A Semidefinite Relaxation Procedure for Fault–Tolerant Observer Design

Felix Rafael Segundo Sevilla, *Member, IEEE,* Imad M. Jaimoukha, Balarko Chaudhuri, *Senior Member, IEEE* and Petr Korba, *Senior Member, IEEE.*

***Abstract*—A fault–tolerant observer design methodology is proposed. The aim is to guarantee a minimum level of closed–loop performance under all possible sensor fault combinations while optimizing performance under the nominal, fault-free condition. A novel approach is proposed to tackle the combinatorial nature of the problem, which is computationally intractable even for a moderate number of sensors, by recasting the problem as a robust performance problem, where the uncertainty set is composed of all combinations of a set of binary variables. A procedure based on an elimination lemma and an extension of a semidefinite relaxation procedure for binary variables is then used to derive sufficient conditions (necessary and sufficient in the case of one binary variable) for the solution of the problem which significantly reduces the number of matrix inequalities needed to solve the problem. The procedure is illustrated by considering a fault–tolerant observer switching scheme in which the observer outputs track the actual sensor fault condition. A numerical example from an electric power application is presented to illustrate the effectiveness of the design.**

***Index Terms*—Estimation, fault–tolerant systems, LMIs, sensor failure, semidefinite relaxation.**

I. Introduction

NOWADAYS advanced systems are required to operate with high reliability in order to ensure safety and deliver good performance. Malfunction of system components such as senors, actuators or other system processes might lead to a degradation in the performance or even cause instability. In order to overcome these problems, fault–tolerant control is an area within control theory devoted to developing architectures that are capable of tolerating potential faults thus improving reliability while providing a desired performance [1].

Fault–tolerant architectures can be classified as either passive or active. In passive schemes, the architectures are fixed and provide robustness against a pre-defined set of faults. The main feature of this structure is that it does not require reconfiguration or fault detection schemes [2], [3], [4]. On the other hand, active architectures reconfigure their structure in order to maintain stability and guarantee acceptable performance following a malfunction of one or more components in the system [5], [6], [7], [8]. The main goal of fault–tolerant architectures is to achieve stability and a minimum level of performance not only when all components are working normally, but also in cases when there are malfunction in components. See [9] for an exhaustive literature review about fault–tolerant control theory.

In this work we consider active fault–tolerant architectures through observer–based state estimation to accommodate sensor faults using Linear Matrix Inequalities (LMIs) as a mathematical designing tool [4]. We propose a semidefinite relaxation approach to ameliorate the difficulty arising from the combinatorial nature of the problem [10], [11], [12] which results in a significant reduction in the number of inequalities to be considered, irrespective of the number of sensors. Moreover, the resulting observer design formulation is linear, obviating the need for iterative solutions. It is assumed that the exact sensor fault scenario is known (which is true for the power systems application considered in this work) and the corresponding outputs within the observers can thus be disconnected immediately. This assumption could be relaxed by using an appropriate sensor fault estimation technique [13].

Our two main contributions are first, the representation of all sensor faults as structured binary uncertainties analogous to the norm-bounded structured uncertainties used in robust control formulation [14], [15] and second, the formulation of the fault–tolerant observer design as a linear multi-objective optimization problem allowing the use of efficient solvers.

The paper is organized as follows: Section II provides a formulation of the problem. The description of the system is given and the design methodology is summarized. Also, a direct procedure to give conditions for the solution of the problem is derived and the main drawbacks of this method are discussed. The solution is given in the form of a linear algorithm, although it requires the solution of a large number of LMI problems, one for every combination of sensor faults. Section III presents our main result in Lemma 4, identifying our problem as an extension of the robustness results in [14], [15] to discrete uncertainties. Section IV presents a tractable solution to the problems introduced in Section II applying the results described in Lemma 4. Section V is an illustrative example from power systems where we demonstrate the effectiveness of the proposed design methodology. Finally, Section VI summarizes our results and suggests future investigations.

II. The fault–tolerant observer problem

In this section we review some background, give a formulation of the problem and present an initial solution.

F.R. Segundo Sevilla and P. Korba are with the Zurich University of Applied Sciences ZHAW, Winterthur, Switzerland (e-mail: *segu@zhaw.ch, petr.korba@zhaw.ch*).

I.M. Jaimoukha and B. Chaudhuri are with the Department of Electrical and Electronic Engineering at Imperial College London, London, UK (e-mail: *i.jaimouka@imperial.ac.uk, b.chaudhuri@imperial.ac.uk*).

A. Notation

The notation we use is fairly standard and is summarized here for convenience. $\Re$ denotes the set of real numbers, $\Re^n$ denotes the space of n-dimensional (column) vectors and $\Re^{n\times m}$ the space of all $n\times m$ matrices whose entries are in $\Re$. A^T denotes the transpose of A. $\mathrm{diag}(A_1,\ldots,A_m)$ denotes the block diagonal matrix whose ith diagonal block is A_i. The $n\times n$ identity matrix is denoted by I_n and the $m\times n$ null matrix by $0_{m,n}$ with the subscripts dropped if they can be inferred from context. If $A=A^T\in\Re^{n\times n}$, $\underline{\lambda}(A)$ denotes the smallest eigenvalue of A and we write $A\succ 0$ if $\underline{\lambda}(A)>0$. Analogous definitions apply to $\overline{\lambda}(A)$ and $A\prec 0$. Applying a congruence T, where T has full column rank, on an inequality $A\prec 0$ ($A\succ 0$) corresponds to pre- and post-multiplying by T to deduce $T^TAT\prec 0$ ($T^TAT\succ 0$). In a partitioned symmetric matrix, we occasionally use a $\star$ to denote an element easily inferred from symmetry. For a square matrix X, we define $\mathcal{H}(X)=X+X^T$. If $x(t)$ is a vector valued signal, we define the $\mathscr{L}_2$-norm of x as $\|x\|_2=\sqrt{\int_{-\infty}^{\infty}x(t)^Tx(t)dt}$. We denote the set of all vector valued signals with finite $\mathscr{L}_2$-norm as $\mathscr{L}_2$.

