A Failure Mode Reconfiguration Strategy Based on Constraint Admissible and Recoverable Sets

Huayi Li, Ilya Kolmanovsky, and Anouck Girard

***Abstract*— This paper proposes a Failure Mode and Effect Management (FMEM) strategy for constrained systems with redundant actuators based on the combined use of constraint admissible and recoverable sets. Several approaches to ensure reconfiguration of the system without constraint violation in the event of actuator failures are presented. Numerical simulation results are reported.**

I. INTRODUCTION

The paper presents an approach to the design of a Failure Mode and Effect Management (FMEM) system based on constraint admissible and recoverable sets for systems with redundant actuators and state and control constraints. Multiple actuator failure modes are considered, and an approach to the design of FMEM system is proposed that ensures constraints are satisfied when operating in normal and failure modes and during mode transitions.

There is great demand for systematic approaches to FMEM system design for industrial systems since the software and algorithmic content of diagnostics and FMEM systems is often larger than what is responsible for the nominal system function. This is notably the case in the area of advanced and autonomous vehicles where redundant actuation (e.g., dual steering motors and multiple brake actuators) is employed to enable safe reconfiguration and the implementation of limited operating strategies in the event of failures. In these applications, a typical requirement for FMEM strategy is to ensure that, in case of a single point of failure, the system operation can be reconfigured so that in the new mode, another single point of failure cannot lead to safety hazards while maximizing system availability.

Figure 1 illustrates modes in a system with two redundant actuators, where a normal mode corresponds to both actuators functioning, and three failure modes correspond to either or both actuators to have failed. Notably the modes form vertices of a unidirectional graph.

The proposed approach to FMEM design builds on the idea of using constraint admissible and recoverable sets proposed in [1] but extends it to multiple failure modes and reference tracking. In each mode, a reference governor [2] is applied to enforce the constraints. When an actuator failure occurs, a recovery sequence is computed by solving a quadratic programming problem to bring the system trajectory into the constraint admissible set for the reference governor in the subsequent mode.

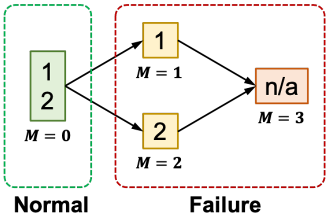

Fig. 1. Possible modes of a system with two actuators labeled by 1 and 2. The numbers in the boxes are the labels of the actuators that work properly. M stands for mode.

In this setting, constraint admissible sets are sets of initial states and constant reference commands for which the ensuing response satisfies state and control constraints. Recoverable sets are sets of initial states that can be steered into the (state projections of) constraint admissible sets within a specified number of steps without constraint violations.

To be able to perform a safe reconfiguration, the state of the system in the preceding mode must be in the recoverable set for the subsequent mode. In the paper, the implications of this set membership condition on the design of FMEM scheme are considered and illustrated with numerical examples. Under the assumptions of a single point of failure (i.e., one actuator failure at a time), instantaneous fault detection and isolation, and large time between subsequent failures, it is sufficient to ensure that a set bounding possible states in the preceding mode is a subset of the interior of the recoverable set in each of the possible subsequent modes. In this paper, we examine the implications of this condition and illustrate three mechanisms by which it can be ensured: (i) by adding extra state constraints in the preceding mode; (ii) by adding range and rate limits to the command in the preceding mode; and (iii) by temporarily relaxing state constraints when determining the recovery sequence. The latter mechanism is suitable for systems with soft constraints when a temporary constraint violation might be permissible.

Systematic recoverability analysis has been addressed in the fault tolerant control literature [3]; however, the existing methods typically do not handle state and control constraints. In a broader sense, this paper compliments set-theoretic control methods such as in [4], [5], [6], [7], [8] and provides extensions relevant to handling systems with multiple failure modes and reconfiguration levels. Set theoretic methods for handling failure modes in constrained systems have been considered in [9] and in the reference governor literature (see [2] and references therein). The present paper is distinguished by addressing multiple failure modes and failure

This research is supported by the National Science Foundation under award number ECCS-1931738.

The authors are with the Department of Aerospace Engineering, University of Michigan, Ann Arbor, MI 48109, USA. e-mail: {huayil, ilya, anouck}@umich.edu

paths/scenarios, by combined use of constrained admissible and recoverable sets and by specific mechanisms used to enforce the reconfigurability.

The paper is organized as follows. In Section II, the basic problem setting including models, failure modes and constraints is introduced. Section III introduces constraint admissible and recoverable sets that are used in Section IV to define a system capable of safe operation and reconfiguration in the event of failures. Two examples in Sections V and VI are used to highlight and illustrate design steps for a mass-spring-damper system and for an aircraft longitudinal flight, respectively. Section VII presents concluding remarks.

