

A Supervisory Active Fault Tolerant Control Framework for Constrained Linear Systems*

Iman Zare¹, Shahram Aghaei², and Vicenç Puig³

Abstract—In this paper, a supervisory active fault tolerant control (SAFTC) scheme is presented for linear systems with constraints. The SAFTC framework is composed of a fault diagnosis module, a reconfigurable controller and a pre-designed command governor. In the presence actuator faults, constraints are guaranteed by governing the setpoint to the nearest admissible value. The command governor is adopted in such a way that no recalculation and reconfiguration is needed even in the presence of actuator fault occurrence and reconfiguration of the main controller. The input redundancy assumption, needed to recover the closed-loop tracking performance of system with faulty constrained actuator, is relaxed. A simulation study on VTOL aircraft is performed to evaluate the effectiveness of the proposed method.

Fault tolerant control, Command governor, Constrained linear systems, Actuator fault

I. INTRODUCTION

Faults in automated processes will often cause undesired reactions and shutdown of the controlled plant, and the consequences could be damage to the plant, to personnel or the environment. Hence, automatic control systems are subject to an increasing demand for safe and highly reliable operation. Fault-tolerant control (FTC) is a recent control field including a set of techniques that were developed to increase plant availability and reduce the risk of safety hazards. The FTC systems are, generally, classified into two types: passive fault tolerant control (PFTC) [1], [2] and active fault tolerant control (AFTC) [3], [4].

The passive approach is able to deal with predefined set of faults using techniques of robust control. However, these faults may be unpredictable or the range of their occurrence may be beyond the range considered in the robust methods. In order to achieve the suitable performance of the system in a wider range of faults occurrence, the use active approaches and reconfiguration of the controller is required [5]. The design objectives of an AFTC system can be divided into two parts: the first part aims at designing a fault diagnosis scheme to provide the information about the fault (time, type and magnitude) and the fault model [6], [7]. The second part involves designing a fault-based reconfigurable controller to reduce the fault effect and to maintain the stability and

to minimise the closed-loop performance degradation. More details have been presented in [8] and references therein.

Control of constrained systems is an important issue in many applications, especially, in safety critical systems such as medical equipment, aerial vehicles, chemical and petrochemical processes, among other. Constraints are due to the physical limitations of the actuators (actuator constraints) and by the necessity to keep some plant variables within safe limits (state constraints). Considering the constraints make the design of the controller a difficult task even for systems described by a linear dynamic model [9]. One of the popular approaches to deal with constraints in both industrial applications and in the research community is reference governor (RG) which also named as command governor (CG) [10]–[12]. Given a primal compensated control system, the RG (or CG) is an additional block which accommodates the reference signal to a manipulated feasible version, when the reference value changes would lead to constraint violation.

Designing the FTC for a constrained system is more complicated and a more challenging problem than for the unconstrained case. In the presence of constraints, the system can not achieve the primal nominal performance after the fault occurrence. In this situation, the reconfiguration of the feedback controller may not be sufficient and FTC also requires to modify the control objectives (as e.g. the reference input). To this end, RG schemes are one of the available approaches in the outreach of FTC for constrained systems, mainly, in the category of AFTC. In this paper, the problem of actuator faults that involves a loss of effectiveness is addressed by designing a supervisory AFTC using RG to ensure the closed-loop stability and avoid input and state constraint violations recovering the tracking performance with a graceful degradation. This problem has been addressed, assuming the existence of the accurate fault diagnosis module, in [13] [14] where the reconfiguration on both controller and reference management module is performed to achieve optimal system performance. The idea of changing the model and the constraints is considered in [15] and [16]. Related to the proposed frameworks in these papers, two critical points are important to note: First, for a system with input and state constraint, input redundancy is unavoidable to recover the tracking performance in the presence of actuator faults involving a loss of effectiveness. In other words, systems without redundancy in the faulty input fail to recover their nominal tracking performance as shown in the simulation results of this paper. Second, the presented reference management based FTC schemes in these papers need to reconfigure the CG module according

*This work has been funded by SMART Project (ref. num. EFA153/16 Interreg Cooperation Program POCTEFA 2014-2020).