B. System description

Consider the linear parameter-varying (LPV) system

$$\begin{aligned}\dot{x}(t)&=Ax(t)+Bu(t)+B_dd(t),\\ y(t)&=\Delta(t)Cx(t)+\Delta(t)D_dd(t),\qquad z(t)=C_zx(t)\end{aligned}\tag{1}$$

where $x(t)\in\Re^n, u(t)\in\Re^{n_u}, y(t)\in\Re^{n_y}, d(t)\in\Re^{n_d}$ and $z(t)\in\Re^{n_z}$ represent the state, control input, measured output, disturbance and output to be estimated, respectively, and where A, B, B_d, C, D_d and C_z are the corresponding distribution matrices with appropriate dimensions. The parameter $\Delta(t)$ is a diagonal matrix and is used to model sensor faults with

$$\Delta(t)\in\mathbf{\Delta}:=\{\Delta=\mathrm{diag}(\delta_1,\ldots,\delta_{n_y}):\delta_i\in\{0,1\}\ \}.\tag{2}$$

Note that $\Delta(t)=I_{n_y}$ if there are no faults. The loss of sensor i is modeled by setting $\delta_i(t)=0$. Thus there are 2^{n_y} possible combinations of sensor failures so that $\mathbf{\Delta}$ has 2^{n_y} elements.

Remark 1: We make the following simplifications:

1) We assume that $\Delta(t)$ is known through suitable fault detection and isolation algorithms [16], [17].
2) Since we allow all switching combinations, including $\Delta(t)=0$, we assume that A is stable.

Although these assumptions can be relaxed, for example by using an estimate of $\Delta(t)$ [13], or assuming that the pair $(A,\Delta C)$ is observable for all $\Delta\in\mathbf{\Delta}$ [10], we will use these simplifications since our focus is on the combinatorial nature of the fault–tolerant estimation problem. ■

To estimate $z(t)$, we consider the state observer

$$\begin{aligned}\dot{\hat{x}}(t)&=A\hat{x}(t)+Bu(t)-L\left(y(t)-\hat{y}(t)\right),\\ \hat{y}(t)&=\hat{\Delta}(t)C\hat{x}(t),\qquad\qquad\hat{z}(t)=C_z\hat{x}(t)\end{aligned}\tag{3}$$

where $\hat{x}(t)\in\Re^n, \hat{y}(t)\in\Re^{n_y}, L\in\Re^{n\times n_y}$ are the observer state, output and gain, respectively and $\hat{z}(t)$ is the estimate of $z(t)$.

Remark 2: The choice of $\hat{\Delta}(t)$ and the dependence of the observer gain L on $\Delta(t)$ defines three types of observer:

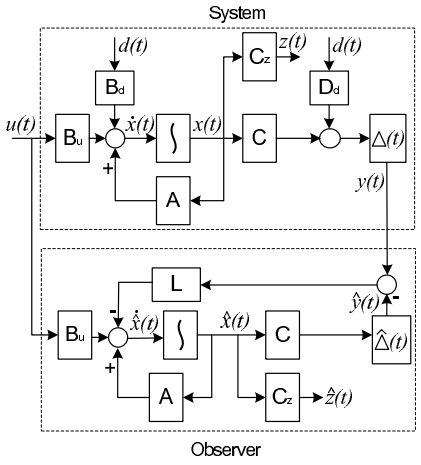

Fig. 1. Fault Tolerant Observer Structure

1) $\hat{\Delta}(t)=I_{n_y}$ and L depends on $\Delta(t)$: this defines an active (also called reconfigurable or full switching) observer.
2) $\hat{\Delta}(t)=I_{n_y}$ and L is fixed: this defines a passive observer.
3) $\hat{\Delta}(t)=\Delta(t)$ and L is fixed: this defines what we call a minimal switching observer [18]. Although the observer is reconfigurable, so that it is a switching observer, the switching is between the observer outputs using a fixed L, hence the designation minimal. ■

In this work, we only consider minimal switching observers since the active observer design problem consists of designing a separate observer for each fault scenario, a good approach can be found in [19], and this may not be feasible for some applications, such as the power transmission application we present below. The system (1) and observer (3) are shown in Figure 1. Although our approach can handle passive observers ($\hat{\Delta}(t)=I_{n_y}$ and L is fixed), the resulting design is too conservative since the estimation error dynamics include the control input as well as disturbances, and therefore the solution is not developed here in the interest of brevity. For the observer structure in Figure 1, define the estimation error as $\tilde{z}(t):=z(t)-\hat{z}(t)$. Then, for the minimal switching observer ($\hat{\Delta}(t)=\Delta(t)$), the estimation error dynamics are:

$$\left[\begin{array}{c}\dot{\tilde{x}}(t)\\ \hline \tilde{z}(t)\end{array}\right]=\left[\begin{array}{c|c}A+L\Delta(t)C & B_d+L\Delta(t)D_d\\ \hline C_z & 0\end{array}\right]\left[\begin{array}{c}\tilde{x}(t)\\ \hline d(t)\end{array}\right]\tag{4}$$

where $\tilde{x}(t):=x(t)-\hat{x}(t)$.