II. Mode-dependent system dynamics, constraints and problem formulation

A. System Dynamics

The development of our FMEM system relies on a discrete-time model of the form,

$$x_{k+1} = A_M x_k + B_M u_k, \quad y_k = C_M x_k, \tag{1}$$

where $k \in \mathbb{Z}_{\geq 0}$, x_k is the state vector, y_k is the output vector, u_k is the input vector, and $M \in \{0, 1, 2, \cdots\}$ designates different operating modes of the system, including normal modes and failure modes caused by actuator failures when specific inputs corresponding to the failed actuators equal zero.

It is assumed that the number of working actuators/inputs are greater than the number of outputs that need to be tracked. Then in each mode, a stabilizing feedback plus feedforward controller is used of the form,

$$u_k = K_M x_k + G_M v_k, \tag{2}$$

where K_M is the feedback gain matrix, G_M is the feed-forward gain matrix, and v_k is the vector of the reference commands (set-points). Depending on the mode M, appropriate rows of K_M and G_M are zeroed out to represent the effect of the actuator failures as the inputs corresponding to the failed actuators are forced to zero.

The closed-loop dynamics in mode M can be represented by the following discrete-time model,

$$\begin{gathered} x_{k+1} = \bar{A}_M x_k + \bar{B}_M v_k, \\ \bar{A}_M = A_M + B_M K_M, \ \bar{B}_M = B_M G_M, \end{gathered} \tag{3}$$

where $\bar{A}_M$ is a Schur matrix (where all eigenvalues are inside the unit disk of the complex plane). Since one of the possible modes is when all actuators fail, this assumption implies that the open-loop system must be stable.

B. Constraints

To ensure safe operation, pointwise-in-time state constraints are defined by a finite set of inequalities and imposed of the form,

$$x_k \in X(v_k) = \{x : \ A_X x \leq b_X(v_k)\}. \tag{4}$$

Since these constraints are imposed on the states of the closed-loop system with the given controllers, they can also represent actuator range and rate limits.

Modifications to these constraints are considered to facilitate the subsequent design of our failure mode reconfiguration approach. Firstly, to satisfy subsequent conditions for safe failure mode reconfiguration, it may be necessary to artificially tighten constraints (4) to

$$x_k \in X_M(v_k) = X(v_k) \cap \bar{X}_M(v_k), \tag{5}$$

where the sets $\bar{X}_M(v)$ need to be appropriately designed. Secondly, upon detection and isolation of the failure mode, a recovery sequence of control inputs is computed and implemented over a short time horizon before the control is relinquished to the reference governor. In practical applications (see e.g., [10]), some of the state constraints could be imposed conservatively to extend system operating life, and they may be relaxed temporarily during the reconfiguration and recovery. Hence during a short period when the recovery sequence is applied, the constraints can be relaxed to

$$x_k \in X_{R_M}(v_k), \tag{6}$$

where $X_{R_M}(v) \supseteq X_M(v)$, and $X_{R_M}(v)$ should also be appropriately designed.

C. Problem Formulation

A Failure Mode and Effect Management (FMEM) system is to be designed which is capable of ensuring safety despite failures. Each failure corresponds to a loss of an actuator and system mode transition. The time between failures is assumed to be large.

III. Constraint Admissible and Recoverable Sets

A. Constraint Admissible Sets

Each operating mode M has its corresponding approximation to the maximum constraint admissible set defined by

$$\begin{aligned} O_{\infty,M} = \{(v, x_0) : \ & x_t \in X_M(v) \ \forall t \in \mathbb{Z}_{\geq 0}, \\ & x_{\mathrm{ss}}(v, M) \oplus \mathcal{B}_\epsilon \subset X_M(v)\}, \quad (7) \\ = \{(v, x_0) : \ & A_{O_{\infty,M}} x_0 \leq b_{O_{\infty,M}}(v)\} \quad (8) \end{aligned}$$

where x_t is the response of (3) to the initial condition x_0 and constant command $v_t = v$, $x_{\mathrm{ss}}(v, M)$ is the steady-state operating point given by $x_{\mathrm{ss}}(v, M) = (I - \bar{A}_M)^{-1} \bar{B}_M v$, and $\mathcal{B}_\epsilon$ is an open ball of radius $\epsilon > 0$. The reasons for adding the constraint $x_{\mathrm{ss}}(v, M) \oplus \mathcal{B}_\epsilon \subset X_M(v)$ in (7) are technical: They ensure, under mild additional assumptions [11], that the set $O_{\infty,M}$ is finitely-determined and can be represented by a finite set of affine inequalities as in (8).

