Yetendje, Alain, De Doná, José A., Seron, Maria M., “Multisensor fusion fault tolerant control". Originally published in Automatica Vol. 47, Issue 7, p. 1461-1466 (2011).

Available from: http://dx.doi.org/10.1016/j.automatica.2011.02.024

# Multisensor Fusion Fault Tolerant Control

Alain Yetendje, José A. De Doná, Maria M. Seron

*ARC Centre of Excellence for Complex Dynamic Systems and Control (CDSC), School of Electrical Engineering and Computer Science, The University of Newcastle, Callaghan, NSW 2308, Australia*

**Abstract**

In this paper, a multisensor fusion fault-tolerant control system with fault detection and identification via set separation is presented. The fault detection and identification unit verifies that for each sensors-estimator combination, the estimation tracking errors lie inside pre-computed sets and discards faulty sensors when their associated estimation tracking errors leave the sets. An active fault tolerant controller is obtained, where the remaining healthy estimates are combined using a technique based on the optimal fusion criterion in the linear minimum-variance sense. The fused estimates are then used to implement a state feedback tracking controller. We ensure closed-loop stability and performance under the occurrence of abrupt sensor faults. Experimental validation, illustrating the multisensor fusion fault tolerant control strategy is included.

*Key words:* Fault tolerant control, optimal estimate fusion, invariant sets, Kalman filter

## 1 INTRODUCTION

Multisensor strategies are a topic of current interest in the research community in order to improve systems reliability. Sensor fusion is one of the most used techniques for integrating data provided by various sensors, in order to obtain the best possible estimate [1]–[2]. However, less attention has been focused on the case when sensors are used in a *feedback* control system. As is the case for all automatic control system components, and sensors in particular, faults can deteriorate the performance and even jeopardize the stability of the whole system. Therefore, it is important to consider the fault tolerance capabilities of a control system at the design stage.

In this paper, we present an active fault tolerant control scheme consisting of multiple sensors-estimator combinations, a fault detection and identification (FDI) unit, an estimate fusion mechanism with reconfiguration capabilities and a state feedback controller with reference tracking. The FDI unit is based on invariant set computation (see, e.g., [3], [4]). The unit tests that for each sensors-estimator combination, the estimation tracking errors lie inside pre-computed "healthy" sets and discards faulty sensors when their associated estimation tracking errors leave the healthy sets to converge towards "under-fault" sets. The proposed technique is suitable for reference tracking problems, especially when the reference signal contains an offset component, since the latter makes possible the separation between healthy and under-fault sets. In the reconfiguration stage, the estimates deemed "healthy" by means of the FDI test are fused based on the optimal fusion steady-state Kalman filter proposed in [1]. The choice of this fusion filter rather than any other decentralised fusion method is motivated by the reduction of on-line computation requirements. Indeed, decentralised fusion time-varying Kalman filter algorithms [5], [6] yield large on-line computational burden resulting from on-line computation of Riccati equations, Kalman filter gains, and weighting matrices or covariances. In the case of the optimal fusion steady-state Kalman filter, on the other hand, gains and covariance matrices are constant and can be pre-computed off line. The optimal fusion steady-state Kalman filter is composed of two layers where the first layer has a netted parallel structure to determine the steady-state cross-covariance between any two faultless groups of sensors. Estimates and covariances of all local subsystems, and the cross-covariances among the local subsystems from the first fusion layer are fused in the second fusion layer to determine the optimal steady-state matrix weights required to obtain the optimal fusion steady-state estimate. Since the steady-state covariances, cross-covariance matrices and weights can be computed off-line for each healthy configuration considered, the on-line reconfiguration task simply consists of selecting the suitable optimal steady-state weighting matrix that corresponds to the healthy groups of sensors diagnosed by the FDI unit. Finally, the optimal fused estimate is used to implement a state feedback controller with integral action that achieves reference tracking. Proofs of fault tolerance and stability of the resulting closed-loop system are given under a set of conditions on the system parameters, such as disturbance bounds, reference signal offset and bounds, etc. Thus, the main contribution of this paper is twofold. Firstly, it provides an integrated strategy for fault tolerant control by adapting estimate fusion techniques and set-based FDI to work in combined form. Secondly, it endows the resulting combined scheme with guaranteed closed-loop stability properties under severe faults in the system sensor configuration. The multisensor fault tolerant control strategy developed in the present paper provides an alternative to a scheme previously reported by the authors in [7] and illustrated experimentally in [8], which relied on estimate switching. Compared with [7] and [8], the present approach has the advantage that estimate fusion (especially if designed according to an optimisation criterion) is generally considered to provide better and smoother estimates than estimate switching. Preliminary conference versions of some parts of this paper have been reported in [9], [10].