¹Iman Zare (MSc student) is with the Department of Electrical Engineering, Yazd University, Yazd, Iran

²Shahram Aghaei (Corresponding Author) is with the Department of Electrical Engineering, Yazd University, Yazd, Iran aghaei@yazd.ac.ir

³Vicenç Puig is with the Department of Automatic Control, UPC, Barcelona, Spain vicenc.puig@upc.edu

to the information provided by the fault diagnosis module. It means that based on the information of any new fault, maximal output admissible set (MOAS) must be recalculated. However, online recalculation of such a set for a CG in operation is not feasible. Moreover, the previously calculated MOASs are not applicable for wide range faults or unpredictable faults.

In this paper, a controller reconfiguration scheme is proposed for constrained systems. In this scheme, the post-fault closed loop system model remains equivalent to the fault-free closed-loop model and hence, the presented supervisory active fault tolerant control (SAFTC) does not need to reconfigure the structure of CG, after the fault occurrence. In other words, the MOAS calculated for fault free nominal model is valid for post-fault model and the nominal tracking performance is recovered also for the systems without actuator redundancy.

The paper is organized as follows. In Section II, the problem is formally stated: the system under control is defined, actuator faults are modeled and the proposed constraint scenario is introduced. Section III presents the proposed SAFTC approach in details. Firstly, an offset free controller for the nominal closed-loop system is designed. Then, the design procedure of a fault diagnosis module is briefly outlined. After that, the controller reconfiguration mechanism is fully discussed and in the sequel the structure of CG for constraints fulfilment is illustrated. Section IV is dedicated to illustrate the proposed method with an example of flight control followed by simulation results.

II. PROBLEM STATEMENT

Consider the following discrete-time linear system:

$$\begin{cases} x(k+1) = Ax(k) + Bu(k) \\ y(k) = Cx(k) \end{cases} \quad (1)$$

where $x(k) \in \mathbb{R}^n$ is the state vector, $u(k) \in \mathbb{R}^m$ is the control input vector, $y(k) \in \mathbb{R}^p$ is the controlled output vector to be steered to the admissible reference input $r(k)$. $A \in \mathbb{R}^{n \times n}$, $B \in \mathbb{R}^{n \times m}$ and $C \in \mathbb{R}^{p \times n}$ are known constant matrices. The system (1) is assumed to be subject to actuator faults that are modelled as follows

$$v_i(k) = \rho_i u_i(k) \quad 0 \leq \rho_i \leq 1 \quad i = 1, 2, \dots, m \quad (2)$$

$$\begin{cases} \rho_i = 1 & \text{healthy.} \\ 0 < \rho_i < 1 & \text{loss of effectiveness} \\ \rho_i = 0 & \text{failure} \end{cases}$$

where v_i denotes the actuator output signal and $\rho_i, i = 1, 2, \dots, m$ is the loss of effectiveness factor which is unknown. Note that, $\rho_i = 1$ implies fault-free operation of the i^{th} actuator and also implies $v_i = u_i$.

Accordingly, by defining the actuator output vector as

$$v(k) = [v_1(k), v_2(k), \dots, v_m(k)]^T = \rho u(k) \quad (3)$$

with $\rho = \text{diag}[\rho_1, \rho_2, \dots, \rho_m]$, the system model (1) considering actuator faults (2) can be described by

$$x(k+1) = Ax(k) + B_f u(k) \quad (4)$$

$$y(k) = Cx(k). \quad (5)$$

where

$$B_f = \rho B \quad (6)$$

is the input matrix of the faulty plant. In the sequel, we assume $u(k) = u_h(k)$ is the control input for the healthy plant and $u(k) = u_f(k)$ is the control input (actuator input) for the faulty plant.

