Fault–Tolerant Observer Design with A Tolerance Measure for Systems with Sensor Failures

Cong Zhang[1], Imad M. Jaimoukha[1] and Felix Rafael Segundo Sevilla[2]

***Abstract*— A fault–tolerant switching observer design methodology is proposed. The aim is to maintain a desired level of closed–loop performance under a range of sensor fault scenarios while the fault–free nominal performance is optimized. The range of considered fault scenarios is determined by a minimum number p of assumed working sensors. Thus the smaller p is, the more fault tolerant is the observer. This is then used to define a fault tolerance measure for observer design. Due to the combinatorial nature of the problem, a semidefinite relaxation procedure is proposed to deal with the large number of fault scenarios for systems that have many vulnerable sensors. The procedure results in a significant reduction in the number of constraints needed to solve the problem. Two numerical examples are presented to illustrate the effectiveness of the fault–tolerant observer design.**

I. INTRODUCTION

The basic purpose of control system and observer design is to maintain a desired performance level despite the presence of uncertainty in the systems, e.g. faults in system devices, disturbances from the external environment. Furthermore, there always exists a trade-off between the achievable performance and the fault tolerance level.

There are two main types of fault tolerant control and observer (FTC/FTO) schemes: active and passive. In the passive fault tolerant design [1], the closed–loop system with a fixed controller is capable of dealing with all possible faults to guarantee normal operation. In the active scheme, the design is updated following the detected faults. These methods require fault detection and isolation (FDI) schemes to provide accurate information about the fault occurrence ([2]). [3] presents an overview of existing approaches to active FTC and FTO in terms of design methodologies and applications.

From the viewpoint of the state space representation of the considered system, the actuator or sensor faults are modeled as a diagonal gain matrix in series with the input and output distribution matrices. The diagonal values are in the range of 0-1 and indicate the effectiveness (or the loss) of the corresponding devices. This fault structure is popular as it can be conveniently incorporated with many mathematical design tools, such as adaptive control [4], generalized internal model control [5] and linear matrix inequality (LMI) design methods [6], [7]. Alternatively, the value is set as 0 or 1, where 0 models the faults in the actuators as the disconnection of the corresponding inputs in [8] while 1 corresponds to the normal operation of the actuator. This idea of disconnection is also employed when sensor faults occur in the design [9] and [10].

To tackle the computational issue in the design, some relaxation procedures are proposed. Due to the nature of the Takagi-Sugeno model in [7], the FTC solution is obtained by solving r^2 LMIs to address the stability constraints where r stands for the number of linear sub-models. The author uses Polyas theorem [11] to relax the problem formulation to one LMI. In [9], there are 2^m possible fault scenarios where m is the number of sensors. Since the faults are of binary-type, the widely used form for representing the norm-bounded structured uncertainty in [12] can be modified to transform the above 2^m LMIs to only one LMI.

[9] presents a FTO structure by considering the system with sensor faults using a linear parameter varying (LPV) system model with the uncertainty as binary type to allow the use of the results in [12]. This is of practical meaning in the FTO problem where all fault situations are regarded as failure and the corresponding model value is set as 0. Hence, it brings out specific fault scenarios. Unlike most of the reconfigurable design where the gain is calculated and switched for each fault case ([5], [7]), the strategy in [9] leads to a fixed observer gain with the switching only to incorporate the fault information. However, it is unlikely that all or most of devices of a large scale system fail simultaneously. The design in [9] sacrifices too much in the nominal performance in order to accommodate very unlikely fault scenarios.

The contribution of this paper is a methodology of fault–tolerant observer design with a fault tolerance measure. In addition to [9], this work adds a constraint that at least p sensors are working where no assumptions are made as to which particular sensors may fail at any one time. The resulting observer gain for one system will be given a measure for the fault tolerance level as p, i.e. choosing different gain will give the closed–loop system different fault tolerance capabilities. Thus if the system has a high probability of have at least p working sensors, the methodology presented here can help to obtain a single FTO gain to tolerate the most likely fault scenarios compared to [9].

II. THE FAULT-TOLERANT OBSERVER PROBLEM FORMULATION

A. Notation

The notation in this paper is standard. $A \prec \ (\succ)\ 0$ denotes that A is a negative (positive) definite matrix. For

[1]Cong Zhang and Imad M. Jaimoukha are with the Department of Electrical and Electronic Engineering at Imperial College London, London, UK cong.zhang12@imperial.ac.uk i.jaimouka@imperial.ac.uk