An important property of $O_{\infty,M}$ is its invariance under constant commands, that is, if $(v_k, x_k) \in O_{\infty,M}$ and $v_{k+1} = v_k$ while the system remains operating in mode M, then $(v_{k+1}, x_{k+1}) \in O_{\infty,M}$.

B. Recoverable Sets

The recoverable set for the system in mode M is defined as

$$\begin{aligned} R^{N_M}_{\infty,M} = \{x_0 : \ & \exists \{v_0, \cdots, v_{N_M - 1}\} \text{ such that} \\ & x_t \in X_{R_M}(v_t) \ \forall t = 0, 1, \cdots, N_M - 1, \quad (9) \\ & x_{N_M} \in \mathrm{Proj}_x O_{\infty,M}\}. \end{aligned}$$

Any initial condition x_0 in the recoverable set $R^{N_M}_{\infty,M}$ can be "steered" into $\text{Proj}_x O_{\infty,M}$ within N_M steps using the command sequence $\{v_0, \cdots, v_{N_M-1}\}$, and the constraints $x_t \in X_{R_M}(v_t), \forall t = 0, \cdots, N_M-1$ and $x_{N_M} \in \text{Proj}_x O_{\infty,M}$ are satisfied.

IV. Employing Admissible and Recoverable Sets for Safe Operation and Reconfiguration

A. Safe Operation in Each Mode Using Reference Governor

The reference/command governor [2] is used for reference tracking and to enforce the constraints in each mode except during the reconfiguration. The reference governor computes the modified command v_k as a function of the state x_k and original reference command r_k based on the solution of the following optimization problem,

$$\begin{aligned} &\text{Minimize } \|r_k - v_k\|^2 \\ &\text{subject to } (v_k,\ x_k) \in O_{\infty,M}. \end{aligned} \tag{10}$$

If $(v_t, x_t) \in O_{\infty,M}$ and the mode remains equal to M, $(v_{t+k}, x_{t+k}) \in O_{\infty,M}$ for all $k \geq 0$ and the constraints (5) remain satisfied.

B. Safe Reconfiguration upon Failure Detection

The failure mode reconfiguration relies on the condition

$$\text{Proj}_x O_{\infty,M} \subseteq R^{N_{M'}}_{\infty,M'},\ \forall M' \in \text{succ}(M), \tag{11}$$

where $R^{N_{M'}}_{\infty,M'}$ denotes the set of all states which are recoverable with command sequences of length $N_{M'}$ in mode M', and succ(M) is the set of all successor modes of mode M.

To ensure that (11) is satisfied, the sets $\bar{X}_M(v)$, $X_{R_{M'}}(v_t)$ and $N_{M'}$ can be varied. One can reduce $\bar{X}_M(v)$ (i.e., tighten constraints for the preceding mode M), enlarge $X_{R_{M'}}(v_t)$ (i.e., relax constraints for the successor mode M' during the recovery) and increase $N_{M'}$ (i.e., allow more elements in the reconfiguration sequence). The last approach has an impact on online computations as increasing $N_{M'}$ increases the size of the optimization problem which needs to be solved online.

With the condition (11) satisfied, if the failure occurs at the time instant t, $x_t \in R^{N_{M'}}_{\infty,M'}$ for the new mode $M' \in \text{succ}(M)$. Then, a recovery sequence of the commands $\{v_t, v_{t+1}, \cdots, v_{t+N_{M'}-1}\}$ can be found by solving a quadratic programming problem of minimizing $\|V_t - R_t\|^2$ where V_t is the vector of the recovery sequence $[v_t^T, v_{t+1}^T, \cdots, v_{t+N_{M'}-1}^T]^T$ and R_t is the vector of the reference sequence $[r_t^T, r_t^T, \cdots, r_t^T]^T$, subject to polyhedral constraints of the form, $x_{t+s} \in X_{R_M}(v_t)\ \forall s = 0, 1, \cdots, N_{M'}-1$, $x_{t+N_{M'}} \in \text{Proj}_x O_{\infty,M'}$. After the recovery sequence is applied, $x_{t+N_{M'}} \in \text{Proj}_x O_{\infty,M'}$. Hence at the time instant $t + N_{M'}$ the reference governor can be activated to continue operating the system in mode M'.