In real systems, system inputs are constrained because of the actuator physical limitations. Similarly, for safety reasons the system outputs are limited during the system operation. These limitations are not considered in the system model (1) and should be added as additional equations in the form of inequalities. The inclusion of these additional conditions makes the design of the controller in both nominal and faulty conditions more challenging. The following constraints are considered to be fulfilled during the system operation,

$$x(k) \in \mathbb{X} := \{x \in \mathbb{R}^n \mid Gx \leq g\}, \quad (7a)$$

$$u(k) \in \mathbb{U} := \{u \in \mathbb{R}^m \mid Hu \leq h\}, \quad (7b)$$

for all $k \in \mathbb{Z}_{\geq 0}$, where $G \in \mathbb{R}^{m_x \times n}$, $g \in \mathbb{R}^{m_x}$, $H \in \mathbb{R}^{m_u \times m}$ and $h \in \mathbb{R}^{m_u}$ are vectors/matrices collecting the system constraints, signifying $m_u \in \mathbb{Z}_{\geq 0}$ and $m_x \in \mathbb{Z}_{\geq 0}$ the number of input and state constraints, respectively.

The aim of this paper is to design an AFTC to accommodate the fault effect with less performance degradation while enforcing the actuator output and state signals to fulfil the constraints under the following assumptions.

Assumption 1. The pair (A, B) is reachable and the pair (A, C) is observable.

Assumption 2. $\text{rank} \begin{bmatrix} I_n - A & -B \\ C & 0_{p \times m} \end{bmatrix} = n + p$

This rank condition indicates that in general, for offset free tracking, the number of controlled variables should not exceed the number of states and the number of control inputs.

III. THE PROPOSED APPROACH

The proposed control scheme is depicted in Figure 1. The fault diagnosis module (FDD) provides the information regarding the loss of effectiveness ρ of the actuator to the reconfiguration mechanism. Once the fault diagnosed by the is by the FDD module, the reconfiguration mechanism is responsible of maintaining the offset free tracking performance and fulfill the constraints.

This section will be presented considering that we have access to full state of the system (1) ($C = I$) or otherwise an observer will be available in place.

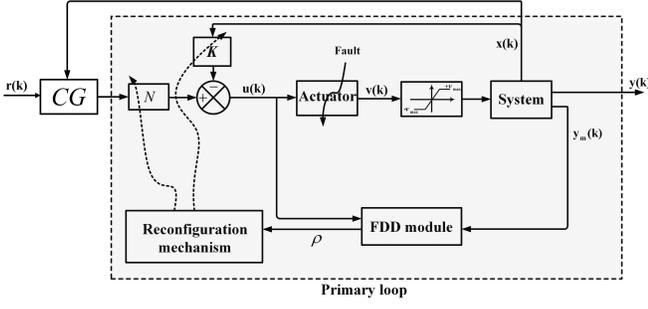


Fig. 1: The proposed SAFTC scheme

A. Offset free control design

Under the Assumption 1, a state feedback gain could be designed for system (1) using the LQR approach

$$u_{fb}(k) = -Kx(k) \quad (8)$$

where the feedback gain K is designed using the LQR approach as follows

$$K = (B^T P B + R)^{-1} (B^T P A) \quad (9)$$

is the stabilizing controller for the fault free system (1). P is a positive definite and symmetric solution of the associated discrete-time Algebraic Riccati Equation (DARE)

$$A^T P A - P - (A^T P B)(B^T P B + R)^{-1} (B^T P A) + Q = 0 \quad (10)$$

To achieve the tracking performance regarding controlled variables under the Assumption 2, a feedforward module is also necessary to compensate the steady-state closed loop gain by applying the following control law:

$$u_h(k) = u_{fb}(k) + u_{ff}(k) \quad (11)$$

where,

$$u_{ff}(k) = N r(k) \quad (12)$$

is applied in this paper as the feedforward control law and N is the feedforward gain.

Calculation of feedforward gain N in (12) requires exact knowledge of the system parameters. Changing in parameters will affect the steady state error. In healthy situation, the feed forward gain matrix N can be determined as follows

$$N = (C(I_n - A + BK)^{-1} B)^{-1} \quad (13)$$

By applying the control law (11) to the system (1), the closed loop system is

$$\begin{aligned} x(k+1) &= A_{cl} x(k) + B_{cl} r(k) \\ y(k) &= Cx(k) \\ y_m(k) &= C_m x(k), \end{aligned} \quad (14)$$

where

$$A_{cl} = A - BK, \quad B_{cl} = BN$$

preserving offset free tracking performance in the absence of fault and constraint, i.e. $\lim_{k \rightarrow \infty} y(k) = r(k)$.