[2]Felix Rafael Segundo Sevilla is with the Zurich University of Applied Sciences ZHAW, Winterthur, Switzerland segu@zhaw.ch

a square matrix A, $\mathcal{H}(A) := A + A^T$. The symbol $\star$ in a matrix entry denotes a term that can be inferred from symmetry. $diag(A_1, A_2, \ldots, A_n)$ denotes a block diagonal matrix whose i^{th} diagonal block is A_i. $\mathcal{D}^m$ denotes the set of diagonal $m \times m$ matrices. Applying a congruence T, where T has full column rank, on $A \prec 0$ ($A \succ 0$) corresponds to pre– and post– multiplying by T and T^T respectively, to deduce that $T^T A T \prec 0$ ($T^T A T \succ 0$). A Schur complement argument refers to the result that if $A = A^T$ and $C = C^T \prec 0$ ($C = C^T$ and $A = A^T \prec 0$) then

$$\begin{bmatrix} A & B \\ B^T & C \end{bmatrix} \preceq 0$$

if and only if $A - BC^{-1}B^T \preceq 0$ ($C - B^T A^{-1} B \preceq 0$).

B. System Description

Consider the linear parameter varying (LPV) system model

$$\begin{aligned} \dot{x}(t) &= Ax(t) + B_u u(t) + B_d d(t) \\ y(t) &= \Delta(t) C x(t) + \Delta(t) D_d d(t) \\ z(t) &= C_z x(t) \end{aligned}$$

where $x(t) \in \Re^n$ is the state of the system, $u(t) \in \Re^{n_u}$ is the control input, $y(t) \in \Re^m$ is the measured output and $d(t) \in \Re^{n_d}$ is the disturbance to be attenuated. $z(t) \in \Re^{n_z}$ is the variable to be estimated. The matrices A, B_u, B_d, C, D_d and C_z are constant matrices of appropriate dimensions. The matrix $\Delta(t)$ is a diagonal matrix and is used to model sensor faults with $\Delta(t) \in \mathbf{\Delta}$ where

$$\mathbf{\Delta} := \{\Delta = diag(\delta_1, \ldots, \delta_m) : \delta_i \in \{0, 1\} \}. \qquad (1)$$

Thus $\Delta(t) = I_m$ if all sensors are working normally and $\Delta(t) = 0_m$ if all sensors fail. If a fault occurs, the loss of the i^{th} sensor can be modeled by setting the i^{th} element of $\Delta(t)$ equal to zero, i.e. $\delta_i(t) = 0$. There are 2^m possible combinations of sensor failures so that the set $\mathbf{\Delta}$ has 2^m elements. Note also that we assume that all sensors are vulnerable to fault. This assumption is made for simplicity of presentation since it is straightforward to modify our model to take account of sensors not vulnerable to faults.

We consider a state observer of the form:

$$\begin{aligned} \dot{\hat{x}}(t) &= A\hat{x}(t) + B_u u(t) - L(y(t) - \hat{y}(t)) \\ \hat{y}(t) &= \Delta(t) C \hat{x}(t) \\ \hat{z}(t) &= C_z \hat{x}(t) \end{aligned}$$

where $\hat{x}(t) \in \Re^n$ is the state of the observer, $\hat{y}(t) \in \Re^m$ is the output of the observer and $L \in \Re^{n \times m}$ is the observer gain to be designed while $\hat{z}(t)$ is the estimate of $z(t)$. The matrix $\Delta(t)$ contains the sensor fault information from the system hence this is an active, or switching observer.

Another simplification is made in the design: $\Delta(t)$ is assumed to be known using some suitable FDI scheme. For the switching observer, we define the state and signal estimate errors as $\tilde{x}(t) = x(t) - \hat{x}(t)$ and $\tilde{z}(t) = z(t) - \hat{z}(t)$, respectively. Then the transfer function from d to $\tilde{z}$ is

$$T_{\tilde{z}d}(\Delta) \stackrel{s}{=} \left[\begin{array}{c|c} A + L\Delta C & B_d + L\Delta D_d \\ \hline C_z & 0 \end{array}\right]. \qquad (2)$$

For $0 \leq p \leq m$, let

$$\mathbf{\Delta}_p := \{\Delta \in \mathbf{\Delta} : e^T \Delta e \geq p\}.$$

where $e = \begin{bmatrix} 1 & 1 & \cdots & 1 \end{bmatrix}^T \in \Re^m$. The set $\mathbf{\Delta}_p$ then defines all fault scenarios for which it is assumed that at least p sensors are working. When $p = 0$, $\mathbf{\Delta}_0 = \mathbf{\Delta}$ then models all possible fault scenarios and when $p = m$, $\mathbf{\Delta}_m = \{I_m\}$ models the nominal, fault free case.

The fault–tolerant observer (FTO) problem considered in this paper is to design an observer which, for any p, achieves a minimum level of performance for all fault combinations modeled by $\mathbf{\Delta}_p$. Since the expectation is that the observer will mostly operate under the nominal (fault-free) condition, we therefore require, in addition, to optimize the fault free performance. The performance objective is disturbance rejection and the performance index is chosen to be the $\mathcal{H}_\infty$– norm of the transfer matrix between the disturbance and estimation error given in (2).