The fault–tolerant observer (FTO) problem is to design a stable observer which achieves a minimal level of performance, in terms of disturbance rejection, under all fault scenarios. Since the expectation is that the observer will mostly operate under the nominal (fault-free) condition, we therefore require, in addition, to optimize the performance in the fault-free case.

To formally capture these requirements, we give some results relating to the stability and performance of LPV systems.

C. LPV systems

LPV systems are a special class of linear time-varying systems where the time dependence enters the state equation

through exogenous parameters [20], [21], [22], [23]. A state-space description of an LPV system can be represented as

$$\left[\begin{array}{c}\dot{x}(t)\\ \hline y(t)\end{array}\right]=\left[\begin{array}{c|c}A(\Delta(t)) & B(\Delta(t))\\ \hline C(\Delta(t)) & D(\Delta(t))\end{array}\right]\left[\begin{array}{c}x(t)\\ \hline u(t)\end{array}\right] \quad (5)$$

where the distribution matrices $A(\cdot), B(\cdot), C(\cdot)$ and $D(\cdot)$ are functions of the parameter $\Delta(t)$, assumed to be measurable at time t and which belongs to a parameter space $\mathbf{\Delta}(t)$. We recall the definition of quadratic stability (Q-stability) and induced $\mathscr{L}_2$ Q-performance and give sufficient conditions for Q-stability and minimum performance levels [20], [24].

***Definition** 1:* Denote the LPV model in (5) by G_Δ.

1) G_Δ is Q-stable if there exists $P=P^T\succ 0$ such that $A(\Delta(t))^T P+PA(\Delta(t))\prec 0\ \forall\Delta(t)\in\mathbf{\Delta}(t)$.
2) If G_Δ is Q-stable and has zero initial conditions, the induced $\mathscr{L}_2$-norm is defined as

$$\|G_\Delta\|_{i,2}:=\sup_{\Delta(t)\in\mathbf{\Delta}(t)}\ \sup_{0\neq u\in\mathscr{L}_2}\frac{\|y\|_2}{\|u\|_2}.$$ ■

***Lemma** 1:* The LPV system G_Δ defined in (5) is Q-stable and $\|G_\Delta\|_{i,2}<\gamma$ if there exists $P=P^T\succ 0$ such that

$$\left[\begin{array}{ccc}\mathcal{H}(PA(\Delta(t))) & \star & \star\\ B(\Delta(t))^T P & -\gamma I & \star\\ C(\Delta(t)) & D(\Delta(t)) & -\gamma I\end{array}\right]\prec 0\ \forall\Delta(t)\in\mathbf{\Delta}(t).$$ ■

Note that the requirement for Q-stability is sufficiently strong to ensure stability even for rapidly changing parameters.

D. Problem formulation

Consider the following problem for minimal switching FTO.

***Problem** 1:* Denote the LPV model (4) by $T_{\tilde{z}d}(\Delta)$. Let $\gamma>0$, $\gamma_F>0$ be given and let all other variables be as defined above. Find $L\in\Re^{n\times n_y}$ such that $T_{\tilde{z}d}(\Delta)$ is Q-stable, $\|T_{\tilde{z}d}(\Delta)\|_{i,2}<\gamma_F$ and $\left\|T_{\tilde{z}d}(\Delta=I_{n_y})\right\|_\infty<\gamma$. L will be called the fault–tolerant minimal switching (FTMS) observer gain. ■

In problem 1, γ gives a measure of the fault-free performance to be optimized, while γ_F ensures a minimum performance level in the case of sensor loss. Lemma 1 gives the following conditions for the solution of Problem 1.

***Theorem** 1:* L is an FTMS observer gain if there exist $P=P^T\succ 0$ and $F\in\Re^{n\times n_y}$ satisfying

$$\left[\begin{array}{ccc}\mathcal{H}(PA+FC) & \star & \star\\ B_d^T P+D_d^T F^T & -\gamma I & \star\\ C_z & 0 & -\gamma I\end{array}\right]\prec 0 \quad (6)$$

$$\left[\begin{array}{ccc}\mathcal{H}(PA+F\Delta C) & \star & \star\\ B_d^T P+D_d^T\Delta^T F^T & -\gamma_F I & \star\\ C_z & 0 & -\gamma_F I\end{array}\right]\prec 0\ \forall\Delta\in\mathbf{\Delta}, \quad (7)$$

where $\mathbf{\Delta}$ is defined in (2), in which case $L=P^{-1}F$.

Proof: The result follows by applying Lemma 1 to the estimation error dynamics in (4) and defining $F=PL$. ■

While Theorem 1 relates problem 1 to the system data, any design procedure based on the theorem is impractical since the inequalities in (7) need to be satisfied for every $\Delta\in\mathbf{\Delta}$ and since $\mathbf{\Delta}$ has 2^{n_y} elements, evaluating L becomes intractable for large n_y. This issue is considered in Sections III and IV.