B. Reconfiguration mechanism

To estimate the actuator fault, an observer based on the descriptor system [17] is used. For more detail please refer to [17]. In order to reconfigure the controller for a faulty system without any constraint, reference [18] describes the pseudo-inverse method (PIM) which minimizes the difference between the closed loop state-transition matrices of the nominal and the post-fault model. This approach enforces the system to recover the specified performance as much as possible. Excluding the constraints on state and system input and based on the PIM, the reconfiguration method presented in this paper leads to an exact solution for the reconfiguration of the controller gain to accommodate the fault effect.

In case of a actuator loss of effectiveness mode (i.e. without actuator failure), the control input (actuator input) for the faulty plant is described as

$$u_f(k) = -K_f x(k) + N_f r(k) \quad (15)$$

where

$$K_f = \rho^{-1} K, \quad N_f = \rho^{-1} N \quad (16)$$

Theorem 1. For the system (1), considering the constraints (7) are satisfied and assuming $\text{rank}([B_f \ BK]) = \text{rank}(B_f)$ where $B_f = B\rho$ and ρ is the estimation of loss of effectiveness factor. Then, the closed loop system model and the corresponding constraint equations remain unchanged after fault occurrence.

Proof: Using the presented reconfiguration scheme, the faulty system is given by

$$x(k+1) = Ax(k) + B_f u_f(k)$$

which according to (15), (16) and (6), after the fault occurrence the closed-loop state space formulation is given by

$$x(k+1) = (A - BK)x(k) + BNr(k). \quad (17)$$

In healthy mode, ρ is an identity matrix, and so $v_h(k) = u(k) = u_h(k)$. On the other hand, after the fault occurrence $v_f(k) = \rho u_f(k)$. where according to (15) $u_f(k) = \rho^{-1} u_h(k)$ and consequently, $v_h(k) = v_f(k) = v(k)$.

Therefore, the closed-loop system model and the constraint vector $y_\eta(k)$ remains without any change when fault occurred.

C. Constraint fulfillment

In this paper, the command governor (CG) approach has been used to fulfill the constraints and its general function is shown in Figure 1. For a constrained system, CG is designed in two steps: First, regardless of the constraints, the primary control-loop is designed in such a way that desirable performances such as stability, offset-free tracking are preserved. Second, the secondary loop is an additional on-line optimization module which manages the reference input, and determines the feasible manipulated reference input as close as possible to the intended reference input guaranteeing that the constraints are always satisfied. From

the functional point of view, the goal of the CG design is to provide an on-line computation of the manipulated reference input $w(k)$ as an alternative for the main reference input $r(k)$, so that:

- In the transient conditions due to reference change or fault occurrence, the output and/or control constraints may be active and hence CG computes $w(k)$ to prevent the constraint violation and steers it to the main feasible reference input value at the steady state.
- In the case of unfeasible reference signals, i.e. values of $r(k)$ which cannot be reached due to the constraints and fault occurrence, is replaced with the nearest computed feasible value $w(k)$.

The CG should be reconfigured once the constraint set or the model parameters are changed. Such a situation appears when a fault occurs. Based on the authors knowledge, the only explicit use of CG-like scheme for faulty constrained systems has been presented in [14], where once the fault occurred, not only the primary controller should be re-configured, but also the on-line computation part must be reformulated. Reformulation of a CG means to compute online the MOAS or to switch to one of the priority determined MOASs computed corresponding to some certain values of fault. However, it is clear that fault could not be priority determined because of the wide range of fault variation. Additionally, the MOAS is not computable along with the system operation because of its computation burden. Then, from the practical point of view, the AFTC schemes for constrained systems, which need to reformulate the CG or any real time optimization part (for fulfilling the constraints), is not reasonable. In this paper, by considering constraints (7) and according to the Theorem 1, the proposed SAFTC approach for faulty constrained systems does not need to reformulate the CG or to change the MOAS in the presence of fault.