C. Problem Formulation

The following result gives sufficient conditions for quadratic stability (Q-stability) and induced Q-performance [9], [13] for LPV systems and forms the basis for our problem formulation. The proof can be found in the above references.

Lemma 1: Let all definitions be as above and let $0 \leq p \leq m$ be given. The LPV system $T_{\tilde{z}d}(\Delta)$ is Q-stable and $\|T_{\tilde{z}d}(\Delta)\|_{i,2} < \gamma$ if there exists $P = P^T \in \Re^{n \times n}$ such that $P \succ 0$ and

$$\begin{bmatrix} \mathcal{H}\{P(A + L\Delta C)\} & P(B_d + L\Delta D_d) & C_z^T \\ \star & -\gamma I & 0 \\ \star & \star & -\gamma I \end{bmatrix} \prec 0, \forall \Delta \in \mathbf{\Delta}_p$$

□

Problem: Let $\gamma_F > 0$ (faulty performance level) and $\gamma > 0$ (nominal performance level) be given and let all other variables be as defined above. We seek $L \in \Re^{n \times m}$ such that

- $\|T_{\tilde{z}d}(\Delta = I_m)\|_\infty < \gamma$
- $T_{\tilde{z}d}(\Delta)$ is Q-stable and $\|T_{\tilde{z}d}(\Delta)\|_{i,2} < \gamma_F$

□

Such a matrix L will be called a fault–tolerant observer gain with a fault tolerance level p or FT_p observer gain for short. The parameter p represents a fault tolerance measure with FT_0 denoting maximally fault–tolerant observers while FT_m denoting the nominal non–fault–tolerant (NFT) observer.

Lemma 1 can be used to give conditions for the solution to this problem. The nonlinearity PL can be linearized by defining a new matrix variable F in the following formulation.

Theorem 1: Let $0 \leq p < m$, $\gamma_F > 0$ and $\gamma > 0$ be given. Then $L \in \Re^{n \times m}$ is an FT_p observer gain if there exist $P = P^T \in \Re^{n \times n}$ and $F \in \Re^{n \times m}$ such that $P \succ 0$ and

the following LMIs

$$\begin{bmatrix} \mathcal{H}(PA+F\Delta C) & PB_d+F\Delta D_d & C_z^T \\ \star & -\gamma_F I & 0 \\ \star & \star & -\gamma_F I \end{bmatrix} \prec 0, \forall \Delta \in \mathbf{\Delta}_p \quad (3)$$

$$\begin{bmatrix} \mathcal{H}(PA+FC) & PB_d+FD_d & C_z^T \\ \star & -\gamma I & 0 \\ \star & \star & -\gamma I \end{bmatrix} \prec 0 \quad (4)$$

are satisfied, in which case $L = P^{-1}F$. □

Note that when the number of faulty sensors is sufficiently small such that the set $\mathbf{\Delta}_p$ can be enumerated, then Theorem 1 can be used directly for the fault–tolerant observer design. The main objective of this paper is to derive a tractable design method when that number is large and therefore enumerating $\mathbf{\Delta}_p$ is infeasible.

III. A SEMIDEFINITE RELAXATION PROCEDURE FOR FT$_p$ OBSERVER DESIGN

In order to provide a tractable solution for the computation of the FT$_p$ observer gain, this section will propose a semidefinite relaxation procedure.

The following result is needed for our relaxation.

***Lemma** 2:* Let $\mathbf{\Delta}$ and $\mathbf{\Delta}_p$ be as defined above.

1) For all $S \in \mathcal{D}^m$ and for all $\Delta \in \mathbf{\Delta}$, we have

$$\mathcal{Z}(\Delta, S) := \Delta S(I-\Delta)^T + (I-\Delta)S^T\Delta^T = 0. \quad (5)$$

2) For all $M \in \mathcal{D}^m$ and for all $\Delta \in \mathbf{\Delta_p}$, we have

$$\mathcal{Q}(\Delta, M) := (m-p)MM^T - (I-\Delta)Mee^TM^T(I-\Delta)^T \succeq 0, \quad (6)$$

$$\mathcal{P}(\Delta, M) := \frac{m-p}{2}\mathcal{H}(MM^T - \Delta MM^T) - (I-\Delta)Mee^TM^T(I-\Delta)^T \succeq 0. \quad (7)$$

Proof:

1) By the definition of $\mathbf{\Delta}$ in (1), the proof for (5) is straightforward.
2) The requirement that $\Delta \in \mathbf{\Delta}$ and $e^T\Delta e \geq p$ is equivalent to

$$m - p \geq e^T(I-\Delta)^T(I-\Delta)e.$$

Using a Schur complement, this is equivalent to

$$\begin{bmatrix} m-p & e^T(I-\Delta)^T \\ \star & I \end{bmatrix} \succeq 0.$$

Using a second Schur complement, this in turn is equivalent to

$$(m-p)I - (I-\Delta)ee^T(I-\Delta)^T \succeq 0.$$

Since $M(I-\Delta) = (I-\Delta)M$ for all diagonal M, effecting the congruence M on the last inequality gives (6).