III. A ROBUSTNESS RESULT FOR BINARY–TYPE UNCERTAINTY

The inequalities in (7) can be written as $T_1+\mathcal{H}\left(T_2\Delta T_3\right)\prec 0$ for appropriate T_1, T_2 and T_3. This is a general and widely used form for representing uncertainty in the control literature, although normally Δ represents a structured norm-bounded uncertainty while in our case Δ represents a structured binary uncertainty. One approach [25] for sensor fault–tolerant passive observer design is to introduce some conservatism by relaxing the discrete set $\mathbf{\Delta}$ in (2) into the interval set

$$\bar{\mathbf{\Delta}}:=\{\Delta=\mathrm{diag}(\delta_1,\ldots,\delta_{n_y}):0\leq\delta_i\leq 1\}\supset\mathbf{\Delta},$$

and solving the problem using the approaches in [14], [15], [25], thus avoiding the combinatorial explosion associated with the discrete case. To avoid the conservatism associated with this approach, and at the same time handle the combinatorial nature of the discrete problem, we develop a procedure for representing a general class of uncertainties involving all combinations of binary variables and then use an elimination lemma and an extension of a semidefinite relaxation procedure for binary $(0,1)$ variables [26], [27], [28], to derive conditions for their solution. That is, we extend the robustness results in [14], [15], which deal with continuous norm-bounded structured uncertainties, to discrete structured uncertainties.

Consider the following inequality:

$$T(\Delta):=T_1+\mathcal{H}\left(T_2\Delta(I-T_4\Delta)^{-1}T_3\right)\prec 0 \quad (8)$$

where $T_1=T_1^T, T_2, T_3, T_4$ are given matrices of appropriate dimensions. It is required to find conditions such that $det(I-T_4\Delta)\neq 0$ and (8) is satisfied for all $\Delta\in\mathbf{\Delta_c}$, where

$$\mathbf{\Delta_c}=\{\mathrm{diag}(\Delta_1,\ldots,\Delta_p):\Delta_i\in\{\underline{\Delta}_i,\overline{\Delta}_i\},i=1,\ldots,p\} \quad (9)$$

and where $\underline{\Delta}_i,\overline{\Delta}_i\subset\Re^{N_i\times N_i}$ are given. Define

$$\underline{\Delta}=\mathrm{diag}(\underline{\Delta}_1,\ldots,\underline{\Delta}_p),\quad \overline{\Delta}=\mathrm{diag}(\overline{\Delta}_1,\ldots,\overline{\Delta}_p). \quad (10)$$

We will use the following version of the elimination lemma which can be found, e.g. in [15].

***Lemma** 2:* Given real matrices $W=W^T, U$ and V of appropriate size, there exists a real matrix X such that

$$W+UXV^T+VX^TU^T\prec 0 \quad (11)$$

if and only if $\tilde{U}^TW\tilde{U}\prec 0$ and $\tilde{V}^TW\tilde{V}\prec 0$, where $\tilde{U}$ and $\tilde{V}$ are orthogonal complements of U and V, respectively. ■

Next, we use Lemma 2 to give necessary and sufficient conditions, in the form of matrix inequalities, for (8) in the case that Δ can take either of two values ($p=1$ in (9)).

***Lemma** 3:* Let $T_1=T_1^T\in\Re^{n\times n}, T_2\in\Re^{n\times N}, T_3\in\Re^{N\times n}, T_4, \underline{\Delta}, \overline{\Delta}\in\Re^{N\times N}$ be given and define $\underline{T}_4:=I-T_4\underline{\Delta}$ and $\overline{T}_4:=I-T_4\overline{\Delta}$. Assume that $det(\underline{T}_4)\neq 0$ and $det(\overline{T}_4)\neq 0$. Then (8) is satisfied for $\Delta\in\{\underline{\Delta},\overline{\Delta}\}$ if and only if there exists $S\in\Re^{N\times N}$ such that

$$\left[\begin{array}{c|c}T_1-T_2\mathcal{H}(\underline{\Delta}S\overline{\Delta}^T)T_2^T & \star\\ \hline T_3+(\underline{T}_4S\overline{\Delta}^T+\overline{T}_4S^T\underline{\Delta}^T)T_2^T & -\mathcal{H}\{\underline{T}_4S\overline{T}_4^T\}\end{array}\right]\prec 0. \quad (12)$$

Proof: (12) can be rewritten as (11) with

$$W=\left[\begin{array}{cc}T_1 & T_3^T\\ T_3 & 0\end{array}\right],\quad X=-S,\quad U=\left[\begin{array}{c}T_2\underline{\Delta}\\ -\underline{T}_4\end{array}\right],\quad V=\left[\begin{array}{c}T_2\overline{\Delta}\\ -\overline{T}_4\end{array}\right].$$

Furthermore, it can be verified that

$$\tilde{U} := \begin{bmatrix} I & T_2\underline{\Delta}\,\underline{T}_4^{-1} \end{bmatrix}^T, \quad \tilde{V} := \begin{bmatrix} I & T_2\overline{\Delta}\,\overline{T}_4^{-1} \end{bmatrix}^T$$

are orthogonal complements of U and V, respectively. The result then follows from Lemma 2 by noting that $\tilde{U}^T W \tilde{U} = T(\underline{\Delta})$ and $\tilde{V}^T W \tilde{V} = T(\overline{\Delta})$. ∎

The following result, which is our main result in this section, is a structured version of the above, and gives sufficient conditions, in the form of matrix inequalities, for (8) in the general case when $p \geq 1$ in (9).