1) *Supervisory CG of proposed SAFTC*: Command governor and extended command governor approaches were proposed in [19]. The command governor considers w as an optimization variable, and in each time instant solves the following constrained quadratic optimization problem

$$\begin{aligned} w(k) = \arg \min_w (r(k) - w(k))^T Q (r(k) - w(k)) \\ \text{s.t. } (x(k), w(k)) \in \mathbb{O}_\varepsilon \end{aligned} \quad (18)$$

where \mathbb{O}_ε , described by

$$\mathbb{O}_\varepsilon = \{(x(k), w(k)) \in \mathbb{R}^{n+p} \mid x(k) \in \mathbb{X}, u(k) \in \mathbb{U}, \forall k > 0\}, \quad (19)$$

is called Maximal Output Admissible Set (MOAS) and computed off-line. The method of computation the MOAS \mathbb{O}_ε has been presented and discussed in detail in [20]. As a result of this block, $w(k)$ is computed online at any sample time k and manipulated to the system as the feasible reference input. And this procedure is repeated at any future time steps. When, one of the system actuators be faulty (loss of effectiveness in this paper), dynamic equations of closed-loop system is changed. So, we need to update the set \mathbb{O}_ε to guarantee the constraints to be fulfilled. However, in this

paper, by defining the presented practical constraint scenario the re-configuration is performed in such a way that the system equations do not change after the fault occurrence. Therefore, the constraint will be guaranteed without updating the \mathbb{O}_ε set.

IV. SIMULATION EXAMPLE

In this section, the vertical take-off and landing (VTOL) aircraft [21] is considered to simulate to illustrate the effectiveness of the proposed SAFTC approach. The system to be studied is not over-actuated and, hence, is suitable to compare the proposed approach with the approaches of literature in the discussed topic for instance ROG based AFTC scheme presented in [14].

A. System description

The linearized continuous-time state space model of the VTOL aircraft in the vertical plane is described as follows:

$$\begin{aligned} \dot{x}(t) &= \begin{bmatrix} -9.9477 & -0.7476 & 0.2632 & 5.0337 \\ 52.1659 & 2.7452 & 5.5532 & -24.4221 \\ 26.0922 & 2.6361 & -4.1975 & -19.2774 \\ 0 & 0 & 1 & 0 \end{bmatrix} x(t) \\ &+ \begin{bmatrix} 0.4422 & 0.1761 \\ 3.5446 & -7.5922 \\ -5.5200 & 4.4900 \\ 0 & 0 \end{bmatrix} u(t) \\ y(t) &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} x(t) \end{aligned} \quad (20)$$

The state variables are horizontal velocity x_1 (kts), vertical velocity x_2 (kts), pitch rate x_3 (deg/s) and pitch angle x_4 (deg). The inputs are the collective pitch control u_1 (deg) and the longitudinal cyclic pitch control u_2 (deg), where the collective control is used for the vertical motion, and the other control input is used to control the horizontal velocity of the aircraft. The control objective is to steer the controlled output vector y as near as possible to the predefined desirable targets and to recover the nominal tracking performance even for the post-fault system. y_m is the vector of measured output also containing the controlled variables. Figure 2 is presented to provide a better physical view of the VTOL aircraft. using sampling time of 0.1s and using the zero order hold method, the discrete-time model is as follows

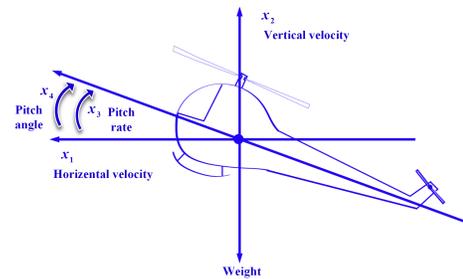


Fig. 2: A generic scheme of a VTOL aircraft in a vertical plane

$$\begin{aligned}
x(k+1) &= \begin{bmatrix} 0.2792 & -0.0502 & 0.0158 & 0.3534 \\ 4.1993 & 1.2016 & 0.4645 & -2.0554 \\ 1.6791 & 0.1698 & 0.6617 & -1.3274 \\ 0.0977 & 0.0099 & 0.0819 & 0.9247 \end{bmatrix} x(k) \\
&+ \begin{bmatrix} 0.0111 & 0.0366 \\ 0.3576 & -0.6936 \\ -0.3736 & 0.3097 \\ -0.0213 & 0.0176 \end{bmatrix} u(k) \\
y(k) &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} x(k). \quad (21)
\end{aligned}$$

Additionally, the input constraints for the VTOL aircraft, transferred to the actuator output and considered as:

$$-40 \leq v_i(k) \leq 40, \quad i = 1, 2. \quad (22)$$

Also, the output constraint $-2 \leq x_4 \leq 2$ is considered to fulfill during the system operation. For simulation, the following fault scenarios are considered:

Scenario 1: fault free system.