## 2 Multisensor fusion scheme

### *2.1 Plant and measurement system*

Consider the linear time-invariant discrete-time plant

$$x(t+1) = Ax(t) + Bu(t) + Ew(t) \tag{1}$$

where $A$, $B$ and $E$ are constant matrices with compatible dimensions, $x(t) \in \mathbb{R}^n$ is the system state, $u(t) \in \mathbb{R}^m$ is the control input and $w(t) \in \mathbb{R}^r$ is a process disturbance, which is componentwise bounded as [1]

$$|w(t)| \leq \overline{w}, \quad \text{for all } t \geq 0 \tag{2}$$

for some known constant nonnegative vector $\overline{w} \in \mathbb{R}^r$. We consider a bank of output equations that combine several sensor measurements as follows:

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

for $i = 1, \ldots, N$, where $y_i(t) \in \mathbb{R}^{p_i}$ is the measured output of the $i$th group of sensors; $\eta_i$, $\eta_i^F \in \mathbb{R}^{p_i}$ are measurement disturbances satisfying the bounds

$$|\eta_i(t)| \leq \overline{\eta}_i, \quad |\eta_i^F(t)| \leq \overline{\eta}_i^F, \quad \text{for all } t \geq 0 \tag{4}$$

where $\overline{\eta}_i \in \mathbb{R}^{p_i}$ and $\overline{\eta}_i^F \in \mathbb{R}^{p_i}$, for $i = 1, \ldots, N$, are known constant nonnegative vectors; and $I_{p_i}$ is the $p_i \times p_i$ identity matrix. The *fault matrix* $\Pi_i \in \mathbb{R}^{p_i \times p_i}$ in (3) characterises the sensor fault situation, and is described as follows:

$$\Pi_i = \begin{cases} I_{p_i} & \text{if all sensors are healthy} \\ \operatorname{diag}\{\pi_{i1}, \ldots, \pi_{ip_i}\} & \text{otherwise} \end{cases} \tag{5}$$

where $\pi_{ij} \in [0,1]$, for $j = 1, \ldots, p_i$. Notice in (3) that $\pi_{ij} < 1$ indicates that the $j$th sensor of the $i$th sensor group has lost effectiveness, and that $\pi_{ij} = 0$ corresponds to outage of the sensor. The pairs $(A, C_i)$ are assumed observable.

### *2.2 Optimal fusion steady-state Kalman estimator*

In accordance with the previous measurement equations, we consider a bank of $N$ steady-state Kalman estimators, where each estimator is associated with one group of sensors and is designed in order to estimate the states of the system (1). To obtain the Kalman estimators we assume, temporarily and only for design purposes, that the process disturbance $w(t)$ in (1) is a zero-mean Gaussian white-noise with covariance $Q$, and that the measurement disturbances $\eta_i$ in (3) are zero-mean Gaussian white-noises with covariances $R_i$, for $i = 1, \ldots, N$, uncorrelated from the process noise $w(t)$. (For the remainder of the paper, in connection with the FTC capabilities of the scheme, we will remove this assumption and only assume (2) and (4), with any stochastic description of the disturbances being possible but whose knowledge is not required.)

The steady-state estimators are then described by the following equations [1], [2]:

$$\hat{x}_i(t+1|t) = A\hat{x}_i(t|t) + Bu(t) \tag{6}$$

$$\hat{x}_i(t|t) = \hat{x}_i(t|t-1) + M_i[y_i(t) - C_i\hat{x}_i(t|t-1)] \tag{7}$$

where $M_i = P_i C_i^T (C_i P_i C_i^T + R_i)^{-1}$ is the optimal steady-state innovation gain, $P_i = A[P_i - P_i C_i^T (C_i P_i C_i^T + R_i)^{-1} C_i P_i]A^T + EQE^T$ is the steady-state prediction error variance matrix, $P_{ii} = P_i - P_i C_i^T (C_i P_i C_i^T + R_i)^{-1} C_i P_i$ is the steady-state estimation error variance matrix, and $P_{ij} = [I - M_i C_i][A P_{ij} A^T + EQE^T][I - M_j C_j]^T$ is the steady-state error cross-covariance between the $i$th and $j$th estimators.

The following result reported in [2] provides the optimal information fusion criterion in the linear minimum-variance sense.

**Lemma 2.1** *(Optimal steady-state fusion estimate, Theorem 1 in [2]). Let $\hat{x}_i(t|t)$, $i = 1, 2, \ldots, \ell$, be unbiased estimators of an $n$-dimensional vector $x(t)$. Let the estimation errors be*

$$\tilde{x}_i(t|t) \triangleq x(t) - \hat{x}_i(t|t) \tag{8}$$

[1] In the sequel, inequalities and absolute values are considered componentwise.

*Assume that $\tilde{x}_i(t|t)$ and $\tilde{x}_j(t|t)$, $(i \neq j)$ are correlated, and let the covariance $(P_{ii})$ and cross-covariance matrices $(P_{ij})$ be given by the expressions provided above, following equation (7). Then the optimal linear minimum-variance information fusion estimator is given by*

$$\hat{x}_{fus}(t) = \lambda_1 \hat{x}_1(t|t) + \lambda_2 \hat{x}_2(t|t) + \ldots + \lambda_\ell \hat{x}_\ell(t|t) \quad (9)$$

*where the optimal matrix weights $\lambda_i$, $i = 1, 2, \ldots, \ell$, are computed from*

$$\lambda = \Sigma^{-1} e (e^T \Sigma^{-1} e)^{-1} \quad (10)$$

*where $\lambda = [\lambda_1^T \; \ldots \; \lambda_\ell^T]^T$ and $e = [I_n \; \ldots \; I_n]^T$ are both $n\ell \times n$ matrices, and $\Sigma = (P_{ij})_{i,j=1,2,\ldots,\ell}$, is an $n\ell \times n\ell$ matrix.* ◦

Every estimator (6)–(7) independently estimates the states of system (1) and gives the unbiased state estimate $\hat{x}_i(t|t)$ to be used in the fusion estimate (9). Only "healthy" estimates, as diagnosed by an FDI mechanism (described in Section 3 below), are fused. That is, for the configuration of groups of sensors deemed healthy by the FDI unit, the appropriate cross-covariance matrix is selected in the first fusion layer and the suitable optimal steady-state matrix weights are chosen in the second fusion layer in order to obtain the optimal fusion estimate.