Lemma 4: Let $T_1, T_2, T_3, T_4, \overline{T}_4$ and $\underline{T}_4$ be as defined in Lemma 3 and $\mathbf{\Delta_c}, \underline{\Delta}$ and $\overline{\Delta}$ be as defined in (9)-(10). Define

$$\mathcal{S} = \{\mathrm{diag}(S_1, \ldots, S_p) : S_i \in \Re^{N_i \times N_i}\}$$
$$\mathcal{G} = \{G \in \Re^{N \times N} : \Delta G + G^T \Delta^T = 0 \ \forall \Delta \in \mathbf{\Delta_c}\}.$$

Then $det(I - T_4\Delta) \neq 0$ and (8) is satisfied for every $\Delta \in \mathbf{\Delta_c}$, if there exist $S \in \mathcal{S}$ and $G \in \mathcal{G}$ such that

$$\begin{bmatrix} T_1 - T_2\mathcal{H}(\underline{\Delta}S\overline{\Delta}^T)T_2^T & \star \\ T_3 + (\underline{T}_4 S\overline{\Delta}^T + \overline{T}_4 S^T\underline{\Delta}^T - G)T_2^T & -\mathcal{H}(\underline{T}_4 S\overline{T}_4^T + GT_4^T) \end{bmatrix} \prec 0. \quad (13)$$

If $p = 1$ the condition is necessary and sufficient.

Proof: It follows from the definitions and structure of $\underline{\Delta}, \overline{\Delta}, \mathcal{S}$ and $\mathbf{\Delta_c}$ and from the definition of $\mathcal{G}$ that

$$\mathcal{H}\big((\Delta - \underline{\Delta})S(\Delta - \overline{\Delta})^T + \Delta G\big) = 0 \quad (14)$$

for all $S \in \mathcal{S}$, for all $G \in \mathcal{G}$ and for all $\Delta \in \mathbf{\Delta_c}$. Next, we prove that (13) implies that $det(I - T_4\Delta) \neq 0 \ \forall \Delta \in \mathbf{\Delta_c}$. Assume, for contradiction, that $det(I - T_4\Delta) = 0$ for some $\Delta \in \mathbf{\Delta_c}$ so that

$$z^T(I - T_4\Delta) = 0 \quad (15)$$

for some $z \neq 0$. Pre- and post-multiplying the $(2,2)$-block in (13) by z^T and z, respectively, and using (15) and (14),

$$-z^T T_4 \mathcal{H}\{(\Delta - \underline{\Delta})S(\Delta - \overline{\Delta})^T + \Delta G\}T_4^T z = 0.$$

This contradicts the negative definite property in (13).

To prove the sufficiency of (13) rewrite (13) as

$$W + UXV^T + VX^TU^T - JGT_{24}^T - T_{24}G^TJ^T \prec 0 \quad (16)$$

where $T_{24} := \begin{bmatrix} T_2^T & T_4^T \end{bmatrix}^T$, $J = \begin{bmatrix} 0 & I \end{bmatrix}^T$, and where W, X, U and V are defined in Lemma 3. Let $Y = \begin{bmatrix} I & T_2\Delta(I - T_4\Delta)^{-1} \end{bmatrix}^T$. Apply the congruence Y on (16) to give

$$T(\Delta) + T_2(I - \Delta T_4)^{-1}\mathcal{H}\{(\Delta - \underline{\Delta})S(\Delta - \overline{\Delta})^T + \Delta G\}(I - \Delta T_4)^{-T}T_2^T \prec 0$$

and the result follows from (14). Necessity when $p = 1$ follows from Lemma 3. In this case, we do not require $\mathcal{G}$. ∎

Remark 3: Note that the results remain valid if $\underline{\Delta}_i = \overline{\Delta}_i$ for some i. ∎

IV. A TRACTABLE SOLUTION TO THE FAULT–TOLERANT MINIMAL SWITCHING OBSERVER DESIGN PROBLEM

Theorem 1 gave a linear algorithm for the solution of Problem 1. An inspection of (6), however, shows that to ensure a γ_F-level performance, these inequalities must be satisfied for every combination of possible sensor faults; 2^{n_y} in total. The next result uses Lemma 4 to provide tractable solutions to Problem 1 for large n_y.

Theorem 2: Let all variables be as defined in Problem 1. Then L is an FTMS observer gain if there exist $P = P^T \succ 0$, $F \in \Re^{n \times n_y}$ and a diagonal $S \in \Re^{n_y \times n_y}$ such that (6) and

$$\begin{bmatrix} \mathcal{H}(PA) & \star & \star & \star \\ B_d^T P & -\gamma_F I & \star & \star \\ C_z & 0 & -\gamma_F I & \star \\ F^T + SC & SD_d & 0 & -\mathcal{H}(S) \end{bmatrix} \prec 0 \quad (17)$$