Scenario 2: 90% loss of effectiveness in the first actuator at $k_f = 15s$ ($\rho_1 = 0.1$)

B. Fault tolerant controller design

Weighting matrices of the feedback LQR controller are defined as follows: $Q = I_{4 \times 4}$ and $R = I_{2 \times 2}$, where I is a identity matrix, such that

$$P = \begin{bmatrix} 190.0466 & 24.6555 & 25.8809 & -104.5035 \\ 24.6555 & 4.6157 & 3.4532 & -12.9225 \\ 25.8809 & 3.4532 & 4.9080 & -12.6247 \\ -104.5035 & -12.9225 & -12.6247 & 78.1325 \end{bmatrix}$$

providing a stabilizing controller. Also, the healthy and faulty mode feedback and feedforward matrices are designed according to the (9) and (16), respectively.

C. Simulation results and discussion

Simulation results based on the mentioned scenarios for the proposed SAFTC, are depicted in Figures 3-5. In any figure, the system state variables along with references and manipulated references are depicted in subfigures a-d, the corresponding fault scenario is shown in subfigure e, and subfigures f-g illustrate the actuator outputs. the dashed-dotted lines in subfigures d, f, and g depicts the corresponding state and actuator constraint. This arrangement is maintained in all simulation scenarios. In Figure 3, in fault free mode, the first reference input is unauthorized and hence, the manipulated reference is converged to the nearest admissible reference input by the CG supervisory module in such a way that, the constraints on the output of the actuators and the fourth state variable are appropriately fulfilled.

The simulation results of the second scenario presented in Figure 4, indicates a good closed loop performance recovery fulfilling the constraints using the presented SAFTC -the reconfiguration of the controller under the supervision of the pre-designed CG.

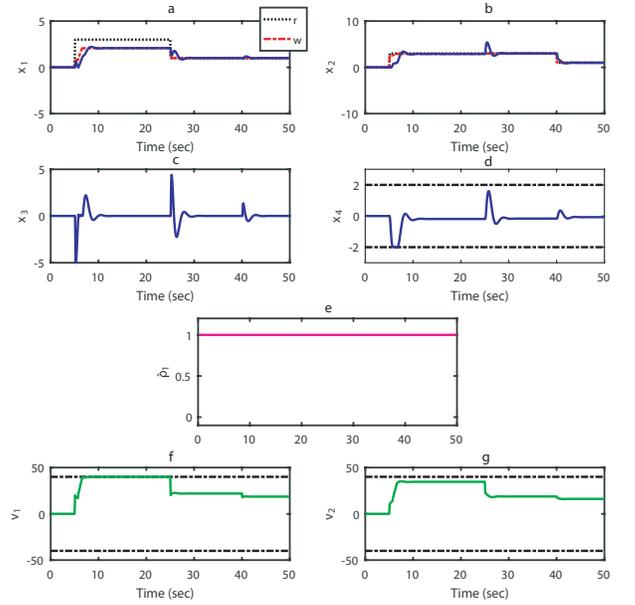


Fig. 3: Simulation results for fault free system (scenario 1)