Finally, effecting the congruence $(I-\Delta)$ on (6) gives (7) and proves the lemma.

□

The next theorem uses Lemma 2 in a relaxation procedure to derive sufficient conditions for the existence of an FT$_p$ observer gain in the form of linear matrix inequalities and is our main result.

***Theorem** 2:* Let $0 \leq p < m$, $\gamma_F > 0$ and $\gamma > 0$ be given. Then $L \in \Re^{n\times m}$ is an FT$_p$ observer gain if there exist $P = P^T \in \Re^{n\times n}$, $F \in \Re^{n\times m}$, scalar $\mu > 0$ and S, $M \in \mathcal{D}^m$ such that $P \succ 0$, (4) and

$$\begin{bmatrix} T_1+pT_2\{\mu I - \mathcal{H}(M)\}T_2^T & T_3^T+T_2S^T & T_2MH & 0 \\ \star & -\mathcal{H}(S) & -MH & M\sqrt{p} \\ \star & \star & -\mu I & 0 \\ \star & \star & \star & -\mu I \end{bmatrix} \prec 0 \quad (8)$$

are satisfied where

$$\left[\begin{array}{c|c} T_1 & T_2 \\ \hline T_3 & 0 \end{array}\right] := \left[\begin{array}{ccc|c} \mathcal{H}(PA) & PB_d & C_z^T & C^T \\ B_d^TP^T & -\gamma_F I & 0 & D_d^T \\ C_z & 0 & -\gamma_F I & 0 \\ \hline F^T & 0 & 0 & 0 \end{array}\right] \quad (9)$$

and where $H \in \Re^{m\times(m-1)}$ is defined by $HH^T = mI - ee^T$. In this case $L = P^{-1}F$.

Proof: Note first that since e is the m–dimensional vector of ones, $mI - ee^T \succeq 0$ and has rank $m-1$ so H is well defined. The inequalities in (3) can be rewritten in the form

$$T(\Delta) := T_1 + \mathcal{H}(T_2\Delta T_3) \prec 0, \forall \Delta \in \mathbf{\Delta}_p \quad (10)$$

where T_1, T_2 and T_3 are defined in (9). A computation verifies that, for all matrices $S \in \mathcal{D}^m$ and $M \in \mathcal{D}^m$, the following identity

$$T(\Delta) = -T_2\mathcal{Z}(\Delta, S)T_2^T - T_2\mathcal{P}(\Delta, M)T_2^T + \begin{bmatrix} I & T_2\Delta \end{bmatrix} \mathcal{L} \begin{bmatrix} I \\ \Delta^T T_2^T \end{bmatrix} \quad (11)$$

is satisfied, where $\mathcal{Z}(\Delta, S), \mathcal{P}(\Delta, M)$ and $T(\Delta)$ are defined in (5), (7) and (10), respectively, and where

$$\mathcal{L} := \begin{bmatrix} T_1 - pT_2MM^TT_2^T & T_3^T + T_2\hat{S}^T \\ \star & -\mathcal{H}(\hat{S}) \end{bmatrix} + \begin{bmatrix} T_2M & 0 \\ -M & M \end{bmatrix} \begin{bmatrix} HH^T & 0 \\ 0 & pI \end{bmatrix} \begin{bmatrix} T_2M & 0 \\ -M & M \end{bmatrix}^T \quad (12)$$

where $\hat{S} := S + M\frac{m+p}{2}M^T$. The first term on the right–hand side of (11) is zero for all diagonal S and all $\Delta \in \mathbf{\Delta}$ from (5) and the second term is negative semidefinite for all diagonal M and all $\Delta \in \mathbf{\Delta}_p$ from (7). It follows that a sufficient condition for (3) is the existence of P, F, M and S (of the appropriate dimensions and structure) such that $\mathcal{L} \prec 0$.

In order to eliminate the nonlinearities in the matrix inequality $\mathcal{L} \prec 0$, we proceed as follows. Since variables M and S are diagonal, we redefine S as $S := \hat{S}$.