Thus, the fusion estimate (9) is computed over only healthy groups of sensors, that is, groups whose indices are in the set

$$\mathbb{H} \triangleq \{i \in \{1, \ldots, N\} : \text{sensor group } i \text{ is healthy}\} \quad (11)$$

yielding

$$\hat{x}_{fus}(t) = \sum_{i \in \mathbb{H}} \lambda_i \hat{x}_i(t|t) \quad (12)$$

The optimal weights $\lambda_i$, $i \in \mathbb{H}$, are recomputed accordingly by taking, e.g., in (10), only subindices belonging to $\mathbb{H}$.

### 2.3 Prediction and estimation errors

We define the prediction errors as

$$\tilde{x}_i(t|t-1) \triangleq x(t) - \hat{x}_i(t|t-1) \quad (13)$$

Provided the $i$th group of sensors is healthy (i.e., $\Pi_i = I_{p_i}$), the associated prediction error (13) satisfies, using (1), (3) [with $\Pi_i = I_{p_i}$], (6) and (7)

$$\tilde{x}_i(t+1|t) = (A - AM_iC_i)\tilde{x}_i(t|t-1) + \begin{bmatrix} E & -AM_i \end{bmatrix} \begin{bmatrix} w(t) \\ \eta_i(t) \end{bmatrix} \quad (14)$$

Note that, due to observability of the pair $(A, C_i)$, for $i = 1, \ldots, N$, the matrices

$$A_{M_i} \triangleq A - AM_iC_i \quad (15)$$

are Schur [2] matrices. Hence, the prediction errors $\tilde{x}_i$ associated to healthy groups of sensors are bounded whenever $w$ and $\eta_i$ are bounded. Moreover, using the procedures in [3], [4], we can obtain invariant sets, denoted as $\Xi_i$, and ultimate bounds for the prediction errors of the form

$$|\tilde{x}_i(t|t-1)| \leq \overline{\tilde{x}}_i \quad (16)$$

where $\Xi_i$ and $\overline{\tilde{x}}_i$ are computed from equation (14) and the bounds (2) and (4) on the disturbance signals.

Note from (3) [with $\Pi_i = I_{p_i}$], (7), (8) and (13) that the estimation errors satisfy

$$\tilde{x}_i(t|t) = (I_n - M_iC_i)\tilde{x}_i(t|t-1) - M_i\eta_i(t) \quad (17)$$

Using the bounds (4) and (16), we can find ultimate bounds for $\tilde{x}_i(t|t)$ in (17) as:

$$|\tilde{x}_i(t|t)| \leq \overline{\tilde{x}}_i{}' \triangleq |I_n - M_iC_i|\overline{\tilde{x}}_i + |M_i|\overline{\eta}_i \quad (18)$$

### 2.4 Feedback tracking control

The control objective is to track a reference signal $x_{ref}$ that satisfies the following dynamics:

$$x_{ref}(t+1) = Ax_{ref}(t) + Bu_{ref}(t) \quad (19)$$

We consider that the reference signals are bounded according to the following assumption.

**Assumption 2.2** *The input reference $u_{ref}(t)$ and the state reference $x_{ref}(t)$ are bounded signals. In particular, constant vectors $x_{ref,0} \in \mathbb{R}^n$ and $\bar{x}_{ref} \in \mathbb{R}^n$ are known such that, for all discrete time instants $t \geq 0$, $x_{ref}(t) \in X_{ref} \triangleq \{x \in \mathbb{R}^n : |x - x_{ref,0}| \leq \bar{x}_{ref}\}$.* ◦

To achieve the reference tracking goal, we will employ a feedback tracking controller with integral action. Let us denote by $\sigma \in \mathbb{R}^q$ the integral action state, defined by

$$\sigma(t+1) = \sigma(t) + T_s(C^* x_{ref}(t) - y^*(t)) \quad (20)$$

where $T_s$ is a scalar constant (typically taken as the sampling period when (1) is the discretisation of a continuous-time system) and $y^*(t) = C^*x(t) + \eta^*(t)$, with $y^*(t) \in \mathbb{R}^q$, $\eta^* \in \mathbb{R}^q$, and $|\eta^*(t)| \leq \bar{\eta}^*$, is a system measured output not affected by faults (typically, measurements that the system cannot afford to lose without affecting detectability).

[2] A Schur matrix is a square matrix with real entries and with eigenvalues of magnitude less than one.