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

Proof: Using Theorem 1, we only need to prove that (17) is sufficient for (7). Now, a manipulation shows that (7) can be written as $T_1 + \mathcal{H}\left(T_2\Delta^T(I - T_4\Delta^T)^{-1}T_3\right)$ with

$$\left[\begin{array}{c|c} T_1 & T_2 \\ \hline T_3 & T_4 \end{array}\right] = \left[\begin{array}{ccc|c} \mathcal{H}(PA) & PB_d & C_z^T & C^T \\ B_d^T P & -\gamma_F & 0 & D_d^T \\ C_z & 0 & -\gamma_F & 0 \\ \hline F^T & 0 & 0 & 0 \end{array}\right].$$

Since $\Delta = \Delta^T$ in our case, the sufficiency of (17) follows from Lemma 4 by noting that $\underline{\Delta} = 0_{n_y \times n_y}$, $\overline{\Delta} = I_{n_y}$, $\mathcal{S} = \{S \in \Re^{n_y \times n_y} : S \text{ is diagonal}\}$ and $\mathcal{G} = \{0_{n_y \times n_y}\}$. ∎

Remark 4: Note the following concerning Theorem 2:

1) Compared with the existing solutions provided by Theorem 1, which require the solution of 2^{n_y} LMIs to ensure γ_F-level performance for the faulty scenarios, those in Theorem 2 require only one. Furthermore, the number of extra variables (in $\mathcal{S}$) is only n_y since $\mathcal{S}$ is diagonal.
2) The conditions in the theorem, which follow from Lemma 4, are only sufficient (except when $p = 1$). This is in common with the corresponding results in [14], [15] for continuous uncertainties. While the results in [27], [28] can be used to investigate the circumstances under which our conditions are also necessary, this falls outside the scope of this work. Our numerical experience, reported in Section V, indicates that they are sufficiently tight for practical systems. It follows that if the number of vulnerable sensors is not too large, so that it is feasible to solve the 2^{n_y} LMIs in (7), then it is preferable to use Theorem 1 for the observer design.
3) Although we have, for ease of presentation, only considered the case when all sensors are vulnerable to faults, and these faults are independent, Lemma 4 is sufficiently general to cover other situations, for example, if some sensors are not vulnerable to faults (see Remark 3) or some sensor faults are linked, say sensors i and j are either both faulty or both functional.
4) If only stability is required under sensor fault scenarios ($\gamma_F \to \infty$), then the inequality in (17) becomes

$$\begin{bmatrix} \mathcal{H}(PA) & \star \\ F^T + SC & -\mathcal{H}(S) \end{bmatrix} \prec 0.$$

∎

V. Illustrative example

An example from electric power transmission application is presented here to illustrate the proposed methodology. Consider a 4th order reduced equivalent of the Nordic power transmission system having the distribution matrices

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

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

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

Further details about this system can be found in [29]. The dynamic response of this system is characterized by two pairs of eigenvalues $\lambda_{1,2} = -0.08 \pm j1.82$ and $\lambda_{3,4} = -0.16 \pm j3.46$. Physically, these modes represent low frequency (less than 1 Hz) oscillations where electric power generators in one geographical area swing against the others in different locations. If not adequately damped, these oscillations could threaten the secure operation of the power systems.

To improve the damping of these modes, supplementary control loops through appropriate actuators (e.g. excitation systems of generators, static VAr compensators, etc.) are employed. The use of multiple feedback signals – both locally measured as well as remotely sensed and communicated – is often more effective due to better observability. With several sensors distributed along the power transmission networks, the potential number of feedback signals available is large. However, there is a risk of loss of one or more of these feedback signals due to sensor failure or communications problems (collectively referred to as 'sensor faults' henceforth) which could adversely affect the closed–loop dynamic response.

In this example we have chosen six feedback signals from different locations and, although the open–loop system is stable, it will be shown that sensor faults could lead to bad tracking of the actual state or even closed–loop instability. In this context, the performance of the two types of observers was compared: the standard non-fault–tolerant observer (satisfying $P = P^T \succ 0$ and inequality (6) only and denoted by the subscript N) and the minimal switching fault–tolerant observer (satisfying the conditions of Theorem 2 and denoted by the subscript $FTMS$) designed using the procedure described in Section IV, where all possible sensor fault combinations are considered (a total of $2^6 = 64$). The optimal values of the performance levels were $\gamma_N = 4 \times 10^{-10}$ and $\gamma_{FTMS} = 1.1775$ while the corresponding observer gains were

$$L_N=\begin{bmatrix} -20.51 & -1.30 & 0.78 & 8.66 & -4.22 & -4.22 \\ 11.50 & 0.66 & 0.06 & -4.26 & 2.50 & 2.50 \\ -9.21 & -0.36 & -0.23 & 3.20 & -2.01 & -2.01 \\ -3.19 & -0.66 & 0.29 & 1.83 & -0.50 & -0.50 \end{bmatrix}$$

Δ	Combinations $[1, 2, \ldots, 13]$												
δ_1	0	0	0	0	0	0	0	0	0	0	0	0	0
δ_2	0	0	0	0	0	0	0	0	0	0	0	0	0
δ_3	0	0	0	0	0	0	0	0	1	1	1	1	1
δ_4	0	0	0	0	1	1	1	1	0	0	0	0	1
δ_5	0	0	1	1	0	0	1	1	0	0	1	1	0
δ_6	0	1	0	1	0	1	0	1	0	1	0	1	0
L_N	*s*	*s*	***u***	*s*	***u***	***u***	***u***	***u***	*s*	*s*	***u***	*s*	***u***
L_{FTMS}	*s*	*s*	*s*	*s*	*s*	*s*	*s*	*s*	*s*	*s*	*s*	*s*	*s*

