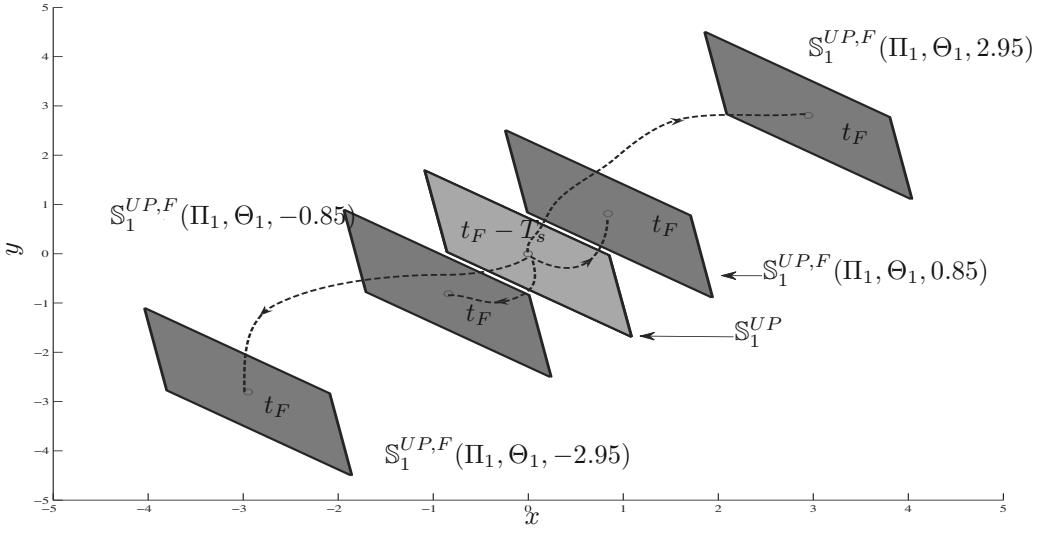



Fig. 3. Separation of sets representing healthy and faulty behaviour for sensor $S_1$. The axes correspond to $(x, y) = e_1^{UP}$.

example shows the effectiveness of the scheme in those situations.

## References

De Doná, J., Seron, M. and Yetendje, A. (2009). Multisensor fusion fault-tolerant control with diagnosis via a set separation principle, *Proceedings of the 48th IEEE Conference on Decision and Control, Shanghai, China*, pp. 7825–7830.

Goodwin, G., Seron, M. and De Doná, J. (2005). *Constrained Control and Estimation—An Optimisation Approach*, Springer-Verlag, London.

Jemaa, L.B. and Davison, E. (2003). Performance limitations in the robust servomechanism problem for discrete-time LTI systems, *IEEE Transactions on Automatic Control* **48**(8): 1299–1311.

Kofman, E., Haimovich, H. and Seron, M.M. (2007). A systematic method to obtain ultimate bounds for perturbed systems, *International Journal of Control* **80**(2): 167–178.

Larson, E.C., Jr, B.P. and Clark, B.R. (2002). Model-based sensor and actuator fault detection and isolation, *Proceedings of the American Control Conference, Anchorage, AK, USA,* Vol. 5, pp. 4215–4219.

Maciejowski, J. (1999). Fault-tolerant aspects of MPC, *Proceedings of the IEEE Workshop on Model Predictive Control:*

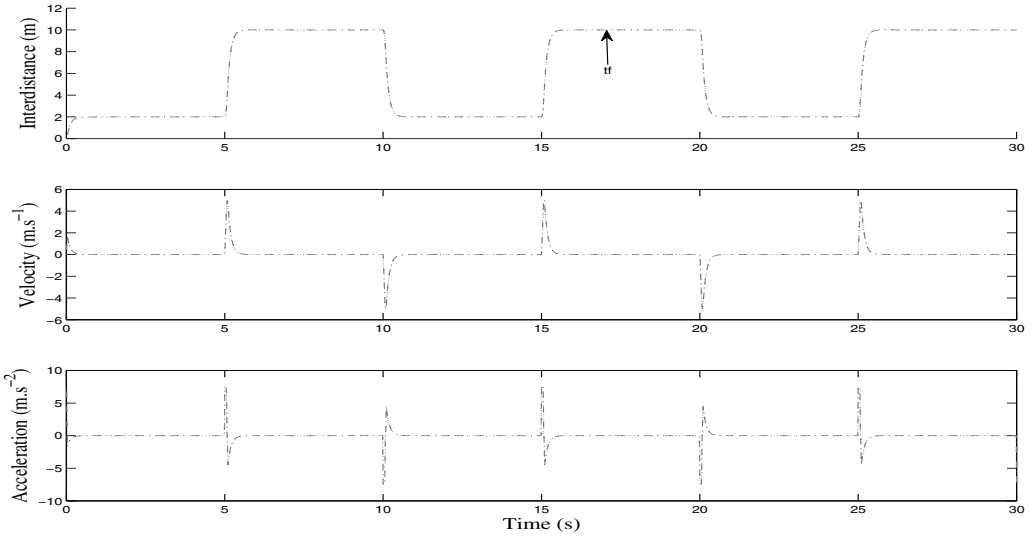



Fig. 4. Interdistance position, velocity and acceleration for a given reference signal.