C. Command Range and Rate Limiting

An additional mechanism to ensure reconfigurability in the design of our FMEM system is to impose artificial range and rate limits on v_k. This results in state trajectories converging to a subset of $\text{Proj}_x O_{\infty,M}$ when operating in mode M. Since the time between failures is assumed to be large, $\text{Proj}_x O_{\infty,M}$ in (11) can be replaced by a smaller subset which ultimately bounds state trajectories, thereby weakening the requirement (11). These ancillary constraints on the command range and rate have the form,

$$v_k \in V_M = \{v :\ A_V v \leq b_V\}, \tag{12}$$

$$\Delta v_k = v_k - v_{k+1} \in \Delta V_M = \{\Delta v :\ A_{\Delta V} \Delta v \leq b_{\Delta V}\}. \tag{13}$$

Let

$$z_k = x_k - \Gamma_M v_k, \quad \Gamma_M = (I - \bar{A}_M)^{-1} \bar{B}_M, \tag{14}$$

then it can be derived that

$$z_{k+1} = \bar{A}_M z_k + \Gamma_M \Delta v_k. \tag{15}$$

With rate limits imposed by (13) and assuming the mode remains in M, $z_k \to F_M$ as $k \to \infty$, where F_M is the minimum invariant set [11] of the system derived from (15). This minimum invariant set is defined as an infinite Minkowski sum

$$F_M = \Gamma_M \Delta V_M \oplus \bar{A}_M \Gamma_M \Delta V_M \oplus \bar{A}_M^2 \Gamma_M \Delta V_M \oplus \cdots,$$

while in the implementation, computable outer approximations of F_M are used.

In addition to the rate limits, if range limits are also imposed on the command as in (12), then the state trajectory converges to the set

$$S_M = F_M \oplus \Gamma_M V_M. \tag{16}$$

With the extra range and rate limits on the commands (12), (13) added to the optimization problem defining the reference governor (10), the state trajectories in mode M will be ultimately bounded in the set $S_M \cap \text{Proj}_x O_{\infty,M}$. Hence the condition (11) can be weakened to

$$S_M \cap \text{Proj}_x O_{\infty,M} \subseteq \text{int} R^{N_{M'}}_{\infty,M'},\ \forall M' \in \text{succ}(M). \tag{17}$$

V. Mass-Spring-Damper System Example

A low order example of a system with redundant actuation is given by a mass-spring-damper system, where $m_0 = 1\ kg$ for the mass, $k_0 = 1\ N/m$ for the spring stiffness and $c_0 = 0.01\ Ns/m$ for the damping coefficient.

A. System Dynamics, Mode Definitions and Constraints

In the normal operating mode (Mode 0), the continuous-time system model is given by

$$\dot{x} = Ax + Bu,\ y = Cx \tag{18}$$

where $u = [f_1 \quad f_2]^T$ is the input with f_1 and f_2 being the forces in N, $x = [d \quad w]^T$ is the state with d being the displacement of the mass in m and w being the velocity of the mass in m/s, $y = d$ is the output, and

$$A = \begin{bmatrix} 0 & 1 \\ -\frac{k_0}{m_0} & -\frac{c_0}{m_0} \end{bmatrix},\ B = \begin{bmatrix} 0 & 0 \\ \frac{1}{m_0} & \frac{1}{m_0} \end{bmatrix},\ C = \begin{bmatrix} 1 & 0 \end{bmatrix}.$$

Three failure modes are possible in this system and the potential failure paths/scenarios are illustrated in Figure 1:

In Mode 1, f_1 operates normally while f_2 fails, that is, $u = [f_1 \;\; 0]^T$; In Mode 2, f_2 operates normally while f_1 fails, that is, $u = [0 \;\; f_2]^T$; In Mode 3, Both f_1 and f_2 fail, that is, $u = [0 \;\; 0]^T$.

The discrete-time model of the form (1) with $M \in \{0, 1, 2, 3\}$ is obtained by converting the model (18) to discrete-time assuming the sampling period of 0.2 sec.

The controller (2) for modes $M = 0, 1, 2$ is designed using Linear Quadratic Regulator (LQR) theory to obtain K_M. The feedforward gain G_M is computed so that the steady-state gain from v to the mass position d is equal to 1. In the selection of the LQR weights Q_M and R_M, it is assumed that the use of f_1 is more expensive than the use of f_2. The closed-loop system of each mode is design using the following parameters:

- For Mode 0, 1, and 2,

$$Q_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},\; Q_1 = Q_0,\; Q_2 = Q_0,$$

$$R_0 = \begin{bmatrix} 1000 & 0 \\ 0 & 250 \end{bmatrix}, R_1 = \begin{bmatrix} 10 & 0 \\ 0 & 0 \end{bmatrix}, R_2 = \begin{bmatrix} 0 & 0 \\ 0 & 2.5 \end{bmatrix}.$$

- For Mode 3, since both actuators fail, the system operates as it is in open-loop, but to keep the consistency of the notation, let

$$K_3 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix},\; G_3 = \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

The constraints are imposed on the position of the mass and on the magnitudes of the actuation forces:

$$|d| \le y_{\max},\; |f_1| \le u_{\max,1},\; |f_2| \le u_{\max,2},$$

where $y_{\max} = 1\ m$ and $u_{\max,1} = u_{\max,2} = 1\ N$. Using (2), these constraints are converted into the form (4).