TABLE I

Closed–loop stability for the first 13 fault combinations using the non-fault–tolerant (L_N) and fault–tolerant minimal switching (L_{FTMS}) observer gains, where"*s*" stands for stable and"*u*" for unstable

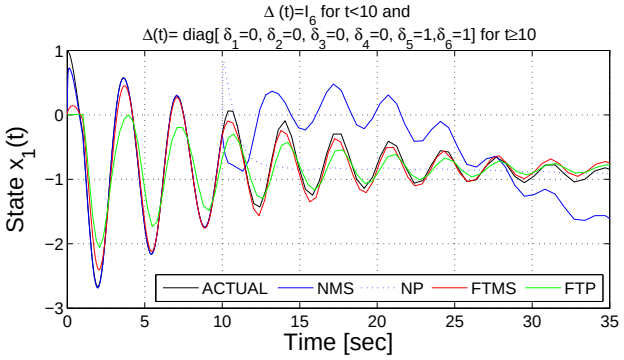

Fig. 2. State estimate comparison showing the actual state, the non-fault–tolerant observer estimates in switching (NMS) and passive (NP) modes, the fault–tolerant minimal switching (FTMS) observer estimate and the fault–tolerant passive (FTP) observer estimate following a fault in sensors 1,2,3 and 4 at 10 sec.

$$L_{FTMS}=\begin{bmatrix} 0.35 & -0.87 & 0 & 3.68 & 0 & -0.01 \\ 1.06 & -0.94 & 0 & 3.84 & 0 & -0.03 \\ -1.87 & 2.07 & 0 & -8.43 & 0 & 0.08 \\ 1.84 & -3.79 & 0 & 11.48 & 0 & 0.01 \end{bmatrix}$$

and where in all cases stability as well as a minimum performance level corresponding to $\gamma_F = 2.8543$ are required under faulty sensor scenarios. The cost function for the non-fault–tolerant observer (γ_N) is close to zero because only one (fault-free) scenario is considered. Note that the exact value (obtained from Theorem 1 by solving the 2^6 LMIs corresponding to each fault scenario) of γ_{FTMS} is 1.1715, so that our approximation is quite accurate in this example. Note also that L_{FTMS} has two zero columns, which corresponds to the 3rd and 5th sensors not being used in the design. It can be shown that these two sensors have the smallest observability indices with respect to the two dominant modes. Thus the benefit of the information provided by these sensors is insufficient to overcome the undesired effect of the associated disturbance on our performance index in Theorem 2 and our scheme then automatically excludes these sensors.

Table I lists whether the estimation error dynamics in (4) are stable ('s') or unstable ('u') using the two different types of observers for the first 13 combinations (out of the possible 64) of Δ. It is evident that with the non-fault–tolerant observer (using the minimal switching structure) the closed–loop system is unstable for several sensor fault combinations while it

always remains stable using the fault–tolerant observer.

Figure 2 compares the time variation of the state $z(t) = x_1(t)$ (black), the estimated states $\hat{x}_1(t)$ using the non-fault–tolerant observer (gain L_N) in the minimal switching (blue, solid) and passive (blue, dotted) modes and the fault–tolerant minimal switching observer (gain L_{FTMS}) in red. Although not explicitly developed in this work, the fault–tolerant passive observer (gain L_{FTP}) is also shown (green). The plots represent one particular situation where sensors $1, 2, 3$ and 4 have failed ($\Delta(t) = I_6,\ t < 10;\ \Delta(t) = \mathrm{diag}(0, 0, 0, 0, 1, 1),\ t \geq 10$). This faulty situation corresponds to column 4 of Table I where the closed–loop is stable for all the observer gains. It can be seen from the plot that before the fault occurs, all the observer gains track the actual state well, with L_N best and L_{FTP} worst, however, following the fault at $10sec$ the non-fault–tolerant observer gain (L_N) diverge significantly from the actual state with L_{FTMS} performing best.

VI. Conclusions

We have presented a fault–tolerant active observer design method that guarantees a minimum level of closed–loop performance under all possible sensor fault combinations while optimizing performance under the fault-free condition. The performance is measured by the induced $\mathscr{L}_2$-norm of the LPV dynamics from the external signals to the estimation error. The problem was first recast in a more general robust design setting where the uncertainty set is composed of all combinations of a set of binary variables. Sufficient conditions (which are also necessary for the case of one binary variable) for the solution of the problem are derived which result in a significant reduction in the number of matrix inequalities needed to solve the problem. Although we considered a fault–tolerant observer design problem against sensor faults, our results are general and apply to other problems involving combinations of sensor, actuator and process faults as well as observer/state-feedback design. In this work we have considered all possible combination of sensor faults. Recognizing that the possibility of this event is highly unlikely, a future direction of this work is to present a formulation specifying a minimum number of sensors which would always remain in operation.

Acknowledgment

Funding from ABB (Grant EESC P26939) and technical inputs from Dr Ernst Scholtz are gratefully acknowledged.

References

[1] M. Blanke, M. Kinnaert, J. Lunze, M. Staroswiecki, and J. Schröder, *Diagnosis and Fault-Tolerant Control*. Springer-Verlag, USA, 2006.