**Remark 2.3** *Notice that, since $\hat{x}_{fus}$ obtained from* (11)–(12) *is computed over only healthy groups of sensors, a valid alternative would be to define the integral action as $\sigma(t+1) = \sigma(t) + T_s C(x_{ref}(t) - \hat{x}_{fus}(t))$ where $C$ is a matrix defining a "performance" output of particular interest.* ◦

We define the plant tracking error, $z(t)$, the integrator-augmented plant tracking error, $\xi(t)$, the prediction tracking errors, $\hat{\xi}_i(t|t-1)$, and the estimation tracking errors, $\hat{\xi}_i(t|t)$, for $i = 1, \ldots, N$, as

$$z(t) = x(t) - x_{ref}(t) \tag{21}$$

$$\xi(t) = \begin{bmatrix} z(t) \\ \sigma(t) \end{bmatrix} \tag{22}$$

$$\hat{\xi}_i(t|t-1) = \hat{x}_i(t|t-1) - x_{ref}(t) \tag{23}$$

$$\hat{\xi}_i(t|t) = \hat{x}_i(t|t) - x_{ref}(t) \tag{24}$$

Note from (1), (19)–(22) that we can express the dynamics of the augmented system as:

$$\begin{aligned} \xi(t+1) = &\begin{bmatrix} A & 0 \\ -T_s C^* & I_q \end{bmatrix} \xi(t) + \begin{bmatrix} B \\ 0 \end{bmatrix} (u(t) - u_{ref}(t)) \\ &+ \begin{bmatrix} E & 0 \\ 0 & -T_s \end{bmatrix} \begin{bmatrix} w(t) \\ \eta^*(t) \end{bmatrix} \end{aligned} \tag{25}$$

Note from (7) that the prediction and estimation tracking errors are related as

$$\hat{\xi}_i(t|t) = \hat{\xi}_i(t|t-1) + M_i[y_i(t) - C_i \hat{x}_i(t|t-1)] \tag{26}$$

Also, using (12), the optimal fusion estimate tracking error is defined as

$$\hat{\xi}_{fus}(t) \triangleq \hat{x}_{fus}(t) - x_{ref}(t) \tag{27}$$

Using (8), (12), (21) and the fact that, from (10) (or the corresponding equation with subindices belonging to $\mathbb{H}$), $\sum_{i\in\mathbb{H}} \lambda_i = e^T \lambda = I_n$, the optimal fusion estimate tracking error (27) satisfies

$$\begin{aligned} \hat{\xi}_{fus}(t) &= \sum_{i\in\mathbb{H}} \lambda_i \hat{x}_i(t|t) - \sum_{i\in\mathbb{H}} \lambda_i x_{ref}(t) \\ &= \sum_{i\in\mathbb{H}} \lambda_i (z(t) - \tilde{x}_i(t|t)) = z(t) - \sum_{i\in\mathbb{H}} \lambda_i \tilde{x}_i(t|t) \end{aligned} \tag{28}$$

The variable $\hat{\xi}_{fus}(t)$ is then applied in a state feedback tracking controller, as follows,

$$\begin{aligned} u(t) &= -K_1 \hat{\xi}_{fus}(t) - K_2 \sigma(t) + u_{ref}(t) \\ &= -K\xi(t) + K_1 \sum_{i\in\mathbb{H}} \lambda_i \tilde{x}_i(t|t) + u_{ref}(t) \end{aligned} \tag{29}$$

where $K = \begin{bmatrix} K_1 & K_2 \end{bmatrix}$ is a stabilising gain obtained via a suitable state feedback design technique (e.g. LQR) for the system (25). To this end, we make the following standard assumption in reference tracking applications (see, e.g., [13] for an equivalent condition in terms of the original system (1) and integral action (20)).

**Assumption 2.4** *The augmented system* (25) *is assumed to be stabilisable, and the design of $K = \begin{bmatrix} K_1 & K_2 \end{bmatrix}$ is assumed to be performed accordingly, such that*

$$A_{cl} = \begin{bmatrix} A - BK_1 & -BK_2 \\ -T_s C^* & I_q \end{bmatrix} \tag{30}$$

*is a Schur matrix.* ◦

This property will be used for the analysis in Section 3.

## 3 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 estimation tracking errors (24) remain under healthy operation, from "under-fault" sets, towards which the estimation tracking errors jump when abrupt sensor faults occur in one or more groups of sensors. The computation of these sets, as well as the derivation of conditions to achieve the aforementioned separation, requires the analysis of the closed-loop system dynamics under the proposed fusion-estimate-based feedback controller both for healthy and under-fault operation. In this analysis, performed in the following subsections, we will assume that the FDI correctly identifies the faulty groups of sensors, so that the fusion estimate (12) is only formed by estimations corresponding to healthy groups of sensors. Later, in Theorem 3.5, we will provide conditions that guarantee the correct selection of healthy groups of sensors by the FDI, thus validating the analysis.

In contrast with other schemes, (see, e.g., [11], [12]), 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.

### *3.1 Closed-loop stability under healthy sensor fusion*

We first establish closed-loop stability of the multisensor fusion scheme described in Section 2 when only healthy sensors are used to compute the fused estimate (12). By using, (25), (29), (30) we obtain

$$\xi(t+1) = A_{cl}\xi(t) + \begin{bmatrix} BK_1 \\ 0 \end{bmatrix} \sum_{i\in\mathbb{H}} \lambda_i \tilde{x}_i(t|t) + \begin{bmatrix} E & 0 \\ 0 & -T_s \end{bmatrix} \begin{bmatrix} w(t) \\ \eta^*(t) \end{bmatrix} \tag{31}$$

Therefore, since $A_{cl}$ is a Schur matrix (see Assumption 2.4), and $\tilde{x}_i(k|k)$ (for healthy groups of sensors, cf.(18)) and $w(k)$ and $\eta^*(t)$ are bounded signals, it follows that the states of the system (31) are also bounded. Moreover, using the procedures in [3], [4], we can obtain an ultimate bound for the tracking error $\xi(t)$ of the form

$$|\xi(t)| \leq \overline{\xi} \tag{32}$$

where $\overline{\xi}$ is computed from the dynamic equation (31) and the bounds [3] (2), (18) and $\bar{\eta}^*$, on its input signals.