Next, the last term in (12) can be linearized by taking Schur complements, leaving only the nonlinear term MM^T in the (1,1) entry: $-pT_2MM^TT_2^T$. This is replaced by the last three terms on the right–hand side of the identity

$$MM^T = (M-\sqrt{\mu}I)(M-\sqrt{\mu}I)^T + \sqrt{\mu}M^T + \sqrt{\mu}M - \mu I \quad (13)$$

which is satisfied for any scalar $\mu \geq 0$, and which, by ignoring the first term on the right–hand side of (13) and redefining $M := \sqrt{\mu} M$ gives (8) as a sufficient condition for $\mathcal{L} \prec 0$ and hence (3). This proves the theorem. □

***Remark** 1:* The theorem shows that the single LMI in (8) is a sufficient condition for the $(2^m - \sum_{k=1}^{p} C(m, k-1))$ LMIs in (3), where $C(a, b)$ denotes the number of b distinct combinations from a set of a elements, although it requires $2m + 1$ extra variables (in S, M and μ). Note that $(2^m - \sum_{k=1}^{p} C(m, k-1)) = 1048555$ when $m = 20$ and $p = 2$, and it is therefore infeasible to enumerate $\Delta \in \mathbf{\Delta}_p$ in (3) even for a moderately large number of sensors. □

***Remark** 2:* Since (8) is only a sufficient condition, it is relevant to comment on the sources of conservatism introduced. The first is the use of Lemma 2 since it gives only sufficient conditions. This may be ameliorated to some extent by e.g. incorporating (6) as well as (7) in the relaxation step in (11). However, in the interest of simplicity of presentation, this will not be pursued here. The second source of conservatism is the linearization step which ignores a nonnegative definite term in (13). This can be ameliorated by using the update algorithm outlined in Remark 5 below. □

***Remark** 3:* If only stability is required under sensor fault scenarios ($\gamma_F \to \infty$), then the definitions in (9) are replaced by

$$\left[\begin{array}{c|c} T_1 & T_2 \\ \hline T_3 & 0 \end{array}\right] = \left[\begin{array}{c|c} \mathcal{H}(PA) & C^T \\ \hline F^T & 0 \end{array}\right]$$

□

***Remark** 4:* Although our development was for fault tolerance in observer design, the results of Theorem 2 are general and are applicable to a wide range of problems provided they can be written in the widely used form in (10). As an example, consider the actuator fault–tolerant state feedback control design problem described by the LPV model

$$\begin{aligned} \dot{x}(t) &= Ax(t) + B_u \Delta(t) u(t) + B_d d(t) \\ z(t) &= C_z x(t) + D_z \Delta(t) u(t) \end{aligned}$$

where now $z(t)$ is the cost signal. Suppose that the state feedback control law $u = Kx$ is used to limit the induced 2–norm of the transfer function from disturbance to cost signal given by

$$T_{zd}(\Delta) \stackrel{s}{=} \left[\begin{array}{c|c} A + B_u \Delta K & B_d \\ \hline C_z + D_z \Delta K & 0 \end{array}\right].$$

Noting that this LPV system is the transpose of that in (2) shows that all our design procedure can be carried out directly for the state feedback tolerant controller design problem. In particular, we can define a FT_p state–feedback controller gain. □

***Remark** 5:* We have used the identity in (13) to obtain a tractable LMI solution by ignoring the first, nonnegative term on the right hand side. If an initial feasible solution M_0 can be obtained, then the use of the identity

$$\begin{aligned} MM^T = (M - \sqrt{\mu} M_0)(M - \sqrt{\mu} M_0)^T \\ + \sqrt{\mu} M_0 M^T + \sqrt{\mu} M M_0^T - \mu M_0 M_0^T \end{aligned}$$

suggests an update scheme to improve the nominal performance level γ. However, the details are omitted in the interest of brevity. □

***Remark** 6:* When $p = 0$, then (12) can be written as

$$\begin{bmatrix} T_1 & T_3^T + T_2 S^T \\ \star & -\mathcal{H}(S) \end{bmatrix} \prec - \begin{bmatrix} T_2 \\ -I \end{bmatrix} MHH^T M^T \begin{bmatrix} T_2^T & -I \end{bmatrix}$$

It follows that $M = 0$ is always a solution and the observer design problem formulation coincides with that in [9]. □

IV. ILLUSTRATIVE EXAMPLES

In this section, two examples are investigated to illustrate our FT_p methodology. The first one focuses on the design of a fault–tolerant observer dealing with potential sensor faults in a power transmission system. To highlight the advantage of our method in reducing the computational burden, a large scale random system is used in the second example, where a fault–tolerant observer is designed to stabilize a potentially faulty system.

A. Fault–Tolerant Observer Design for Power Transmission System

The 4^{th} order reduced equivalent of the Nordic power transmission system [14] will be chosen as the considered plant. The parameters of the system are

$$A = \begin{bmatrix} -0.096 & 1.931 & -0.082 & -0.420 \\ -1.975 & -0.104 & -0.237 & -0.826 \\ 0.230 & 0.375 & -0.097 & 3.232 \\ 0.526 & 0.874 & -3.241 & -0.207 \end{bmatrix}, B_u = \begin{bmatrix} -1.774 \\ -1.772 \\ 1.544 \\ 2.166 \end{bmatrix}$$

$$C = \begin{bmatrix} 1.161 & -1.431 & 0.104 & -0.777 \\ -0.574 & 0.618 & -0.147 & 0.287 \\ -0.796 & -0.346 & 1.086 & -1.364 \\ -0.802 & -0.341 & 1.073 & -1.381 \\ -0.119 & 0.156 & 0.100 & 0.188 \\ 0.421 & -0.671 & 0.114 & -0.447 \end{bmatrix}, D_d = \begin{bmatrix} 0.666 \\ -1.392 \\ -1.300 \\ -0.605 \\ -1.488 \\ 0.558 \end{bmatrix}$$

$$B_d = \begin{bmatrix} -0.330 & 0.795 & -0.784 & -1.263 \end{bmatrix}^T, C_z = \begin{bmatrix} 1 & 0 & 0 & 0 \end{bmatrix}$$