B. FMEM Strategy Design

The development of the FMEM strategy based on constraint admissible and recoverable sets proceeds backward beginning from Mode 3 to the predecessor modes.

Since in Mode 3 the system runs in open-loop, the constraint admissible set in Mode 3 can be computed directly for the states (compare with (7)) as

$$\begin{aligned} \text{Proj}_x O_{\infty,3} &= \{x_0 :\; x_t \in X_3(0)\; \forall t \in \mathbb{Z}_{\ge 0}\} \\ &= \{x_0 :\; A_{O_{\infty,3}} x_0 \le b_{O_{\infty,3}}\}, \end{aligned} \qquad (19)$$

and the recoverable set of Mode 3 is

$$R^{N_3}_{\infty,3} = \text{Proj}_x O_{\infty,3} \quad \forall N_3 \ge 0, \qquad (20)$$

The equation (20) implies that (11) can be satisfied only if $x_k \in \text{Proj}_x O_{\infty,3}$ is imposed as the state constraint during the operation in Modes 1 and 2. To demonstrate using mechanisms in Section IV-B and IV-C to satisfy this requirement, two case studies are considered.

In the first case, state constraints of Mode 1 and 2 are tightened while the command range and rate limits are not used. This can be done by imposing state constrains of Mode 3 to Mode 1 and 2. Since the number of the inequalities in the representation of $\text{Proj}_x O_{\infty,3}$ can be large, this can result in highly complex $O_{\infty,1}$ and $O_{\infty,2}$ and large computational effort in using them in the implementation of the reference governor. Consequently, we use a simpler subset $P_3 \subset \text{Proj}_x O_{\infty,3}$. Such a subset is generated by removing close to being redundant inequalities from the representation of $\text{Proj}_x O_{\infty,3}$ and a scaling transformation to ensure that $P_3 \subset \text{Proj}_x O_{\infty,3}$. This leads to

$$P_3 = \{x_0 :\; A_{P_3} x_0 \le b_{P_3}\}. \qquad (21)$$

Now for $M \in \{1, 2\}$, we let $\bar{X}_M = P_3$. Then, $X_M(v)$ and $O_{\infty,M}$ can be constructed by (5) and (7).

The second case relies on having the command range and rate limits (12) and (13) of the form $|v| \le v_{\max}$ and $|\Delta v| \le \Delta v_{\max}$. No additional state constraints are added to further restrict the operation in Mode 1 and 2. That is, for $M \in \{1, 2\}$, we let $X_M(v) = X(v)$ and construct $O_{\infty,M}$ using (7).

Finally, for both cases, $O_{\infty,0}$ is computed based on (7) with $X_0(v) = X(v)$.

The value of $\epsilon = 0.01$ was used in computing $O_{\infty,M}$ for $M \in \{0, 1, 2\}$. The projections $\text{Proj}_x O_{\infty,M}$ computed using `Bensolve` [12] are shown in Figure 2(a) for the first case and in Figure 3(a) for the second case, with Figures 2(b) and 3(b) showing the zoom-in views.

Recoverable sets in the first case for mode switching between Mode 0 and Mode 1 or 2 are based on (9) where $X_{R_M}(v) = X_M(v)$, and N_M is chosen sufficiently large to satisfy (11). Figures 2(a) and (b) show the recoverable sets of Mode 2 as examples. After comparing the admissible and recoverable sets for both Mode 1 and Mode 2, N_M should at least be 3 to satisfy (11). Hence, we set $N_1 = N_2 = 3$ to minimize the length of the recovery sequence. Note that for transitions to Mode 3, the condition (11) is satisfied as by construction so both $\text{Proj}_x O_{\infty,1}$ and $\text{Proj}_x O_{\infty,2}$ are subsets of $\text{Proj}_x O_{\infty,3}$

For the second case, $\text{Proj}_x O_{\infty,2} \supseteq \text{Proj}_x O_{\infty,0}$ as shown in Figure 3(a), and so is for $\text{Proj}_x O_{\infty,1}$. Thus, for mode transitioning from Mode 0 to Mode 1 or 2, since $x_k \in \text{Proj}_x O_{\infty,M}$ for $M \in \{1, 2\}$ is automatically satisfied, a recovery sequence is not needed. Now, to safely switch from Mode 1 or 2 to Mode 3, $v_{\max}$ and $\Delta v_{\max}$ need to be chosen so that the condition (17) holds. In order to maximize the size of $S_M \cap \text{Proj}_x O_{\infty,M}$ for $M \in \{1, 2\}$ that restrict the operation of the system in Mode 1 and Mode 2, we set $v_{\max} = 1$ and $\Delta v_{\max} = 0.007$ for Mode 1, and $v_{\max} = 1$ and $\Delta v_{\max} = 0.01$ for Mode 2.