### *3.2 Prediction and estimation tracking errors associated with healthy sensors*

We develop the dynamics of the prediction tracking errors $\hat{\xi}_i(t|t-1)$ (see (23)), for $i \in \mathbb{H}$ (cf.(11)), in order to obtain attractive invariant sets and ultimate bounds for these variables and for the estimation tracking errors $\hat{\xi}_i(t|t)$ (see (24)) when only healthy sensors are used to compute the fused estimate (12). By using (3) [with $\Pi_i = I_{p_i}$], (6), (7), (19), (21)–(23), and (29) we obtain

$$\hat{\xi}_i(t+1|t) = A_{M_i}\hat{\xi}_i(t|t-1) + B_{i1}\xi(t) + B_{i2} \begin{bmatrix} \sum_{\ell\in\mathbb{H}} \lambda_\ell \tilde{x}_\ell(t|t) \\ \eta_i(t) \end{bmatrix} \tag{33}$$

where $A_{M_i}$ is as in (15) and $B_{i1} = [AM_iC_i - BK_1 \; -BK_2]$, $B_{i2} = \begin{bmatrix} BK_1 & AM_i \end{bmatrix}$. Note that the inputs to (33), namely,

$$w_i(t) \triangleq \left[ \xi^T(t) \;\; \sum_{\ell\in\mathbb{H}} (\lambda_\ell \tilde{x}_\ell(t|t))^T \;\; (\eta_i)^T(t) \right]^T \tag{34}$$

can be bounded componentwise as $|w_i(t)| \leq \overline{w}_i$ using the bounds (18), (32), and the bounds on the disturbances. Then, since the matrices $A_{M_i}$ are Schur, the prediction tracking error $\hat{\xi}_i(t|t-1)$ is also bounded. Using the procedure in [3], we can compute the following attractive invariant set for each healthy sensors-estimator combination in which, in the absence of sensor faults, the trajectories of (33) will remain if started inside or towards which they will converge if started outside:

$$\Omega_i = \left\{ \hat{\xi}_i \in \mathbb{R}^n : \left| V_i^{-1}\hat{\xi}_i \right| \leq r_i + \epsilon_i \right\} \tag{35}$$

where $A_{M_i} = V_i\Lambda_i V_i^{-1}$ is the Jordan decomposition of $A_{M_i}$, $r_i = (I_n - |\Lambda_i|)^{-1} \left| V_i^{-1} \begin{bmatrix} B_{i1} & B_{i2} \end{bmatrix} \right| \overline{w}_i$ and $\epsilon_i \in \mathbb{R}^n$ is any vector with (arbitrarily small) positive components. The set (35) can be refined by means of the contractive procedure of [4].

Next, substituting (3) (with $\Pi_i = I_{p_i}$) in (26), and using (13), we have that the estimation tracking errors (24), for $i \in \mathbb{H}$, satisfy

$$\hat{\xi}_i(t|t) = \hat{\xi}_i(t|t-1) + M_iC_i\tilde{x}_i(t|t-1) + M_i\eta_i(t) \tag{36}$$

Thus, $\hat{\xi}_i(t|t)$, for $i \in \mathbb{H}$, belongs to the set [4]

$$\Gamma_i \triangleq \Omega_i \oplus M_iC_i\Xi_i \oplus M_i\mathcal{N}_i \tag{37}$$

(where $\mathcal{N}_i$ is a bounding box associated with the noise bounds), whenever the prediction errors (13) belong to the invariant sets $\Xi_i$ defined in Section 2.3 and the prediction tracking errors (23) belong to the invariant set (35).

### *3.3 Conditions for fault tolerance*

Consider a fault in the $j$th group of sensors, characterised by a change of the fault matrix $\Pi_j$ in (3) from the identity matrix (healthy case, see (5)) to a new "under fault" value. At the time of the fault, substituting (3) into (26), and using (13) and (23), we have that the "under fault" estimation tracking error $\hat{\xi}_j^F(t|t)$ satisfies

$$\begin{aligned} \hat{\xi}_j^F(t|t) = {} & [I_n + M_j(\Pi_j - I_{p_j})C_j]\hat{\xi}_j(t|t-1) \\ & + M_j(\Pi_j - I_{p_j})C_jx_{ref}(t) + M_j\Pi_jC_j\tilde{x}_j(t|t-1) \\ & + M_j[\Pi_j\eta_j(t) + (I_{p_j} - \Pi_j)\eta_j^F(t)] \end{aligned} \tag{38}$$

Thus, provided the prediction tracking error $\hat{\xi}_j(t|t-1)$ defined in (23) belongs to the invariant set (35) and the prediction error (13) belongs to the invariant set $\Xi_j$ defined in Section 2.3, then the estimation tracking error $\hat{\xi}_j^F(t|t)$ at the time of the fault belongs to the following set

$$\begin{aligned} \Gamma_j^F(\Pi_j) \triangleq {} & [I_n + M_j(\Pi_j - I_{p_j})C_j]\Omega_j \\ & \oplus M_j(\Pi_j - I_{p_j})C_jX_{ref} \oplus M_j\Pi_jC_j\Xi_j \\ & \oplus M_j\Pi_j\mathcal{N}_j \oplus M_j(I_{p_j} - \Pi_j)\mathcal{N}_j^F \end{aligned} \tag{39}$$

[3] Note, in particular, that the bound (18) applies, since we have assumed that only healthy sensors take part in the fusion estimate. This situation will be later guaranteed by the FDI Criterion 3.4 and the corresponding analysis in Section 3.3

[4] The symbol $\oplus$ denotes the Minkowski sum of sets.

where $X_{ref}$ is as in Assumption 2.2 and $\mathcal{N}_j$ and $\mathcal{N}_j^F$ are bounding boxes associated with the noise bounds (4). Note that expressions (38)–(39) coincide with (36)–(37) in the healthy case (when $\Pi_j = I_{p_j}$).