Although the open loop is stable, the loss of sensors will lead to poor tracking of states and, even worse, the overall system may become unstable. In this context, the performance of three types of observers will be compared. The first observer is solved with Theorem 1 in Section II, in which (3) contains $2^m - \sum_{k=1}^{p} C(m, k-1)$ LMIs that correspond to each fault case constrained by the fault tolerance measure p. In the software implementation, this realization needs a loop to enumerate all the fault scenarios. We label the results from this method with the subscript $_{\text{EXACT}_p}$. The second observer design uses Theorem 2 in Section III and the results will be labeled with the subscript $_{\text{FT}_p}$. When using the update iterative procedure outlined in Remark 5, the results are labeled with the subscript $_{\text{FTI}_p}$. For an initial solution, Theorem 2 is used to obtain M and μ. In all the designs, the integer p indicates that the closed–loop system can tolerate up to $(m - p)$ sensor failures.

TABLE I

OPTIMAL PERFORMANCE LEVEL FOR THE THREE DESIGN APPROACHES IN EXAMPLE *A* FOR DIFFERENT LEVELS OF p

p	0	1	2	3	4	5
γ_{EXACT_p}	1.1770	1.1715	0.7135	0.3455	0.1264	0.0150
γ_{FT_p}	1.1775	1.1775	1.1775	1.1187	0.5409	0.1761
γ_{FTI_p}	1.1775	1.1775	1.1477	0.7619	0.3148	0.0804

The desired performance level for the faulty system in the design, measured by γ_F, is first determined. The value used for γ_F is obtained by slightly increasing the value of the minimum γ obtained from optimizing the performance for all the fault scenarios. In this example, we increase the optimal level by 1%. Then, the value used is $\gamma_F = 2.8543$. Note that the smaller γ_F is, the worse the resulting optimized nominal performance level γ will be.

Since the number of vulnerable sensors is $m = 6$, there will be six designs with each approach. Each design assumes there exists at least p normally working sensors with p ranging from 0 to 5. When $p=0$, all sensor fault combinations are considered. In addition, if $p=6$, the result is obtained from solving the nominal LMI which is $\gamma_{\text{NFT}} = 4.2852 \times 10^{-10}$ where the subscript $_{\text{NFT}}$ means non fault–tolerant and the corresponding observer gain is given in [9] as L_{NFT}.

The observer gains are obtained by $L = P^{-1}F$. Hence, P should be well conditioned. However, P is nearly singular if $P \succ 0$ is satisfied at its minimum, which will lead to large numerical values for the observer gain. To deal with this issue, the condition number of P is evaluated. If it is larger than a certain value, in our case 10^4, we relax γ to $1.001 \times \gamma_{\text{optimal}}$ and resolve the problem by minimizing the condition number of P to guarantee a reasonable observer gain. In Example A, this extra step is carried out for γ_{EXACT_4}, γ_{EXACT_5} and γ_{FTI_5}.

The results of the optimized nominal performance levels from all considered design approaches with different values of p are displayed in Table I.

γ_{NFT} is nearly zero as none of the fault scenarios is taken into account. As can be seen from Table I, in each approach, the optimized nominal performance level decreases with increasing p as when p increases, the number of considered fault scenarios in the design decreases. The resulting decrease in the value of γ is not large for small p $(= 0, 1)$, as the considered fault scenarios are similar.

The results from the approach using the loop are regarded as the exact values since the method directly solves the primary problem while the other two approaches solve the relaxed problem. When p is small, the FT_p method tends to give similar nominal performance levels compared to the one based on the loop approach. However, when p is large, the nominal performance is worse. When adopting the update procedure, the resulting performance levels γ_{FTI_p}, shown in Table I, are closer to the values from the loop method compared to the ones with the FT_p method. This demonstrates that the iterative algorithm is required for a more accurate design.