C. Simulation Results

Results of the two case studies are shown in Figures 2 and 3, where the trajectories are plotted in (a) and (b), and time-based signals are in (c) and (d).

In both cases, the system begins with operation in the normal mode (Mode 0), and then sequentially switches to Mode 2 and Mode 3. The reference is set to be switching between $-0.99\ m$ and $0.99\ m$. The time-based results show that all state and control input constraints are satisfied throughout

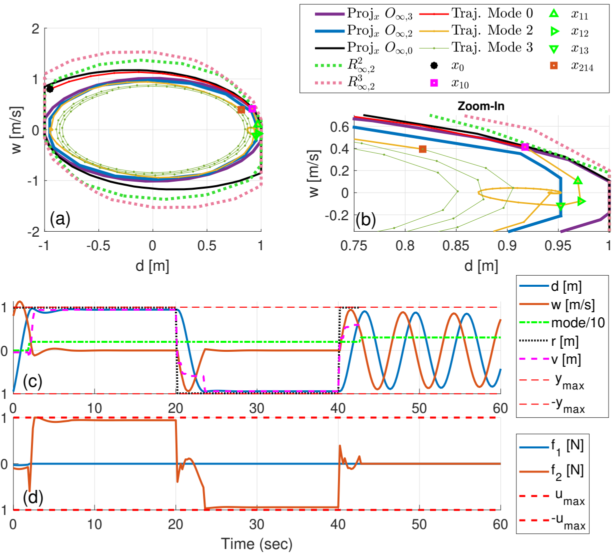

Fig. 2. Projections of sets and simulation results for the first case.

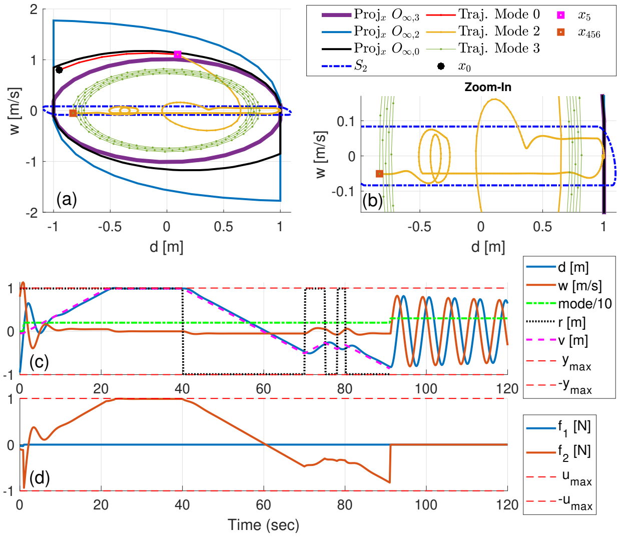

Fig. 3. Projections of sets and simulation results for the second case.

the simulation. When the system switches to Mode 2, in comparison with the first case study, the trajectory in the second case immediately starts approaching $S_2 \cap \text{Proj}_x O_{\infty,2}$ and stays inside it after the state converges. Effects of command rate limiting are clearly visible from the time-based signals.

VI. Aircraft Longitudinal Flight Control Example

We now consider a higher order example of aircraft longitudinal flight control with engine thrust and elevator actuators.

A. System Dynamics, Mode Definitions and Constraints

The aircraft model represents a Boeing 747-100 aircraft at steady level flight corresponding to Mach 0.5 cruise at 20,000 feet [13]. The linearized longitudinal flight dynamics under the normal operating conditions can be represented by the form (18) where $x = [\Delta\mu \quad \Delta w \quad \Delta q \quad \Delta\theta]^T$, $u = [\Delta a_T \quad \Delta\delta_e]^T$, and $y = \Delta\dot{h}$, μ and w, respectively, are the projection of the velocity vector on the x-axis and z-axis of the body-fixed frame in m/s, q is the projection of the angular velocity vector on the y-axis in $^\circ/s$ (degree per second), θ is the pitch angle in $^\circ$ (degree), a_T is the thrust-to-mass ratio in m/s^2, δ_e is the elevator deflection in $^\circ$, $\dot{h}$ is the climb rate in m/s, and Δ denotes the deviation from the trim value. In this model,

$$A = \begin{bmatrix} -0.0073 & 0.0274 & -0.0040 & -0.1713 \\ -0.1205 & -0.4350 & 2.7645 & 0 \\ 0.0188 & -0.3196 & -0.4850 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$
$$B = \begin{bmatrix} 1 & -0.0053 \\ 0 & 0.1170 \\ 0 & 14.5 \\ 0 & 0 \end{bmatrix}, \; C = \begin{bmatrix} 0 & -1 & 0 & 2.7645 \end{bmatrix}. \tag{22}$$

The model is then converted to discrete-time assuming 0.2 sec update period.