To ensure that the sets $\Gamma_i$ and $\Gamma_i^F(\Pi_i)$ characterise the estimation tracking errors under healthy operation and at the time of the fault, respectively, we assume the following.

**Assumption 3.1** *Before the occurrence of any sensor fault, the system has been operating under healthy condition for a sufficiently long time such that all the prediction error trajectories are inside the attractive invariant sets $\Xi_i$ defined in Section 2.3 and all prediction tracking error trajectories are inside the attractive invariant sets $\Omega_i$ defined in* (35)*, for $i = 1, \dots, N$. Moreover, we assume that at least one group of sensors (which may consist of just one sensor) is operational at all times.* ○

In order to ensure an effective fault detection and identification by the FDI criterion, given later, we need to verify that the sets $\Gamma_j$ and $\Gamma_j^F(\Pi_j)$ are separated.

**Assumption 3.2** *The condition $\Gamma_j \cap \Gamma_j^F(\Pi_j) = \emptyset$ holds for all $j = 1, \dots, N$, for any of the possible values*[5] *of the fault matrix $\Pi_j$ characterising the considered fault situation for the $j$th group of sensors.* ○

Note that the sets $\Gamma_i$ given by (37) are centred at 0 (this is so because the sets $\Omega_i$ given in (35); $\Xi_i$ defined by the dynamics (14); and $\mathcal{N}_i$ defined as a bounding box associated with the noise bounds (4), are all centred at 0). The set $\Gamma_j^F(\Pi_j)$ defined in (39), on the other hand, is offset around a centre point $c_j(\Pi_j)$ given by

$$c_j(\Pi_j) = M_j(\Pi_j - I_{p_j})C_j x_{ref,0} \tag{40}$$

where $x_{ref,0}$ is as in Assumption 2.2. Thus, the reference offset $x_{ref,0}$—which in turn shifts the centre $c_j(\Pi_j)$ in (40)—provides a mechanism to achieve the set separation condition of Assumption 3.2. Notice from (40) that the value of the optimal steady-state innovation gain $M_j$ also affects the offset and, hence, is important in achieving set separation. In addition, $M_i$ influences the *size* of the sets through the matrix $A_{M_i}$ in (15) [see, e.g., the computation of the set $\Omega_i$ in (35)]. Notice, in particular, from the Riccati equations defining $M_i$, that the matrix gain depends on the values of the noise variances $Q$ and $R_i$. Since the approach followed in this paper is mainly deterministic, the aforementioned matrices $Q$ and $R_i$ can be treated as "design parameters" that can be chosen so as to aid set separation.

[5] Note that, depending on the problem characteristics, more than one value of the fault matrix $\Pi_j$ can be considered for the $j$th group of sensors.

**Remark 3.3** *Notice that Assumption 3.1 guarantees that when the fault in the $j$th sensor group occurs at some time instant $t$, $\tilde{x}_j(t|t-1)$ is in $\Xi_j$ and $\hat{\xi}_j(t|t-1)$ is in $\Omega_j$ (the invariant sets corresponding to the healthy operation of the $j$th sensor). Hence we have from* (39) *that, at the time of the fault, $\hat{\xi}_j^F(t|t) \in \Gamma_j^F(\Pi_j)$. Combining this condition with Assumption 3.2, we conclude that the $i$th group of sensors, for $i \in \{1, \dots, N\}$, is healthy at any time $t$ (and thus can be fused) if $\hat{\xi}_i(t|t) \in \Gamma_i$; and that the moment $\hat{\xi}_i(t|t)$ leaves the set $\Gamma_i$ 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 3.4 (FDI)** *At each time step, for each $i = 1, \dots, N$: if the estimation tracking error satisfies $\hat{\xi}_i(t|t) \in \Gamma_i$ then the $i$th group of sensors is deemed healthy and considered for fusion in* (12)*; if $\hat{\xi}_i(t|t) \notin \Gamma_i$ then the $i$th group of sensors is deemed faulty and discarded for all future times.* ○

We then have the following result.

**Theorem 3.5** *Under the conditions stated in Assumptions 2.2, 2.4, 3.1 and 3.2, the system* (1) *with control* (29) *reconfigured by the use of the FDI Criterion 3.4 to select the index set $\mathbb{H}$ in* (11) *[used to compute the optimal fused estimates* (12)*], preserves closed-loop stability whenever a $j$th group of sensors fails with fault matrix $\Pi_j$. Moreover, in the absence of disturbances and measurement noise in the healthy sensors, the integrator-augmented tracking error $\xi(t)$ defined in* (22) *converges asymptotically to zero.*

*Proof:* As explained in Remark 3.3, Assumptions 3.1 and 3.2 guarantee that the FDI Criterion 3.4 only selects healthy groups of sensors to compute the optimal fused estimates (12) used in the control law (29). Thus, the analysis of Sections 3.1 to 3.3 is validated, achieving the desired boundedness and stability requirements.