*Techniques and Applications, London, UK*, pp. 1/1–1/4.

Maciejowski, J. (2002). *Predictive Control with Constraints*, Prentice-Hall, Pearson Education Limited, Harlow.

Martínez, J.J. and de Wit, C.C. (2004). Model reference control approach for safe longitudinal control, *Proceedings of the 2004 American Control Conference, Boston, MA, USA,* Vol. 3, pp. 2757–2762.

Mayne, D.Q., Rakovic, S.V., Findeisen, R. and Allgöwer, F. (2006). Robust output feedback model predictive control of constrained linear systems, *Automatica* **42**(7): 1217–1222.

Mendonça, L., Vieira, S., Sousa, J. and da Costa, J.S. (2006). Fault accommodation using fuzzy predictive control, *Proceedings of the IEEE International Conference on Fuzzy Systems, Vancouver, BC*, pp. 1535–1542.

Mhaskar, P. (2006). Robust model predictive control design for fault-tolerant control of process systems, *Industrial & Engineering Chemistry Research* **45**(25): 8565–8574.

Mhaskar, P., Gani, A. and Christofides, P. (2006). Fault-tolerant control of nonlinear processes: Performance-based reconfiguration and robustness, *International Journal of Robust Nonlinear Control* **16**(3): 91–111.

Ocampo-Martinez, C. and Puig, V. (2008). Fault-tolerant control model predictive control within the hybrid systems framework: Application to sewer networks, *International Journal of Adaptive Control and Signal Processing* **23**(8): 757–787.

Patwardhan, S., Manuja, S., Narsimhan, S. and Shah, S. (2006). From data to diagnosis and control using generalized orthonormal basis filters, Part II: Model predictive and fault tolerant control, *Journal of Process and Control* **16**(2): 157–175.

Pranatyasto, T.N. and Qin, S. (2001). Sensor validation and process fault diagnosis for FCC units under MPC feedback, *Control Engineering Practice* **9**(8): 877–888.

Rawlings, J.B. and Mayne, D.Q. (2009). *Model Predictive Control: Theory and Design*, Nob Hill Publishing, Madison, WI.

Seron, M., Zhuo, X., De Doná, J. and Martínez, J. (2008). Multisensor switching control strategy with fault tolerance guarantees, *Automatica* **44**(1): 88–97.

Sheng-Qi, S., Dong, L., Lin, L. and Shu-Sheng, G. (2008). Fault-tolerant control for constrained linear systems based on MPC and FDI, *International Journal of Information and Systems Sciences* **4**(4): 512–523.

Sun, S. and Deng, Z. (2008). Distributed optimal fusion steady-state Kalman filter for systems with coloured measurement noises, *International Journal of Systems Science* **36**(3): 113–118.

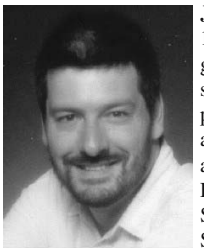
Yetendje, A., De Doná, J. and Seron, M. (2011). Multisensor fusion fault-tolerant control, *Automatica* **47**(7): 1461–1466.

Yetendje, A., Seron, M. and De Doná, J. (2010). Robust MPC design for fault tolerance of constrained multisensor linear systems, *Conference on Control and Fault-Tolerant Systems (SysTol' 10), Nice, France*, pp. 752–758.

Yetendje, A., Seron, M., De Doná, J. and Martínez, J.J. (2010). Sensor fault-tolerant control of a magnetic levitation system, *International Journal of Robust and Nonlinear Control* **20**(18): 2108–2121.

**Alain Yetendje** received the Master by Research degree in computer sciences and control theory from Paul Cezanne Aix-Marseille III University, France (2007), the M.Sc. degree in industrial engineering from Marseille Polytechnic University, France (2007), and the Ph.D. in electrical engineering from the University of Newcastle, Australia (2011). His research interests include fault tolerant control, diagnosis, set invariance, and robust constrained control.

**Maria M. Seron** received the Electronic Engineer degree from Rosario National University, Argentina, in 1988 and the Ph.D. degree from the University of Newcastle, Australia, in 1996. In the years 1997–1998, she held post doctoral positions in Belgium, Australia and the USA. From 1999 to 2002, she was an associate professor with the Department of Electronic Engineering, Rosario National University. Since 2002, she has been an Australian Research Fellow with the Centre for Complex Dynamic Systems and Control, University of Newcastle. Her research interests include constrained control, fault tolerant control and hybrid systems.



**José A. De Doná** received his B.E. degree in 1989 from Comahue National University, Argentina, and his Ph.D. in 2000 from the University of Newcastle, Australia. In 2000 he held a postdoctoral position in the Universities of Liege and Gent, Belgium. In 2001 he held a research academic position with the Centre for Integrated Dynamics and Control, University of Newcastle. Since 2002 he has been a senior lecturer with the School of Electrical Engineering and Computer Science, University of Newcastle. In 2008/2009 he held a visiting academic position at Mines ParisTech Graduate School, France. His research interests include constrained control and estimation, model predictive control, nonlinear control and fault tolerant control systems.

Received: 9 November 2010
Revised: 1 March 2011