The normal and failure modes are defined and the controller for each mode is designed similar to Section V. In Mode 0, the controller is designed to track a given climb rate deviation and a zero deviation of the velocity magnitude from the nominal, that is, to hold $\sqrt{\mu^2 + w^2}$ at constant. During Modes 2 and 3, $\Delta a_T = 0$ in the linearized model can represent FADEC maintaining engine availability when handling an internal engine failure mode but having to restrict the ability to change engine thrust.

The constraints are imposed on the climb rate and on the thrust and the elevator inputs as $|\Delta\dot{h}| \leq y_{\max}$, $|\Delta a_T| \leq u_{\max,1}$ and $|\Delta\delta_e| \leq u_{\max,2}$, where $y_{\max} = 5\ m/s$, $u_{\max,1} = 5\ N/kg$ and $u_{\max,2} = 5^\circ$. These constraints define $X(v_k)$ and can be put into the form (4).

B. FMEM Strategy Design

The design process of admissible and recoverable sets for this aircraft example is similar to the first case in Section V-B, except for two main differences. First, in Mode 0, the state constraints $X_0(v)$ in (7) had to be tighten. Second, $X_{R_M}(v_t)$ in (9) exploits the relaxation in Mode 1 and 2.

The rationale for these two steps is illustrated in Figure 4 as an example, showing the projection of $O_{\infty,0}$ and $R^{N_1}_{\infty,1}$ on the first two coordinates $\Delta\mu$ and Δw. It shows that the change of N_1 has little impact on the shape of $R^{N_1}_{\infty,1}$ relative to $O_{\infty,0}$ in the Δw direction. In order to satisfy (11), a large value for N_1 is required, meaning the reconfiguration will take a long time. Similar situation also occurs in Mode 2. Thus, in order to have a reasonable value of N_M for $M \in \{1,2\}$, $X_0(v)$ and $X_{R_M}(v_t)$ for $M \in \{1,2\}$ need to be adjusted.

The first change is to reduce the size of $O_{\infty,0}$ by adding extra state constraints. This is done by having $X_0(v) = X(v) \cap \bar{X}_0$ where

$$\bar{X}_0 = \{x : \; A_{P_3}x \leq \eta_O b_{P_3}\}. \tag{23}$$

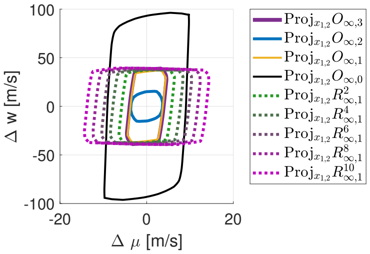

Fig. 4. Projections of admissible and recoverable sets as N_M changes.

Here, $\eta_O \geq 1$ is a design parameter. Smaller values of η_O make it more likely that (11) can be satisfied with small N_1 and N_2, but at the same time, $O_{\infty,0}$ shrinks, meaning that the system operation in the normal mode is more restricted. Thus, the value of η_O needs to be optimized and carefully chosen.

To avoid the need for over restriction in Mode 0, the second change is introduced, that is, to relax state constraints during the application of the recovery sequence in Mode 1 and 2 based on (9), with

$$X_{R_M} = \{x : \ A_X x \leq \eta_{R_M} b_X\}, \tag{24}$$

where $\eta_{R_M} \geq 1$ is also a design parameter. The "size" of $R^{N_M}_{\infty,M}$ increases as the value of η_{R_M} increases, while the trade-off is that the system could operate far outside from the normal constraints if the value of η_{R_M} gets too large. Thus, the value of η_{R_M} also needs to be optimized and chosen with care.

Based on optimization over a grid of values, we have $\eta_O = 1.5$, and we choose $N_1 = 9$, $\eta_{R_1} = 8$ for Mode 1, and $N_2 = 10$, $\eta_{R_2} = 11$ for Mode 2.