Moreover, in the absence of disturbances, $w(t) \equiv 0$, and of measurement noise in healthy sensors, $\eta_i(t) \equiv 0$ for $i \in \mathbb{H}$ (this collection includes the noises affecting the measured output used in the integral action (20); that is, $\eta^*(t) \equiv 0$), we conclude from (14) and the stability of the matrix $A_{M_i}$, that the prediction errors $\tilde{x}_i(t|t-1)$ for $i \in \mathbb{H}$ converge asymptotically to zero. Equation (17) then implies that the estimation errors $\tilde{x}_i(t|t)$ also converge asymptotically to zero. Then, we have from (31) and Assumption 2.4 that $\xi(t)$ converges asymptotically to zero. The results then follows. □

In the following section we illustrate the simplicity and effectiveness of the proposed fusion fault tolerant control approach through an experimental example.

## 4 Experimental example

The Quanser Magnetic levitation system (MAGLEV) is a nonlinear electromagnetic suspension system acting on a solid one-inch-ball. It consists of an electromagnet, which can lift the ball from a post and sustain it in the air by counteracting the ball's weight with the electromagnetic force (see, e.g., [8], [14] for details). The states of the system consist of ball position, ball velocity and current intensity. The system is linearised around the equilibrium point $x_{eq} = \begin{bmatrix} 10\times 10^{-3} & 0 & 1.2690 \end{bmatrix}^T$ and discretised with sampling period $T_s = 2$ms, yielding a model of the form (1) with

$$A = \begin{bmatrix} 1.0018 & 0.0020 & 0 \\ 1.8011 & 1.0018 & -0.0301 \\ 0 & 0 & 0.9481 \end{bmatrix}; B = E = \begin{bmatrix} 0 \\ -0.0001 \\ 0.0047 \end{bmatrix}$$

The states of the system are measured via 2 "physical" sensors: a photo-sensitive sensor, $S_1$, which measures the ball elevation or position, and a current sensing resistor, $S_3$, which provides measurements of the coil current. The velocity measurement is obtained via a "soft" sensor (emulator), $S_2$, that operates by differentiating the ball position (this component is part of the standard setup provided by Quanser). We notice that, if the measurements provided by $S_1$ are lost (outage of the sensor), then the system is no longer observable. However, the outage of $S_2$ or $S_3$ does not affect observability as long as sensor $S_1$ remains functional. Thus, the following matrices are considered in the measurement equations (3)

$$C_1 = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix}; C_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}; C_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

The steady-state Kalman estimators parameters ($M_i$, $P_{ii}$, $P_{ij}$) are computed as explained in Section 2, with

$$M_1 = \begin{bmatrix} 0.9999 \\ 35.2560 \\ -37.1972 \end{bmatrix}, M_2 = \begin{bmatrix} 0.5674 & 0.1052 \\ 0.1052 & 0.7453 \\ 2.3208 & -3.5601 \end{bmatrix},$$
$$M_3 = \begin{bmatrix} 0.1131 & -0.0001 \\ 3.3924 & -0.0180 \\ 0 & 0.2399 \end{bmatrix}$$

The bounds on the process disturbances and measurement noises are taken as: $\bar{w} = 2\times 10^{-6}$, $\bar{\eta}_1 = 9\times 10^{-7}$, $\bar{\eta}_2 = \bar{\eta}_3 = \bar{\eta}_2^F = \bar{\eta}_3^F = 10^{-7}\times \begin{bmatrix} 9 & 5 \end{bmatrix}^T$.

The objective is for the first component of the state, corresponding to ball position, to track a square-like wave generated by (19). This results in a reference for the state vector, $x_{ref}(t)$, satisfying the following bounds: $\begin{bmatrix} 9\times 10^{-3} & -6\times 10^{-3} & 1.2108 \end{bmatrix}^T \leq x_{ref} \leq \begin{bmatrix} 11\times 10^{-3} & 6\times 10^{-3} & 1.3272 \end{bmatrix}^T$. The feedback gain $K = 10^5 \times \begin{bmatrix} -0.4714 & -0.0354 & 0.0203 & 1.6919 \end{bmatrix}$ is computed as described in Section 2.4 using LQR. We used $T_s = 2$ms and sensor $S_1$, that is, $C^* = C_1$, $\eta^* = \eta_1$, in the integrator equation (20). (Note that faults in sensor $S_1$ cannot be considered without losing system's detectability.) The following fault scenario is considered: all the sensors start under healthy operation, and an outage of Sensor $S_3$ occurs at time $t_F = 111s$ and remains in this state, so that the fault parameter in (3) is $\Pi_3 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$. Fig. 1 shows the set $\Gamma_3$ defined in (37) (top set centred at zero) and $\Gamma_3^F(\Pi_3)$ defined in (39) (bottom set centred away from zero). The set separation condition of Assumption 3.2 is satisfied for Sensor $S_3$, through its third component. A similar test is carried out for Sensor $S_2$, and the condition stated in Assumption 3.2 also holds. According to Theorem 3.5, we can conclude that the scheme preserves closed-loop stability whenever sensor $S_2$ or $S_3$ fails. Fig. 1 also shows the evolution of the estimation tracking error $\hat{\xi}_3(t|t)$ at times, $t_F^- = t_F - T_s$, $t_F$, and $t_F^+ = t_F + T_s$. At time $t_F^-$, $\hat{\xi}_3(t|t)$ belongs to $\Gamma_3$. At time $t_F$, it is shifted to the set $\Gamma_3^F(\Pi_3)$, making fault diagnosis possible. At the next sampling time $t_F^+$, the corresponding estimation tracking error jumps toward a different set (not represented). Fig. 2 shows the effectiveness of the scheme as the reference signal (dash-dotted red line) is tracked by the ball position (solid blue line) under the fault situation considered.