[2] J. Jiang and Q. Zhao, "Design of reliable control systems possessing actuator redundancies," *Journal of Guidance, Control, and Dynamics*, vol. 23, no. 4, pp. 709–7180, 2000.

[3] Y. Yang, G.-H. Yang, and Y. Soh, "Reliable control of discrete-time systems with actuator failure," *IEE Proceedings - Control Theory and Applications*, vol. 147, no. 4, pp. 428–432, 2000.

[4] F. Liao, J. L. Wang, and G.-H. Yang, "Reliable robust flight tracking control: an LMI approach," *IEEE Transactions on Control Systems Technology*, vol. 10, no. 1, pp. 76–89, 2002.

[5] R. Veillette, "Reliable state feedback and reliable observers," in *Proceedings of the 31st IEEE Conference on Decision and Control*, vol. 3, 1992, pp. 2898–2903.

[6] Y. Zhang and J. Jiang, "Active fault-tolerant control system against partial actuator failures," *IEE Proceedings - Control Theory and Applications*, vol. 149, no. 1, pp. 95–104, 2002.

[7] K. Kim and K. Lee, "Reconfigurable flight control system design using direct adaptive method," *Journal of Guidance, Control, and Dynamics*, vol. 26, no. 4, pp. 543–550, 2003.

[8] M. Mahmoud, J. Jiang, and Y. Zhang, *Active Fault Tolerant Control Systems: Stochastic Analysis and Synthesis*. Lecture Notes in Control and Information Sciences, Volume 287, Springer-Verlag, 2003.

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

[10] M. Staroswiecki, G. Hoblos, and A. Aitouche, "Sensor network design for fault tolerant estimation," *International Journal of Adaptive Control and Signal Processing*, vol. 18, no. 1, pp. 55–72, 2004.

[11] M. Cattafi, M. Gavanelli, M. Nonato, S. Alvisi, and M. Franchini, "Optimal placement of valves in a water distribution network with CLP(FD)," *Theory and Practice of Logic Programming*, vol. 11, pp. 731–747, 2011.

[12] S. Alvisi, M. Franchini, M. Gavanelli, and M. Nonato, "Near-optimal scheduling of device activation in water distribution systems to reduce the impact of a contamination event," *Journal of Hydroinformatics*, vol. 14, no. 2, pp. 345–365, 2012.

[13] C.-C. Feng, "Fault-tolerant control and adaptive estimation schemes for sensors with bounded faults," in *IEEE International Conference on Control Applications,*, 2007, pp. 628–633.

[14] M. Fan, A. Tits, and J. Doyle, "Robustness in the presence of mixed parametric uncertainty and unmodeled dynamics," *IEEE Transactions on Automatic Control*, vol. 36, no. 1, pp. 25–38, 1991.

[15] 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.

[16] I. Jaimoukha, Z. Li, and V. Papakos, "A matrix factorization solution to the $\mathcal{H}_-/\mathcal{H}_\infty$ fault detection problem," *Automatica*, vol. 42, no. 11, pp. 1907–1913, 2006.

[17] Z. Li, E. Mazars, and I. M. Jaimoukha, "State space solution to the $\mathcal{H}_-/\mathcal{H}_\infty$ fault detection problem," *International Journal of Robust and Nonlinear Control*, vol. 22, no. 3, pp. 282–299, 2012.

[18] F. 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, 2014.

[19] D. Ichalal, B. Marx, D. Maquin, and J. Ragot, "New fault tolerant control strategy for nonlinear systems with multiple model approach," in *Conference on Control and Fault-Tolerant Systems (SysTol)*, 2010, pp. 606–611.

[20] G. Becker and A. Packard, "Robust performance of linear parametrically varying systems using parametrically-dependent linear feedback," *Systems and Control Letters*, vol. 23, no. 3, pp. 205–215, 1994.

[21] I. M. Jaimoukha, H. El-Zobaidi, D. J. Limebeer, and N. Shah, "Controller reduction for linear parameter-varying systems with a priori bounds," *Automatica*, vol. 41, no. 2, pp. 273–279, 2005.

[22] J. Mohammadpour and C. W. Scherer, *Control of Linear Parameter Varying Systems with Applications*. Springer, 2012.

[23] O. Sename, P. Gaspar, and J. Bokor, *Robust Control and Linear Parameter Varying Approaches*. Spinger, Feb. 2013.

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

[25] G.-H. Yang, J. L. Wang, and Y. C. Soh, "Reliable $\mathcal{H}_\infty$ controller design for linear systems," *Automatica*, vol. 37, no. 5, pp. 717–725, 2001.

[26] S. Poljak and H. Wolkowicz, "Convex relaxations of (0,1)-quadratic programming." *Mathematics of Operations Research*, vol. 20, no. 3, p. 550, 1995.

[27] U. Malik, I. M. Jaimoukha, G. D. Halikias, and S. K. Gungah, "On the gap between the quadratic integer programming problem and its semidefinite relaxation," *Mathematical Programming*, vol. 107, no. 3, pp. 505–515, 2006.

[28] G. D. Halikias, I. M. Jaimoukha, U. Malik, and S. K. Gungah, "New bounds on the unconstrained quadratic integer programming problem," *Journal of Global Optimization*, vol. 39, no. 4, pp. 543–554, 2007.

[29] 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, 2010.