C. Simulation Results

Figure 5 shows an example of the simulation with mode switching from Mode 0 to Mode 1 at 72.2 sec and then from Mode 1 to Mode 3 at 120.2 sec. The time-based signals show that all input and output constraints are respected through out the simulation.

VII. Concluding Remarks

To be able to handle onboard failures safely (i.e., without violation of constraints), Failure Mode and Effect Management (FMEM) systems have to be appropriately designed. In systems with multiple redundant actuators, system operating modes can be defined dependent on functioning actuators. The operation in the preceding mode may have to be restricted either by imposing extra pointwise-in-time state constraints or by deliberately slowing down the response in order to ensure that in the event of a failure there exists a recovery control sequence that can avoid constraint violation. The paper illustrated some of the ingredients and approaches that can be used in a systematic FMEM system design based on reference governors, and based on recoverable and constraint admissible sets. The development of comprehensive numerical procedures which can be used to guarantee the set inclusion conditions for safe reconfigurability will be addressed in future publications.

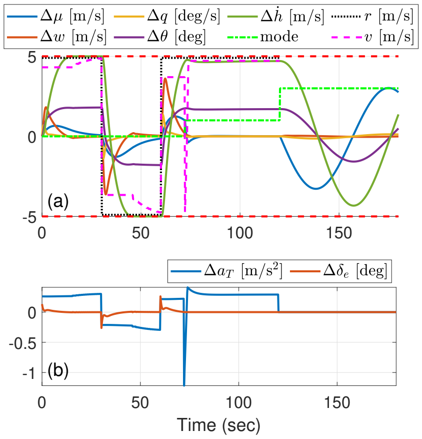

Fig. 5. Simulation results with failure path from Mode 0 to Mode 1 to Mode 3.

References

[1] K. McDonough and I. Kolmanovsky, "Fast computable recoverable sets and their use for aircraft loss-of-control handling," *Journal of Guidance, Control, and Dynamics*, vol. 40, no. 4, pp. 934–947, 2017.

[2] E. Garone, S. Di Cairano, and I. Kolmanovsky, "Reference and command governors for systems with constraints: A survey on theory and applications," *Automatica*, vol. 75, pp. 306–328, 2017.

[3] M. Blanke, M. Kinnaert, J. Lunze, M. Staroswiecki, and J. Schröder, *Diagnosis and Fault-Tolerant Control*, vol. 2. Springer, 2006.

[4] F. Blanchini and S. Miani, *Set-Theoretic Methods in Control*. Springer, 2008.

[5] C. Danielson, K. Berntorp, A. Weiss, and S. D. Cairano, "Robust motion planning for uncertain systems with disturbances using the invariant-set motion planner," *IEEE Transactions on Automatic Control*, vol. 65, no. 10, pp. 4456–4463, 2020.

[6] A. Weiss, C. Petersen, M. Baldwin, R. S. Erwin, and I. Kolmanovsky, "Safe positively invariant sets for spacecraft obstacle avoidance," *Journal of Guidance, Control, and Dynamics*, vol. 38, no. 4, pp. 720–732, 2015.

[7] F. Blanchini, F. A. Pellegrino, and L. Visentini, "Control of manipulators in a constrained workspace by means of linked invariant sets," *International Journal of Robust and Nonlinear Control: IFAC-Affiliated Journal*, vol. 14, no. 13-14, pp. 1185–1205, 2004.

[8] K. Berntorp, A. Weiss, C. Danielson, I. Kolmanovsky, and S. Di Cairano, "Automated driving: safe motion planning using positively invariant sets," in *2017 IEEE 20th International Conference on Intelligent Transportation Systems (ITSC)*, pp. 1–6, IEEE, 2017.

[9] W. Lucia, D. Famularo, and G. Franze, "A set-theoretic reconfiguration feedback control scheme against simultaneous stuck actuators," *IEEE Transactions on Automatic Control*, vol. 63, no. 8, pp. 2558–2565, 2017.

[10] I. Kolmanovsky, A. Weiss, and W. Merrill, "Incorporating risk into control design for emergency operation of turbo-fan engines," in *Infotech@ Aerospace 2011*, p. 1591, 2011.

[11] I. Kolmanovsky and E. G. Gilbert, "Theory and computation of disturbance invariant sets for discrete-time linear systems," *Mathematical Problems in Engineering*, vol. 4, pp. 317–367, 1998.

[12] A. Löhne and B. Weißing, "The vector linear program solver bensolve–notes on theoretical background," *European Journal of Operational Research*, vol. 260, no. 3, pp. 807–813, 2017.

[13] A. Girard and I. Kolmanovsky, *Lecture Notes on Control of Aerospace Vehicles*. Department of Aerospace Engineering, The University of Michigan, Ann Arbor, January 2019.