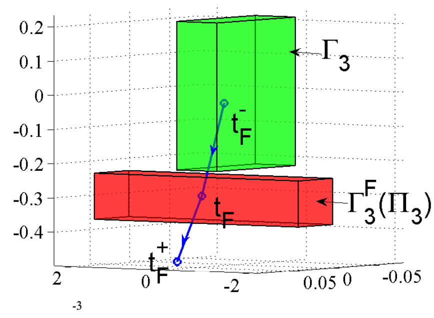


Fig. 1. Separation of sets representing healthy and faulty behaviour for MAGLEV's sensor $S_3$.

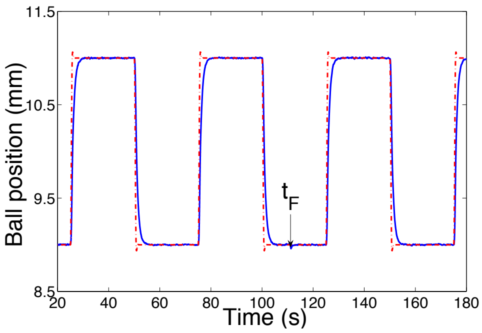


Fig. 2. Reference tracking for MAGLEV's ball position

## 5 Conclusion

In this paper, a multisensor fusion fault tolerant control strategy based on set separation to achieve fault detection and identification (FDI) is proposed. The FDI module provides a mechanism where the estimation tracking error of each sensor is tested for containment in a pre-computed "healthy" set. If the trajectories for an estimation tracking error jump to a pre-computed "under-fault" set, which is separated from the "healthy" one, the sensor is deemed to be faulty and is discarded from the closed-loop feedback control. The jump from a "healthy" to an "under-fault" set is guaranteed for all faults considered through a detailed analysis of the dynamics involved. Thus, only healthy sensor estimates are fused in a two-layer fusion scheme in order to obtain the optimal fusion estimate used by the controller. We have given conditions that guarantee closed-loop stability of the system in normal operation and under abrupt faults in some of the sensors. The experimental example presented in the paper confirms the effectiveness of the scheme in those situations.

## References


[1] S.L Sun and Z.L. Deng, Distributed optimal fusion steady-state Kalman filter for systems with coloured measurement noises, *International Journal of Systems Science*, Vol. 36, No. 3, 113–118, 20 February 2005

[2] S.L Sun and Z.L. Deng, Multisensor optimal information fusion Kalman filter, *Automatica*, 40, pp.1017–1023, 2004.

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

[4] S. Olaru, J.A. De Doná, and M.M. Seron. Positive invariant sets for fault tolerant multisensor control schemes. *Proceedings 17 IFAC World Congress*, Seoul, Korea, July 2008.

[5] Y. Zhu, ZH. You, J. Zhao, KS. Zhang, and XR. Li. The optimality for the distributed Kalman filtering fusion with feedback. *Automatica*, 37, 1489–1493, 2001.

[6] RK. Saha and KC. Chang. Efficient algorithm for multisensor track fusion. *IEEE Transactions on Aerospace and Electronic Systems*, 34(1), 200–210, 1998.

[7] MM. Seron , XW. Zhuo , JA. De Doná , and JJ. Martínez. Multisensor switching control strategy with fault tolerance guarantees. *Automatica* 2008; **44**(1): 88–97.

[8] A. Yetendje, M.M. Seron, and J.A. De Doná. Fault-Tolerant Switching Control of a Magnetic Levitation System. *Proceedings of 7th IFAC Safeprocess*, Barcelona, Spain, June 2009.

[9] J.A. De Doná, M.M. Seron, and A. Yetendje. Multisensor Fusion Fault-Tolerant Control with Diagnosis via a Set Separation Principle. *Proceedings 48th IEEE Conference on Decision and Control*, Shangai, China, December 2009.

[10] A. Yetendje, M. Seron, J.A. De Doná, Multisensor Fusion Fault- Tolerant Control of a Magnetic Levitation System *Proceedings of the 18th Mediterranean Conf. on Control and Automation*, Marrakech, Morocco, June 2010.

[11] C. Hajiyev and F. Caliskan. Sensor/actuator fault diagnosis based on statistical analysis of innovation sequence and robust Kalman filtering.*Aerosp. Sci. Technol.*, 4:415–422, 2000.

[12] E.C. Larson, B.E. Parker Jr, and B.R. Clark. Model-based sensor and actuator fault detection and isolation. *In Proceedings of the American Control Conference*, Anchorage, AK, May 2002.

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

[14] Quanser Inc. *Magnetic Levitation Plant Manual.* Markham, Ontario, Canada. 2006