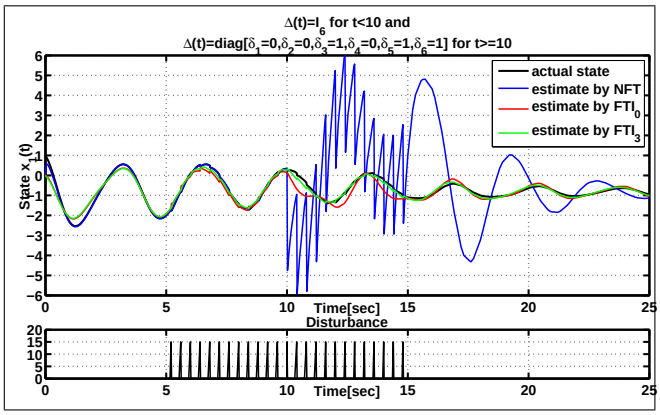

Fig. 1. State estimate comparison among the actual state, the non fault–tolerant (NFT) observer estimate and fault–tolerant observer with the tolerance level 0, 3 using an iterative process (FTI_0, FTI_3) estimates following a fault in the sensors 1,2,4 after 10sec

The results can also be compared to those in [9] where a procedure was developed to find an observer gain considering all fault scenarios. With that method, γ is 1.1775 which is slightly worse than the one from the loop but taking much less time to compute. This corresponds to FT_0, FTI_0 in our approach which gives the same γ as that obtained in [9].

Figure 1 illustrates the state–tracking property of three observer designs. The figure shows the actual state $z(t) = x_1(t)$ (black), and the estimated state $\hat{z}(t) = \hat{x}_1(t)$ using the NFT observer (blue), FTI_p observers. In the experiment, the input is set as 1, the disturbance is shown at the bottom of Figure 1 and the fault occurs in the sensors 1, 2, 4 after 10sec, i.e. $\Delta(t) = I_6, t < 10; \Delta(t) = diag(0, 0, 1, 0, 1, 1), t \geq 10$. Hence, 4 FTI_p designs with $p = 0, 1, \cdots, 3$ can be satisfactory. Here, the observers designed with the constraint $p = 0$ and $p = 3$ are chosen. The FT observer gains for these two fault–tolerance levels are given by L_{FTI_0} and

$$L_{\text{FTI}_3} = \begin{bmatrix} 1.027 & -1.014 & 0.116 & 2.554 & 0.291 & 0.429 \\ 2.251 & -1.598 & 0.255 & 2.445 & 0.837 & 0.614 \\ -4.186 & 3.518 & -0.508 & -4.988 & -1.703 & -1.255 \\ 3.769 & -3.045 & 0.325 & 7.365 & 0.583 & 1.122 \end{bmatrix}$$

where L_{FTI_0} is the same as the FTO design in [9] where the resulting observer gain was denoted as L_{FTMS}. All three observers can stabilize the closed–loop system for this specific fault scenario. The state estimates from FTI_0 and FTI_3 observer are shown in red and green respectively. As can be seen from Figure 1, before the faults at 10s, all state estimates track the actual state well, among which, the NFT observer performs the best as expected. However, after the fault occurrence, the state estimate using the NFT observer diverges from the actual state while the two FTI_p observers still do well in tracking, with L_{FTI_3} performing best, again as expected.

TABLE II

OPTIMAL PERFORMANCE LEVEL AND TIME COST RATIO FOR THE FTI_p AND LOOP APPROACHES AND THE NUMBER OF LMIS REQUIRED IN THE LOOP APPROACH IN EXAMPLE *B* FOR SOME VALUES OF p

p	1	2	3
γ_{FTI_p}	2.8467	0.4196	0.3355
TR_{FTI_p}	15	11	13
No. of LMIs in (3)	4095	4083	4017
p	6	7	11
γ_{FTI_p}	0.0487	0.9968×10^{-7}	0.4068×10^{-7}
TR_{FTI_p}	30	7	4
γ_{EXACT_p}	0.5812×10^{-8}	0.4219×10^{-8}	0.2069×10^{-8}
$\text{TR}_{\text{EXACT}_p}$	742	452	1
No. of LMIs in (3)	2510	1568	13

B. Fault–Tolerant Observer Design for a Large Scale System

This example highlights the effectiveness of our fault–tolerant observer design for systems that have a large number of vulnerable sensors. The loop approach is not feasible as explained in Remark 1 except for large p. Using our method even with the iterative process, the solution can be obtained at reasonable time cost. The system is randomly generated with $n = 6$ states, $m = 12$ vulnerable sensors, $n_d = 4$ and $n_z = 3$ and has one unstable pole. Since the system is unstable, we assume that $p > 0$. Although the system data are not given here because of lack of space, the results presented below are typical for such systems.

Table II lists the optimal nominal performance level from each design for several values of p. For the sake of comparison, the smallest time cost to obtain the exact design with fault tolerance level $p = 11$ is regarded as the unit 1. The table presents the time cost ratio (TR_) of each design to the standard one. Also shown are the numbers of LMIs required for the stability constraint in the loop method.