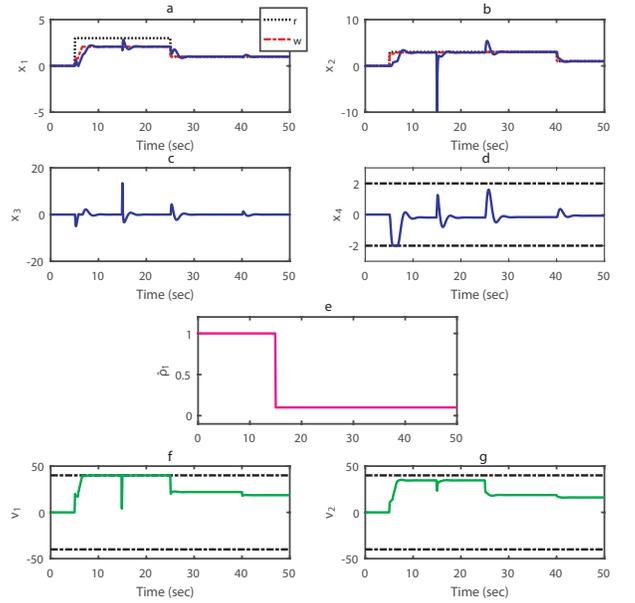


Fig. 4: Simulation results for faulty system (scenario 2: 90% loss of effectiveness)

To illustrate the effectiveness of the proposed approach in this paper, the VTOL aircraft model is also used to simulate the ROG based approach outlined in reference [14]. The simulation result for the situation where the first actuator is faced with a 10% loss of effectiveness is shown in Figure 5. For the loss of effectiveness factor with a larger value, the optimization problem in ROG is encountered with the

infeasibility. Therefore, using the ROG based approach, the problem is feasible only for small faults. The reasons for this situation can be summarized as follows:

- In the ROG approach, the system needs to be degree of redundancy so that the ROG, while guaranteeing the constraints, re-distributes the control signal to the actuators. It should be noted that in the study system in this paper, there is no degree of redundancy.
- In ROG based approach, the constraint is considered only on control signals while in this paper the constraints is considered in actuator output and state.

Also please note that, in a ROG-based approach and other literature in the subject of this paper, after the fault occurrence, re-computation of the MOAS (or replacement of the MOAS) is necessary, while, this requirement has been eliminated with the proposed approach in this paper in the case of the practical considered constraint scenario.

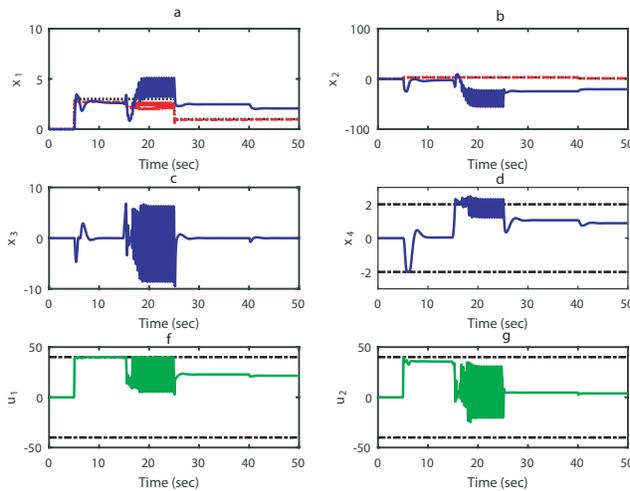


Fig. 5: Simulation result for ROG based approach proposed in [14] with $\rho = 0.9$ (10% loss of effectiveness)

V. CONCLUSION

In this paper, a supervisory active fault tolerant control (SAFTC) approach managing the reference input has been proposed for constrained systems. Fulfilling the constraint in the presence of actuator fault makes the fault recovery issue more complicated. After the occurrence of the actuator fault of loss of actuator effectiveness type and based on the fault diagnosis information, the controller reconfiguration is done while, the CG module is fix and does not need any reconfiguration. The proposed approach also works well for desirable performance recovery for the systems with faulty constrained actuator with no redundancy. A simulation study on a VTOL aircraft system has been performed to illustrate the proposed approach.

REFERENCES

[1] J.-X. Zhang and G.-H. Yang, "Robust adaptive fault-tolerant control for a class of unknown nonlinear systems," *IEEE Transactions on Industrial Electronics*, vol. 64, no. 1, pp. 585–594, 2017.

[2] D. Zhai, L. An, D. Ye, and Q. Zhang, "Adaptive reliable H_∞ static output feedback control against markovian jumping sensor failures," *IEEE transactions on neural networks and learning systems*, vol. 29, no. 3, pp. 631–644, 2018.