From Table II, it is obvious that the nominal performance level improves with increasing p. When p is small, it is not feasible to use the loop method since the number of fault scenarios is too large. However, when p is large, the number of required LMIs becomes smaller and the method gives better solutions with smaller values of γ's compared to the one solved by the FTI_p method. The last two lines of values in the bottom table show that the time cost increases with the number of LMIs in the loop approach. Note that the solution time is largely independent of the number of fault scenarios with the FTI_p method. A short time cost can also be expected if the number of sensors m reduces.

V. FUTURE WORK

The choice of p, the minimum number of assumed working sensors, as a measure of the fault tolerance capability of the observer assumes that all sensors have equal probability of developing a fault. A more general setting assigns a different probability for each sensor, and the problem then is to design an observer that tolerates all faults whose probability of occurring is above a threshold value.

In this work we have assumed a binary structure for the faults, that is, either a sensor is fully working ($\delta_i = 1$) or faulty ($\delta_i = 0$). A more general setting would consider several fault modalities. For example, assuming the ith sensor output is $y_i(t) = C_i x(t) + D_i d(t)$, then a fault model would assign $C_i \in \{C_i^0, \ldots, C_i^{m_i}\}$, and similarly with D_i, perhaps with a different probability for the occurrence of each fault mode.

In the control system design setting, our work is applicable to sensor or actuator fault–tolerance in the design of observers or state feedback controllers. A more general setting would be the design of dynamic controllers that are tolerant to sensor, actuator and process faults.

REFERENCES

[1] Z. Gao, B. Jiang, P. Shi and J. Liu, "Passive fault–tolerant control design for near-space hypersonic vehicle dynamical system, " Circuits Systems and Signal Processing, vol. 31, no. 2, pp. 565-581, Apr. 2012.

[2] J C. Tudon-Martinez, S. Varrier, O. Sename, R. Monrales-Menendez, J. Martinez and L. Dugard,"Fault tolerant strategy for semi-active suspensions with LPV accommodation," Conference on Control and Fault–Tolerant Systems, pp. 631-636, 2013.

[3] Y. Zhang and J. Jiang, "Bibliographical review on reconfigurable fault–tolerant control systems," Annual Reviews in Control, vol.32, no. 2, pp. 229-252, Dec 2008.

[4] H. Qiao, J. C. Liang and X. H. Chang, "Reliable and adaptive compensation controller design for continuous-time systems with actuator failures, " 2008 Chinese Control and Design Conference, pp. 4700-4705, 2008.

[5] D. U. Campos-Delgado and K. Zhou, "Reconfigurable fault–tolerant control using GIMC structure," IEEE Transactions on Automatic Control, vol. 48, no. 5, pp. 832-838, May 2003.

[6] Y. Cheng, B. Jiang, Y. Fu and Z. Gao, "Robust observer based reliable control for satellite attitude control systems with sensor faults" International Journal of Innovative Computing Information and Control, vol. 7, no. 7B, pp. 4149-4160, Jul. 2011.

[7] D. Ichalal, B. Marx, D. Maquin and J. Ragot, "New fault tolerant control strategy for nonlinear systems with multiple model approach," 2010 Conference on Control and Fault Tolerant Systems, Nice, France, pp. 606-611, October 6-8, 2010.

[8] F. Liao, J. Wang and G. Yang, "Reliable robust flight tracking control: An LMI approach" ISA Transactions on Control Systems Technology, vol.10, no.1, pp. 76-89, Jan. 2002.

[9] F. R. Segundo Sevilla, I. Jaimoukha, B. Chaudhuri and P. Korba, "A semidefinite relaxation procedure for fault–tolerant observer design," to appear, IEEE Transactions on Automatic Control, 2015.

[10] F. R. Segundo Sevilla, I. Jaimoukha, B. Chaudhuri and P.Korba, "Fault tolerant control design to enhance damping of inter-area oscillations in power grids," International Journal of Robust and Nonlinear Control, vol. 24, no. 8-9, pp. 1304-1316, May 2014.

[11] A. Sala and C. Arino, "Asymptotically necessary and sufficient conditions for stability and performance in fuzzy control: Applications of Polyas theorem," Fuzzy Sets and Systems, vol. 158, no. 24, pp. 2671 2686, 2007.

[12] L. E. Ghaoui and H. Lebret, "Robust solutions to least-squares problems with uncertain data," SIAM Journal on Matrix Analysis and Applications, vol. 18, no. 4, pp. 1035-1064, Oct. 1997.

[13] H. El-Zobaidi and I. M. Jaimoukha, "Robust control and model and controller reduction of linear parameter varying systems, " in Proceedings of the 37^{th} IEEE Conference on Decision and Control, vol. 3, pp. 3015-3020, 1998.

[14] N. Chaudhuri, A. Domahidi, R. Majumder, B. Chaudhuri, P. Korba, S. Ray and K. Uhlen, "Wide-area power oscillation damping control in Nordic equivalent system," IET Generation, Transmission & Distribution, vol. 4, no. 10, pp. 1139-1150, Oct. 2010.