[3] R. E. Bavili, M. J. Khosrowjerdi *et al.*, "Active fault tolerant controller design using model predictive control," *Journal of Control Engineering and Applied Informatics*, vol. 17, no. 3, pp. 68–76, 2015.

[4] Q. Shen, B. Jiang, and P. Shi, "Active fault-tolerant control against actuator fault and performance analysis of the effect of time delay due to fault diagnosis," *International Journal of Control, Automation and Systems*, vol. 15, no. 2, pp. 537–546, 2017.

[5] 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.

[6] N. Gao, M. Darouach, and M. Alma, " H_∞ dynamic observer design for linear discrete-time systems," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 2756–2761, 2017.

[7] Z. Wang, M. Rodrigues, D. Theilliol, and Y. Shen, "Fault-tolerant control for discrete linear systems with consideration of actuator saturation and performance degradation," *IFAC-PapersOnLine*, vol. 48, no. 21, pp. 499–504, 2015.

[8] T. Jain, J. J. Yamé, and D. Sauter, *Active Fault-tolerant Control Systems: A Behavioral System Theoretic Perspective*. Springer, 2017, vol. 128.

[9] J. M. Maciejowski, *Predictive control: with constraints*. Pearson education, 2002.

[10] E. G. Gilbert and C.-J. Ong, "Constrained linear systems with hard constraints and disturbances: An extended command governor with large domain of attraction," *Automatica*, vol. 47, no. 2, pp. 334–340, 2011.

[11] S. Aghaei, F. Sheikholeslam, M. Farina, and R. Scattolini, "An mpc-based reference governor approach for offset-free control of constrained linear systems," *International Journal of Control*, vol. 86, no. 9, pp. 1534–1539, 2013.

[12] I. Kolmanovsky, E. Garone, and S. Di Cairano, "Reference and command governors: A tutorial on their theory and automotive applications," in *American Control Conference (ACC), 2014*. IEEE, 2014, pp. 226–241.

[13] P. Weber, B. Boussaid, A. Khelassi, D. Theilliol, and C. Aubrun, "Reconfigurable control design with integration of a reference governor and reliability indicators," *International Journal of Applied Mathematics and Computer Science*, vol. 22, no. 1, pp. 139–148, 2012.

[14] B. Boussaid, C. Aubrun, J. Jiang, and M. N. Abdelkrim, "Ftc approach with actuator saturation avoidance based on reference management," *International Journal of Robust and Nonlinear Control*, vol. 24, no. 17, pp. 2724–2740, 2014.

[15] G. Franze, A. Furfaro, M. Mattei, and V. Scordamaglia, "An hybrid command governor supervisory scheme for flight control systems subject to unpredictable anomalies," in *Control and Fault-Tolerant Systems (SysTol), 2013 Conference on*. IEEE, 2013, pp. 31–36.

[16] G. Franzè, A. Furfaro, M. Mattei, and V. Scordamaglia, "A safe supervisory flight control scheme in the presence of constraints and anomalies," *International Journal of Applied Mathematics and Computer Science*, vol. 25, no. 1, pp. 39–51, 2015.

[17] Z. Wang, Y. Shen, X. Zhang, and Q. Wang, "Observer design for discrete-time descriptor systems: an lmi approach," *Systems & Control Letters*, vol. 61, no. 6, pp. 683–687, 2012.

[18] Z. Gao and P. J. Antsaklis, "Stability of the pseudo-inverse method for reconfigurable control systems," *International Journal of Control*, vol. 53, no. 3, pp. 717–729, 1991.

[19] A. Casavola, E. Mosca, and D. Angeli, "Robust command governors for constrained linear systems," *IEEE transactions on Automatic Control*, vol. 45, no. 11, pp. 2071–2077, 2000.

[20] E. G. Gilbert and K. T. Tan, "Linear systems with state and control constraints: The theory and application of maximal output admissible sets," *IEEE Transactions on Automatic control*, vol. 36, no. 9, pp. 1008–1020, 1991.

[21] C. P. Tan and C. Edwards, "Sliding mode observers for robust detection and reconstruction of actuator and sensor faults," *International Journal of Robust and Nonlinear Control*, vol. 13, no. 5, pp. 443–463, 2003.